multicert
Engineering for digital security

Multicert Certification Practices Statement

Policies

MULTICERT_PJ.ECRAIZ_427_en

Project identification: MULTICERT PKI

Access level: Public

Version: 4.0

Date: 25/03/2019

Normative Version

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

Document identifier: MULTICERT_PJ.ECRAIZ_427_en

Key-words: MULTICERT CA, Certification Practices Statement

Type of document: Policies

Title: Certification Practices Statement

Original language: English

Publication language: English

Access level: Public

Date: 25/03/2019

Current version: 4.0

Project identification: MULTICERT PKI

Version history

Version no.	Date	Details	Author(s)
1.0	15/06/2018	Reviewed according to RFC 3647 and CABForum Baseline Requirements, version 1.5.7	Multicert S.A.
1.1-1.7	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.
2.1	29/01/2019	Prohibition of usage for man-in-middle Review of revocation reasons	Multicert S.A.
3.0	29/01/2019	Approval	Multicert S.A.
3.1	25/03/2019	Review in accordance with Baseline Requirements v1.6.4	Multicert S.A.
4.0	25/03/2019	Approval	Multicert S.A.

Related documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_426_en	Multicert PKI Certificate Policy	Multicert S.A.
MULTICERT_PJ.ECRAIZ_428_en	Certificate Profiles List	Multicert S.A.

Annexes

Document ID	Details	Author(s)

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Summary

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

1 Introduction

1.1 Overview

This document is a Certification Practices Statement, or CPS, whose purpose is to define a set of practices for issuing and validating certificates and for ensuring the reliability of such certificates. While it is not the purpose of this document to name legal rules or obligations but rather to inform, it is intended that this document be simple, direct and understood by a broad public, including people without technical or legal knowledge.

This document describes the general practices relating to issuing and managing certificates followed by Multicert – Serviços de Certificação Eletrónica S.A. and in accordance with the Certificate Policy (CP) defined by this entity, further explaining the meaning and function of a certificate, as well as the procedures to be followed by the Relying Parties and any other interested parties to rely on the certificates issued by the CAs managed by Multicert (Multicert PKI). This document may undergo regular updates.

Certificates issued via Multicert PKI include a reference to the CPS in order to allow the Relying Parties and other interested parties to find information about the certificate and the issuing authority.

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

The first seven chapters are dedicated to describing the most important procedures and practices within the scope of digital certification of Multicert PKI. Chapter eight describes compliance audits and other assessments. Chapter nine refers to legal matters.

Multicert PKI conforms to the current version of the baseline requirements for Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum in document “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, v1.5.7, available at http://www.cabforum.org. In the event of any discrepancy between this document and that described in the Baseline document, what is established in the document issued by the CA/Browser Forum supersedes what is described in this document.

1.2 Document name and identification

This document represents the Multicert PKI Certification Practice Statement. The CPS is represented in a certificate by a unique number designated as "object identifier" (OID). The Certificate Policy OID is used as explained in section 3.1.1.

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

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

DOCUMENT INFORMATION	
Document version	Version 4.0
Document Status	Approved
OID	1.3.6.1.4.1.25070.1.1.1.0.7
Issuing date	25/03/2019
Validity	1 year
Location	https://pki.multicert.com/index.html

In order to standardize the information corresponding to the Multicert PKI, this CPS, and from this issue onwards, will incorporate the CPSs so far managed and made available by the CA. In this sense, the OIDs corresponding to each of these CPSs are discontinued but remain valid for the lifetime of the certificates already issued. The following OIDs are to be discontinued but the information is now present in this document:

- 1.3.6.1.4.1.25070.1.1.1.1.0.7: CPS of Multicert Accredited Certification Authority (Multicert Certification Authority 001 and Multicert Certification Authority 002) ;
- 1.3.6.1.4.1.25070.1.1.1.2.0.7: CPS of the Multicert Trust Services Certification Authority (Multicert Trust Services Certification Authority 001).

Multicert PKI issues the certificates with the following OIDs:

Type of Certificate	Multicert OID
OCSP on-line 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[2])	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

[2] Organizational Validation

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

1.3 PKI Participants

1.3.1 Certification Authorities

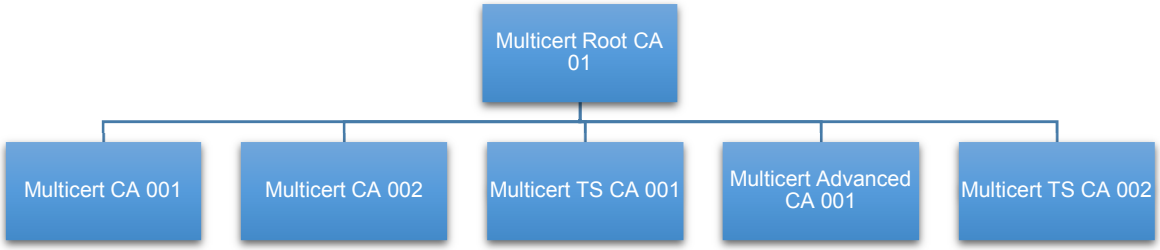
All CAs managed by Multicert are accredited by the National Security Authority (http://www.gns.gov.pt/trusted-lists.aspx), as provided for in Portuguese and European legislation, being therefore legally empowered to issue all types of digital certificates, including qualified digital certificates (the highest security level of digital certificates provided by law).

They fall into two trust hierarchies:

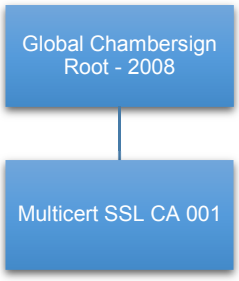
- The Multicert Root Certification Authority, duly accredited by the National Security Authority;
- The Global Chambersign Root - 2008with accreditation by the WebTrust (http://www.webtrust.org/) and present in most operating systems and web browsers; this hierarchy is only disseminated in the issuance of SSL certificates.

Multicert-managed CAs are recognized in most operating systems and web browsers and their main function is to manage certification services: issuing, operation, suspension and revocation for their subscribers.

Schematically, the following CAs are part of the Multicert Root Certification Authority hierarchy:



The following CA is included in the Global Chambersign Root - 2008 hierarchy:



Multicert Root CA 001

CERTIFICATE INFORMATION	
Distinguished Name	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT
Validity	04/04/2039
Thumbprint	46 af 7a 31 b5 99 46 0d 46 9d 60 41 14 5b 13 65 1d f9 17 0a

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Issuer	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert CA 001

CERTIFICATE INFORMATION	
Distinguished Name	CN=MULTICERT Certification Authority 001, OU = Accredited Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT
Validity	29/05/2020
Thumbprint	ef 2e 98 f4 42 ee cd 10 b9 8f 2a da 72 16 09 8c e4 83 53 18
Issuer	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A,C = PT

The CA named **Multicert CA 001** is active for status alteration and issuing of CRLs.

Multicert CA 002

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

Multicert TS CA 001

CERTIFICATE INFORMATION	
Distinguished Name	CN=MULTICERT Trust Services Certification Authority 001,OU=MULTICERT Trust Services Provider, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validity	01/10/2025
Thumbprint	6d f6 56 30 59 eb 2a 64 3f 74 74 4e 94 56 26 33 92 b8 bf ea
Issuer	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert Advanced CA 001

CERTIFICATE INFORMATION	
Distinguished Name	CN=MULTICERT Advanced Certification Authority 001,OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validity	12/06/2030

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Thumbprint	f8 25 77 a2 a8 c0 fc 1c 57 d2 d8 f3 7e 6c 0f fc 83 b3 3b 09
Issuer	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert TS CA 002

CERTIFICATE INFORMATION	
Distinguished Name	CN=MULTICERT Trust Services Certification Authority 002,OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validity	12/06/2030
Thumbprint	c8 e5 b7 b4 2d 07 2f 4e 03 fb db 3e 59 8d 51 c1 4c 0a 17 99
Issuer	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert SSL CA 001

CERTIFICATE INFORMATION	
Distinguished Name	CN=MULTICERT SSL Certification Authority 001,OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validity	20/05/2025
Thumbprint	67 b7 1d b0 25 0d 73 b0 68 f9 2e 19 e8 6d ad 89 a4 06 03 fe
Issuer	CN = Global Chambersign Root - 2008,O = AC Camerfirma S.A.,SERIALNUMBER= A82743287,L= Madrid (see current address at www.camerfirma.com/address),C = EU

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

The Registration Authority (RA) is the entity that approves the distinguished names (DN) of the subscribers of the certificates and upon evaluation of the request, accepts or rejects the request of the certificate. In addition, the RA also has to authority to approve the revocation or suspension of the certificates.

Multicert PKI has the following RAs:

- Internal RA – Operated by Multicert internal services, holder of the CA.
    - Multicert (RA MC)
- External RA – Operated by entities external to Multicert, who requests qualified digital certificates from Multicert CA:
    - Parliament (RA AR),

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

- Doctors' Association (RA OM),
- Pharmaceuticals' Association (RA OF) and,
- Institute of Financial Management and Equipment of Justice (RA IGFEJ).

PKI Multicert Registration Authorities comply with the requirements set forth in this document and are subject to External Audits, carried out for the National Security Cabinet, as well as Internal Audits, carried out by Multicert.

The issuance of digital certificates attaches the following General Conditions of the Digital Certificate Issuance Agreement:

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

Multicert PKI Registration Authorities (internal/external) have the following OIDs:

Registration Authority	OID of the Registration Authority
Registration Authorities	1.3.6.1.4.1.25070.1.3
Multicert Registration Authority	1.3.6.1.4.1.25070.1.3.1
Medical Association Registration Authority	1.3.6.1.4.1.25070.1.3.2
Pharmacists Association Registration Authority	1.3.6.1.4.1.25070.1.3.3
Parliament Registration Authority	1.3.6.1.4.1.25070.1.3.4
Institute of Financial Management and Equipment of Justice Registration Authority	1.3.6.1.4.1.25070.1.3.5

The assignment of names complies with the provisions in the Policy for Signature and Electronic Seal Qualified Certificates.

1.3.2.1 Internal RA

Within the scope of Multicert PKI, the registration authority is materialized by the relevant internal services that register and validate the necessary data, as explained in the Certificate Policy for each type of certificate issued.

1.3.2.2 External RAs

Multicert PKI decentralizes this function by means of external RAs which carry out the following activities regarding Qualified Digital Signatures:

- Validation of certificate request;
- After approval, submission of certificate issuance request to Multicert PKI;

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

- The CA will return the certificate, customized using a secure device;
- The RA is responsible for guaranteeing the delivery of the general conditions of the digital certificate issuance agreement and the certificate to the relevant subscriber or to whom legally represents it.

In addition to these activities, these RAs may also request Multicert PKI to revoke certificates as soon as the relevant subscriber ceases to perform functions within the scope for which the certificate was issued.

It should be noted that the Registration Authorities associated with Multicert are typically organizations that provide certificates in a controlled environment and only to signatories.

Multicert Registration Authorities only issue the following types of certificates:

- Medical Association Registration Authority: Qualified Digital Signature and Authentication;
- Pharmacists Association Registration Authority: Qualified Digital Signature and Authentication;
- Parliament Registration Authority: Qualified Digital Signature and Authentication;
- Institute of Financial Management and Equipment of Justice Registration Authority: Qualified Digital Signature, Authentication and Encryption.

1.3.3 Subscribers

Within the context of this document the term subscriber / subscriber applies to all end-users who have been awarded certificates by the Multicert PKI.

The subscribers of certificates issued by the Multicert PKI are those whose name appears in the "Subject" field of the certificate and use the certificate and its private key according to that defined in the various certificate policies detailed in this document, being issued the following certificates for the following subscriber classes:

- Individual or legal body;
- Corporate body (Organizations), or
- Services (such as computers, firewalls, routers, servers, etc.).

In some cases, certificates are issued directly to individuals or legal bodies for personal use however, there are situations in which the person requesting the certificate is different from the subscriber of the certificate, for instance, an organization may request certificates for its employees so that they can represent the organization in transactions / e-commerce applications. In such situations, the entity requesting the certificate is different from the subscriber of the certificate.

1.3.3.1 Sponsor

The issuance of certificates for technological equipment is always carried out under human responsibility, being this entity designated as sponsor.

The sponsor shall accept the certificate and will be responsible for its proper use, as well as for the protection and safekeeping of the relevant private key.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

1.3.4 Relying Parties

The relying parties or recipients are natural persons, entities or equipment that rely on the validity of the mechanisms and procedures used in the process of associating the name of the subscriber with its public key, i.e., they trust that the certificate corresponds in fact to whoever says it belongs to.

In this document, it is considered a relying party the one that relies in the content, validity and applicability of the certificate issued by the Multicert PKI.

1.3.5 Other participants

1.3.5.1 Supervisory Authority

The Supervisory Authority is the competent entity for the accreditation and inspection of the certification authorities.

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

The Supervisory Authority is one of the "parts" that contributes towards the reliability of the Qualified Certificates due to the competences it has over the issuing CAs. Within the scope of its functions, it exercises the following roles regarding the CAs:

a) Accreditation: CA approval procedure regarding the relevant activity, based on an evaluation made to different parameters, such as physical security, HW and SW, access and operation procedures;

b) Registration: procedure required by the CA to issue Qualified Certificates;

c) Inspection: procedure based on inspections carried out to the CA aimed at regularly checking the compliance parameters.

1.3.5.2 Registration Authority

Detailed in section 1.3.1.1.

1.3.5.3 Service provision external authorities

The entities providing support services to Multicert PKI have their responsibilities defined by means of agreements entered into with them.

1.3.5.4 OCSP Validation Authority

The purpose of the OCSP Validation Authorities is to verify the status of issued certificates using the Online Certificate Status Protocol[3] (OCSP) in order to determine the current status of the

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

certificate, upon request from an entity, without resorting to status verification through consultation of the Certificates Revocation List (CRL).

The OCSP Validation Authority service is provided by the Multicert PKI.

1.3.5.5 Security Auditor

An independent element, external to the Certification Authority, duly accredited by the National Accreditation Authority. Its mission is to audit the infrastructure of the Certification Authority in terms of equipment, human resources, processes, policies and rules for conformity assessment of the relying services under Regulation 910/2014.

The Certification Authorities managed by Multicert are audited by a Conformity Assessment Entity (duly accredited by the National Accreditation Authority) which issues a Compliance Report (CAR) to the provided to the Supervisory Authority, to assess the continuity of provision of reliable services.

Compliance Audits shall take place at least every 12 months to confirm that Multicert, as qualified service provider of reliable services and the reliable services it provides comply with the requirements defined in Regulation 910/2014.

1.4 Certificate Usage

The certificates issued within the scope of Multicert PKI are used by the various subscribers, systems, applications, mechanisms and protocols in order to guarantee the following security services:

a) Access control;

b) Confidentiality;

c) Integrity;

d) Authentication and;

e) Non-repudiation.

These services are obtained through the use of private-key encryption, through its use in the relying structure that the Multicert PKI provides. As such, the identification and authentication, integrity and non-repudiation services are obtained through the use of digital signatures. Confidentiality is guaranteed by using cypher algorithms when coupled with establishment and key distribution mechanisms.

1.4.1 Appropriate certificate uses

The requirements and rules defined herein apply to all certificates issued by the Multicert PKI.

Certificates issued for services are intended for use in authentication services and in establishing encrypted channels.

Certificates issued by Multicert PKI CAs are also used by the Relying Parties for verifying the chain of trust of a certificate issued by them, as well as to ensure the authenticity and identity of the issuer of a digital signature generated by the private key corresponding to the public key included in a certificate issued by Multicert PKI CAs.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

1.4.1.1 Certificates issued for an individual or legal body

Certificates issued for an individual or legal body, according to the type of certificate purchased, can be used for:

- Signing documents;
- Signing e-mails.

1.4.1.2 Certificates issued for organizations

Certificates issued for organizations are used to guarantee ownership of the website domain and/or identification of the organization.

1.4.2 Prohibited certificate uses

Certificates may be used in other contents only to the extent of that permitted by the applicable law.

Certificates issued by the Multicert PKI cannot be used for any function outside the scope of the previously described uses.

The certification services provided by the Multicert PKI have not been designed and are not authorized to be used in high-risk activities or activities that require a fail-safe operation, such as those related to the operation of hospital or nuclear facilities, air traffic control, rail traffic control, or any other activity where a fault could lead to death, personal injury or serious damage to the environment.

Additionally, certificates issued under this CPS may not be used for “traffic management” or man-in-the-middle purposes.

1.5 Policy administration

1.5.1 Organization administering the document

Management of this certificates policy is the responsibility of the Multicert PKI Authentication Working Group.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

1.5.2 Contact person

NAME	Multicert PKI 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
Web page	www.multicert.com
Phone:	+351 217 123 010

1.5.3 Person determining CPS suitability for the policy

The Multicert PKI Authentication Working Group shall determine compliance and internal applicability of this CPS (and/or relevant CPs) by submitting it to the Management Group for approval.

1.5.4 CPS approval procedures

Validation of this CPS (and/or relevant CPs) and the subsequent amendments (or updates) must be carried out by the Authentication Working Group. Amendments (or updates) must be published as new issues of this CPS (and/or relevant CPs) superseding any CPS (and/or relevant CPs) previously established. The Authentication Working Group must further determine when the amendments to the CPS (and/or relevant CPs) shall entail an amendment to the object identifiers (OID) of the CPS (and/or relevant CPs).

After validation, the CPS (and/or relevant CPs) shall be submitted to the Management Group, who is responsible for approving and authorizing the amendments in this type of document.

1.6 Definitions and acronyms

1.6.1 Definitions

Item	Definition
Digital signature	Advanced electronic signature mode based on an asymmetric cryptographic system consisting of an algorithm or series of algorithms, through which a unique and interdependent pair of asymmetric keys, one of which is private and one is public, is generated and which allows the subscriber to use the private key to declare the authorship of the electronic document to

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

	which the signature is affixed and the agreement with its contents; it further allows the recipient to use the public key to verify that the signature was created by using the corresponding private key and if the electronic document was changed after being signed.
Electronic signature	The result of an electronic data processing that may constitute an exclusive and individual right and be used to disclose the authorship of an electronic document.
Extended electronic signature	Electronic signature that meets the following requirements: i) Uniquely identifies the subscriber as author of the document; ii) Its affixing to the document depends only on the will of the subscriber; iii) It is created with means that the subscriber can maintain under its exclusive control; iv) Its connection to the document allows detecting any changes in the content thereof.
Qualified electronic signature	Digital signature or other advanced electronic signature mode that satisfies security requirements identical to those of the digital signature based on a qualified certificate and created through a secure signature creation device.
Accreditation Authority	Entity competent for the accreditation and supervision of certification authorities.
Certificate	Electronic document that links signature verification data to its subscriber and confirms the identity of such subscriber.
Website Authentication Certificate	Certification that makes it possible to authenticate a website and associate it with the natural or legal person for whom the certificate has been issued.
Extended Certificate	Certificate that offers the same quality as a qualified certificate however without the legal constraints implicit in the qualified signature and without the requirement of using a secure device for its creation. It does not confer the legal probative value of a qualified signature.
Website Authentication Qualified Certificate	Certificate for website authentication which is issued by a trusted service provider and complies with the requirements set out in Annex IV to Regulation EU No. 910/2014.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Qualified Certificate	Electronic signature certificate, issued by a trusted service provider and which complies with the requirements set out in Annexes I, II III and IV to Regulation EU No. 910/2014.
Standard Certificate	The same as extended certificate.
Private Key	Element of the asymmetric key pair intended to be known only by its owner, by which the digital signature is affixed to the electronic document or a previously encrypted electronic document is decrypted with the corresponding public key.
Public Key	Element of the asymmetric key pair intended to be disclosed and which verifies the digital signature affixed to the electronic document by the owner of the asymmetric key pair or encrypts an electronic document to be transmitted to the owner of the same key pair.
Accreditation	Act by which it is recognized to an entity that requests it and that performs the activity of a certification authority the fulfilment of the requirements defined in this document for the purposes provided therein.
Signature creation data	Unique set of data, such as private keys, used by the subscriber to create an electronic signature.
Signature verification data	Set of data, such as public keys, used to verify an electronic signature.
Signature creation device	Software or hardware used to enable the processing of signature creation data.
Signature creation safe device	A signature creation device ensuring, through the appropriate technical and procedural means, that: i) The data necessary for the creation of a signature used to generate a signature can only occur once and that the confidentiality of such data is ensured; ii) The data necessary for the creation of a signature used to generate a signature cannot, with a reasonable degree of security, be deducted from other data and that the signature is protected against forgery carried out using the available technologies;

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

	iii) The data necessary for the creation of a signature used to generate a signature can be effectively protected by the subscriber against unlawful use by third parties; iv) Data that need to be signed are not modified and can be presented to the subscriber before the signature process.
Electronic document	Document prepared using electronic data processing.
Electronic address	Identification of a proper computer equipment to receive and file electronic documents.
Certification Authority	Entity or natural or legal person that creates or provides means for the creation and verification of signatures, issues the certificates, ensures their publicity and provides other services related to electronic signatures.
Certification Body	Public or private body competent to evaluate and certify the compliance of electronic signature processes, systems and products with the requirements set out in line c), paragraph 1, article 12 of Decree-Law 62/2003.
Electronic Signature Product	Software, hardware or specific components indented for use in the provision of qualified electronic signature services by a certification authority or in the establishment and verification of qualified electronic signature.
Electronic Seal	Data in electronic format attached or logically associated with other data in electronic format to guarantee the origin and integrity of the latter.
Extended Electronic Seal	An electronic seal complying with the requirements laid down in Article 36 of Regulation 910/2014 EU of the European Parliament and the Council.
Qualified Electronic Seal	Extended electronic seal created by a qualified electronic seal creation device based on an electronic seal certificate.
Subscriber	Natural or legal person identified in a certificate as the subscriber of a signature creation device.
Timestamp validation	Declaration of the certification authority certifying the date and time of creation, sending, or reception of an electronic document.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

1.6.2 Acronyms

Acronyms	Definition
ANSI	American National Standards Institute
BR	Baseline Requirements
CA	Certification Authority (same as CA)
CRL	See CRL
DL	Decree-law
DN	Distinguished Name
CPS	Certification Practice Statement
EAL	Evaluation Assurance Level
CA	Certification Authority
CRL	Certificates revocation list
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
CLMS	Certificates Lifecycle Management System
SSCD	Secure Signature-Creation Device

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

CAA	Certification Authority Authorization

1.6.3 Bibliography

CA/Browser Forum – Baseline Requirements, v1.6.4;

CWA 14167 - *Cryptographic Module for CSP Signing Operations - Protection Profile*;

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

ETSI EN 319 411-1 v1.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

ETSI EN 319 411-2 V2.2.2 (2018-04) - 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;

ETSI TS 119 412-1 v1.2.1 (2018-05) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data sctructures;

ETSI EN 319 412-2 v2.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;

ETSI EN 319 412-3 V1.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;

ETSI EN 319 412-4 V1.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;

ETSI EN 319 412-5 v2.2.1 (2017-11) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;

Regulation EU No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on for electronic transactions in the internal market and repealing Directive 1999/93/EC

FIPS 140-1. 1994, *Security Requirements for Cryptographic Modules*.

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

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

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

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

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

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

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

RFC 6960. 2013, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

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

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

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

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

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

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

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

RFC 6844. 2013, *DNS Certification Authority Authorization (CAA) Resource Record.*

RFC 6962. 2013, *Certificate Transparency.*

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

2 Publication and repository responsibilities

2.1 Repositories

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

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

- Availability of platform services of 99.9% (24x7) excluding the necessary maintenance actions carried out during non-peak hours, ensuring during the availability time:
    - Minimum 99.990% response to requests to obtain the CRL;
    - Minimum 99.990% response to document requests from the CPS.
- Maximum number of CRL requests: 50 requests/minute;
- Maximum number of CPS requests: 50 requests/minute;
- Average number of CRL requests: 20 requests/minute;
- Average number of CPS requests: 20 requests/minute.

Access to the information provided by the repository is done via HTTPS and HTTP protocol, being implemented the following security mechanisms:

- CRL and CPS can only be altered using well-defined processes and procedures;
- The repository technological platform is duly protected by the most updated software and hardware security mechanisms;
- Human resources managing the platform have been properly trained for such service.

2.2 Publication of certification information

Multicert has a repository in web environment, allowing the Relying Parties to make on-line searches regarding revocation and other information related to the certificates.

Multicert always provides the following public information on-line:

- Electronic copy of this CPS and of the most updated Certificates Policy (CP) of Multicert PKI, with electronic signature by a duly authorized individual and with a digital certificate issued for that purpose:
    - Multicert PKI CPS available at URI: https://pki.multicert.com/index.html
    - Multicert PKI CP available at URI: http://pki.multicert.com/index.html
- CRL of Multicert PKI CAs:

  – CA Multicert Root 001:
    - CRL - URI: http://pkiroot.multicert.com/crl/root_mc_crl.crl

  – CA Multicert 001

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

- CRL - URI: http://pki.multicert.com/crl/crl_mca001.crl
  - Delta-CRL – URI: http://pki.multicert.com/crl/crl_mca001_delta.crl

– CA Multicert 002

- CRL - URI: http://ec2pki.multicert.com/crl/crl_mca002.crl
  - Delta-CRL – URI: http://ec2pki.multicert.com/crl/crl_mca002_delta.crl

– CA Multicert TS 001

- CRL – URI: http://ts4pki.multicert.com/crl/crl_mtsca001.crl
  - Delta-CRL – URI: http://ts4pki.multicert.com/crl/crl_mtsca001_delta.crl

– CA Multicert Advanced 001

- CRL – URI: http://pki.multicert.com/crl/crl_adv001.crl
  - Delta-CRL – URI: http://pki.multicert.com/crl/crl_adv001_delta.crl

– CA Multicert TS 002

- CRL – URI: http://pki.multicert.com/crl/crl_ts002.crl
  - Delta-CRL – URI: http://pki.multicert.com/crl/crl_ts002_delta.crl

– Multicert PKI CAs Certificates:

- CA Multicert Root 01 – URI : http://pkiroot.multicert.com/cert/MCRootCA.cer
- CA Multicert 001 - URI: https://pki.multicert.com/cert/MULTICERT_CA/mca_001_2.cer
- CA Multicert 002 - URI: http://ec2pki.multicert.com/cert/mca_002_2.cer
- CA Multicert TS 001 – URI : http://ts4pki.multicert.com/cert/MTS_CA.cer
- CA Multicert Advanced 001 – URI : https://pki.multicert.com/cert/MULTICERT_CA/TSCA_002.cer
- CA Multicert TS 002 – URI : https://pki.multicert.com/cert/MULTICERT_CA/TSCA_002.cer

– Other relevant information - URI: http://pki.multicert.com.

In addition, all previous versions of Multicert PKI's CP and CPS are kept, being available upon request (provided justified) being however outside of the free access public repository.

Any compliance declarations will be provided upon request sent via email to pki.documentacao@multicert.com.

2.3 Time or frequency of publication

Updates to this CPS and the relevant CPs are carried out annually and will be published immediately after their approval by the Management Group, in accordance with section 9.12.

Certificates for the CAs managed by Multicert are published immediately after their issuance.

The CLR issued by the Multicert Root CA must be published at least once every 4 months.

CRLs issued by CAs that issue Multicert end-user certificates will be published at least once every week. The relevant Delta-CRL will be published on a daily basis.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

2.4 Access controls on repositories

Information published by Multicert S.A. is available online, being subject to access control mechanisms (reading access only). Multicert S.A. has implemented hardware and software security measures to prevent non-authorized parties from adding, deleting or modifying repository records.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

3 Identification and authentication

3.1 Naming

Naming will be carried out as follows:

- Certificates issued for natural persons will receive the real name (or pseudonym) of the subscriber;
- Certificates issued for legal persons will receive the name of the entity, with the name of the legal representative being stated in the certificate;
- Service certificates will receive the domain qualified name and/or the scope of the relevant usage.

3.1.1 Types of names

Multicert PKI CAs certificates, as well as the certificates issued by the CAs, are identified with a unique name (DN – Distinguished Name) according to standard X.500.

The unique name of these certificates is identified in Multicert PKI Certificates Policy:

Type of Certificate	OID of type of certificate
OCSP on-line 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 Authentication (OV[4])	1.3.6.1.4.1.25070.1.1.1.1.0.1.5
Application	1.3.6.1.4.1.25070.1.1.1.1.0.1.6
Virtual TPA	1.3.6.1.4.1.25070.1.1.1.1.0.1.8

3.1.2 Need for names to be meaningful

Multicert will ensure, within its trust hierarchies:

- Non-existence of certificates that, having the same unique name, identify different entities;
- The relation between the subscriber and the organization it belongs to is the same that is referred in the certificate and can be easily perceived and identified by humans (with exception of pseudonym certificates).

[4] Organizational Validation

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

3.1.3 Anonymity or pseudonymity of subscribers

Multicert PKI can issue certificates with subscriber pseudonym, being guaranteed for that purpose that:

- The certificate shall bear the subscriber's pseudonym, clearly identified as such, and shall retain the evidence of the true identity of subscribers of certificates issued with a pseudonym;
- The legal authority shall be informed, whenever it orders it in accordance with the law, of the data relating to the identity of the subscribers of certificates issued with a pseudonym following, if applicable, the provisions of article 182 of the Code of Criminal Procedure.

3.1.4 Rules for interpreting various name forms

The rules used by Multicert for interpreting the name forms comply with that defined in RFC 5280[5], ensuring that all DirectoryString attributes of the fields “issuer” and “subject” of the certificate are coded using the UTF8String format, with exception of the “country” and “serialnumber” attributes which are coded using the PrintableString format.

3.1.5 Uniqueness of names

Identifiers of the DN type are unique for each certificate subscriber issued by the Multicert PKI and will not cause any ambiguity.

According to the relevant issuing processes, Multicert rejects the issuing of certificates with the same DN for different subscribers. For each type of certificate issued, its Certificate Policy indicates the contents of the serialnumber that should be chosen in order to ensure the uniqueness of the field and not cause ambiguity for a Relying Party.

3.1.6 Recognition, authentication and role of trademarks

Certificate requesting entities must demonstrate that they are entitled to use the requested name and the designations used in the certificates issued by the Multicert PKI cannot violate the intellectual property rights of other individuals or organizations.

During the certificate subscriber's authentication and identification procedure, before the certificate is issued, the requesting entity must submit any legal documents evidencing its right to use the requested name.

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

3.2 Initial identity validation

3.2.1 Method to prove possession of a private key

3.2.1.1 Signature (eSign)

The key pair and the certificate are provided using an encrypted token (SmartCard or USB token) with an encrypted chip, physically customized for the subscriber. Ownership of the private key is ensured by the issuance and customization process of the encrypted token, thus ensuring that:

- The key pair is generated in the cryptographic HSM and included in the encrypted token, using a secure and direct communication, without any record in any device;
- The encrypted token is customized for the subscriber;
- The public key is sent to Multicert CA for issuance of the corresponding digital certificate being the latter also included in the encrypted token;
- The encrypted token is delivered either in person or via mail;
- The certificate is issued with a "suspended" status being activated by a link provided to the subscriber, by which the latter will be authenticated using the authentication certificate included in the encrypted token. Upon authentication, the subscriber will receive a temporary password (OTP) in his/her cell phone that must be entered in the certificate activation page. As soon as this process is successfully completed, the certificate will be active and ready to be used.

3.2.1.2 Electronic Seal (eSeal)

In case of a certificate qualified for Electronic Seal, in addition to the method described in 3.2.1.1, there is also the option of the key being generated by the person Responsible referred to by the legal person (Organization) using its own HSM. In this case:

- The person responsible and the relevant organization is responsible for the key generated and by the HSM used for that purpose;
- Multicert must be provided with all the necessary documentation along with a CSR;
- The certificate, after validation of the submitted documentation, is returned to the person responsible.

The method used to prove ownership of the private key must comply with standard PKCS#10.

3.2.1.3 Authentication of website - Certificate for Organization (OV)

It must be guaranteed that the certificate request includes the private key corresponding to the public key to be listed in the certificate. The method used to prove ownership of the private key must comply with standard PKCS#10.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

3.2.1.4 Services certificate

Issuance of certificates for Multicert PKI services is carried out by elements belonging to the PKI Working Groups, who receive the CSR generated in the relevant services.

The method used to prove ownership of the private key must comply with standard PKCS#10.

3.2.1.5 Extended Certificate (NC)

It must be guaranteed that the certificate request includes the private key corresponding to the public key to be listed in the certificate. The method used to prove ownership of the private key must comply with standard PKCS#10.

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 digital certificate, the subscriber must prove that controls the email address.

To do that, the CA performs a challenge-response procedure, which consists of generating a token, and send it by email to the email address to be included in the certificate. To prove the control of the email address, the subscriber click on the link that contains the token, sent inside the email. The CA receives the response and prove of email address control is concluded with success.

3.2.3 Method to validate Domain Control

Multicert validates the Applicant`s right to use or control each domain name that will be listed in the Common Name and Subject Alternative Name fields of a Certificate, by using at least one of the following procedures from section 3.2.2.4 of the Baseline Requirements:

1. Agreed-Upon Change to website – by the Applicant placing an agreed-upon Request Token or Random Value in the “/.well-known/pki-validation” directory, performed in accordance with Baseline Requirements section 3.2.2.4.6;
2. Email to DNS TXT Contact – confirming the Applicant`s control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value. The Radom Value remains valid for 7 days. Performed in accordance with Baseline Requirements section 3.2.2.4.14;
3. Phone Contact with Domain Contact – confirming the Applicant`s control over the FQDN by calling the Domain Contact`s phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with Baseline Requirements section 3.2.2.4.15.

3.2.4 Method to validate IP Control

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 procedures:

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

1. 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;
2. 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);
3. Research on the IP address followed by verification of control over the resulting Domain Name;
4. 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.

3.2.5 Authentication of organization identity

Validation of the legal person's data is carried out using documents issued by legal bodies defined for that purpose (e.g.: Commercial Registry Office or Permanent Certificate). The data of the technical manager and of the organization representative(s) are validated using a copy of the identification document or, in case it is not available, the issuance contract (form) must be duly authenticated by a legal entity with powers for such act (notary public or lawyer).

Validation of the certificate requests is carried out using evidencing documents issued by trusted entities that allow verification of the requesting organization data as well as those of its legal representatives (e.g.: Permanent Certificate).

When a domain name is included in the certificate, Multicert shall authenticate the Organization's right to use the domain name as a fully qualified domain name (Certificates Policy available at https://pki.multicert.com). In these cases, confirmation of the certificate request is made by means of a recorded phone call to the number provided by a trusted source (official website, whois, etc.) and the information is confirmed with the technical manager responsible for requesting the certificate.

3.2.6 Authentication of individual identity

The Digital Signature Qualified Certificates are issued in a "suspended" status and their activation is carried out using a digital mechanism that uses an authentication via the Authentication certificate issued for the subscriber. Electronic Seal Qualified Certificates are issued in the "active" status with authentication of the identity of the technical manager being carried out with the delivery, either in person or by registered mail with an additional service or personal delivery.

Initial validation of the applicant's identity for an extended certificate, issued within the scope of Multicert PKI, is carried out using the documentation requested and submitted by the applicant along with the form for issuance of the extended certificate, which allows validation of the data included in the request, namely the subscriber's data and the data of the Responsible Body requesting the certificate. The signatures in the form are verified by comparing them to the copies of the requested identification documents.

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

3.2.7 Non-verified subscriber information

All information provided by the subscriber/subscriber is verified.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

3.2.8 Validation of authority

The data of the technical manager and of the organization representative(s) are validated using a copy of the identification document or, in case it is not available, the issuance contract (form) must be duly authenticated by a legal entity with powers for such act (notary public or lawyer).

In case of request for a Website Authentication certificate, Multicert further performs the verification of the relevant CAA records before issuance of the certificate. The CA will act in compliance with the CAA records, if existing. Multicert CA identification domain in CAA records is 'multicert.com'[6].

3.2.9 Criteria for interoperation

Certificates issued by Multicert PKI are issued under a single trust hierarchy. In case of SSL certificates, the sub-CA responsible for their issuance has been subject to cross-certification in order to ensure Mozilla's recognition.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-keys

There is no routine re-keys process. Renewal of certificates uses the same procedures as for the initial authentication and identification where new key pairs are generated.

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 following are deemed as authenticated forms for revocation request:

- Revocation request made in the Client Area;
- Revocation request made in the Partner Area;
- Revocation request made by elements of the Multicert PKI Registration Operation Working Group;
- By the Issuing CA.

If the request is made in any other way, the revocation process for certificates issued by Multicert PKI will start with the SUSPENSION, allowing for the request authenticity validation to be

[6] cf. RFC 6844. 2013, *DNS Certification Authority Authorization (CAA) Resource Record*

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

performed properly. Identification and authentication of those involved in the revocation request will be made by comparing the signatures in the form with the copies of the requested identification documents.

3.4.1 Who can request certificate revocation

The revocation request can be made by one of the following elements:

- The subscriber or a representative,
- The Organization who requested the certificate,
- Multicert, whenever it becomes aware that the data included in the certificate do not correspond to the true or are not owned by the subscriber;
- External Registration Authority(ies) of Multicert CA, whenever they become aware that the data included in the certificate do not correspond to the true or are not owned by the subscriber or whenever there is a suspicion of a confidentially breach or loss or theft of the private key.

3.4.2 How to request certificate revocation

The revocation request can be presented in three different ways:

- On-line, using a service provided for that purpose in one of the addresses listed below, where the certificate status will change to SUSPENDED; only after the documentation relevant for the request has been duly received and validated, Multicert will change the certificate status to REVOKED:
    - Suspension interface for certificates issued up to 26/05/2015 (certificated with reference MAE or MRA): https://pki.multicert.com/suspensao;
    - Suspension interface for certificates issued as of 27/05/2015 (certificates with reference MTC): https://www.multicert.com/suspensao.
- By sending directly to Multicert the Revocation Request Form, provided by Multicert in its *site*, duly completed and along with the documentation requested for that purpose;
- Using the online services of the Client Area or Multicert Partner Area, not being necessary to submit any documentation.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

The request for issuance of a certificate by Multicert PKI starts with completing a form corresponding to the intended certificate. The forms for each type of certificate are available at the Multicert Online Store. For each type of certificate, the information necessary and the process to follow is indicated.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

As soon as Multicert receives the form for issuance of a certificate, as well as the information required for complying with such request, it will proceed with validation of the information provided in order to verify data authenticity (see section 3.2).

For the requests regarding Website Authentication certificates, Multicert further performs the verification of the relevant CAA records before issuing SSL certificates. The CA will act in compliance with the CAA records, if existing. Multicert CA identification domain in CAA records is 'multicert.com'[7].

4.2.2 Approval or rejection of certificate applications

Multicert will only accept the certificate application if all data included in the request are true; if so, the application will be approved.

In case the information included is not true or is lacking, Multicert will reject the application and the person responsible for the request will be informed accordingly.

4.2.3 Time to process certificate applications

Multicert has Service Level Agreements (SLAs) which information is available in the Online Store regarding issuance of certificates. However, issuance of the certificates and the time elapsing between the application and the delivery of the certificate will depend mostly on the submission of the information required and on its authenticity.

4.3 Certificate issuance

Certificates issued by Multicert PKI are issued using the Multicert platform automatically, after registration and approval of the certificate application. After approval, the application is sent directly to the Certification Authority which will proceed with issuance of the certificate.

[7] cf. RFC 6844. 2013, *DNS Certification Authority Authorization (CAA) Resource Record*

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

4.3.1 CA actions during certificate issuance

For any certificate issued by Multicert PKI, the application is subject to approval. This approval will depend on the type of certificate and of the Certification Authority. In case of approval of end-user certificates, the Registration Operation Working Group is responsible for managing and approving the certificates applications.

4.3.1.1 Issuance of Signature and Electronic Seal Qualified Digital Certificates

In case of Signature and Electronic Seal Qualified Digital Certificates, the certificate will be stored in a secure storage device that, depending on the selected option, may be SmartCard (a card with an encrypted ship) or a USB token.

4.3.1.2 Issuance of Website Authentication Certificates

In order to issue Webserver Certificates, the client will generate a certificate application which is then submitted to Multicert. The Certificate (CER) is issued and provided by Multicert to the client via e-mail.

4.3.1.3 Issuance of Extended Certificates

Extended Certificates can be provided in a secure storage device, like the qualified digital certificates, but can also be provided via download or a CD (depending on the selected option).

4.3.1.4 Issuance of Virtual TPA Certificates

Multicert will issue the certificate and it will be provided in a CD.

4.3.1.5 Issuance of Application Certificates

In order to issue Application Certificates, the certificate application is generated by the client and then submitted to Multicert.

Multicert will issue the certificate based on the application and will provide it via download or in a CD.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The subscriber or responsible for the certificate application will be automatically notified when the certificate is issued.

All website Authentication Certificates are registered in Certificate Transparency log servers immediately after being issued[8].

[8] cf. RFC 6962. 2013, *Certificate Transparency*

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

4.4 Certification acceptance

4.4.1 Conduct constituting certificate acceptance

For each type of certificate, the relevant Certificate Policy describes how the certificate is accepted.

Signature Qualified Certificates are issued in a suspended status being the subscriber's responsibility to activate them using an information exchange set between the subscriber and Multicert.

4.4.2 Publication of the certificate by the CA

Certificates for Website Authentication are published in Certificate Transparency log servers[8].

In addition to these, Multicert does not publish the certificates it issues with exception of the certificates and relevant public keys of the Certification Authorities it manages.

4.4.3 Notification of certificate issuance by the CA to other

Multicert does not notify other entities regarding the issuance of certificates except if previously agreed for the issuance of certificates with a proprietary approval system.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The use of the private key corresponding to the public key must only be allowed when the subscriber agrees and accepts the general conditions for issuance of a certificate upon subscription thereof by means of the agreement provided by Multicert.

Subscribers of certificates can only use the private key of their certificates for the exclusive purpose the key is intended to (defined in the field "KeyUsage" of the certificate) and always within the scope of the legal framework; usage of the key is the exclusive responsibility of the subscriber.

4.5.2 Relying party public key and certificate usage

Not applicable.

4.6 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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.

4.6.1 Circumstance for certificate renewal

No remarks.

4.6.2 Who may request renewal

No remarks.

4.6.3 Processing certificate renewal requests

No remarks.

4.6.4 Notification of new certificate issuance to subscriber

No remarks.

4.6.5 Conduct constituting acceptance of a renewal certificate

No remarks.

4.6.6 Publication of the renewal certificate by the CA

No remarks.

4.6.7 Notification of certificate issuance by the CA to other entities

No remarks.

4.7 Certificate re-key

4.7.1 Circunstances for certificate re-key

Multicert will accept the certificate re-key, being always deemed as a new issuance.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 entitites

N.A.

4.8 Certificate modification

Certificate modification is the process by which a certificate is issued for a subscriber (or sponsor) keeping the relevant keys with alterations only to the certificate information.

This practice is not supported by Multicert PKI.

4.8.1 Circumstance for certificate modification

No remarks.

4.8.2 Who may request certificate modification

No remarks.

4.8.3 Processing certificate modification requests

No remarks.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

4.8.4 Notification of new certificate issuance to subscriber

No remarks.

4.8.5 Conduct constituting acceptance of modified certificate

No remarks.

4.8.6 Publication of the modified certificate by the CA

No remarks.

4.8.7 Notification of certificate issuance by the CA to other entities

No remarks.

4.9 Certificate revocation and suspension

Revocation and suspension of certificates are actions by which the certificate is no longer valid before the end of its validity period, losing its operability.

Certificates in SUSPENDED state can revert to ACTIVE state. Certificates with a REVOKED state cannot revert to ACTIVE.

The revocation process for a certificate issued by Multicert PKI does not imply the submission of documentation if the relevant request is made in an authenticated manner:

- By the client/subscriber, using the Client Area;
- By the partner/person responsible for the Organization, using the Partner Area;
- By an element of the Registration Operation Working Group of Multicert`s PKI, due to a duly founded reason and using the backoffice provided for that purpose;
- By the Issuing CA, due to a duly founded reason and using the backoffice provided for that purpose.

Otherwise, the Revocation process will start with the SUSPENSION of the certificate.

In case of a Qualified Digital Certificate, it can only remain SUSPENDED for a period of 3 days; after this period has elapsed, the certificate will change into one of the two following conditions:

- Revoked, if the revocation request form is received and validated, along with the necessary documentation, or
- ACTIVE, if no revocation request form is received.

4.9.1 Circumstances for revocation

If one of the following reasons occurs, the certificate is revoked within 24 hours:

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

- The Subscriber requests, through a submission of a writing revocation request form, that the CA revoke the certificate;
- The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The private key and/or the password to access the private key (e.g. PIN) has been compromised or it is suspected to be compromised;
- The private key was lost;
- The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the certificate should not be relied upon.

If one of the following reasons occurs, the certificate is revoked within 5 days:

- The certificate was misused;
- The CA is made aware of a material change in the information contained in the certificate;
- The CA determines or is made aware that any of the information appearing in the certificate is innacurate;
- The CA is made aware that the Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
- The CA is made aware that the certificate was not issued in accordance with the requirements of the CA`s CPS, CP or applicable normative requirements;
- The certificate`s algorithm type and key size, or the public key parameters generation and quality checking are no longer comply with the i) Baseline Requirements for the SSL certificates; and/or ii) ETSI TS 119 312;
- The CA is made aware of any circunstances indicating that use of a Fully-Qualified Domain Name or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant`s right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- The CA is made aware of a demonstrated or proven method that exposes the Subscriber`s private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, or if there is clear evidence that the specific method used to generate the private key was flawed;
- When applicable, the cryptographic token/smartcard where the private key is stored have been lost, destruct or deteriorated.

If one of the following reasons occurs, the certificate may be revoked by the CA:

- The CA is notified due to a legal or administrative resolution;
- The CA is made aware that the certificate was used for illegal activities;
- The CA ceased operations and did not arrange another CA to provide revocation support for the certificates.

4.9.2 Who can request certificate revocation

Section 3.4 defines who can request the revocation of a certificate and how to do it.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

4.9.3 How to request certificate revocation

Section 3.4 defines who can request the revocation of a certificate and how to do it.

4.9.4 Revocation request grace period

The certificate revocation process, if made in a non-authenticated manner, will start with the suspension of the certificate. The subscriber/person responsible for the certificate has 3 working days to submit the relevant documentation, otherwise the certificate will be reactivated.

4.9.5 Time within which CA must process the revocation request

When the revocation request is made by the subscriber or the person responsible for the organization, through a written revocation request form, the The Registration Operation Working Group have 24 hours to process the request and revoke the certificate, after receiving the revocation request form.

The time to process the revocation request is defined in section 4.9.1.

Multicert guarantees publication of the certificate new status within 24 hours after the revocation request, whenever such request proves to be true.

4.9.6 CRL issuance frequency

Multicert Certification Authorities allowed to issue end-user certificates will issue CRLs every seven days, being issued Delta CRLs every 24 hours.

4.9.7 On-line validation of certificates

Multicert has a responder service for online validation of certificate status, with an availability corresponding to 99.9%.

The OCSP service provides a real-time validation of the certificate status.

4.10 Certificate status services

4.10.1 Operational characteristics

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

4.10.2 Service availability

The certificate status service is available 24 hours/days, 7 days/week.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

4.10.3 Optional features

No remarks.

4.11 End of subscription

The operability of a certificate will end upon one of the following circumstances:

a) Certificate revocation;

b) The certificate validity period has expired.

4.12 Key escrow and recovery

Multicert PKI can only perform key escrow for the private keys it manages.

4.12.1 Key escrow and recovery policies and practices

Private keys of the CAs managed the Multicert are stored in a secure token hardware, being made a backup copy using a hardware to hardware direct connection between the two secure tokens. Generation of the backup is the last step when issuing a new key pair by a CA managed by Multicert.

The backup process uses an HSM with double-factor authentication (portable authentication console and PED keys – small digital identification tokens, in the form of USB pen – identifying the different roles when accessing the HSM), where different persons, each one with a PED key, must authenticate before it is possible to perform the backup.

The secure token hardware with the backup of the private key of the CA managed by Multicert is placed in a safe deposit box located in secure secondary facilities and accessible only to authorized members of the Working Groups. Physical access control to such facilities prevents non-authorized access to the private keys.

The backup of the private key of the CA managed by Multicert can be recovered in case of malfunction of the original key. The key recovery process uses the same double-factor authentication mechanisms and with multiple elements as in the backup process.

4.12.2 Session key encapsulation and recovery policies and practices

No remarks.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

5 Facility, management and operational controls

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

5.1 Physical controls

5.1.1 Site location and construction

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

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

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

a) Masonry, concrete or brick walls;

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

c) Nonexistence of windows;

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

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

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

5.1.2 Physical access

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

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

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

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

5.1.3 Power and air conditioning

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

- Uninterrupted continuous energy feeding with enough power to maintain an autonomous electrical network during periods when power is off and to protect the equipment in case of electrical surges that may damage it (the redundant equipment consists of uninterrupted power supply batteries, and diesel electric generators), and

Refrigeration/ventilation/air conditioning, that control the temperature and humidity levels, ensuring adequate conditions for the correct operation of all the electronic and mechanical equipment present inside the environment. A temperature sensor activates a GSM alert whenever the temperature reaches abnormal values. This GSM alert consists of phone calls with a previously recorded message to the maintenance team elements.

5.1.4 Water exposures

High security zones have the proper mechanisms installed (flood detectors) to minimize the flood impact on Multicert's PKI systems.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

5.1.5 Fire prevention and protection

Multicert's 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 equipments are available and positioned on strategical and easy access places in order to be quickly used at the beginning of a fire and successfully extinguishing it;
- Well defined emergency procedures in case of fire.

5.1.6 Media storage

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

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

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

5.1.7 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 equipments (hard discs, *tapes*, ...) shall be duly cleaned in a way it is not possible to retrieve any information (through safe formatting, or physical destruction of the equipment).

5.1.8 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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

access only to authorized personnel, also ensuring the protection against accidental damages (e.g., caused by water or fire).

5.2 Procedural controls

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

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

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

5.2.1 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 nine different categories (which correspond to six distinct Working Groups) in order to ensure that the sensitive operations are performed by different authenticated people, eventually belonging to different Working Groups.

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

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

5.2.1.1 Setup Working Group

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

The group duties are:

- to install, interconnect and configure the CA's *hardware*;
- to install and configure the CA's base *software*;
- to configure the required initial passwords[9], 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;

[9] BIOS, SO administrator account, etc

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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

5.2.1.3 Authentication Working Group

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

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

This group's responsibilities are:

- To define all CA policies and ensure that they are updated and adapted to its reality;
- To ensure that the CA CPs are supported by the CA CPS;
- To ensure that all documents relevant and directly or indirectly related with the CA operation are stored in the Information Environment;
- Management of the "Authentication Environment";
- Management of all non-personal passwords;
- To keep an updated inventory of all the authentication *tokens* used in the "Production environment", and when the *tokens* are at the responsibility of some member(s), to register the identification of that(those) member(s), and safekeeping those registrations in the "Authentication Environment";
- To keep an updated inventory of all the passwords[10] used in the "Production environment", and when the passwords are at the responsibility of some member(s), to

[10] By registering the value

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 CA's operability. This group shall have at least 2 (two) members.

This group's responsibilities are:

- To audit the performance and to confirm the accuracy of the CA's processes and ceremonies;
- To register all sensitive operations;
- To investigate procedural fraud suspects;
- To regularly verify the functionality of the security controls (alarm devices, access control devices, fire sensors, etc.) present in the several environments;
- To register the results of all the actions they perform;
- To assume the role of “System Auditor”,
- To validate that all used resources are secure;
- To verify periodically the integrity of the Custody Environments, ensuring that the respective artefacts are found there[11] and are duly identified;
- To verify periodically the records/logs of the CA.

[11] 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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[12]. 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 subscriber for the issuance/revocation of certificates;
- To issue certificates when the procedure is not automatised;
- To revoke/suspend certificates in case this procedure is not automatised.

5.2.1.7 Monitoring and Control Working Group

The mission of this group consists in the monitoring consolidation and analysis of the security control points of all the resources used in Multicert’s PKI, 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’s PKI, still assuming a relevant role in the incident control and related management process.

This group's responsibilities are:

- To consolidate and analyse the monitoring of the resources used in Multicert’s PKI;
- 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;

[12] Defined for each artefact in its custody.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

- To make production passages required by pre-production;
- To monitor events, manage alarms and classify incidents;
- To define, support the implementation and continuous improvement of incident response procedures;
- To make production passages required by pre-production.

5.2.1.8 Management Working Group

It is the decision-making body of Multicert's PKI, and 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 the Multicert PKI CAs, enhancing the revision and approval of all documents and policies of the CAs. 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 CAs operation;
- To review and approve all the forms resulting from the performed ceremonies and all the documents related to the CAs 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 CA'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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

5.2.3 Identification and authentication for each role

It is the responsibility of the Management Working Group to name the elements that form part of the remaining groups.

The result of this nomination is described in the Multicert PKI Human Resources Policy document, which is distributed by all elements.

Based on this document, the access to environments and systems related to Multicert PKI are configured.

5.2.4 Functions that require separation of responsibilities

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

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		✘	✘	✘	✘	✘		✘	✘
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;

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

- 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 CAs) regarding any information about the CAs, its operation, its environments and human resources at its service and about the subscribers 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[13] 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 CAs;
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.

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 CAs;

Whenever there are changes introduced to the Certificate Policies or Certification Practices Statement, recycling sessions are held for all the elements of the CAs.

5.3.5 Job rotation frequency and sequence

Nothing to remark.

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 [14], 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 resources of CAs;

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

- Operations performed by members of the Working Groups,
- Physical safety devices of entry/exit of several levels of security.

The entries in the records include the following information:

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

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

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

5.4.5 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 CA system.

5.4.7 Notification to event-causing subject

Auditable events are 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

5.5 Records archival

5.5.1 Types of records archived

All auditable data are stored (as indicated in section 5.4.1**Erro! A origem da referência não foi encontrada.**), 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.

5.5.3 Protection of archive

The archive:

- Is protected so that only authorised members of the Working Groups may consult and access to its content,
- Is protected against any change or attempt to remove it,
- Is protected against the deterioration of the media where it is stored, through the regular migration to a new media,
- Is protected against obsolescence of the *hardware*, operating systems and other *software*, through the conservation of the *hardware*, operating systems and other *software* which then make part of the archive itself, in order to allow the access and use of the stored records in a timeless manner, and
- Is stored in a safe manner in external environments.

5.5.4 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 private keys of CAs (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 of CAs 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 shall suspend the services of the affected CAs and notify the accreditation authority.

5.7.3 Entity private key compromise procedures

In the event that the private key of one of the Multicert PKI CAs 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 affected CA certificate and all certificates issued in the “branch” of its trust hierarchy;
- Notification of the Accreditation Authority and all subscribers of certificates issued in the “branch”of the affected CA trust hierarchy;
- Generation of a new key pair for the affected CA;
- Renewal of all certificates issued in the trust hierarchy “branch” of the affected CA.

5.7.4 Business continuity capabilities after a disaster

Multicert has the computing resources, *software*, backup copies and records stored in its secondary security 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

5.8 CA or RA termination

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

a) Inform the Accreditation Authority;

b) Inform all certificate subscribers;

c) Revoke all issued certificates;

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

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

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

In case of changes in the organization/structure responsible for the management of the activity of the CAs, Multicert shall inform the entities listed in the previous lines of that fact.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

6 Technical security controls

This section defines the security measures implemented for Multicert's PKI 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 the key pairs of Multicert PKI CAs is processed in accordance with the requirements and algorithms defined in this policy.

6.1.1 Key pair generation

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

The cryptographic *hardware* used for the generation of keys of Multicert PKI CAs 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 keys for Qualified Digital Signature and Electronic Seal certificates (if not generated by the certificate subscriber in a secure module) are generated by Multicert 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

The delivery of the private key associated with the Qualified Digital Signature and Electronic Seal certificates (when not generated by the certificate holder in a secure module) 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 Multicert CA, according to the procedures mentioned in section 4.3.

6.1.4 CA public key delivery to relying parties

The public keys of Multicert PKI CAs shall be made available through the respective certificates, according to section 2.2.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 Multicert PKI CAs keys;
- 2048 *bits* RSA for the keys associated to the remaining certificates issued by Multicert PKI CAs 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)

According to section 7.1.

6.2 Private key protection and cryptographic module engineering controls

In this section are considered the requirements for private key protection and for Multicert PKI cryptographic modules. 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 of Multicert PKI CAs, 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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

- 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 subscriber.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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

The activation data necessary for using the private key of a Multicert PKI 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 a CA's private key stored in the *hardware* cryptographic module.

Two parts (n) are necessary for the activation of a CAs private key.

6.2.3 Private key escrow

Retention of the Multicert PKI CAs private key is explained in detail in section 4.12.

6.2.4 Private key backup

The private keys of Multicert PKI CAs have at least one backup copy with the same security level as the original key, according to section 4.12.

6.2.5 Private key archival

The private keys of Multicert PKI CAs, subject to backup copies, are stored as identified in section 4.12.

6.2.6 Private key transfer into or from a cryptographic module

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

Even if a backup copy of the private keys of Multicert PKI CAs 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 of Multicert PKI CAs are stored in an enciphered way in the cryptographic *hardware* modules.

6.2.8 Method of activating private key

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

For activating the private keys of a Multicert PKI 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 of a Multicert PKI CA is deactivated when the CA's system is disconnected.

To deactivate a Multicert PKI CA's private key 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 of Multicert PKI CAs (including backup copies) are erased/destroyed in a procedure duly identified and audited, as soon as their expiry date (or if they are revoked before that period).

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

A backup copy of all public keys of Multicert PKI CAs 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:

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Certificate type	Private key usage	Certificate validity
Multicert Root CA	12 years	25 years
Sub CAs	5 years	11 years and 4 months
OCSP *on-line* validation	4 months	5 years
Qualified Digital Signature and Electronic Seal	3 years	3 years
Authentication	3 years	3 years
Advanced Digital Signature	3 years	3 years
Web Server Certificate (OV[15])	2 years	2 years
Application	3 years	3 years
Virtual TPA	3 years	3 years

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data necessary for using the private keys of Multicert PKI CAs 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 of Multicert PKI CAs 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 of 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.

[15] Organizational Validation

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The access to the Multicert PKI servers is restrict to the members of the Working Groups with a valid reason for that access.

Multicert Root CA 001 is an offline CA, which is only activated for periodic maintenance and deactivated immediately after.

Multicert PKI Sub CAs work online, and the certificate issuance request is done from the Certificate Lifecycle Management System (SGCVC) and/or the operation console.

Multicert PKI Sub CAs 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 Multicert PKI are reliable and protected against changes.

The hardware cryptographic module of Multicert PKI CAs complies 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 Multicert PKI CAs software was not changed before it was first used. All software configurations and changes 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 PKI systems. The system used to manage the Multicert PKI CAs, 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

6.7 Network security controls

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

6.8 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 subscriber (person or system) with which they will use the encipher mechanism or digital signature. The trust is obtained through the use of X.509 v3 digital certificates, which are a data structure that makes the connection between the public key and its subscriber. This connection is stated through the digital signature of each certificate by a trusted CA. The CA may base this statement on technical means (for example, proof of the possession of the private key through a challenge-response protocol), on the presentation of the private key or on the registration made by the subscriber.

A certificate has a limited validity period, indicated in its content and signed by the CA. Since the signature of the certificate and its validity may be independently verified by any software that uses certificates, the certificates may be distributed through communication lines and public systems, and may also be stored in any type of storage units.[5]

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. [5]

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

- ITU.T recommendation X. 509[16];
- RFC 5280[5];
- Applicable legislation, national and European;
- CABForum Baseline Requirements.

The certificate profiles may be consulted in Certificate Policy document associated to this CPS.

7.1.1 Version number(s)

All certificates issued in the Multicert PKI are in compliance with version 3 of X.509.

7.1.2 Certificate extensions

The extensions of certificates issued in Multicert PKI are in compliance with RFC 5280.

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

7.1.3 Algorithm object identifiers

Certificates issued in Multicert PKI are signed using the algorithm sha256WithRSAEncryption (1.2.840.113549.1.1.11):

{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

7.1.4 Name forms

As defined in section 3.1.

7.1.5 Name constraints

Nothing to remark.

7.1.6 Certificate policy object identifier

All certificates issued in Multicert PKI contain the qualifiers:

- "*policyQualiflierID*: 1.3.6.1.5.5.7.2.1" and "*cPSuri*", which point to the URI where the Certification Practices Statement with the OID identified by the "*policyIdentifier*" can be found;
- "*policyQualiflierID*: 1.3.6.1.5.5.7.2.2" and "*userNotice explicitText*", which point to the URI where the Certificate Policy with the OID identified by the "*policyIdentifier*" can be found.

Web Server Certificates contain also the qualifier 0.4.0.194112.1.4 (regulation EU nº 910/2014).

7.1.7 Usage of Policy Constraints extension

Nothing to remark.

7.1.8 Policy qualifiers 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.

7.1.9 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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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.[5]

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.[5]

The profile of the CRLs issued by Multicert PKI CAs conforms to:

- ITU.T Recommendation X.509[16];
- RFC 5280[5] and;
- Applicable legislation, national and European.

The certificate profiles may be consulted in Certificate Policy document associated to this CPS, regarding to Multicert PKI.

7.2.1 Version number(s)

The CRLs issued in Multicert PKI conform to version 2 of RFC 5280, and include the following fields:

Field	Value
Version	2
Signature Algorithm	sha-256WithRSAEncryption
Issuer Name	DN of the CA issuing the CRL
This Update	CRL issuing date
Next Update	Date of the next CRL issuance
Revoked Certificates List	List of revoked certificates. The certificate serial number and the revocation date are included for each list entry.
Signature	Signature produced by the CA issuing the CRL

7.2.2 CRL and CRL entry extensions

The CRLs issued in Multicert PKI have the following extensions:

Extension	Value
Authority Key Identifier	Identifier of the CA issuing the CRL
CRL Number	Sequential CRL number
CRL Reason Code	Revocation reason (optional)

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

7.3 OCSP profile

The profile of the OCSP certificates issued in Multicert PKI is compliant with:

- ITU.T recommendation X.509[16];
- RFC 6960[17] and;
- Applicable legislation, national and European.

The OCSP certificate profiles may be consulted in the Certificate Policy document associated to this CPS, regarding to Multicert PKI.

7.3.1 Version number(s)

The OCSP requests and responses issued in Multicert PKI conform to version 1 of RFC 6960.

7.3.2 OCSP Extensions

Nothing to remark.

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 PKI.

Besides the compliance audits, Multicert shall perform other inspections and investigations to ensure the compliance of Multicert PKI CAs 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. Multicert must prove, through audit and anual safety reports (produced by the conformity assessment body accredited by the National Accreditation 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 recognised suitability, holding proved experience and qualifications in the field of security of information and information systems, public key infrastructures, acquainted with applications and programs of digital certification and with the performance of safety audits. His/her mission is to audit the 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 subscribers.

8.4 Topics covered by assessment

The scope of audits and other assessments include the accordance with the national legislation and this CPS and other rules, procedures and processes (especially the ones related with key

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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

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

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

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

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

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

    c. Proceeds to the immediate revocation of the activity.

8.6 Communication of results

The results shall always be communicated Supervisory Body.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

9 Other business and legal matters

This section deals with business aspects and legal matters.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

Nothing to remark.

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

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

9.1.5 Refund policy

Nothing to remark.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other assets

Nothing to remark.

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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 of Multicert PKI CAs;

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

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

d) Business continuity and recovery plans;

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

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

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

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

i) The location of Multicert PKI'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).

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

9.3.3 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

9.4 Privacy of personal information

9.4.1 Privacy plan

The Certificate Lifecycle Management System (SGCVC) is responsible for implementing the measures ensuring the privacy of personal data, according to the Portuguese legislation.

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

In accordance with the Portuguese legislation.

9.4.5 Notice and consent to use private information

In accordance with the Portuguese legislation.

9.4.6 Disclosure pursuant to judicial or administrative process

Nothing to remark.

9.4.7 Other information disclosure circumstances

Nothing to remark.

9.5 Intellectual property rights

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

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

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Multicert S.A., as an entity that provides certification services, is obliged to:

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

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

c) Protect its private keys;

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

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

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

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

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

i) Store the certificates issued without any changes;

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

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

l) Revoke the certificates under the terms of section “Certificate Suspension and Revocation” of this document and publish the revoked certificates on the CRL of Multicert PKI CAs repository, 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 subscribers in case one of the CAs 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 subscribers 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;

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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

w) Make available the certificates of Multicert PKI CAs.

9.6.2 RA representations and warranties

Registration Authorities are obliged to:

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

b) Allow the issuance of certificates free of errors of data entry;

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

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

e) Store the certificates issued without any changes;

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

g) Collaborate with the audits performed by the Accreditation Nacional Body;

h) Operate in accordance with applicable legislation, namely in accordance with the Regulation 910/2014

i) Protect the keys under their custody, in case they exist;

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

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

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

9.6.3 Subscriber representations and warranties

It is the obligation of the subscribers 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;

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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

9.6.4 Relying party representations and warranties

It is the obligation of the parties that are entrusted with the certificates issued by Multicert PKI CAs 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, using the means indicated by Multicert S.A. in its website.

9.6.5 Representations and warranties of other participants

Nothing to remark.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

Multicert S.A., as a Certification Authority:

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

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

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

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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

f) shall not answer when the subscriber exceeds the limits set out in the certificate regarding its possible usages, in accordance with the conditions that were established and communicated to the subscriber;

g) 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

h) 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 PKI CAs.

9.9 Indemnities

In accordance with the legislation in force.

9.10 Term and termination

9.10.1 Term

The documents related with Multicert PKI (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 Multicert repository.

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

9.10.2 Termination

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

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

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

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

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

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

9.10.3 Effect of termination and survival

After the Management Working Group decides in favour of the elimination of the document related to the PKI, 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 PKI, 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

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

9.12 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.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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 S.A. 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.1.6.4.

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 v2.2.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

f) ETSI EN 319 411-1 v1.2.2 – 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 v2.2.2 (2018-04) 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 TS 119 412-1 v1.2.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

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

j) 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;

k) 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;

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

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

m) ETSI EN 319 412-5 v2.2.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;

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

o) 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

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

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

9.16.3 Severability

Nothing to remark.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Nothing to remark.

9.16.5 Force Majeure

Nothing to remark.

9.17 Other provisions

Nothing to remark.

Copyright © 2002 - 2019 MULTICERT - All rights reserved.

Approval

[Assinatura Qualificada] José Jorge Oliveira da Fonseca Alcobia

Digitally signed by [Assinatura Qualificada] José Jorge Oliveira da Fonseca Alcobia
Date: 2019.03.25 17:59:35 Z

Copyright © 2002 - 2019 MULTICERT - All rights reserved.