Engineering for digital security

Multicert Certificate Policy

Policies

MULTICERT_PJ.ECRAIZ_426_en

CA Identification: PKI

Rating: Public

Version: 5.0

Date: 09/12/2019

Normative Version

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

Document Identification: MULTICERT_PJ.ECRAIZ_426_en

Keywords:

Document Type: Policies

Title: Multicert Certificate Policy

Original Language: English

Language of Publication: English

Rating: Public

Date: 09/12/2019

Current Version: 5.0

CA Identification: PKI

Version History

Version no.	Date	Details	Author(s)
1.0	29/05/2018	Revision according to the RFC 3647 and the CABForum Baseline Requirements 1.5.7	Multicert S.A.
1.1-1.4	25/09/2018	Inclusion of procedure for method to prove email address control. Inclusion of practices for re-key. Inclusion of statement for external CA`s	Multicert S.A.
2.0	01/10/2018	Approval	Multicert S.A.
2.1	29/01/2019	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.
4.1	25/03/2019	Inclusion of PSD2 information	Multicert, S.A.
5.0	09/12/2019	Approval	Multicert, S.A.

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_427_en	Certification Practices Statement	Multicert S.A
MULTICERT_PJ.ECRAIZ_428_en	Certificate Profiles List	Multicert S.A.

Table of Contents

Multicert Certificate Policy 1

Table of Contents 3

1 Introduction 10

1.1 Overview 10
1.2 Document Name and Identification 10
1.3 PKI Participants 13
1.3.1 Multicert Certification Authorities 13
1.3.1.1 External Certification Authorities 13
1.3.2 Registration Authorities 13
1.3.3 Subscribers 13
1.3.4 Relying Parties 14
1.3.5 Other Participants 14
1.4 Certificate Usage 14
1.4.1 Appropriate Certificate Uses 14
1.4.2 Prohibited Certificate Uses 14
1.5 Policy Administration 15
1.5.1 Organization Administering the Document 15
1.5.2 Contact Person 15
1.5.3 Person Determining CP Suitability for the Policy 16
1.5.4 CP Approval Procedures 16
1.6 Definitions and Acronyms 16
1.6.1 Definitions 16
1.6.2 Acronyms 20
1.6.3 Bibliography 21

2 Publication and Repository Responsibilities 24

2.1 Repositories 24
2.2 Publication of Certification Information 24
2.3 Time or Frequency of Publication 24
2.4 Access Controls on Repositories 24

3 Identification and Authentication 25

3.1 Naming 25
3.1.1 Types of Names 25
3.1.2 Need for Names to be Meaningful 25
3.1.3 Anonymity or Pseudonymity of Subscribers 25
3.1.4 Rules for Interpreting Various Name Forms 25
3.1.5 Uniqueness of Names 25
3.1.6 Recognition, Authentication and Role of Trademarks 25
3.2 Initial Identity Validation 25
3.2.1 Method to Prove Possession of Private Key 26

3.2.2 Authentication of Organization Identity ... 26
3.2.2.1 Method to Prove Email Address Control ... 26
3.2.2.2 Method to Validate Domain Name / IP Address Control ... 26
3.2.3 Authentication of Individual Identity ... 26
3.2.4 Non-Verified Subscriber Information ... 27
3.2.5 Validation of Authority ... 27
3.2.6 Criteria for Interoperation ... 28
3.3 Identification and Authentication for Re-Key Requests ... 28
3.3.1 Identification and Authentication for Routine Re-Key ... 28
3.3.2 Identification and Authentication for Re-Key after Revocation ... 28
3.4 Identification and Authentication for Revocation Request ... 28
4 Certificate Life-Cycle Operational Requirements ... 30
4.1 Certificate Application ... 30
4.1.1 Who Can Submit a Certificate Application ... 30
4.1.2 Enrolment Process and Responsibilities ... 30
4.2 Certificate Application Processing ... 30
4.2.1 Performing Identification and Authentication Functions ... 30
4.2.2 Approval or Rejection of Certificate Applications ... 30
4.2.3 Time to Process Certificate Applications ... 30
4.3 Certificate issuance ... 31
4.3.1 CA Actions during Certificate Issuance ... 31
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate ... 31
4.4 Certificate Acceptance ... 31
4.4.1 Conduct Constituting Certificate Acceptance ... 31
4.4.2 Publication of the Certificate by the CA ... 31
4.4.3 Notification of Certificate Issuance by the CA to Other Entities ... 31
4.5 Key Pair and Certificate Usage ... 31
4.5.1 Subscriber Private Key and Certificate Usage ... 31
4.5.2 Relying Party Public Key and Certificate Usage ... 32
4.6 Certificate Renewal ... 32
4.6.1 Circumstance for Certificate Renewal ... 32
4.6.2 Who May Request Renewal ... 32
4.6.3 Processing Certificate Renewal Requests ... 32
4.6.4 Notification of New Certificate Issuance to Subscriber ... 32
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate ... 33
4.6.6 Publication of the Renewal Certificate by the CA ... 33
4.6.7 Notification of Certificate Issuance by the CA to Other Entities ... 33
4.7 Certificate Re-Key ... 33
4.7.1 Circumstance for Certificate Re-Key ... 33
4.7.2 Who may Request Certification of a New Public Key ... 33
4.7.3 Processing Certificate Re-Keying Requests ... 33
4.7.4 Notification of New Certificate Issuance to Subscriber ... 33
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate ... 34
4.7.6 Publication of the Re-Keyed Certificate by the CA ... 34
4.7.7 Notification of Certificate Issuance by the CA to Other Entities ... 34

4.8 Certificate Modification 34
4.8.1 Circumstance for Certificate Modification 34
4.8.2 Who May Request Certificate Modification 34
4.8.3 Processing Certificate Modification Requests 34
4.8.4 Notification of New Certificate Issuance to Subscriber 34
4.8.5 Conduct Constituting Acceptance of Modified Certificate 34
4.8.6 Publication of the Modified Certificate by the CA 34
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 35
4.9 Certificate Revocation and Suspension 35
4.9.1 Circumstances for revocation 35
4.9.2 Who Can Request Revocation 36
4.9.3 Procedure for Revocation Request 37
4.9.4 Revocation Request Grace Period 37
4.9.5 Time within which CA must Process the Revocation Request 37
4.9.6 Revocation Checking Requirement for Relying Parties 37
4.9.7 CRL Issuance Frequency 37
4.9.8 Maximum Latency for CRL`s 37
4.9.9 On-Line Revocation/Status Checking Availability 37
4.9.10 On-Line Revocation Checking Requirements 38
4.9.11 Other Forms of Revocation Advertisements Available 38
4.9.12 Special Requirements Related to Key Compromise 38
4.9.13 Circumstances for Suspension 38
4.9.14 Who Can Request Suspension 38
4.9.15 Procedure for Suspension Request 38
4.9.16 Limits on Suspension Period 38
4.10 Certificate Status Services 39
4.10.1 Operational Characteristics 39
4.10.2 Service Availability 39
4.10.3 Optional Features 39
4.11 End of Subscription 39
4.12 Key Escrow and Recovery 39
4.12.1 Key Escrow and Recovery Policy and Practices 39
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 39
5 Facility, Management and Operational Controls 40
5.1 Physical Controls 40
5.1.1 Site Location and Construction 40
5.1.2 Physical Access 41
5.1.3 Power and Air Conditioning 41
5.1.4 Water Exposures 41
5.1.5 Fire Prevention and Protection 42
5.1.6 Media Storage 42
5.1.7 Waste Disposal 42
5.1.8 Off-Site Backup 42
5.2 Procedural Controls 43
5.2.1 Trusted Roles 43

5.2.1.1 Setup Working Group 43
5.2.1.2 Operation Working Group 44
5.2.1.3 Authentication Working Group 44
5.2.1.4 Audit Working Group 45
5.2.1.5 Custody Working Group 46
5.2.1.6 Registration Operation Working Group 46
5.2.1.7 Monitoring and Control Working Group 46
5.2.1.8 Management Working Group 47
5.2.2 Number of Persons Required per Task 47
5.2.3 Identification and Authentication for each Role 48
5.2.4 Roles Requiring Separation of Duties 48
5.3 Personnel Controls 48
5.3.1 Qualifications, Experience and Clearance Requirements 49
5.3.2 Background Check Procedures 49
5.3.3 Training Requirements 49
5.3.4 Retraining Frequency and Requirements 50
5.3.5 Job Rotation Frequency and Sequence 50
5.3.6 Sanctions for Unauthorized Actions 50
5.3.7 Independent Contractor Requirements 50
5.3.8 Documentation Supplied to Personnel 50
5.4 Audit Logging Procedures 50
5.4.1 Types of Events Recorded 50
5.4.2 Frequency of Processing Log 51
5.4.3 Retention Period for Audit Log 51
5.4.4 Protection of Audit Log 51
5.4.5 Audit Log Backup Procedures 51
5.4.6 Audit Collection System (Internal vs External) 51
5.4.7 Notification to Event-Causing Subject 51
5.4.8 Vulnerability Assessments 51
5.5 Records Archival 52
5.5.1 Types of Records Archived 52
5.5.2 Retention Period for Archive 52
5.5.3 Protection of Archive 52
5.5.4 Archive Backup Procedures 52
5.5.5 Requirements for Time-Stamping of Records 52
5.5.6 Archive Collection System (Internal or External) 52
5.5.7 Procedures to Obtain and Verify Archive Information 52
5.6 Key Changeover 53
5.7 Compromise and Disaster Recovery 53
5.7.1 Incident and Compromise Handling Procedures 53
5.7.2 Computing Resources, Software, and/or Data are Corrupted 53
5.7.3 Entity Private Key Compromise Procedures 53
5.7.4 Business Continuity Capabilities after a Disaster 53
5.8 CA or RA Termination 54
6 Technical Security Controls 55

6.1 Key Pair Generation and Installation 55
6.1.1 Key Pair Generation 55
6.1.2 Private Key Delivery to Subscriber 55
6.1.3 Public Key Delivery to Certificate Issuer 55
6.1.4 CA Public Key Delivery to Relying Parties 55
6.1.5 Key Sizes 56
6.1.6 Public Key Parameters Generation and Quality Checking 56
6.1.7 Key Usage Purposes (as per X.509 v3 key usage field) 56
6.2 Private Key Protection and Cryptographic Module Engineering Controls 56
6.2.1 Cryptographic Module Standards and Controls 56
6.2.2 Private Key (n out of m) Multi-Person Control 58
6.2.3 Private Key Escrow 58
6.2.4 Private Key Backup 58
6.2.5 Private Key Archival 58
6.2.6 Private Key Transfer into or from a Cryptographic Module 58
6.2.7 Private Key Storage on Cryptographic Module 59
6.2.8 Method of Activating Private Key 59
6.2.9 Method of Deactivating Private Key 59
6.2.10 Method of Destroying Private Key 59
6.2.11 Cryptographic Module Rating 59
6.3 Other Aspects of Key Pair Management 59
6.3.1 Public Key Archival 59
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 60
6.4 Activation Data 60
6.4.1 Activation Data Generation and Installation 60
6.4.2 Activation Data Protection 60
6.4.3 Other Aspects of Activation Data 60
6.5 Computer Security Controls 60
6.5.1 Specific Computer Security Technical Requirements 60
6.5.2 Computer Security Rating 61
6.6 Life Cycle Technical Controls 61
6.6.1 System Development Controls 61
6.6.2 Security Management Controls 61
6.6.3 Life Cycle Security Controls 61
6.7 Network Security Controls 61
6.8 Time-Stamping 61
7 Certificate, CRL and OCSP Profiles 62
7.1 Certificate Profile 62
7.1.1 Version Number(s) 62
7.1.2 Certificates Extensions 62
7.1.3 Algorithm Object Identifiers 63
7.1.4 Name Forms 63
7.1.5 Name Constraints 63
7.1.6 Certificate Policy Object Identifier 63
7.1.7 Usage of Policy Constraints Extension 63

7.1.8 Policy Qualifier Syntax and Semantics ... 63
7.1.9 Processing Semantics for the Critical Certificate Policies Extension ... 63
7.2 CRL Profile ... 64
7.2.1 Version Number(s) ... 64
7.2.2 CRL and CRL Entry Extensions ... 64
7.3 OCSP Profile ... 64
7.3.1 Version Number(s) ... 64
7.3.2 OCSP Extensions ... 64
8 Compliance Audit and Other Assessments ... 65
8.1 Frequency or Circumstances of Assessment ... 65
8.2 Identity/Qualifications of Assessor ... 65
8.3 Assessor's Relationship to Assessed Entity ... 65
8.4 Topics Covered by Assessment ... 66
8.5 Actions Taken as a Result of Deficiency ... 66
8.6 Communication of Results ... 66
9 Other Business and Legal Matters ... 67
9.1 Fees ... 67
9.1.1 Certificate Issuance or Renewal Fees ... 67
9.1.2 Certificate Access Fees ... 67
9.1.3 Revocation or Status Information Access Fees ... 67
9.1.4 Fees for Other Services ... 67
9.1.5 Refund Policy ... 67
9.2 Financial Responsibility ... 67
9.2.1 Insurance Coverage ... 67
9.2.2 Other Assets ... 67
9.2.3 Insurance or Warranty Coverage for End-Entities ... 67
9.3 Confidentiality of Business Information ... 68
9.3.1 Scope of Confidential Information ... 68
9.3.2 Information not within the Scope of Confidential Information ... 68
9.3.3 Responsibility to Protect Confidential Information ... 68
9.4 Privacy of Personal Information ... 69
9.4.1 Privacy Plan ... 69
9.4.2 Information Treated as Private ... 69
9.4.3 Information not Deemed Private ... 69
9.4.4 Responsibility to Protect Private Information ... 69
9.4.5 Notice and Consent to Use Private Information ... 69
9.4.6 Disclosure Pursuant to Judicial or Administrative Process ... 69
9.4.7 Other Information Disclosure Circumstances ... 69
9.5 Intellectual Property Rights ... 69
9.6 Representations and Warranties ... 70
9.6.1 CA Representations and Warranties ... 70
9.6.2 RA Representations and Warranties ... 71
9.6.3 Subscriber Representations and Warranties ... 71
9.6.4 Relying Party Representations and Warranties ... 72

9.6.5 Representations and Warranties of other Participants 72
9.7 Disclaimers of Warranties 72
9.8 Limitations of Liability 72
9.9 Indemnities 73
9.10 Term and Termination 73
9.10.1 Term 73
9.10.2 Termination 73
9.10.3 Effect of Termination and Survival 74
9.11 Individual Notices and Communications with Participants 74
9.12 Amendments 74
9.12.1 Procedure for Amendment 74
9.12.2 Notification Mechanism and Period 74
9.12.3 Circumstances under which OID must be Changed 75
9.13 Dispute Resolution Provisions 75
9.14 Governing Law 75
9.15 Compliance with Applicable Law 75
9.16 Miscellaneous Provisions 76
9.16.1 Entire Agreement 76
9.16.2 Assignment 76
9.16.3 Severability 76
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) 76
9.16.5 Force Majeure 76
9.17 Other Provisions 76
Approval 77

1 Introduction

1.1 Overview

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

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

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

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

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

1.2 Document Name and Identification

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

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

DOCUMENT INFORMATION	
Document Version	Version 5.0
Document State	Approved
OID	1.3.6.1.4.1.25070.1.1.1.0.1
Issuing Date	09/12/2019

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

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

The OID for Multicert is:

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

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

Type of Certificate	Multicert OID
Qualified Digital Signature	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Qualified Electronic Seal	1.3.6.1.4.1.25070.1.1.1.1.0.1.14
PSD2 Qualified Electronic Seal	1.3.6.1.4.1.25070.1.1.1.1.0.1.14 (until 18/10/2019) 1.3.6.1.4.1.25070.1.1.1.1.0.1.18 (after 18/10/2019)
Authentication	1.3.6.1.4.1.25070.1.1.1.1.0.1.3
Advanced Digital Signature	1.3.6.1.4.1.25070.1.1.1.1.0.1.4
Web Server Certificate (OV[1] and Wildcard)	1.3.6.1.4.1.25070.1.1.1.1.0.1.17
Qualified Website Authentication Certificate	1.3.6.1.4.1.25070.1.1.1.1.0.1.15
PSD2 Qualified Website Authentication Certificate	1.3.6.1.4.1.25070.1.1.1.1.0.1.12
Advanced Seal	1.3.6.1.4.1.25070.1.1.1.1.0.1.13
Confidentiality	1.3.6.1.4.1.25070.1.1.1.1.0.1.16

[1] Organizational Validation

CIV (Commercial Identity Verification)	1.3.6.1.4.1.25070.1.1.1.1.0.1.9

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

Type of Certificate	Object Identifier (OID)	Description
Qualified Digital Signature	0.4.0.194112.1.2	QCP-n-qscd: certificate policy for European Union (EU)
Qualified Electronic Seal	0.4.0.194112.1.3	QCP-l-qscd: certificate policy for European Union (EU)
PSD2 Qualified Electronic Seal	0.4.0.194112.1.1	QCP-l: certificate policy for European Union (EU)
Qualified Website Authentication Certificate and PSD2 Qualified Website Authentication Certificate	0.4.0.194112.1.4	QCP-w: certificate policy for European Union (EU)
Web Server Certificate (OV)	0.4.0.2042.1.7	OVCP: Organizational Validation Certificate Policy

1.3 PKI Participants

1.3.1 Multicert Certification Authorities

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

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

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

1.3.1.1 External Certification Authorities

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

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

1.3.2 Registration Authorities

Registration Authorities (RA) are responsible for the Identification of the subscribers within an organization or an association.

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

1.3.3 Subscribers

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

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

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

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

1.3.4 Relying Parties

Relying parties are natural persons, entities or equipment that act in reliance on a certificate and/or digital signature issued by the Issuer CA.

Relying Parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate.

1.3.5 Other Participants

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

1.4 Certificate Usage

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

a) Access control;

b) Confidentiality;

c) Integrity;

d) Authentication and,

e) Non-repudiation.

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

1.4.1 Appropriate Certificate Uses

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

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

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

1.4.2 Prohibited Certificate Uses

Certificates can be used in other contexts only to the extent of what is allowed by the applicable legislation and not in conflict with the CPS.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

Organization	Multicert S.A.
Address:	Multicert S.A. Lagoas Park Edifício 3, Piso 3 2740-266 Porto Salvo – Oeiras, Portugal
E-mail:	pki.documentacao@multicert.com For PSD2 certificates: psd2@multicert.com
Webpage:	https://www.multicert.com
Telephone number:	+351 217 123 010

1.5.2 Contact Person

Name	Authentication Working Group
Address:	Attn: Authentication Working Group Multicert – Serviços de Certificação Electrónica, S.A. Lagoas Park Edifício 3, Piso 3 2740-266 Porto Salvo – Oeiras, Portugal
E-mail:	pki.documentacao@multicert.com For PSD2 certificates: psd2@multicert.com
Webpage:	https://www.multicert.com
Telephone number:	+351 217 123 010

In the scope of PSD2 certificates, if the NCA would like to notify or communicate with the TSP, regarding for instance the communication of changes to relevant regulatory information of PSD2, or if they would like to be notified each time a PSD2 certificate is issued or revoked, or if they would like to request the revocation of PSD2 certificates issued for a PSP, the NCA shall use the email above registed for communications of PSD2 certificates.

1.5.3 Person Determining CP Suitability for the Policy

The Authentication Working Group determines the suitability of this CP and is responsible for verifying the compliance of CPS with this CP.

1.5.4 CP Approval Procedures

The Management Working Group is responsible for this policy approval.

1.6 Definitions and Acronyms

1.6.1 Definitions

Item	Definition
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.
Accreditation Authority	Entity competent for the accreditation and supervision of certification authorities.
Certification Authority (CA)	Authority trusted by one or more users to create and assign certificates. A CA can be: i) a trust service provider that creates and assigns public key certificates; or ii) a technical certificate generation service that is used by a certification service provider that creates and assign publick key certificates.
Certificate Policy	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issiuing, managing, revoking, and renewing or re-keying certiicates.
Certificate Revocation List (CRL)	Signed list indicating asset of certificates that have been revoked by the certificate issuer.
Conformity Assessment Body (CAB)	Means a body defined in point 13 of Article 2 of Regulation (EC) Nº 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualifed trust service privder and the qualifed trust services it provides.
Digital Certificate	Electronic document that links signature verification data to its subscriber and confirms the identity of such subscriber.

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 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 address	Identification of a proper computer equipment to receive and file electronic documents.
Electronic document	Document prepared using electronic data processing.
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.
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.
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.
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.
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.
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.

OCSP Responder	An online server operated under the authority of the CA and connected to its repository for processing certificate status requests.
Online Certificate Status Protocol (OCSP)	An online certificate checking protocol that enables relying-party application software to determine the status of an identified 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.
PSD2 Certificate	A Qualified Certificate that includes PSD2 Specific Attributes.
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.
Public Key Infrastructure (PKI)	A set of hardware, software, people, procedures, rules, policies and obligations used to facilitate the trustworthy creation, issuance, management, and use of certificates and keys based on Public Key Cryptography.
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.
Qualified Electronic Seal	Extended electronic seal created by a qualified electronic seal creation device based on an electronic seal certificate.
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.
Relying Party	Any natural person or legal entity that relies on a valid certificate.
Registration Authority (RA)	Entity that is responsible for identification and authentication of subjects of certificates mainly. An RA can assist in the certificate application process or revocation process or both.
Root CA	The top level Certification Authority whose Root Certificate is distributed by application software suppliers and that issues Subordinate / Intermediate CA certificates.
Signature creation data	Unique set of data, such as private keys, used by the subscriber to create 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; 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.
Subject	The natural person, device, system, unit or legal entity identified in a certificate as the Subject. The subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subordinate CA / Intermediate CA	Certification Authority whose certificate is signed by the Root CA, or another Subordinate CA. A Subordinate CA normally either issues and user certificates or other Subordinate CA certificates.
Subscriber	A natural person or legal entity to whom a certificate is issued and who is legally bound by a subscriber agreement or terms of use.
Supervisory body	Public or private entity qualified to assess and certify the conformity of processes, systems and electronic signature products with the requirements refered in paragraph c), no. 1, article 12 from Decree-Law 62/2003.
Timestamp validation	Declaration of the certification authority certifying the date and time of creation, sending, or reception of an electronic document.
Trust Service Provider (TSP)	Means a natural or a legal person who provides one or more trust services either as a qualifed or as a non-qualified trust service provider.
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.
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.

1.6.2 Acronyms

Acronyms	Definition
ANSI	American National Standards Institute
BR	Baseline Requirements
CA	Certification Authority
CAA	Certification Authority Authorization
CAB	Conformity Assessment Body
CLMS	Certificates Lifecycle Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DL	Decree-law
DN	Distinguished Name
EAL	Evaluation Assurance Level
MAC	Message Authentication Codes
NCA	National Competent Authority
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object identifier
OVCP	Organizational Validation Certificate Policy
PKCS	Public-Key Cryptography Standards

PKI	Public Key Infrastructure
PSD2	Payment Services Directive 2
QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QCP-w	Policy for EU qualified website certificate issued to a natural or legal person and linking the website to that person
QSCD	Qualified electronic Signature/Seal Creation Device
SSCD	Secure Signature-Creation Device
TSP	Trust Service Provider

1.6.3 Bibliography

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

CA/Browser Forum, v1.6.65 – Baseline Requirements;

CA/Browser Forum, v1.7.0 – Guidelines for The Issuance and Management of Extended Validation Certificates;

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

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

ETSI EN 319 401, v2.2.1 (2018-04) – Electronic Signatrues and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

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 319 412-1, v1.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

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;

ETSI EN 319 421, v1.1.1 (2016-03) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;

ETSI EN 319 422, v1.1.1 (2016-03) – Electronic Signatures and Infrastructure (ESI); Time-stamping protocol and time-stamp token profiles;

ETSI TS 119 495, v1.3.21 (2019-063) – Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366;CEN/TS 419 241 (2014) – Security Requirements for Trustworthy Systems Supporting Server Signing;

CEN/TS 419 241 v2014 – Security Requirements for Trustworthy Systems Supporting Server Signing;

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.

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.

2 Publication and Repository Responsibilities

2.1 Repositories

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

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

2.2 Publication of Certification Information

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

- CA Certificates,
- CRL`s,
- CP`s and CPS`s.

2.3 Time or Frequency of Publication

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

The certificate from Multicert CA shall be published immediately after its issuing. The CRL from Multicert CA shall be published at least once a day. Delta CRL from Multicert CA shall be published, at least, every 12 hours.

2.4 Access Controls on Repositories

The information published by Multicert S.A. shall be available on the Internet, being subject to access control mechanisms (read-only access). Multicert S.A. has implemented hardware and software security measures to prevent non-authorized parties from adding, deleting or modifying repository records.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

All certificates issued under this policy have a serial number that provided them uniqueness. In case of SSL certificates, the domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Recognition, Authentication and Role of Trademarks

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

3.2 Initial Identity Validation

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

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization Identity

For all certificates that include an organization identity, validation of the legal person’s data is carried out using one of the following:

- Using documents issued by Governmental Agencies (e.g.: Commercial Registry Office, Permanent Certificate, etc).
- Authentication of the Certificate Request Form that contains the data of the organization, by a legal entity with powers for such act (lawyer, notary or solicitor).
- A third-party database that is periodically updated.

In case of SSL certificates, the authority of the Subscriber to request a certificate on behalf of the organization is verified in accordance with section 3.2.5 of Baseline Requirements.

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 domain control it is required.

3.2.2.1 Method to Prove Email Address Control

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

3.2.2.2 Method to Validate Domain Name / IP Address Control

The CA confirms that, to date of issuance of the certificate, the certificate subscriber is the *Domain Name* responsible or has control over the *Full Qualified Domain Name*, through the procedures described in section 3.2.2.2 of the CPS.

3.2.3 Authentication of Individual Identity

The CA issuing certificates must confirm the authenticity of the individual identity.

When a certificate includes the identity of a natural person, it is performed one of the following identity validation:

1. Qualified digital signature included in the Certificate Request Form.
2. Recognition of the natural person identity by a legal entity with powers for such act (lawyer, notary or solicitor).
3. By physical presence of the natural person in the RA facilities, accompanied by the identification document.

Whenever an email address is included in the Distinguished Name or Subject Alternative name attributes of the digital certificate, the subscriber must prove the control as described in 3.2.2.1.

3.2.4 Non-Verified Subscriber Information

All subscriber information is verified before certificate issuance.

3.2.5 Validation of Authority

The authority of the individual requesting the certificate on behalf of the Applicant, when the Applicant is an organization, is verified according to the following methods:

Website Authentication Certificates	Verifying the CAA Records if existing (Multicert CA identification domain in CAA records is 'multicert.com'[2]). Verifying through a reliable method of communication after been confirmed (using a contact verified in a government agency, a third party database, or an attestation letter) used to validate if the person requesting the certificate have authority to do so.
Qualified Website Authentication Certificates	Verifying the CAA Records if existing (Multicert CA identification domain in CAA records is 'multicert.com'), or verified by reliance on a contract between the CA and the Applicant provided that the contract is signed by the minimum number of persons with power to enforce the Applicant, or through a reliable method of communication after been confirmed (using a contact verified in a government agency, a third party database, or an attestation letter), or through a corporate resolution.
Advanced Signature Certificates	The subscriber of the certificate, or in case of a legal certificate, with the authorization of the Legal Entity. The data of the subscriber and the organization representative(s) authorization are validated by: digitally signing the certificate request form with a qualified certificate; or the certificate request form must be duly authenticated by a legal entity with powers for such act (notary public, solicitor, or lawyer); or by physical presence in the RA facilities accompanied with an identification document.
Qualified Signature Certificates (eSign)	The subscriber of the certificate, or in case of a legal certificate, with the authorization of the Legal Entity. The data of the subscriber and the organization representative(s) authorization are validated by: digitally

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

	signing the certificate request form with a qualified certificate; or the certificate request form must be duly authenticated by a legal entity with powers for such act (notary public, solicitor, or lawyer); or by physical presence in the RA facilities accompanied with an identification document.
Qualified Electronic Seals (eSeals)	An authorization from the Legal Entity or from a Legal and Authenticated Representative. The data of the subscriber and of the organization representative(s) are validated by: digitally signing the certificate request form with a qualified certificate; or the certificate request form must be duly authenticated by a legal entity with powers for such act (notary public, solicitor, or lawyer); or by physical presence in the RA facilitites accompanied with an identification document.

3.2.6 Criteria for Interoperation

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

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

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Multicert requires the Subscriber to use the same authentication details which they used in the original purchase of the certificate.

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, subject to the same initial validation process.

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 – inserting username and password;
- Revocation request made in the Partner Area – presenting a digital certificate, username and password;

- Revocation request made in the Revocation Request Web Form – receiving a revocation token through a relying method of communication;
- Revocation request made in the Revocation Request Form – digitally signed, or authenticated by a legal entity with powers for such act (notary public, solicitor, or lawyer), or by upon physical presence of the person requesting the revocation in the RA facilities;
- Revocation request made by elements of the Multicert PKI Registration Operation Working Group – presenting a digital certificate, username and password;
- By the Issuing CA – presenting a digital certificate, username and password;
- Revocation request made by the NCA (applicable to PSD2 certificates) – submitted through the email accorded between the NCA and the TSP.

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 performed properly.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Either the Subscriber or an individual authorized to request the certificate on behalf of the Subscriber can submit a certificate request. Subscribers are responsible for any data that the Subscriber or an individual authorized by the Subscriber supplies to Multicert.

- The certificate request must be accompanied by a Certificate Request Form fulfilled.

4.1.2 Enrolment Process and Responsibilities

The enrolment process includes the following steps:

- Fulfilling the certificate request form;
- Agreeing with the terms and conditions of the certificate;
- Submiting the certificate request form;
- Generating a key pair and sending a CSR, when applicable depending on the type of certificate;
- Paying any applicable fees;
- Providing the information/documentation and/or performing the actions requested by the RA in order to allow the validation process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate issuance

4.3.1 CA Actions during Certificate Issuance

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

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

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Issuers CAs shall notify the Subscriber when its certificate is issued using a contact provided on the certificate application.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The passage of time after delivery or notice of issuance of a certificate to the Subscriber or the actual use of a certificate constitutes Subscriber`s acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

In case of PSD2 certificates, the NCA from the country of the Subscriber may be notified if they have previously indicated that intention to Multicert.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

The private keys shall only be used for their intended purpose.

4.5.2 Relying Party Public Key and Certificate Usage

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

Relying Parties should always verify the certificate validity and status through the available methods by the Issuer CA, such as CRL's or/and OCSP.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

An Issuer CA may renew a certificate on its own initiative or on the initiative of the Subscriber 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. In case of certificate replacement the Distinguished Name and/or Subject Alternative Name may change, in this case additional validation is performed if needed;
- 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.

When the certificate renewal process does not fulfil the conditions above, the process is assumed as a new issuance.

4.6.2 Who May Request Renewal

Issuer CA may initiate a certificate renewal in its own discretion, after notifying the certificate Subscriber.

The Subscriber may request the certificate renewal after paying additional fees.

4.6.3 Processing Certificate Renewal Requests

When a certificate renewal occurs, the key pair, Not After date, and the data of the Distinguished Name and Subject Alternative Name of the certificate remains the same as the first issuance. For that reason, Multicert reuses the previous verified information in its sole description.

When certificate replacement occurs, the Distinguished Name and/or Subject Alternative Name information may change. In this case, additional validation is provided if needed.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The passage of time after delivery or notice of issuance of a certificate to the Subscriber or the actual use of a certificate constitutes Subscriber`s acceptance of the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

See section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-Key

Re-keying a certificate consists of creating a new certificate with a new public key, but maintaining the same Not After date and information in the Distinguished Name and Subject Alternative Name fields of the previous certificate. Re-Key is only possible when the certificate it is not revoked. After the re-key be performed and the new certificate is issued, the previous certificate is revoked.

4.7.2 Who may Request Certification of a New Public Key

Issuer CA may initiate a certificate re-key at the request of the certificate Subscriber or an Entity/Organization Representative, when applicable. Multicert may also initiate a certificate re-key in it`s own discretion.

4.7.3 Processing Certificate Re-Keying Requests

Issuer CA may request additional information befor processing a re-key and may re-validate the Subscriber subject to re-verification of any previously validated data, if needed.

The new certificate issued is send through a relyable method of communication previously verified.

4.7.4 Notification of New Certificate Issuance to Subscriber

Issuer CA notifies the Subscriber within a reasonable time after the certificate issues.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The passage of time after delivery or notice of issuance of a certificate to the Subscriber or the actual use of a certificate constitutes Subscriber`s acceptance of the certificate.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Issuer CA publishes rekeyed certificates by delivering them to Subscribers.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for 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 Issuer CA`s.

4.8.2 Who May Request Certificate Modification

No Stipulation.

4.8.3 Processing Certificate Modification Requests

No Stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No Stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No Stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No Stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

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.

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

- 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.

If one of the following reasons occurs, the PSD2 certificate may be revoked through a request by NCA:

- The NCA removes one or more roles to the PSP that were included in the certificate;
- The NCA removes the PSD2 authorization for the PSP that requested the certificate.

If one of the following reasons occurs, the Subordinate CA certificate is revoked within seven (7) days:

- The Subordinate CA requests revocation in writing;
- The Surbordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The Issuing CA obtains evidence that the Subordinate CA`s private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements of section 6.1.5 and 6.1.6 of Baseline Requirements, in case of SSL and QWAC certificates;
- The Issuing CA obtains evidence that the certificate was misused;
- The Issuing CA is made aware that the certificate was not issued in accordance with or that Subordinate CA has not complied with Baseline Requirements or the applicable Certificate Policy or Certificate Practice Statement, in case of SSL and QWAC certificates;
- The Issuing CA determines that any of the information appearing in the certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
- The Issuing CA or Subordinate CA`s right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP repository;
- Revocation is required by the Issuing CA`s Certificate Policy and/or Certification Practice Statement.

4.9.2 Who Can Request Revocation

The Issuer CA or RA shall accept revocation requests from authenticated and authorized parties, such as the Subscriber or the Entity/Organization associated, when applicable. The Issuer CA or RA may establish procedures that allow other entities to request certificate revocation, such as the NCA in case of PSD2 certificates.

4.9.3 Procedure for Revocation Request

The Issuer CA shall provide a process for Subscribers to request revocation of their own certificates. The process must be described in the Issuer`s CA CPS.

The Issuer CA will always revoke a certificate if the request is authenticated as originating from the Subscriber or the associated Entity/Organization, when applicable.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available for a Subscriber to take any necessary actions themselves to request revocation of a suspected key compromise, use of a weak key or discovery of inaccurate information within an issued certificate.

In this situation, the Subscriber must require the revocation within 24 hours after detection.

4.9.5 Time within which CA must Process the Revocation Request

An Issuer CA shall revoke a certificate within 24 hours when the request is made through a written revocation request form. When the revocation request is made in an authenticated manner, the revocation is processed immediately.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties must confirm the validity of the certificate trough the services that the Issuer CA make available, such as OCSP and/or CRL.

4.9.7 CRL Issuance Frequency

The CA's working under this policy must issue its CRL`s with the following frequency:

- Intermediate/Subordinate CA's – Every 24 hours;
- Root CA – Every month or whenever a Subordinate CA certificate is revoked.

4.9.8 Maximum Latency for CRL`s

CRL`s for certificates issued to end entity Subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation.

When CRL`s for Root CA are issued due to a Subordinate CA revocation, the CRL is published within 1 day after issuance. Regularly scheduled CRL`s are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9 On-Line Revocation/Status Checking Availability

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

OCSP responses must be compliant with RFC 6960 or RFC 5019. OCSP responses must be always signed by an OCSP responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked.

4.9.10 On-Line Revocation Checking Requirements

A Relying Party must confirm the validity of a certificate in accordance with section 4.9.6 prior to relying on the certificate.

OCSP responders that receive a request for status of a certificate that has not been issued yet, shall not respond with a "good" status for such certificate.

4.9.11 Other Forms of Revocation Advertisements Available

No Stipulation.

4.9.12 Special Requirements Related to Key Compromise

The Issuer CA or RA shall use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that its Private Key has been compromised. The Issuer CA must have the ability to transition any revocation reason to code to "key compromise".

4.9.13 Circumstances for Suspension

Certificate suspension is allowed, except for SSL/QWAC certificates.

4.9.14 Who Can Request Suspension

The Issuer CA and RA shall accept authenticated requests for suspension. Authorization for suspension shall be accepted if the suspension request is received from either the Subscriber or an associated Entity/Organization, when applicable. The Issuer CA may also suspend the certificate at their own discretion.

4.9.15 Procedure for Suspension Request

Due to the nature of suspension requests and the need for efficiency, the Issuer CA and RA may provide automated mechanisms for requesting and authenticating suspension requests.

4.9.16 Limits on Suspension Period

The limit on suspension period depends on the mean used to suspend the certificate:

- Through the client area – until 3 days;
- Through the partner area or through the Suspension Request Web Form – until 6 days;
- Through other means – no limit on the suspension period.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Issuer CA shall make certificate status information available via CRL and OCSP. The Issuer CA shall list revoked certificates in the appropriate CRL, and they must remain after the expiration date.

4.10.2 Service Availability

The certificate status services shall be available 24 hours per day, 7 days per week.

4.10.3 Optional Features

No Stipulation.

4.11 End of Subscription

The Issuer CA shall allow Subscribers to end their subscription to certificate services by having their certificate revoked or by allowing the certificate to expire without renewal.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Multicert PKI does not perform key escrow for end entity certificates.

Multicert PKI can perform key escrow for the CA`s private keys, in this case a ceremony is planned and realized by the working group members necessary according to the artifacts needed for this operation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No Stipulation.

5 Facility, Management and Operational Controls

The CA's under this policy must implemented several rules and policies focusing on physical, procedural and human controls that support the security requirements present on this CP. This section briefly describes the non-technical security aspects that allow to perform the key generation, 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 a CA.

5.1 Physical Controls

5.1.1 Site Location and Construction

The facilities of the CA's under this policy must be designed so as to provide an environment capable of controlling and auditing access to the certification systems, and to be physically protected from non-authorized access, damage or interference. The architecture need to use a deep 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 must be performed in a room within a high security zone, inserted in another high security zone, and inside a building that combines several security conditions, namely the total access control that prevents, detects and hinders unauthorized accesses based on multiple physical security levels.

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

a) Masonry, concrete or brick walls;

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

c) Nonexistence of windows;

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

Additionally, the following security conditions must be ensured:

- Clearly defined security perimeters;
- Masonry walls, ceiling and floor, no windows, which hinder unauthorized accesses;
- High security anti-theft bolts and locks on the access doors to the security environment;
- The building perimeter is tightly closed since there are no doors, windows or any other uncontrolled openings that allow unauthorized accesses;

- The access to the environment necessarily passes through human-control areas and through other control means that restrict the physical access only to duly authorized personnel.

5.1.2 Physical Access

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

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

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

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

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

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

5.1.6 Media Storage

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

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

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

5.1.7 Waste Disposal

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

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

5.1.8 Off-Site Backup

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

5.2 Procedural Controls

A CA activity depends on the coordinated and complementary intervention of an extensive human resource cast, namely because:

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

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

5.2.1 Trusted Roles

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

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

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

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

5.2.1.1 Setup Working Group

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

The group duties are:

- to install, interconnect and configure the CA's *hardware*;
- to install and configure the CA's base *software*;
- to configure the required initial passwords[3], which will be then changed by the Authentication Working Group;
- to prepare statements about:
    - Initial passwords;
    - Identification of the Setup Working Group members;

[3] BIOS, SO administrator account, etc

  - *Hash* of the CD(s) used in the setup;
  - List of all artefacts (unequivocally identified) indispensable to the CA's initial setup and operation.

5.2.1.2 Operation Working Group

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

This group's responsibilities are:

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

5.2.1.3 Authentication Working Group

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

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

This group's responsibilities are:

- To define all CA policies and ensure that they are updated and adapted to its reality;
- To ensure that the CA CPs are supported by the CA CPS;
- To ensure that all documents relevant and directly or indirectly related with the CA operation are stored in the Information Environment;
- Management of the "Authentication Environment";
- Management of all non-personal passwords;
- To keep an updated inventory of all the authentication *tokens* used in the "Production environment", and when the *tokens* are at the responsibility of some member(s), to register the identification of that(those) member(s), and safekeeping those registrations in the "Authentication Environment";
- To keep an updated inventory of all the passwords[4] used in the "Production environment", and when the passwords are at the responsibility of some member(s),

[4] Recording their value

to register the identification of that(those) member(s), and safekeeping those registrations in the “Authentication Environment”;

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

5.2.1.4 Audit Working Group

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

This group's responsibilities are:

- To audit the performance and to confirm the accuracy of the CA's processes and ceremonies;
- To register all sensitive operations;
- To investigate procedural fraud suspects;
- 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[5] and are duly identified;

[5] 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.

- To verify periodically the records/logs of the CA.

5.2.1.5 Custody Working Group

It is responsible for the custody of some sensitive artefacts (authentication *tokens*, etc.), which may be collected by the members of the other Working Groups by the fulfilment of certain conditions[6]. 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 automatized;
- To revoke/suspend certificates in case this procedure is not automatized.

5.2.1.7 Monitoring and Control Working Group

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

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

This group's responsibilities are:

- To consolidate and analyse the monitoring of the resources used in Multicert CA;
- To ensure the continuous improvement to the “Incident management process” and related operational management;

[6] Defined for each artefact in its custody.

- To collaborate with the Audit Working Group with the purpose of promoting continuous improvement actions;
- To monitor the operation of the existing alarms;
- To make production passages required by pre-production;
- To monitor events, manage alarms and classify incidents;
- To define, support the implementation and continuous improvement of incident response procedures;
- To make production passages required by pre-production;
- To assume the Security Administrator role.

5.2.1.8 Management Working Group

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

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

This group's responsibilities are:

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

5.2.2 Number of Persons Required per Task

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

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

5.2.3 Identification and Authentication for each Role

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

5.2.4 Roles Requiring Separation of Duties

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

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

5.3 Personnel Controls

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

- Being formally appointed to the function;
- Having proper training for the function;
- Prove his/her identity through documentation issued by reliable sources;
- Prove that he/she doesn't have criminal record;
- Present proof of the qualifications and experience demanded by the entity or group which formally appointed him/her;

- Ensure (formally) confidentiality (unless expressly authorized by the legal representatives of the entity that holds the CA) regarding any information about the CA, its operation, its environments and human resources at its service and about the 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[7] includes:

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

5.3.3 Training Requirements

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

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

a) Digital certification and Public Key Infrastructures;

b) General concepts on information security;

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

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

e) Certificate Policy and Certification Practices Statement;

f) Recovery from disasters;

g) Procedures for the continuation of the activity, and

h) Basic legal aspects regarding the certification services.

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

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

No Stipulation.

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 Non Disclosure Agreement, existing for this purpose.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

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

The entries in the records include the following information:

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

5.4.2 Frequency of Processing Log

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

5.4.4 Protection of Audit Log

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

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs External)

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

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

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

5.5 Records Archival

5.5.1 Types of Records Archived

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

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

The archive:

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

The stored data collection systems are internal.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

No Stipulation.

5.7 Compromise and Disaster Recovery

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

5.7.1 Incident and Compromise Handling Procedures

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

5.7.2 Computing Resources, Software, and/or Data are Corrupted

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

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

5.7.3 Entity Private Key Compromise Procedures

In case the private key from Multicert CA is compromised or there is a suspicion of its compromise, appropriate measures shall be taken to respond to the incident. The responses to that incident may include:

- Revocation of the certificate from Multicert CA and all certificates issued in the trust hierarchy “branch” from Multicert CA;
- Notification of the Accreditation Authority and all subscribers of certificates issued in the trust hierarchy “branch” from Multicert CA;
- Generation of a new key pair for Multicert CA;
- Renewal of all certificates issued in the trust hierarchy “branch” from Multicert CA.

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

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

a) Inform the Supervision Authority;

b) Inform all certificate 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 TSP) of all information relative to the CA's activity, namely CA key, certificates, documentation stored (internally or externally), repositories and event records storage.

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

6 Technical Security Controls

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

6.1 Key Pair Generation and Installation

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

6.1.1 Key Pair Generation

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

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

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

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

The public key is delivered to the CA, according to the procedures mentioned in section 4.3.

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1 Cryptographic Module Standards and Controls

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

- Physical Security
  - Common Criteria EAL 4+ and/or
  - FIPS 140-2, level 3
- Regulatory Certifications
  - U/L 1950 & CSA C22.2 *safety compliant*
  - FCC Part 15 – Class B
  - ISO – 9002 Certification

- Papers
  - Two factor authentication
- API support
  - PKCS#11
  - Microsoft CryptoAPI
  - Java JCE/JCE CSP
  - Open SSL
- Creation of random numbers
  - *ANSI* X9.17 (Annex C)
- Key change and asymmetric key cipher
  - RSA (512-4096 bit), PKCS#1 v1.5, OAEP PKCS#1 v2.0
  - Diffie-Hellman (512-1024 bit)
- Digital Signature
  - RSA (512-4096 bit)
  - DSA (512-1024 bit)
  - PKCS#1 v1.5
- Symmetric key algorythms
  - DES
  - 3DES (double and triple length)
  - RC2
  - RC4
  - RC5
  - AST
  - CAST-3
  - CAST-128
- Hash Algorythms
  - SHA-1
  - SHA-256
  - MD-2
  - MD-5
- Message Authentication Codes (MAC)
  - HMAC-MD5
  - HMAC-SHA-1
  - SSL3-MD5-MAC
  - SSL3-SHA-1-MAC

6.2.2 Private Key (n out of m) Multi-Person Control

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

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

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

6.2.3 Private Key Escrow

Private keys of the CAs managed by 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.

6.2.4 Private Key Backup

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

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

6.2.10 Method of Destroying Private Key

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

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

6.2.11 Cryptographic Module Rating

Described in section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

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

- Root CA certificate issued under this policy has a validity of 25 years, being used to sign Subordinate CA`s certificates during its 12 years of validity;
- Subordinate CA`s certificates issued under this policy has a validity of 12 years and 64 months, being used to sign certificates during its five years of validity;
- End entity certificates issued under this policy has a maximum validity of 4 years, depending on the type of certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data necessary for using the private key from the CA are divided in several parts (stored in PED keys – small digital identification *tokens*, with physical USB pen format, identifying different access roles to HSM), and are at the responsibility of the different members of the Working Group. The different parts are generated according to what was defined in the process/ceremony for the key generation, and obey to the requirements defined by standard FIPS 140-2 level 3.

6.4.2 Activation Data Protection

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

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

6.4.3 Other Aspects of Activation Data

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

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

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

6.5.2 Computer Security Rating

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

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

The CA’s under this policy shall have border protection devices, namely a *firewall* system, and comply with the necessary requirements for identification, authentication, access control, administration, audit, reuse, service responsibility and recovery, and information exchange.

6.8 Time-Stamping

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

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

The users of a public key have to trust that the associated private key is held by the correct remote 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 CE. The CE may base this statement on technical means (for example, proof of the possession of the private key through a challenge-response protocol), on the presentation of the private key or on the registration made by the subscriber.

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

The user of a security system that requires the knowledge of the user's public key usually has to obtain and validate the certificate holding that key. If the service does not hold a trustful copy of the public key from the CA that signed the certificate, as well as the name of the CA and related information (such as the validity period), then there may be required an additional certificate to obtain a public key from the CA and validate the user's public key. Generally, to validate the public key from a user, there may be needed a network of multiple certificates, including the public key certificate of the user signed by a CA, and zero or more additional certificates from CAs signed by other CAs.

The profile of the web server certificate is compliant with:

- ITU.T recommendationX.509[8];
- RFC 5280[9], and
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.

7.1.1 Version Number(s)

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

7.1.2 Certificates Extensions

The components and extensions defined for X.509 v3 certificates provide methods for associating additional attributes to users or public keys, as well as for managing the certification hierarchy.

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

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

7.1.3 Algorithm Object Identifiers

The "*signatureAlgorithm*" certificate field contains the OID for the cryptographic algorithm used by the CA to sign the certificate: 1.2.840.113549.1.1.11 (*sha-2WithRSAEncryption*[10]).

7.1.4 Name Forms

As defined in section 2.1.

7.1.5 Name Constraints

Multicert may include name constraints in the nameConstraints field when appropriate.

7.1.6 Certificate Policy Object Identifier

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

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

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

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation.

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

7.2 CRL Profile

When a certificate is issued, it is expected to be in use for its entire validity period. However, several circumstances may cause a certificate to become invalid before the expiration of its validity period. Such circumstances include change of name, change of association between the subject and the certificate data (for example, an employee who terminates employment) and compromise or suspected compromise of the corresponding private key. Under such circumstances, the CA has to revoke the certificate[9].

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[9].

The CRL profile conforms to:

- ITU.T Recommendation X.509[8];
- RFC 5280[9] and,
- Applicable legislation, national and European.

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

The profile of the OCSP certificates is compliant with:

- ITU.T recommendation X.509[8];
- RFC 6960[11] and,
- Applicable legislation, national and European.

7.3.1 Version Number(s)

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

7.3.2 OCSP Extensions

No Stipulation.

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

8 Compliance Audit and Other Assessments

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

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

8.1 Frequency or Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

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

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

8.3 Assessor's Relationship to Assessed Entity

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

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

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

The fulfilment 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 European legislation and this CPS and other rules, procedures and processes (especially the ones related with key management operations, resources, management and operation controls and management of the certificates life-cycle).

8.5 Actions Taken as a Result of Deficiency

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

a) Documents all faults found during the audit;

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

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

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

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

f) The Accreditation Authority, after 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 to the Supervisory Body.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

No Stipulation.

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

No Stipulation.

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

No Stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

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

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

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

d) Business continuity and recovery plans;

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

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

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

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

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

9.3.2 Information not within the Scope of Confidential Information

It is considered as information for public access:

a) Certificates Policy;

b) Certification Practices Statement;

c) CRL;

d) Delta-CRL;

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

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

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

In accordance with GDPR.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No Stipulation.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

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

The private keys and the public keys are propriety of the 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.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CA's are obliged to:

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

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

c) Protect its private keys;

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

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

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

i) Store the certificates issued without any changes;

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

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

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

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

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

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

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

q) Operate in accordance with the applicable legislation;

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

s) Guarantee the availability of the CRL in accordance with the dispositions in section 4.9,

t) In case its activity ceases this shall be communicated with a minimum prior notice of two months to all 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;

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

w) Make the certificates from CA available.

9.6.2 RA Representations and Warranties

Registration Authorities are obliged to:

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

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

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

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

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

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

g) Store the certificates issued without any changes;

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

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

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

k) Operate in accordance with the Regulation 910/2014

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

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

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

9.6.3 Subscriber Representations and Warranties

It is the obligation of the 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 4.9.1;

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

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

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

9.6.4 Relying Party Representations and Warranties

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

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

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

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

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

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

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

9.6.5 Representations and Warranties of other Participants

No Stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

Multicert CA:

a) 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;

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

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

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

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

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

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

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

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

9.9 Indemnities

In accordance with the legislation in force.

9.10 Term and Termination

9.10.1 Term

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

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

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

9.10.2 Termination

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

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

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

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

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

9.10.3 Effect of Termination and Survival

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

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

9.11 Individual Notices and Communications with Participants

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.

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

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

9.13 Dispute Resolution Provisions

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

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

9.14 Governing Law

Multicert is obliged to fulfil the requirements established in the current Portuguese and European Union law as a company that provides trust services, such as digital certification services.

More information regarding the Multicert`s PKI applicable law and standards can be found in section 1.6.3.

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

No Stipulation.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No Stipulation

9.16.5 Force Majeure

No Stipulation.

9.17 Other Provisions

No Stipulation.

Approval

Jorge Alcobia (Management Working Group)

[Assinatura Qualificada] José Jorge Oliveira da Fonseca Alcobia

Digitally signed by [Assinatura Qualificada] José Jorge Oliveira da Fonseca Alcobia
Date: 2019.12.18 14:53:36 Z