Multicert Certificate Policy

Policies

MULTICERT_PJ.ECRAIZ_426_en

CA Identification: PKI

Rating: Public

Version: 2.0

Date: 01/10/2018

Document Identification: MULTICERT_PJ.ECRAIZ_426_en

Keywords:

Document Type: Policies

Title: Multicert Certificate Policy

Original Language: English

Language of Publication: English

Rating: Public

Date: 01/10/2018

Current Version: 2.0

CA Identification: PKI

Version History

Version no.	Date	Details	Author(s)
1.0	29/05/2018	Revision according to the RFC 3647 and the CABForum Baseilne Requirements 1.5.7	Multicert S.A.
1.1-1.4	25/09/2018	Inclusion of procedure for method to prove email address control. Inclusion of practices for re-key. Inclusion of statement for external CA`s	Multicert S.A.
2.0	01/10/2018	Approval	Multicert S.A.

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_427_en	Certification Practices Statement	Multicert S.A

Table of Contents

1 Introduction

1.1 Overview

This document has the purpose of defining a set of requirements which define how subscribers shall manage the digital certificates they acquire from Multicert. It is not meant to name legal rules or obligations, but to inform. Therefore, this document is intended to be simple, straightforward, and understood by a wide public.

The Certificates and the Timestamps issued by MULTICERT CA, contain a reference to this Certificate Policy, so that the relying parties and other interested entities or individuals may find information on the certificate and the policies of the entity which issued it.

This document is managed by the Security/Authentication Working Group and the Security Administrators and adopts the current versions of:

- REGULATION (EU) nº 910/2014;
- Certification Authority Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”);
- General Policy Requirements for Trust Service Providers
- Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
- Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- Policy and Security Requirements for Trust Service Providers issuing ElectronicTime-Stamps.

Not less important, Multicert is always attentive to the browsers own Policies in order to be compliant with their specifications.

1.2 Document Name and Identification

This document is a Certificate Policy. The CP is represented in a certificate by a unique number called “object identifier” (OID). The value of the OID associated with this document is “1.3.6.1.4.1.25070.1.0”.

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

DOCUMENT INFORMATION	
Document Version	Version 2.0
Document State	Approved
OID	1.3.6.1.4.1.25070.1.0
Issuing Date	01/10/2018

DOCUMENT INFORMATION	
Validity	1 Year
Location	http://pki.multicert.com/

An historical of this document versions can be consulted on the History Version section.

The OID for Multicert is:

1	ISO assigned
3	ISO Identified Organization
6	DOD
1	Internet
4	Private
1	Enterprise
25070	Multicert

Multicert organizes its own OID's in the following way:

Type of Certificate	Multicert Object Identifier (OID)
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 Digital Signature	1.3.6.1.4.1.25070.1.1.1.1.0.1.4
Web Server Certificate (OV[1])	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

[1] Organizational Validation

Besides Multicert OID, the following certificates are duly compliant with the EU Certifcate Policy:

Type of Certificate	Object Identifier (OID)	Description
Qualified Digital Signature	0.4.0.194112.1.2	QCP-n-qscd: certificate policy for European Union (EU)
Electronic Seal	0.4.0.194112.1.3	QCP-l-qscd: certificate policy for European Union (EU)
Web Server Certificate (OV[2])	0.4.0.194112.1.4	QCP-w: certificate policy for European Union (EU)

1.3 PKI participants

1.3.1 Multicert Certification Authorities

Multicert owns and manage its own infrastructure. Multicert Root CA as well as Multicert Sub CAs are operated by Working Groups with different roles.

The Authentication Working Group is responsible to set all security Policies including manage this Document as well as Certificate Practice Statement and the Management Working Group is responsible for its approval.

This policy grants that all Multicert Certification Authorities are meant to comply with all the requirements listed here.

1.3.1.1 External Certification Authorities

Multicert Root CA is currently signing Subordinate CA`s, which are operated by external entities.

The definition of policies and data for the issuance and management of certificates for external Subordinate CA`s are defined in the Subordinate CA Policy, which is available at https://pki.multicert.com.

1.3.2 Registration Authorities

Registration Authorities (RA) are responsible for the Identification of the subscribers within an organization or an association. In case of SSL (webserver) certificates, they only identify the needs and the CA is responsible for the identification process.

Multicert RA's must sign an agreement with Multicert CA in order to comply with all the requirements for Identification. A process is established and the Registration Officers are duly identified and compromised with their Job Description.

[2] Organizational Validation

1.3.3 Subscribers

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.

1.3.4 Relying parties

Trusting or Relying 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 and that that certificate is valid through the CRL or OCSP service.

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

Other participants includes all the Entities that somehow participate in the CA activity, like software development, cross-signing, etc.

1.4 Certificate usage

The certificates issued in the Multicert CA domain are used by different titleholders, 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 cipher algorithms, along with mechanisms to establish and distribute keys.

1.4.1 Appropriate certificate uses

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

The certificates issued for persons or Entities are aimed to be used in Digital Signatures, authentication or document encryption.

The certificates issued by Multicert PKI 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.

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

This CP and all public documents belonging to Multicert PKI are managed by the Authentication Working Group:

Organization	Multicert S.A.
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

1.5.2 Contact person

Name	Authentication Working Group
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 Person determining CP suitability for the policy

The Authentication Working Group determines the suitability of this CP and is responsible for verify the compliance of relative CPS's with this CP.

1.5.4 CP approval procedures

The Management Working Group is responsible for this policy approval.

1.6 Definitions and acronyms

1.6.1 Definitions

Item	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) Nº 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.
Certification Authority	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.
Supervisory 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	Definition
ANSI	American National Standards Institute
CA	Certification Authority
CAB	Conformity Assessment Body
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
QSCD	Qualified Signature-Creation Device
SSCD	Secure Signature-Creation Device

2 Publication and repository responsibilities

2.1 Repositories

The CA's under this policy shall ensure that the revocation data for issued Certificates is publicly available through a repository 24 hours a day, 7 days a week with a minimum of 99% availability.

The CA's under this policy must make available a CP and a CPS, which shall be annually updated.

2.2 Publication of certification information

Multicert PKI public information is available on the web. This includes:

- CA Certificates,
- CRLs,
- CPs and CPSs.

2.3 Time or frequency of publication

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

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 controls on 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

3.1.1 Types of names

Multicert certificates are issued in accordance with ITU X.500 standard and their Distinguished Name (DN) is build according with ETSI EN 319 412-1 v1.1.1.

3.1.2 Need for names to be meaningful

The certificate types described in this document are issued using Unique Names in order to clarify a unique and identifiable name. Some attributes can be in place on order to turn names meaningful. An example of these attributes are the serial number and the organization identifier.

3.1.3 Anonymity or pseudonymization of subscribers

The certificate types described in this document can be issue with pseudonyms, since this information is provided in the certificate and all validation of the titleholder authenticity is correctly performed.

3.1.4 Rules for interpreting various name forms

Distinguished names are made in accordance with the ETSI EN 319 412-1 v1.1.1 and RFC 5280.

3.1.5 Uniqueness of names

All certificates issued under this policy have a serial number that provided them uniqueness.

3.1.6 Recognition, authentication and role of trademarks

Subscribers may not request Certificates with contents that infringes the intellectual property rights of a third party. The issuance of a certificate with a trademark is always subject of a meticulous verification.

3.2 Initial identity validation

The certificates issued under this policy are always subject of a meticulous verification of the individual and/or the organization for which the certificate will be issued.

3.2.1 Method to prove possession of private key

In the case of the subscriber issuing the private key, the CA issuing the certificate must confirm the possession of the key in the certificate request. Once the certificate is a EU Qualified certificate, the key must be generated and stored on a QSCD (Qualified Secure Cryptographic Provider).

3.2.2 Method to prove Email Address control

When the email address is included in the Distinguished Name or Subject Alternative name attributes of the certificate, the subscriber must prove that controls de email address to be included in the certificate. To do that, the CA perform a challenge-response procedure, which is detailed in the CPS.

3.2.3 Authentication of Service

3.2.3.1 Authorization by the Responsible of the *Domain Name*

The CA confirms that, to date of issuance of the certificate, the certificate applicant is the *Domain Name* responsible or has control over the *Full Qualified Domain Name*, through following procedures:

- Confirmation that the certificate applicant has the *Domain Name* registration directly at the domain registrar[3];
- Verification about the Organization and its legal existence;
- Direct communication with the responsible for the *Domain Name*, using the address, email or phone number provided by the domain registrar;
- Direct communication with the responsible for the *Domain Name* using the contact information listed in the file "*registrant*", "*technical*" or "*administrative*" of WHOIS database[4];
- Communication with the domain administrator using the email address created with the prefix "*admin*", "*administrator*", "*webmaster*", "*hostmaster*" or "*postmaster*", followed by the "@" symbol and the *Domain Name*;
- Trust in a Domain Authorization Document;
- Statement by the Applicant that he/she has practical control over the *Fully Qualified Domain Name*, by pre-agreement on an amendment to certain information contained in an online Web page identified by a URI[5] that contains the *Fully Qualified Domain Name*; or
- Using any other method of confirmation (as long as it provides the same level of reliability of the verification methods mentioned above), and the CA will keep the record as evidence to confirm that the Applicant is responsible for the *Domain Name* or has control over the *Fully Qualified Domain Name*.

3.2.3.2 Authorization for a IP Address

For each IP address listed in the certificate, the CA confirms that, to date of issuance of the certificate, the Applicant has control over the IP address, through following

[3] Entity which manages the domain registration of a certain country.
[4] Database which allows the IP query to access information about its owner.
[5] Uniform Resource Identifier

procedures:

- Statement by the Applicant that he/she has practical control over the *Fully Qualified Domain Name*, by pre-agreement on an amendment to certain information contained in an online Web page identified by a URI that contains the *Fully Qualified Domain Name*;
- Obtaining information about the assignment of the IP address from the *Internet Assigned Numbers Authority* (IANA) or *Regional Internet Registry* (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
- Research on the IP address followed by verification of control over the resulting Domain Name.

Using any other method of confirmation (as long as it provides the same level of reliability of the verification methods mentioned above), and the CA will keep the record as evidence to confirm that the Applicant is responsible for the *Domain Name* or has control over the *Fully Qualified Domain Name.*

3.2.3.3 Authorization for an Organization

When issuing eSeals, the issuing CA must verify al the organization (or trademark) information and confirm that the private key of the certificate reside on a SQCD. The identity of the applicant must be confirmed and dully verified.

3.2.4 Authentication of individual identity

The CA issuing certificates must confirm the authenticity of the requests according to the following types:

Advanced Signature Certificates	The request is delivery to the CA in the form of an agreement where all the information is present. This information is then verified as well as its authenticity. In the case of being a natural certificate the information is only about the person who request the certificate. For Legal certificates, the Organization Information is also verified and an organization authorization is requested for the certificate issuance.
Qualified Signature Certificates (eSign)	Qualified Signature Certificates are issued only to person's, whatever they are or not associated to an organization. The process of verifying the authenticity of the request is similar to the Advanced Signature Certificate, however, physical presence it is needed in hits case, or a similar one.
Authentication Certificates	The certificate are only issued together with eSign Certificates
Cipher Certificates	The certificate are only issued together with eSign Certificates

3.2.5 Non-verified subscriber information

All subscriber information is verified before certificate issuance.

3.2.6 Validation of authority

The CA issuing certificates shall verify the authorization for certificate requests:

OV webserver certificates	An authorized contact listed with the Domain Name Registrar, a person with control over the domain name, or through Reliable communication with the applicant, as defined in the Baseline Requirements.
Advanced Signature Certificates	The titleholder of the certificate, or in case of a legal certificate, with the authorization of the Legal Entity.
Qualified Signature Certificates (eSign)	The titleholder of the certificate, or in case of a legal certificate, with the authorization of the Legal Entity.
eSeals	An authorization from the Legal Entity or from a Legal and Authenticated Representative.

3.2.7 Criteria for interoperation

The certificates issued under this policy are issued under a sole Multicert chain.

For SSL certificates, the Multicert CA responsible for SSL certificates issuance is cross signed to assure Mozilla recognition.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The certificates issued under this certificate policy are always subject of new issuances which means that every single re-key process correspond to a new issuance.

OV webserver certificates	According to Baseline Requirements
Advanced Signature Certificates	Every new issuance (at least every 36 months)
Qualified Signature Certificates (eSign)	Every new issuance (at least every 36 months)
eSeals	Every new issuance (at least every 36 months)
(Professional Associations) Qualified Signature Certificates (eSign)	Every new issuance (at least every 60 months). Certificates issued to Legal Associations (usually acting as Registration Authorities) usually have 5 years of validity.

3.3.2 Identification and authentication for re-key after revocation

All requests after a revocation are treated like new issuances for certificates issued under this policy.

3.4 Identification and authentication for revocation request

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

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

The first two bullets only take place on a duly identified revocation request by the Titleholder or the entity responsible for the certificate.

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

The following are able to submit an application under this certificate policy:

- A Subscriber;
- A legal representative of the subscriber dully authorized;
- A legal person who is the holder of the certificate;
- A Registration Authority belonging to Multicert CA.

4.1.2 Enrolment process and responsibilities

The issuers CA's under this Certificate Policy are responsible to verifying the identity of each applicant according to this policy. After this process is successful completed the CA is responsible for the certificate Issuance.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The CA (and existents RA's if applicable) must identify and verify all certificate requests according to the CPS of the issuer CA on an auditable way. For SSL certificates, the Baseline Requirements must be applicable for identification and authentication.

4.2.2 Approval or rejection of certificate applications

All application that have been successfully identified and verified, the issuer CA must approve the certificate issuance.

Once an application cannot be verified the issuer CA must reject its certificate issuance.

4.2.3 Time to process certificate applications

Once an application is successful verified the CA takes no more than 5 days do issue the certificate.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Issuer CAs shall verify all the sources of information they use to verify applications.

All the systems that belongs to the certificate issuance process should be protected against modification, through an access control policies, protection of the data bases, authentication between systems, etc.

When the certificate issuance involves the Root CA, individual authorized personnel belonging to the working groups are needed in order to issue a certificate manually in the Root CA.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The issuers CAs always notify the subscriber when its certificate is issued using a contact provided on the certificate application.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The absent of communication after the certificate delivery to the subscriber is interpreted as a Subscriber acceptance of the certificate.

4.4.2 Publication of the certificate by the CA

The Issuer CA publish all the issued certificates in its own repository.

4.4.3 Notification of certificate issuance by the CA to other entities

In the cases that the application was submitted thought a RA the CA shall notify the RA about the certificate issuance.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber shall use its private keys in accordance with the terms accepted on the agreement. The private keys are personal in a way that the subscriber must not make them available to third parties.

4.5.2 Relying party public key and certificate usage

Relying Parties should be in accordance with the Issuer CA CPS and this CP in a way that understands and trusts the usage of the certificate.

Relying Parties should always verify the certificate validity through the methods make available by the Issue CA, like CRL's or/and OCSP.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Multicert may renew a certificate on its own initiative if:

- The certificate is not expired nor revoked;
- The certificate data (distinguished name and subject alternative name data attributes) remains the same as the previous certificate;
- The validity of the new certificate remains the same as the previous certificate;
- The documents and data obtained to verify certificate information, and the validation itself have no more than 825 days.

Multicert CA may initiate a certificate renewal in its own discretion, after notifying the certificate subscriber.

The CA shall notify the subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the certificate to the subscriber.

The passage of time after delivery or notify of issuance of the certificate to the subscriber or the use of the certificate constitutes the subscriber`s acceptance.

When the certificate renewal process does not fulfil de conditions above or when it is initiated by the subscriber`s initiative, the process are assumed as a new issuance.

4.6.2 Who may request renewal

N.A.

4.6.3 Processing certificate renewal requests

N.A.

4.6.4 Notification of new certificate issuance to subscriber

N.A.

4.6.5 Conduct constituting acceptance of a renewal certificate

N.A

4.6.6 Publication of the renewal certificate by the CA

N.A.

4.6.7 Notification of certificate issuance by the CA to other entities

N.A.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

As the section before, Multicert only uses new issuances.

4.7.2 Who may request certification of a new public key

N.A.

4.7.3 Processing certificate re-keying requests

N.A.

4.7.4 Notification of new certificate issuance to subscriber

N.A.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

N.A.

4.7.6 Publication of the re-keyed certificate by the CA

N.A.

4.7.7 Notification of certificate issuance by the CA to other entities

N.A.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

The issuer CA under this policy doesn't use a certificate modification process.

4.8.2 Who may request certificate modification

N.A.

4.8.3 Processing certificate modification requests

N.A.

4.8.4 Notification of new certificate issuance to subscriber

N.A.

4.8.5 Conduct constituting acceptance of modified certificate

N.A.

4.8.6 Publication of the modified certificate by the CA

N.A.

4.8.7 Notification of certificate issuance by the CA to other entities

N.A.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A revocation process inactivates a certificate definitely. However, before performing that revocation, a process of identification and authentication of the parts involved in the revocation process request must be taken in place.

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

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

- The titleholder or the representative person,
- The entity which required the certificate,
- The under this Policy, every time that 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 should be done through verification, in a way that the CA trust that the request is authentic.

4.9.3 Procedure for revocation request

Who performs a certificate request should make its identity available to the CA. It is only after verifying the authenticity of the certificate request that the revocation is processed and 24hrs from this on, the new status of the certificate is make available.

4.9.4 Revocation request grace period

The subscriber should request the revocation as soon as possible. If the subscriber is not sure if his certificate should be revoked, he could request for suspension, however this status is only possible during 3 days. After that, if no certificate request was make, the certificate is reactivated.

4.9.5 Time within which CA must process the revocation request

The CA’s under this policy should make available the new status of an authenticated certificate request no more than 24h later.

4.9.6 Revocation checking requirement for relying parties

Relying Parties must confirm the validity of the certificate trough the services that the issuer CA make available, like OCSP e CRL.

4.9.7 CRL issuance frequency (if applicable)

The CA’s working under this policy must issue its CRLs with the following frequency:

- Intermediate CA’s and Sub CA’s – Every 24hrs;
- Root CA – Every 3 months and whenever a certificate is revoked.

4.9.8 Maximum latency for CRLs (if applicable)

The CA’s working under this policy must publish its CRLs no later than:

- 30 minutes after the CRL issuance for Intermediate CA’s and SubCA’s;
- 24 hours after the CRL issuance for Root CA.

4.9.9 On-line revocation/status checking availability

All CA’s under this policy must make available an OCSP Service.

OCSP responses must be compliant with RFC 6960 and the Certificate which signs the OCSP response must be always issued by the same CA who issue the certificate.

4.9.10 On-line revocation checking requirements

The CA’s under this Policy have a valid online certificate status validation service with a 99.9% availability service.

The OCSP service must be compliant with all requirements of the current version of Baseline Requirements, as well as RFC 6960.

4.9.11 Other forms of revocation advertisements available

N.A.

4.9.12 Special requirements related to key compromise

If the revocation of a certificate impacts other systems not directly related with the CA, the same has to contact Relying parties in order to inform about the certificate request.

4.9.13 Circumstances for suspension

A suspension request is taken in place if there is a suspicion that the key can be compromised. In that case, the relative certificate should be suspended until a confirmation of the compromised key happen.

4.9.14 Who can request suspension

A suspension request can be made by:

- The titleholder;
- The entity that requested the certificate;
- A relying party that has reasons to believe that the key of the certificate was compromised.

4.9.15 Procedure for suspension request

The CA's under this policy must maintain a link permanently available required for a certificate suspension. The certificate must be suspended in the next 24hrs and the status cannot be longer than 6 days.

4.9.16 Limits on suspension period

N.A.

4.10 Certificate status services

4.10.1 Operational characteristics

The CA's under this Policy shall make available certificate status information via CRL and OCSP. For CA's issuing EU qualified certificates, CRL must include all revoked certificates even if they have expired, for at least 7 years after the expiration date.

4.10.2 Service availability

The CRL and OCSP services shall be available 24 hours per day, 7 days per week.

4.10.3 Optional features

N.A.

4.11 End of subscription

The subscriber is free to end his subscription of certificate services at any time he wants by revoking his certificate. In this situation the issuer CA stores all information relative to the subscriptions 7 years from the revocation date.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

N.A.

4.12.2 Session key encapsulation and recovery policy and practices

N.A.

5 Facility, management and operational controls

The CA's under this policy must implemented several rules and policies focusing on physical, procedural and human controls that support the security requirements present on this CP. 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 a CA.

5.1 Physical controls

5.1.1 Site location and construction

The facilities of the CA's under this policy must be designed so as to provide an environment capable of controlling and auditing access to the certification systems, and to be physically protected from non-authorized access, damage or interference. The architecture need to use a deep defense 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 must be 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 must be ensured:

- 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 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

Systems must be 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 unrecognized 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 Power and air conditioning

The security environment must have 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 Water exposures

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

5.1.5 Fire prevention and protection

The safe environment 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 equipment 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 Media storage

All sensitive information supports holding production *software* and data, audit information, archive or backup copies must be 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 must have 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 Waste disposal

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 equipment (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 Off-site backup

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 Procedural controls

A CA activity 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 Trusted roles

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 eight different categories (which correspond to eight 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[6], 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.

This group's responsibilities are:

- Management of the "Production Environment" and of the "Operation Environment";
- To perform the CA's routine tasks, including backup copy operations of its systems;
- To perform the CA'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 "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;

[6] BIOS, SO administrator account, etc

- 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[7] 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;
- 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;

[7] Registando o seu valor

- 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[8] 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[9]. 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";
- 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 automatized;
- To revoke/suspend certificates in case this procedure is not automatized.

[8] 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.

[9] Defined for each artefact in its custody.

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 analyze 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;
- To assume the Security Administrator role.

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 required 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 Identification and authentication for each role

The CA personnel must authenticate to the certificate management system before they are access the systems necessary to perform their tasks.

5.2.4 Roles requiring separation of duties

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		✘		▨	✘	✘	✘	✘
Audit	✘	✘	✘	✘	▨	✘	✘	✘
Custody	✘	✘	✘	✘	✘	▨	✘	✘

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

5.3 Personnel controls

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 Qualifications, experience and clearance requirements

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 procedures

Background check results from the accreditation process of individuals nominated to hold positions in any one of the trust functions. The background check[10] includes:

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

5.3.3 Training 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 Retraining frequency and requirements

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 Job rotation frequency and sequence

Nothing to remark.

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

5.3.6 Sanctions for unauthorized actions

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

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 Independent contractor requirements

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 [11], existing for this purpose.

5.3.8 Documentation supplied 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 Audit logging procedures

5.4.1 Types of events recorded

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.

[11] MULTICERT_PJ.CA3_28_0001_en - Privacy Statement for External Contributor or Guest

5.4.2 Frequency of processing log

The records must be analyzed 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 Retention period for audit log

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

5.4.4 Protection of audit log

The records shall be exclusively analyzed by authorized members belonging to the Working Groups.

The records must 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 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

5.5.1 Types of records archived

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 Retention period for archive

The data subject to archiving is retained for a period of time of not less than 7 years from the end of life of the certificate.

5.5.3 Protection of archive

The archive:

- Is protected so that only authorized 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 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

The stored data collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key changeover

Nothing to remark.

5.7 Compromise and disaster recovery

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

5.7.1 Incident and compromise handling procedures

The backup copies of the CA'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 Computing resources, software, and/or data are corrupted

In case the computer resources, *software* and/or data are compromised or corruption is suspected, the backup copies of the private keys from the CA 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 Entity private key compromise procedures

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 Business continuity capabilities after a disaster

The computing resources, *software*, backup copies and records of the CA should be 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 CA or RA termination

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 Supervision 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 organization) 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 security controls

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 Key pair generation and installation

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

6.1.1 Key pair generation

The generation of cryptographic keys must be 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 the CA using cryptographic *hardware* compliant with FIPS 140-2 level 3 and/or *Common Criteria* EAL 4+ requirements.

6.1.2 Private key delivery to subscriber

In the case that the CA generates the Key Pair, the delivery of the private key associated to the EU Qualified certificates of a natural or collective person is performed in SSCD cryptographic device (*Secure Signature-Creation Device*).

6.1.3 Public key delivery to certificate issuer

The public key is delivered to the CA, according to the procedures mentioned in section 4.1.

6.1.4 CA public key delivery to relying parties

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

6.1.5 Key sizes

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 CA;
- 2048 *bits* RSA for the keys associated to the remaining certificates issued by the CA with signature algorithm sha256RSA.

6.1.6 Public key parameters generation and quality checking

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 usage purposes (as per X.509 v3 key usage field)

The subscriber certificates issued under this policy cannot be used to sign other certificates and must have an Extended Key Usage that determines the purpose of such certificate.

CA’s certificate must be only used to sign other certificates and CRL’s.

6.2 Private key protection and cryptographic module engineering controls

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 Cryptographic module standards and controls

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 Private key (n out of m) multi-person control

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) shall be necessary for the activation of the private key from CA.

6.2.3 Private key escrow

N.A.

6.2.4 Private key backup

The private key from CA has at least one backup copy with the same security level as the original key.

6.2.5 Private key archival

The private keys from CA, subject to backup copies, are stored as identified in section 6.2.4.

6.2.6 Private key transfer into or from a 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 Private key storage on cryptographic module

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

6.2.8 Method of activating private key

For activating the private keys from 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 Method of deactivating private key

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

To deactivate 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 Method of destroying private key

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

The CA 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 Cryptographic Module Rating

Described in section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

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 Certificate operational periods and key pair usage periods

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 certificates form SubCA's issued under this policy has a minimum validity of eleven years and four months, being used to sign certificates during its 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 two years;

- the certificate of natural person has a maximum validity period of 3 three years, except certificates issued Registration Authorities where the validity is for four years;
- the certificate of collective person has a maximum validity of three years.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data necessary for using the private key from the 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 Activation data protection

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 the CA are stored in an enciphered way in cryptographic *token*.

6.4.3 Other aspects of 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 security controls

6.5.1 Specific computer security 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 Computer security rating

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

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

6.6 Life cycle technical controls

6.6.1 System development controls

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 Security management controls

Multicert has mechanisms and/or Working Groups to control and monitor the configuration of the CA'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 Life cycle security controls

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 security controls

The CA’s under this policy shall 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.

6.8 Time-stamping

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 CE. The CE may base this statement on technical means (for example, proof of the possession of the private key through a challenge-response protocol), on the presentation of the private key or on the registration made by the titleholder.

A certificate has a limited validity period, indicated in its content and signed by the CE. Since the signature of the certificate and its validity may be independently verified by any software that uses certificates, the certificates may be distributed through communication lines and public systems, and may also be stored in any type of storage units.

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.

The profile of the web server certificate is compliant with:

- ITU.T recommendationX.509[12];
- RFC 5280[13], and
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum, v1.3.0.

7.1.1 Version number(s)

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

7.1.2 Certificates extensions

The components and extensions defined for X.509 v3 certificates provide methods for

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

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

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

7.1.3 Algorithm object identifiers

The "*signatureAlgorithm*" certificate field contains the OID for the cryptographic algorithm used by the CA to sign the certificate: 1.2.840.113549.1.1.11 (*sha-2WithRSAEncryption*[14]).

7.1.4 Name forms

As defined in section 2.1.

7.1.5 Name constraints

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

7.1.6 Name constraints serverAuth CA

If a Subordinate CA Certificate issues ssl certificates than it must include the id-kp-serverAuth extended key usage. This is applicable to all SubCA's that are under this policy since December 2017.

7.1.7 Certificate policy object identifier

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

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

The qualifier 0.4.0.194112.1.4 refers to Certificate Politic for qualified certificates authentication of web server, under the regulation EU nº 910/2014.

7.1.8 Usage of policy constraints extension

Nothing to remark.

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

7.1.9 Policy qualifier syntax and semantics

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

7.1.10 Processing semantics for the critical Certificate Policies extension

Nothing to remark.

7.2 CRL profile

When a certificate is issued, it is expected to be in use for its entire validity period. However, several circumstances may cause a certificate to become invalid before the expiration of its validity period. Such circumstances include change of name, change of association between the subject and the certificate data (for example, an employee who terminates employment) and compromise or suspected compromise of the corresponding private key. Under such circumstances, the CA has to revoke the certificate[13].

The protocol X.509 defines a method of certificate revocation, which involves the periodic issuing, by the CA, of a signed data structure called a certificate revocation list (CRL). A CRL is a time stamped list identifying revoked certificates, which is signed by the CA and made freely available in a public repository. Each revoked certificate is identified in the CRL by its serial number. When an application uses a certificate (e.g., for verifying a remote user's digital signature), that application not only verifies the certificate signature and validity; it also obtains the most recent CRL and checks if the serial number of the certificate is not in it. Note that a CA issues a new CRL on a regular periodic basis[13].

The CRL profile conforms to:

- ITU.T Recommendation X.509[12];
- RFC 5280[13] and,
- Applicable legislation, national and European.

7.2.1 Version number(s)

Issuer CAs shall issue version 2 CRLs compliant with RFC 5280.

7.2.2 CRL and CRL entry extensions

Issuer CAs shall issue CRL entry extensions according to RFC 5280.

7.3 OCSP profile

The profile of the OCSP certificates is compliant with:

- ITU.T recommendation X.509[12];
- RFC 6960[15] and,
- Applicable legislation, national and European.

7.3.1 Version number(s)

CA's under this policy must support the version 1 of OCSP requests and responses.

7.3.2 OCSP extensions

N.A.

[15] cf. RFC 6960. 2013, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.

8 Compliance audit and other 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 circumstances of assessment

The compliance audits are performed periodically in annual basis. The CA must prove, through audit and annual 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/qualifications of assessor

The auditor is independent from the circle of influence of the CA, with recognized 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 CA’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.

8.3 Assessor's relationship to assessed 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 Topics covered by assessment

The scope of audits and other assessments include the accordance with the European 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 Actions taken as a result of deficiency

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) Bearing in mind the irregularities stated on the report, the entity subject to the audit will send a correction of irregularities report to the Auditor, where the actions, methodology and time needed for correcting the irregularities (no later than 3 months), shall be described;

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

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

f) The Accreditation Authority, after analyzing 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.

9 Other business 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

N.A.

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

The fees for the chronological validation is identified in a formal proposal to be made by Multicert.

9.1.5 Refund policy

N.A.

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 assets

N.A.

9.2.3 Insurance or warranty coverage for end-entities

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 business information

9.3.1 Scope of confidential information

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

a) The private keys from any CA under this policy;

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

c) All information of a personal nature provided to 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 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 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 CA;

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

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

9.3.2 Information not within the scope of confidential information

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).

The 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 Responsibility to protect 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 information

9.4.1 Privacy plan

The CA is responsible for implementing the measures ensuring the privacy of personal data, according to the GDPR.

9.4.2 Information treated as private

It is considered private information all the information supplied by the certificate titleholder and that makes possible his identification.

9.4.3 Information not deemed private

It is considered information not protected by privacy all the information that does not enables a Titleholder Identification.

9.4.4 Responsibility to protect private information

In accordance with GDPR.

9.4.5 Notice and consent to use private information

In accordance with the GDPR. The CA's under this policy should only request the information needed to provide a certificate issuance.

9.4.6 Disclosure pursuant to judicial or administrative process

N.A.

9.4.7 Other information disclosure circumstances

N.A.

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 warranties

9.6.1 CA representations and warranties

CA's are obliged to:

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

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

c) Protect its private keys;

d) Issue certificates in accordance with 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 unauthorized people from changing data;

i) Store the certificates issued without any changes;

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

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

l) Revoke the certificates under the terms of 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 4.9,

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 recognized certificate and the Certification Practices Statements in force at each moment and for fifteen years from issuance; and

w) Make the certificates from CA available.

9.6.2 RA representations and warranties

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 unauthorized 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 recognized certificate at each moment and for seven years from issuance.

9.6.3 Subscriber representations and warranties

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 4.9.1;

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 the CA.

9.6.4 Relying party representations and warranties

It is the obligation of the parties that are entrusted with the certificates issued by a 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 Representations and warranties of other participants

N.A.

9.7 Disclaimers of warranties

9.8 Limitations of liability

Multicert CA:

a) 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;

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

c) 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;

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

e) 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

f) 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 Term and termination

9.10.1 Term

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 Termination

The Management Working Group may decide in favor 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 autonomy 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 Effect of termination and survival

After the Management Working Group decides in favor 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 notices and communications with participants

9.12 Amendments

9.12.1 Procedure for amendment

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 mechanism and period

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 Circumstances under which OID must be changed

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 Dispute resolution provisions

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 Governing law

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.

9.15 Compliance with applicable law

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 Miscellaneous provisions

9.16.1 Entire agreement

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

9.16.2 Assignment

N.A.

9.16.3 Severability

N.A:

9.16.4 Enforcement (attorneys' fees and waiver of rights)

N.A.

9.16.5 Force Majeure

9.17 Other provisions

N.A.

Bibliographic References

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

NIST FIPS PUB 180-2. 2002, *Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.*

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

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

Approval

[Assinatura Qualificada] José Jorge Oliveira da Fonseca Alcobia

Digitally signed by [Assinatura Qualificada] José Jorge Oliveira da Fonseca Alcobia
Date: 2018.10.01 17:51:20 +01'00'