multicert
Engineering for digital security

Multicert Certification Practices Statement

Policies

MULTICERT_PJ.ECRAIZ_427_en

Project identification: MULTICERT PKI

Access level: Public

Version: 10.0

Date: 17/12/2020

Normative Version

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

Document identifier: MULTICERT_PJ.ECRAIZ_427_en

Key-words: MULTICERT CA, Certification Practices Statement

Type of document: Policies

Title: Certification Practices Statement

Original language: English

Publication language: English

Access level: Public

Date: 17/12/2020

Current version: 10.0

Project identification: MULTICERT PKI

Version history

Version	Date	Details	Author(s)
1.0	15/06/2018	Reviewed according to RFC 3647 and CABForum Baseline Requirements, version 1.5.7	Multicert S.A.
1.1-1.7	25/09/2018	Inclusion of procedure for method to prove email address control. Inclusion of practices for re-key. Inclusion of statement for external CA`s	Multicert S.A.
2.0	01/10/2018	Approval	Multicert S.A.
2.1	29/01/2019	Prohibition of usage for man-in-middle Review of revocation reasons	Multicert S.A.
3.0	29/01/2019	Approval	Multicert S.A.
3.1	25/03/2019	Review in accordance with Baseline Requirements v1.6.4	Multicert S.A.
4.0	25/03/2019	Approval	Multicert S.A.
4.1	25/03/2019	Inclusion of PSD2 information	Multicert S.A.
4.2	16/07/2019	Inclusion of information for electronic invoice and general review	Multicert S.A.
5.0	16/07/2019	Approval	Multicert S.A.
5.1	09/12/2019	Revision in accordance with Baseline Requirements v1.6.6, inclusion of new CA`s	Multicert S.A.
6.0	09/12/2019	Approval	Multicert S.A.
6.1	06/04/2020	Revision in accordance with Baseline Requirements v1.6.7,1.6.8,1.6.9	Multicert S.A.
7.0	06/04/2020	Approval	Multicert S.A.
7.1	31/08/2020	Revision of contacts in section 1.5.2	Multicert S.A.
8.0	31/08/2020	Approval	Multicert S.A.
8.1	03/09/2020	Revision in accordance with BR 1.7.1 e EVBR 1.7.3	Multicert S.A.
9.0	28/09/2020	Approval	Multicert S.A.

9.1	10/12/2020	Inclusion of information about qualified digital signature and electronic seal for electronic invoice | Removal of expired CA | Revision of revocation reasons | Revision of trusted roles | General revision of section 8 and 9	Multicert S.A.
10.0	17/12/2020	Approval	Multicert S.A.

Related documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_426_en	Multicert Certificate Policy	Multicert S.A.
MULTICERT_PJ.ECRAIZ_428_en	Certificate Profiles List	Multicert S.A.
MULTICERT_PJ.ECRAIZ_405_en	Subordinate CA Policy	Multicert S.A.
MULTICERT_PJ.ECRAIZ_621_en	List of Approved Incorporating Agencies	Multicert S.A.

Annexes

Document ID	Details	Author(s)

Summary

Multicert Certification Practices Statement 1

Summary 4

1 Introduction 11

1.1 Overview 11
1.2 Document Name and Identification 11
1.3 PKI Participants 13
1.3.1 Certification Authorities 13
1.3.1.1 External Certification Authorities 17
1.3.2 Registration Authorities 18
1.3.2.1 Internal Registration Authority 18
1.3.2.2 External Registration Authorities 18
1.3.3 Subscribers 19
1.3.3.1 Sponsor 19
1.3.4 Relying Parties 19
1.3.5 Other Participants 19
1.3.5.1 Supervisory Authority / Supervisory Body 19
1.3.5.2 Registration Authority 20
1.3.5.3 Service Provision External Authorities 20
1.3.5.4 OCSP Validation Authority 20
1.3.5.5 Auditor from a Conformity Assessment Body 20
1.4 Certificate Usage 21
1.4.1 Appropriate Certificate Uses 21
1.4.2 Prohibited Certificate Uses 23
1.5 Policy Administration 24
1.5.1 Organization Administering the Document 24
1.5.2 Contact Person 25
1.5.3 Person Determining CPS Suitability for the Policy 25
1.5.4 CPS Approval Procedures 25
1.6 Definitions and Acronyms 26
1.6.1 Definitions 26
1.6.2 Acronyms 31
1.6.3 Bibliography 32

2 Publication and Repository Responsibilities 35

2.1 Repositories 35
2.2 Publication of Certification Information 35
2.3 Time or Frequency of Publication 35
2.4 Access Controls on Repositories 36

3 Identification and Authentication 37

3.1 Naming 37
3.1.1 Types of Names 37
3.1.2 Need for Names to be Meaningful 37
3.1.3 Anonymity or Pseudonymity of Subscribers 37
3.1.4 Rules for Interpreting Various Name Forms 38
3.1.5 Uniqueness of Names 38
3.1.6 Recognition, Authentication, and Role of Trademarks 38
3.2 Initial Identity Validation 38
3.2.1 Method to Prove Possession of Private Key 39
3.2.1.1 Signature (eSign) 39
3.2.1.2 Electronic Seal (eSeal) 39
3.2.1.3 Website Authentication Certificates and Qualified Website Authentication Certificates 39
3.2.1.4 Services Certificate 40
3.2.2 Authentication of Organization Identity 40
3.2.2.1 Method to Prove Email Address Control 40
3.2.2.2 Method to Validate Domain Name / IP Address Control 40
3.2.3 Authentication of Individual Identity 41
3.2.4 Non-Verified Subscriber Information 41
3.2.5 Validation of Authority 41
3.2.6 Criteria for Interoperation 43
3.3 Identification and Authentication for Re-Key Requests 43
3.3.1 Identification and Authentication for Routine Re-Key 43
3.3.2 Identification and Authentication for Re-Key after Revocation 43
3.4 Identification and Authentication for Revocation Request 43
4 Certificate Life-Cycle Operational Requirements 45
4.1 Certificate Application 45
4.1.1 Who Can Submit a Certificate Application 45
4.1.2 Enrollment Process and Responsibilities 45
4.2 Certificate Application Processing 45
4.2.1 Performing Identification and Authentication Functions 45
4.2.2 Approval or Rejection of Certificate Applications 46
4.2.3 Time to Process Certificate Applications 46
4.3 Certificate Issuance 46
4.3.1 CA Actions during Certificate Issuance 46
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 46
4.4 Certification Acceptance 46
4.4.1 Conduct Constituting Certificate Acceptance 46
4.4.2 Publication of the Certificate by the CA 47
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 47
4.5 Key Pair and Certificate Usage 47
4.5.1 Subscriber Private Key and Certificate Usage 47
4.5.2 Relying Party Public Key and Certificate Usage 47
4.6 Certificate Renewal 47

4.6.1 Circumstance for Certificate Renewal 47
4.6.2 Who may Request Renewal 48
4.6.3 Processing Certificate Renewal Requests 48
4.6.4 Notification of New Certificate Issuance to Subscriber 48
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 48
4.6.6 Publication of the Renewal Certificate by the CA 48
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 48
4.7 Certificate Re-Key 49
4.7.1 Circumstance for Certificate Re-Key 49
4.7.2 Who may Request Certification of a New Public Key 49
4.7.3 Processing Certificate Re-Keying Requests 49
4.7.4 Notification of New Certificate Issuance to Subscriber 49
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 49
4.7.6 Publication of the Re-Keyed Certificate by the CA 49
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 49
4.8 Certificate Modification 49
4.8.1 Circumstance for Certificate Modification 50
4.8.2 Who may Request Certificate Modification 50
4.8.3 Processing Certificate Modification Requests 50
4.8.4 Notification of New Certificate Issuance to Subscriber 50
4.8.5 Conduct Constituting Acceptance of Modified Certificate 50
4.8.6 Publication of the Modified Certificate by the CA 50
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 50
4.9 Certificate Revocation and Suspension 50
4.9.1 Circumstances for Revocation 50
4.9.2 Who Can Request Revocation 52
4.9.3 Procedure for Revocation Request 52
4.9.4 Revocation Request Grace Period 53
4.9.5 Time within which CA must Process the Revocation Request 53
4.9.6 Revocation Checking Requirement for Relying Parties 53
4.9.7 CRL Issuance Frequency 53
4.9.8 Maximum Latency for CRLs 54
4.9.9 On-Line Revocation/Status Checking Availability 54
4.9.10 On-Line Revocation Checking Requirements 54
4.9.11 Other Forms of Revocation Advertisements Available 54
4.9.12 Special Requirements Re Key Compromise 54
4.9.13 Circumstances for Suspension 54
4.9.14 Who Can Request Suspension 55
4.9.15 Procedure for Suspension Request 55
4.9.16 Limits on Suspension Period 55
4.10 Certificate Status Services 55
4.10.1 Operational Characteristics 55
4.10.2 Service Availability 55
4.10.3 Optional Features 56

4.11 End of Subscription 56
4.12 Key Escrow and Recovery 56
4.12.1 Key Escrow and Recovery Policy and Practices 56
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 56
5 Facility, Management and Operational Controls 57
5.1 Physical Controls 57
5.1.1 Site Location and Construction 57
5.1.2 Physical Access 58
5.1.3 Power and Air Conditioning 58
5.1.4 Water Exposures 58
5.1.5 Fire Prevention and Protection 59
5.1.6 Media Storage 59
5.1.7 Waste Disposal 59
5.1.8 Off-Site Backup 59
5.2 Procedural Controls 60
5.2.1 Trusted Roles 60
5.2.1.1 Setup Working Group 60
5.2.1.2 Operation Working Group 60
5.2.1.3 Authentication Working Group 60
5.2.1.4 Audit Working Group 61
5.2.1.5 Custody Working Group 61
5.2.1.6 Registration Operation Working Group 61
5.2.1.7 Monitoring and Control Working Group 61
5.2.1.8 Management Working Group 61
5.2.2 Number of Persons Required per Task 61
5.2.3 Identification and Authentication for each Role 62
5.2.4 Roles Requiring Separation of Duties 62
5.3 Personnel Controls 63
5.3.1 Qualifications, Experience, and Clearance Requirements 63
5.3.2 Background Check Procedures 63
5.3.3 Training Requirements 63
5.3.4 Retraining Frequency and Requirements 64
5.3.5 Job Rotation Frequency and Sequence 64
5.3.6 Sanctions for Unauthorized Actions 64
5.3.7 Independent Contractor Requirements 64
5.3.8 Documentation Supplied to Personnel 64
5.4 Audit Logging Procedures 65
5.4.1 Types of Events Recorded 65
5.4.2 Frequency of Processing Log 65
5.4.3 Retention Period for Audit Log 65
5.4.4 Protection of Audit Log 65
5.4.5 Audit Log Backup Procedures 65
5.4.6 Audit Collection System (Internal vs. External) 65
5.4.7 Notification to Event-Causing Subject 66

5.4.8 Vulnerability Assessments 66
5.5 Records Archival 66
5.5.1 Types of Records Archived 66
5.5.2 Retention Period for Archive 66
5.5.3 Protection of Archive 66
5.5.4 Archive Backup Procedures 66
5.5.5 Requirements for Time-Stamping of Records 66
5.5.6 Archive Collection System (Internal or External) 67
5.5.7 Procedures to Obtain and Verify Archive Information 67
5.6 Key Changeover 67
5.7 Compromise and Disaster Recovery 67
5.7.1 Incident and Compromise Handling Procedures 67
5.7.2 Computing Resources, Software and/or Data are Corrupted 67
5.7.3 Entity Private Key Compromise Procedures 67
5.7.4 Business Continuity Capabilities after a Disaster 68
5.8 CA or RA Termination 68
6 Technical Security Controls 69
6.1 Key Pair Generation and Installation 69
6.1.1 Key Pair Generation 69
6.1.2 Private Key Delivery to Subscriber 69
6.1.3 Public Key Delivery to Certificate Issuer 69
6.1.4 CA Public Key Delivery to Relying Parties 69
6.1.5 Key Sizes 70
6.1.6 Public Key Parameters Generation and Quality Checking 70
6.1.7 Key Usage Purposes (as per X.509 v3 key usage field) 70
6.2 Private Key Protection and Cryptographic Module Engineering Controls 70
6.2.1 Cryptographic Module Standards and Controls 70
6.2.2 Private Key (n out of m) Multi-Person Control 70
6.2.3 Private Key Escrow 71
6.2.4 Private Key Backup 71
6.2.5 Private Key Archival 71
6.2.6 Private Key Transfer into or from a Cryptographic Module 71
6.2.7 Private Key Storage on Cryptographic Module 71
6.2.8 Method of Activating Private Key 72
6.2.9 Method of Deactivating Private Key 72
6.2.10 Method of Destroying Private Key 72
6.2.11 Cryptographic Module Rating 72
6.3 Other Aspects of Key Pair Management 72
6.3.1 Public Key Archival 72
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 72
6.4 Activation Data 73
6.4.1 Activation Data Generation and Installation 73
6.4.2 Activation Data Protection 73
6.4.3 Other Aspects of Activation Data 74

6.5 Computer Security Controls 74
6.5.1 Specific Computer Security Technical Requirements 74
6.5.2 Computer Security Rating 74
6.6 Life Cycle Technical Controls 74
6.6.1 System Development Controls 74
6.6.2 Security Management Controls 74
6.6.3 Life Cycle Security Controls 75
6.7 Network Security Controls 75
6.8 Time-Stamping 75
7 Certificate, CRL and OCSP Profiles 76
7.1 Certificate Profile 76
7.1.1 Version Number(s) 76
7.1.2 Certificate Extensions 76
7.1.3 Algorithm Object Identifiers 77
7.1.4 Name Forms 77
7.1.5 Name Constraints 77
7.1.6 Certificate Policy Object Identifier 77
7.1.7 Usage of Policy Constraints Extension 77
7.1.8 Policy Qualifiers Syntax and Semantics 77
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 77
7.2 CRL Profile 77
7.2.1 Version Number(s) 78
7.2.2 CRL and CRL Entry Extensions 78
7.3 OCSP Profile 79
7.3.1 Version Number(s) 79
7.3.2 OCSP Extensions 79
8 Compliance Audit and Other Assessments 80
8.1 Frequency or Circumstances of Assessment 80
8.2 Identity/Qualifications of Assessor 80
8.3 Assessor's Relationship to Assessed Entity 80
8.4 Topics Covered by Assessment 80
8.5 Actions Taken as a Result of Deficiency 81
8.6 Communication of Results 81
9 Other Business and Legal Matters 82
9.1 Fees 82
9.1.1 Certificate Issuance or Renewal Fees 82
9.1.2 Certificate Access Fees 82
9.1.3 Revocation or Status Information Access Fees 82
9.1.4 Fees for Other Services 82
9.1.5 Refund Policy 82
9.2 Financial Responsibility 82
9.2.1 Insurance Coverage 82
9.2.2 Other Assets 82
9.2.3 Insurance or Warranty Coverage for End-Entities 82

9.3 Confidentiality of Business Information 83
9.3.1 Scope of Confidential Information 83
9.3.2 Information not within the Scope of Confidential Information 83
9.3.3 Responsibility to Protect Confidential Information 83
9.4 Privacy of Personal Information 84
9.4.1 Privacy Plan 84
9.4.2 Information Treated as Private 84
9.4.3 Information not Deemed Private 84
9.4.4 Responsibility to Protect Private Information 84
9.4.5 Notice and Consent to Use Private Information 84
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 84
9.4.7 Other Information Disclosure Circumstances 84
9.5 Intellectual Property Rights 84
9.6 Representations and Warranties 85
9.6.1 CA Representations and Warranties 85
9.6.2 RA Representations and Warranties 86
9.6.3 Subscriber Representations and Warranties 86
9.6.4 Relying Party Representations and Warranties 87
9.6.5 Representations and Warranties of other Participants 87
9.7 Disclaimers of Warranties 87
9.8 Limitations of Liability 87
9.9 Indemnities 88
9.10 Term and Termination 88
9.10.1 Term 88
9.10.2 Termination 88
9.10.3 Effect of Termination and Survival 88
9.11 Individual Notices and Communications with Participants 89
9.12 Amendments 89
9.12.1 Procedure for Amendment 89
9.12.2 Notification Mechanism and Period 89
9.12.3 Circumstances under which OID must be Changed 89
9.13 Dispute Resolution Provisions 89
9.14 Governing Law 90
9.15 Compliance with Applicable Law 90
9.16 Miscellaneous Provisions 90
9.16.1 Entire Agreement 90
9.16.2 Assignment 90
9.16.3 Severability 90
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) 90
9.16.5 Force Majeure 90
9.17 Other Provisions 90
Approval 91

1 Introduction

1.1 Overview

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

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

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

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

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

Multicert PKI conforms to the current version of the baseline requirements for Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum in document “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, version identified in section 1.6.3 of this document, available at https://www.cabforum.org. In the event of any discrepancy between this document and that described in the Baseline document, what is established in the document issued by the CA/Browser Forum supersedes what is described in this document.

1.2 Document Name and Identification

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

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

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

DOCUMENT INFORMATION	
Document version	Version 10.0
Document Status	Approved
OID	1.3.6.1.4.1.25070.1.1.1.0.7
Issuing date	17/12/2020
Validity	1 year
Location	https://pki.multicert.com/index.html

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

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

Multicert PKI issues the certificates with the following OIDs:

Type of Certificate	Multicert OID
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
Qualified Electronic Seal for Electronic Invoice	1.3.6.1.4.1.25070.1.1.1.1.0.1.19
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[2] 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
CIV (Commercial Identity Verification)	1.3.6.1.4.1.25070.1.1.1.1.0.1.9

1.3 PKI Participants

1.3.1 Certification Authorities

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

They fall into the following trust hierarchy:

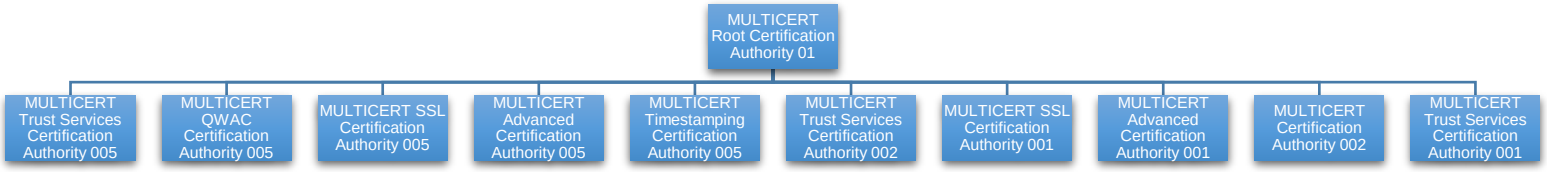
- The MULTICERT Root Certification Authority 01, duly accredited by the National Security Authority.

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

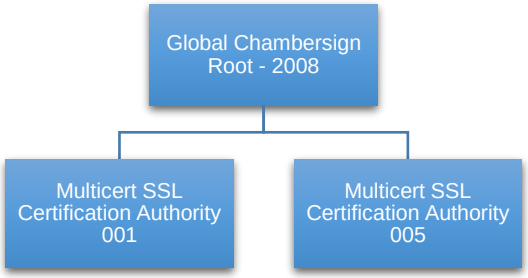
Schematically, the following CAs are part of the Multicert Root Certification Authority 01 hierarchy:

[2] Organizational Validation

CA`s issuing certificates:



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



Multicert Root Certification Authority 01

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

Multicert Certification Authority 002

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

Multicert Trust Services Certification Authority 001

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

Multicert Advanced Certification Authority 001

CERTIFICATE INFORMATION	
Distinguished Name	CN=MULTICERT Advanced Certification Authority 001,OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validity	12/06/2030
Thumbprint	f8 25 77 a2 a8 c0 fc 1c 57 d2 d8 f3 7e 6c 0f fc 83 b3 3b 09
Issuer	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert Trust Services Certification Authority 002

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

Multicert SSL Certification Authority 001 (signed by Global Chambersign Root – 2008)

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

Multicert SSL Certification Authority 001 (signed by MULTICERT Root Certification Authority 01)

CERTIFICATE INFORMATION	
Distinguished Name	CN=MULTICERT SSL Certification Authority 001,OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validity	12/06/2030
Thumbprint	a4 b4 02 47 5d 97 6f 6a de fb 01 1d b0 4e 85 9d bb 37 bd 5f
Issuer	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT Trust Services Certification Authority 005

CERTIFICATE INFORMATION	
Distinguished Name	CN = MULTICERT Trust Services Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validity	06/08/2032
Thumbprint	75 d1 aa fa d8 82 5c b9 ea ef 92 f7 7f a3 4e 66 e2 ba b6 dc
Issuer	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT QWAC Certification Authority 005

CERTIFICATE INFORMATION	
Distinguished Name	CN = MULTICERT QWAC Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validity	06/08/2032
Thumbprint	14 5d 4b 69 f8 93 99 f0 55 ed 1b b9 c2 62 f2 72 ef b3 d5 9b
Issuer	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT Timestamping Certification Authority 005

CERTIFICATE INFORMATION	
Distinguished Name	CN = MULTICERT Timestamping Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validity	06/08/2032
Thumbprint	50 01 f3 1a 1a b8 b1 56 57 f1 77 7a f8 5b a7 37 b4 dc 93 68
Issuer	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT Advanced Certification Authority 005

CERTIFICATE INFORMATION	
Distinguished Name	CN = MULTICERT Advanced Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validity	06/08/2032
Thumbprint	18 8f 27 88 1f ef a7 99 cb f4 9a 1a 79 ad d6 07 f5 56 6e 5d
Issuer	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT SSL Certification Authority 005 (signed by MULTICERT Root Certification Authority 01)

CERTIFICATE INFORMATION	
Distinguished Name	CN = MULTICERT SSL Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validity	06/08/2032
Thumbprint	3a f8 63 01 f6 37 e6 a2 a0 29 22 7a 46 51 a0 37 3d 90 41 c1
Issuer	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT SSL Certification Authority 005 (signed by Global Chambersign Root – 2008)

CERTIFICATE INFORMATION	
Distinguished Name	CN = MULTICERT SSL Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validity	02/06/2030
Thumbprint	a2 b2 43 bd ee dc d0 80 66 0b 35 a6 d0 f8 c1 f5 b9 de 96 c6
Issuer	CN = Global Chambersign Root – 2008, O = AC Camerfirma S.A., SERIALNUMBER = A82743287, L = Madrid (see current address at www.camerfirma.com/address), C = EU

1.3.1.1 External Certification Authorities

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

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

1.3.2 Registration Authorities

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

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

1.3.2.1 Internal Registration Authority

Within the scope of Multicert PKI, the registration authority is materialized by the relevant internal services that register and validate the necessary information.

1.3.2.2 External Registration Authorities

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

- The RA is responsible for the validation of certificate request;
- After approval, the RA is responsible for the submission of certificate issuance request to Multicert CA;
- The CA will return the certificate, customized using a secure device;
- The RA is responsible for guaranteeing the delivery of the general conditions of the digital certificate issuance agreement and the certificate to the relevant subscriber or to whom legally represents it;
- The RA is responsible to process the revocation requests, and when applicable the suspension requests, and to perform the status change of the digital certificates as soon as the relevant subscriber ceases to perform functions within the scope for which the certificate was issued or when one of the revocation/suspension reasons describe in sections 4.9 occurs.

Externa RA`s which are in the scope of SSL certificates issuances, perform the following activities:

- The RA is responsible for the validation of certificate request;
- After approval, the RA is responsible for the submission of certificate issuance request to Multicert CA;
- The CA will perform the automatic validations;
- The CA will return the certificate;
- The RA is responsible for guaranteeing the delivery of the general conditions of the digital certificate issuance agreement and the certificate to the relevant subscriber or to whom legally represents it;
- The RA is responsible to process the revocation requests, and to perform the status change of the digital certificates as soon as they receive a validated revocation request or when one of the revocation reasons describe in sections 4.9 occurs.

1.3.3 Subscribers

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

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

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

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

1.3.3.1 Sponsor

The issuance of certificates for technological equipment is always carried out under human responsibility, being this entity designated as Sponsor. In this case, validation of authority for the Sponsor to represent the entity/organization is performed by the RA.

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

1.3.4 Relying Parties

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

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

Relying Parties must check the appropriate CRL and OCSP response prior to relying on information featured in a certificate. The location of the CRL distribution point and OCSP is detailed within the certificate.

1.3.5 Other Participants

1.3.5.1 Supervisory Authority / Supervisory Body

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

In general, the role of the Supervisory Body, carried out in Portugal by the National Security Authority (ANS), is related to the audit / compliance inspection in order to assess if the processes

used by the CAs in their certification activities are in accordance with the minimum requirements established in the Portuguese and European legislation, as well as with the provisions of this CPS.

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

- Accreditation: CA approval procedure regarding the relevant activity, based on an evaluation made to different parameters, such as physical security, HW and SW, access and operation procedures;
- Registration: procedure required by the CA to issue certificates;
- Inspection: procedure based on inspections carried out to the CA aimed at regularly checking the compliance parameters.

1.3.5.2 Registration Authority

Detailed in section 1.3.2.

1.3.5.3 Service Provision External Authorities

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

1.3.5.4 OCSP Validation Authority

The purpose of the OCSP Validation Authority is to verify the status of issued certificates using the Online Certificate Status Protocol[3] (OCSP) in order to determine the current status of the certificate, upon request from an entity, without resorting to status verification through consultation of the Certificates Revocation List (CRL).

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

1.3.5.5 Auditor from a Conformity Assessment Body

An independent element, external to the Certification Authority, belonging to an accredited CAB (Conformity Assessment Body). It`s mission is to audit the infrastructure of the Certification Authority in terms of equipment, human resources, processes, policies and rules for conformity assessment of the relying services under Regulation 910/2014 and applicable criteria.

The Certification Authorities managed by Multicert are audited by a CAB identified in the European Union List of Conformity Assessment Bodies (CABs) Accredited against the Requirements of eIDAS Regulation[4], which issues a Conformity Assessment Report (CAR) provided to the Supervisory Body, to assess the continuity of provision of reliable services.

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

[3] *cf.* RFC 2560. 1999, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.
[4] List available at https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation

1.4 Certificate Usage

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

a) Access control;

b) Confidentiality;

c) Integrity;

d) Authentication and;

e) Non-repudiation.

These services are obtained through the use of private-key encryption, through its use in the relying structure that the Multicert PKI provides.

1.4.1 Appropriate Certificate Uses

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

Certificates issued pursuant to this CPS may be used for access control, confidentiality, integrity, authentication or non-repudiation, depending on the key usage and extended key usage existent in the certificate.

Certificate	Appropriate Use
Qualified Digital Signature	Used for transactions that support digital signing of electronic forms, electronic documents, or electronic email. When The Serial Number field in the Subject Distinguished Name contains the prefix “TIN”, the certificate should be used for signing electronic invoices and request forms for same usage certificates. Issued for an individual, with or without an associated entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by individuals. This signature has the same probative legal value as a handwritten signature.
Qualified Electronic Seal	Used for transactions that support digital signing of electronic forms, electronic documents, or electronic email. Issued for a legal person/entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by entities/organizations.
Qualified Electronic Seal for Electronic Invoice	Used for transactions that support digital signing of electronic invoices and certificate request form. Issued for a legal person/entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by entities/organizations.
Authentication	Used for specific electronic authentication transactions that support accessing web sites and other online content, electronic email, organizational systems, etc. Issued for an individual, with or without an associated entity/organization. Guarantee the authenticity of individuals (with or without an associated entity/organization).
Confidentiality	Used to cipher information to be communicated, such as electronic documents or email content. Issued for an individual, with or without an associated entity/organization. Guarantee the confidentiality of content.

Advanced Digital Signature	Used for transactions that support digital signing of electronic forms, electronic documents, or electronic email. Issued for an individual, with or without an associated entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by individuals. Used for specific electronic authentication transactions that support accessing web sites and other online content, electronic email, organizational systems, etc. Guarantee the authenticity of individuals (with or without an associated entity/organization). Used to cipher information to be communicated, such as electronic documents or email content. Guarantee the confidentiality of content.
SSL OV and Wildcard	Used to secure online communication. Associates a domain name with an organization. Issued for a legal person/entity/organization. Guarantee the authenticity and confidentiality.
PSD2 Qualified Electronic Seal	Used for transactions that support digital signing of electronic forms, electronic documents, or electronic email. Issued for a legal person/entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by entities/organizations.
PSD2 Qualified Website Authentication	Used to secure online communication where risks and consequences of data compromise are high. Associates a domain name with an organization. Issued for a legal person/entity/organization. Guarantee the authenticity and confidentiality.

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

1.4.2 Prohibited Certificate Uses

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

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

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

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

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A certificate only establishes that the information in the certificate was verified in accordance with this CPS when the certificate was issued.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The management of this CPS is the responsibility of the Multicert PKI Authentication Working Group, which can be contacted at:

Multicert – Serviços de Certificação Electrónica, S.A.

Lagoas Park

Edifício 3, Piso 3

2740-266 Porto Salvo – Oeiras, Portugal

Tel: +351 217 123 010

https://www.multicert.com

ca.forum@multicert.com

For PSD2 certificates: psd2@multicert.com

1.5.2 Contact Person

NAME	Multicert PKI 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:	ca.forum@multicert.com For PSD2 certificates: psd2@multicert.com
Web page	https://www.multicert.com
Phone:	+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 registered for communications of PSD2 certificates.

The Subscribers, Relying Parties, Application Software Suppliers, and other third parties may report suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates by sending email to the contacts above.

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

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

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

1.6 Definitions and Acronyms

1.6.1 Definitions

Item	Definition
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 public 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 issuing, managing, revoking, and renewing or re-keying certificates.
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 qualified trust service provider and the qualified 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.
Qualified Website Authentication 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.

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.
SSL certificate	Advanced certificate that makes it possible to authenticate a website and associate it with the natural or legal person for whom the certificate has been issued.
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	Body responsible for supervisory tasks in the designating Member State, namely: - Supervise qualified trust service providers established in the territory of the designating Member State to ensure, through *ex ante* and *ex post* supervisory activities, that those qualified trust service provides and the qualified trust services that they provide meet the requirements laid down in the Regulation 910/2014; - Take action if necessary, in relation to non-qualified trust service providers established in the territory of the designated Member State, through *ex post* supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in the Regulation 910/2014.
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 qualified or as a non-qualified trust service provider.
Website Authentication Certificate	Certificate that makes it possible to authenticate a website and associate it with the natural or legal person for whom the certificate has been issued.

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
QSealC	Qualified Electronic Seal Certificate
QSCD	Qualified electronic Signature/Seal Creation Device
QWAC	Qualified Website Authentication Certificate
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, v1.7.3 – Baseline Requirements;

CA/Browser Forum, v1.7.4 – Guidelines for The Issuance and Management of Extended Validation Certificates;

Despacho 154/2017 da Entidade Supervisora nacional, de 5 de dezembro – Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a videoconferência;

Despacho 155/2017 da Entidade Supervisora nacional, de 5 de dezembro – Criação de assinaturas eletrónicas à distância, com gestão porum prestador qualificado de serviços de confiança em nome do signatário;

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 Signatures 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, v1.4.1 (2020-07) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

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, v2.2.1 (2020-07) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;

ETSI EN 319 412-3, V1.2.1 (2020-07) - 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, v2.3.1 (2020-04) - 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, v1.4.1 (2019-11) – 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

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

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

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

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

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

2.2 Publication of Certification Information

Multicert has a repository in web environment, allowing the Relying Parties to make on-line searches regarding CPS, CP, CA`s certificates, revocation (CRL`s) and other information related to the certificates, available at https://pki.multicert.com/index.html (and via URI`s included in the certificates themselves).

Any compliance declarations will be provided upon request sent via email to the email indicated in section 1.5.2.

2.3 Time or Frequency of Publication

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

Certificates for the CAs managed by Multicert are published as soon as possible after their issuance.

The CRL issued by the Multicert Root CA must be published at least once every 12 (twelve) months or within 24 (twenty four) hours after revoking a Subordinate CA Certificate.

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

2.4 Access Controls on Repositories

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

3 Identification and Authentication

3.1 Naming

Naming will be carried out as follows:

- Certificates issued for natural persons will receive the real name (or pseudonym) of the subscriber;
- Certificates issued for natural persons associated with a legal person will receive the name of the natural person in the Common Name field, with the name of the legal person being stated in the Organization field;
- Certificates issued for legal persons will receive the name of the entity/organization;
- Service certificates will receive the domain qualified name and/or the scope of the relevant usage.

3.1.1 Types of Names

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

The unique name of these certificates is identified in document Certificate Profiles List (MULTICERT_PJ.ECRAIZ_428_en) available at https://www.pki.multicert.com.

3.1.2 Need for Names to be Meaningful

Multicert will ensure, within its trust hierarchies:

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

3.1.3 Anonymity or Pseudonymity of Subscribers

Typically Multicert does not issue pseudonymous certificates.

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

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

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

According to the relevant issuing processes, Multicert rejects the issuing of certificates with the same DN for different subscribers.

The uniqueness of each subject name in a certificate is enforced as follows:

- Certificate for electronic signature (qualified or non-qualified), authentication, confidentiality – inclusion of the subscriber name (natural person or legal person) plus a DN serial number that is unique. When the subscriber has an association with an entity/organization, the entity name will also be included in the DN.
- SSL Certificate – inclusion of the domain name in the certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN)

3.1.6 Recognition, Authentication, and Role of Trademarks

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

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

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.

When the certificate contains the jurisdictionCountryName field, a verification is made by consulting an Incorporating Agency or Registration Agency listed in document “Approved Incorporating Agencies” available at https://pki.multicert.com.

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

3.2.1 Method to Prove Possession of Private Key

3.2.1.1 Signature (eSign)

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

1. The key pair is generated in the cryptographic HSM and included in the encrypted token, using a secure and direct communication, without any record in any device;
2. The encrypted token is customized for the subscriber;
3. The public key is sent to Multicert CA for issuance of the corresponding digital certificate being the latter also included in the encrypted token;
4. The encrypted token is delivered either in person or via mail;
5. The certificate is issued with a "suspended" status being activated by a link provided to the subscriber, by which the latter will be authenticated using the authentication certificate included in the encrypted token. Upon authentication, the subscriber will receive a temporary password (OTP) in his/her cell phone that must be entered in the certificate activation page. As soon as this process is successfully completed, the certificate will be active and ready to be used. This last step will not be performed in non-qualified certificates for signature, authentication and confidentiality.

In case of remote certificates, the private key is generated and maintained in a HSM. In this case, the previous steps are not performed.

3.2.1.2 Electronic Seal (eSeal)

In case of a qualified certificate for Electronic Seal, it is performed the same steps as identified in section 3.2.1.1, except step 5 which is not performed in this case.

For the electronic seal certificates, there is also the option of the key being generated by the person requesting the issuance of the certificate, provided that it is duly authorized by the Legal Responsible for the entity/organization, using its own HSM. In this case:

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

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

3.2.1.3 Website Authentication Certificates and Qualified Website Authentication Certificates

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

3.2.1.4 Services Certificate

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

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

3.2.2 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. In these cases, confirmation of the domain control it is required, using one of the methods described in section 3.2.2.2.

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

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

This same procedure is used to confirm the subscriber email address included in the certificate request form (subscriber email contact).

3.2.2.2 Method to Validate Domain Name / IP Address Control

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

Domain Name	IP Address
Agreed-Upon Change to website – by the Applicant placing an agreed-upon Request Token or Random Value in the "/.well-known/pki-validation" directory, performed in accordance with Baseline Requirements section 3.2.2.4.18	Agreed-Upon Change to website – by the Applicant placing an agreed-upon Request Token or Random Value in the "/.well-known/pki-validation" directory, performed in accordance with Baseline Requirements section 3.2.2.5.1

Email to DNS TXT Contact – confirming the Applicant`s control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value. Performed in accordance with Baseline Requirements section 3.2.2.4.14	Email to IP Address Contact – confirming the Applicant`s control over the IP Address by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. Performed in accordance with Baseline Requirements section 3.2.2.5.2
Phone Contact with Domain Contact – confirming the Applicant`s control over the FQDN by calling the Domain Contact`s phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with Baseline Requirements section 3.2.2.4.15	Phone Contact with IP Address Contact – confirming the Applicant`s control over the IP Address by calling the IP Address contact`s phone number and obtaining a response confirming the Applicant`s request for validation of the IP Address. This method can only be applied if the IP Address Contact is visible in the IP Address registry. Performed in accordance with Baseline Requirements section 3.2.2.5.5

3.2.3 Authentication of 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;
4. Through a remote videoconference session with the natural person, in accordance with *Despacho* 154/2017 of the Portuguese national Supervisory Body.

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

These practices comply with document ETSI TS EN 319 411-1 and ETSI TS EN 319 411-2 (when the certificate is qualified).

3.2.4 Non-Verified Subscriber Information

All information provided by the subscriber is verified.

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'[6]). 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'). 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. The data 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 facilities accompanied with an identification document; or through a remote videoconference session.
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; or through a remote videoconference session.
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 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

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

	in the RA facilities accompanied with an identification document; or through a remote videoconference session.
Qualified Electronic Seals (eSeal)	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 facilities accompanied with an identification document; or through a remote videoconference session.

3.2.6 Criteria for Interoperation

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

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-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 procedure.

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

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

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 Enrollment Process and Responsibilities

The enrolment process includes the following steps:

1. SSL, PSD2 and QSealC in a customer on premises QSCD: Generating a key pair and sending a CSR;
   1.1. All other certificates: the key pair is generated in a QSCD/SSCD by the CA at the moment of the certificate issuance, after all the following activities being performed.
2. Fulfilling the certificate request form;
3. Agreeing with the terms and conditions of the certificate;
4. Submitting the certificate request form;
5. Paying any applicable fees;
6. 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

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

For the requests regarding Website Authentication certificates, Multicert performs the verification of the relevant CAA records at the moment of the certificate request form submission and immediately before issuing SSL certificates. The CA will act in compliance with the CAA records, if existing. Multicert CA identification domain in CAA records is 'multicert.com'[6].

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

For any certificate issued by Multicert PKI, the application is subject to approval. This approval will depend on the type of certificate and Certification Authority.

Certificate issuance by Multicert Root CA requires a ceremony performed by multiple working group members that need to individually authorize operations, in order to perform a certificate signing operation.

In case of approval of end-user certificates, the Registration Operation Working Group is responsible for managing and approving the certificates applications.

All SSL OV and WC certificates are registered in Certificate Transparency log servers[7] immediately after being issued.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

4.4 Certification Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

Certificates are considered accepted seven (7) days after the certificate`s issuance, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

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

4.4.2 Publication of the Certificate by the CA

SSL OV and WC are published in Certificate Transparency log servers[7].

Multicert publishes all CA certificates in its repository available at https://pki.multicert.com. The publication of end-entity certificates is made by delivering them to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Multicert RA`s or partners/resellers may be informed of the issuance if they were involved in the initial enrolment.

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

Subscribers of certificates can only use the private key of their certificates for the exclusive purpose the key is intended to (defined in the fields "KeyUsage" and “Extended Key Usage” of the certificate) and always within the scope of the legal framework. Usage of the key is the exclusive responsibility of the Subscriber. Terms and conditions for the certificate issuance identifies the obligations of the Subscriber with respect to the private key protection and acceptable usage.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties should use software fully compliant with X.509 standards and should only rely on the certificate if it is not expired, suspended nor revoked.

Multicert provides in this CPS information about the appropriate services available to verify the certificate validity and status, such as OCSP and CRL.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

A certificate can be replaced by Multicert on its own initiative, or can be renewed on the initiative of the Subscriber in the following situations:

Website Authentication certificates can be renewed if:

- The certificate is not expired nor revoked;
- The domain(s) remain unchanged. If the domain(s) is (are) changed, a new domain control validation as described in section 3.2.2.2 has to be performed.
- The validity of the new certificate remains the same as the previous certificate;
- Only applicable to SSL OV and WC certificates: the documents and data obtained to verify certificate information, and the validation itself have no more than 825 days.

Regardless of the remaining validations, before the renewed certificate is issued, CAA Records is verified.

For QWAC PSD2 certificates the following conditions also apply:

- The documents and following data obtained to verify the certificate information, and the validation itself have no more than 13 months.
- The renewed certificate can have a different validity, provided that it does not exceed the limit established in section 6.3.2.

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

Multicert CA may initiate a certificate renewal (certificate replacement) in its own discretion, after notifying the certificate Subscriber. The Subscriber may initiate a certificate renewal in its own discretion, only in the conditions described in section 4.6.1.

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 within the limits of information reuse described in section 4.6.1.
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

Multicert notify the Subscriber within a reasonable time after certificate issuance, typically by email, and may use any reliable mechanism to deliver the certificate to the subscriber.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Renewed certificates are considered accepted after seven (7) days after delivery or notify of issuance of the certificate to the Subscriber, or when evidence exists that the Subscriber used 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 information in the Distinguished Name and Subject Alternative Name fields of the previous certificate.

4.7.2 Who may Request Certification of a New Public Key

Multicert may accept a certificate re-key request provided that it is from the certificate Subscriber or an Entity/Organization Representative, when applicable.

4.7.3 Processing Certificate Re-Keying Requests

Multicert may request additional information before 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 reliable method of communication previously verified.

4.7.4 Notification of New Certificate Issuance to Subscriber

Multicert notifies the Subscriber within a reasonable time after the certificate issues.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Issued certificates are considered accepted seven (7) days after the certificate is rekeyed, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Multicert 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

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

This practice is not supported by Multicert PKI.

4.8.1 Circumstance for Certificate Modification

No Stipulation.

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 (twenty four) 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 is made aware of a demonstrated or proven method that can easily compute the Subscriber`s private key based on the public key in the certificate;
- 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 (five) 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 inaccurate;
- 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 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 circumstances 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 that a SSL Wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified 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 7 (seven) days:

- The Subordinate CA requests revocation in writing;
- The Subordinate 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 i) Baseline Requirements for the SSL certificates; and/or ii) ETSI TS 119 312;
- 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 revocation request can be made by one of the following elements:

- By the client/subscriber or a representative;
- By the Entity/Organization who requested the certificate;
- By an element of the Registration Operation Working Group of Multicert`s PKI or by the Issuing CA, whenever it becomes aware that the data included in the certificate do not correspond to the true or are not owned by the subscriber or when one of the revocation reasons defined in section 4.9.1 occurs;
- By the NCA, when it is PSD2 certificates, due to a duly founded reason such as the data included in the certificate it is no longer valid.

4.9.3 Procedure for Revocation Request

The revocation request can be presented in the following different ways:

- On-line, using a Revocation Request Web Form, where the certificate status will change to REVOKED:
    - https://www.multicert.com/3ws/certRevocationForm
- By sending directly to Multicert the Revocation Request Form, provided by Multicert in its *site*, duly completed and along with the documentation requested for that purpose.
- Using the online services of the Client Area or Partner Area, not being necessary to submit any documentation.
- If the NCA is requesting revocation (only applicable in the PSD2 certificates): the NCA send an email requesting the revocation of the certificate, submitting the certificate

revocation request form and indicating which method to validate the authenticity of the request they want to use, of the methods described in section 6.2.3 of ETSI TS 119 495:

- Shared Secret – The CA will contact the NCA, by telephone, to share a secret with the NCA. The NCA shall send an email containing the shared secret and submitting the certificate revocation request form;
- Digital Signature – The NCA send an email containing the certificate revocation request form digitally signed, with a qualified certificate. The qualified certificate shall be one of the following: qualified seal with the Organization field containing the name of the NCA, or a qualified signature in name of the person in the NCA that is requesting the certificate (in this case, the certificate shall contain in the Organization field the NCA name).

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

When the revocation request is made by the Subscriber or the person responsible for the Entity/Organization, through a written revocation request form, the Registration Operation Working Group have 24 hours to process the request and revoke the certificate, after receiving the revocation request form. If the revocation request is made in an authenticated manner, the revocation is processed immediately. Multicert guarantees publication of the certificate new status within the following time frames:

- 12 hours through Delta CRL;
- 24 hours through CRL;
- Immediately through OCSP.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on the information listed in a certificate, a Relying Party must validate the suitability of the certificate to the purpose intended and ensure the certificate is valid. Relying Parties need to consult the OCSP responders or CRL identified in each certificate to verify its status.

4.9.7 CRL Issuance Frequency

Multicert Certification Authorities allowed to issue end-user certificates will issue CRLs every day, being issued Delta CRLs every 12 hours.

For Root CA, a CRL is published at least once every 12 (twelve) months or within 24 (twenty four) hours if a Subordinate/Intermediate CA is revoked.

4.9.8 Maximum Latency for CRLs

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 24 (twenty four) hours 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

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

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

OCSP responses conforms to RFC 6960 or RFC 5019. OCSP responses are 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 Re Key Compromise

Multicert and Registration Authorities shall use commercially reasonable methods to inform Subscribers that their private key may been compromised. If a certificate is revoked because of compromise, Multicert will issue a new CRL within 24 hours and a Delta CRL within 12 hours after revoking the certificate.

4.9.13 Circumstances for Suspension

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

Certificate suspension can be used when the Subscriber, the Responsible for the Entity/Organization (when applicable), or the Registration Authority wants to disable the certificate temporarily. Such situations may include temporary loss of certificate, temporary leave of the Subscriber from the Entity/Organization, etc. Unlike certificate revocation, the suspension allows a certificate to switch its status to active or revoked.

4.9.14 Who Can Request Suspension

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

- By the client/subscriber or a representative;
- By the Entity/Organization who requested the certificate;
- By an element of the Registration Operation Working Group of Multicert`s PKI or by the Issuing CA.

4.9.15 Procedure for Suspension Request

The suspension request can be presented in the following different ways:

- On-line, using a Suspension Request Web Form (not applicable to SSL certificates), where the certificate status will change to SUSPENDED: https://www.multicert.com/3ws/certSuspensionForm.
- Using the online services of the Client Area or Partner Area, not being necessary to submit any documentation.

4.9.16 Limits on Suspension Period

In case of qualified digital certificates for signature (eSign or eSeal), if the certificate is suspended:

- Through the client area – the Subscriber have three (3) days to activate the certificate, otherwise it will be revoked;
- Through the partner area or through the Suspension Request Web Form – the Subscriber have six (6) days to submit the revocation request, otherwise it will be activated;
- Through other means – the Subscriber must submit to the RA a request to activate or revoke the certificate. If the Subscriber does not submit this request, the certificate suspension may last as long as the validity period of the certificate.

In case of non-qualified certificates, the Subscriber must submit to the RA a request to activate or revoke the certificate. If the Subscriber does not submit this request, the certificate suspension may last as long as the validity period of the certificate.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

If a certificate is revoked, it remains on the CRL after the expiration date.

4.10.2 Service Availability

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

4.10.3 Optional Features

No Stipulation.

4.11 End of Subscription

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

- Certificate revocation;
- The certificate validity period has expired;
- The applicable Subscriber Agreement expires 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. Multicert CA`s private keys are subject to the technical security controls described in section 6.2.3.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No Stipulation.

5 Facility, Management and Operational Controls

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

5.1 Physical Controls

5.1.1 Site Location and Construction

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

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

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

a) Masonry, concrete or brick walls;

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

c) Nonexistence of windows;

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

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

- Clearly defined security perimeters;
- Masonry walls, ceiling and floor, no windows, which hinder unauthorized accesses;
- High security anti-theft bolts and locks on the access doors to the 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

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

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

The access to the red identification card requires a double individual access authentication control. The entrance and stay in security areas is not allowed to unaccompanied personnel, including unauthenticated employees or visitors. Unless all personnel who move around these security areas is guaranteed recognized by all, it is required the use of the respective access card in a visible way as to ensure that no 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

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

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

5.1.6 Media Storage

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

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

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

5.1.7 Waste Disposal

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

It is assured that it is not possible to recover any information from the information supports used to store or transmit sensitive information (through low level "safe" formatting or physical destruction), before they are eliminated. Cryptographic elements or logic access physical keys are either physically destroyed or follow the destruction recommendations of the respective manufacturer prior to its elimination. Other storage equipment's (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

The activity of a Certification Authority 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 8(eight) different categories (which correspond to 5 (five) 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.

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.

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*, and the definition, update, and proposal of the CA policies.

5.2.1.4 Audit Working Group

It is responsible for performing the internal audit to the relevant and necessary actions to ensure the CA's operability.

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[8]. 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.

5.2.1.6 Registration Operation Working Group

It is responsible for validate the documentation related to the certificate request, ensuring the issuance, renewal, suspension and revocation of certificates.

5.2.1.7 Monitoring and Control Working Group

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

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

5.2.1.8 Management Working Group

It is the decision-making body of Multicert's PKI, and its members are directly appointed and / or 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 the Multicert PKI CAs, enhancing the revision and approval of all documents and policies of the CAs. The Management Working Group is also responsible for naming and/or destitution members of the other Working Groups and the safekeeping of some sensitive artefacts (authentication *tokens*, etc.).

5.2.2 Number of Persons Required per Task

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

The internal control procedures were elaborated in order to ensure a minimum of 2 authenticated individuals to be able to have physical and logical access to the security equipment. The access to the CA's cryptographic *hardware* follows strict procedures involving multiple individuals

[8] Defined for each artefact in its custody.

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

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

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

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

5.2.4 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 Multicert's PKI:

If belonging to the Group / Subgroup ...	May belong to the Group / Subgroup ... ?	Installation	Operation	Authentication	Registration Operation	Audit	Custody	Management	Monitoring and Control
Installation					✘	✘	✘	✘	
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 CAs) regarding any information about the CAs, its operation, its environments and human resources at its service and about the subscribers of the digital certificates issued by it;
- Compromise (formally) to perform the functions for which he/she was appointed and not assume responsibilities which may lead to ethical or deontological problems to their performance. In that sense it is necessary to declare not only knowing the terms and conditions for the performance of the respective functions, as well as the capacity and availability to do them.

5.3.1 Qualifications, Experience, and Clearance Requirements

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

5.3.2 Background Check Procedures

Background check results from the accreditation process of individuals nominated to hold positions in any one of the trust functions. The background check[9] 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;

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

b) General concepts on information security;

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

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

e) Certificate Policy and Certification Practices Statement;

f) Recovery from disasters;

g) Procedures for the continuation of the activity;

h) Basic legal aspects regarding the certification services.

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

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

The entries in the records include the following information:

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

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

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

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

The records are simultaneously collected internal and externally to the CA system.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

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

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 7 years after the expiry date of the certificate to which it relates.

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 authorized 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 private keys of CAs (created and stored according to section 6.2.4) and of the archived records (section 5.5.1) are stored in external safe environments and available in case of disaster or compromise.

5.7.2 Computing Resources, Software and/or Data are Corrupted

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

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

5.7.3 Entity Private Key Compromise Procedures

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

- Revocation of the affected CA certificate and all certificates issued in the “branch” of its trust hierarchy;
- Notification of the Supervisory Body and all subscribers of certificates issued in the “branch” of the affected CA trust hierarchy;
- Generation of a new key pair for the affected CA;

- Renewal of all certificates issued in the trust hierarchy “branch” of the affected CA.

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

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

a) Inform the Supervisory Body;

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 related to the activity of the CAs, namely CA key, certificates, CRL`s availability, documentation stored (internally or externally), repositories and event records storage.

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

6 Technical Security Controls

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

6.1 Key Pair Generation and Installation

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

6.1.1 Key Pair Generation

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

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

The private keys for Qualified Digital Signature and Electronic Seal certificates (if not generated by the certificate subscriber in a secure module) are generated by Multicert CA using cryptographic *hardware* compliant with FIPS 140-2 level 3 and/or *Common Criteria* EAL 4+ requirements.

6.1.2 Private Key Delivery to Subscriber

The delivery of the private key associated with the Qualified Digital Signature and Electronic Seal certificates is performed in QSCD cryptographic devices.

For the other certificate types, where the private key is not required to be in a QSCD,, the private key is provided by the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

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

- 4096 bits RSA for Multicert PKI CAs keys;
- 2048 *bits* RSA for the keys associated to the remaining certificates issued by Multicert PKI CAs with signature algorithm sha256RSA.

For RSA keys, the modulus size in bits must be evenly divisible by 8.

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).

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

According to section 1.4 and document Certificate Profiles List available at https://pki.multicert.com.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1 Cryptographic Module Standards and Controls

For the generation of the key pairs of Multicert PKI CAs, as well as for the storage of the private keys, Multicert uses a cryptographic module in hardware evaluated according to FIPS 140-2 Level 3 OR according to Common Criteria (pursuant to Protection Profile EN 419 211-5.

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 Groups to perform sensitive cryptographic operations in CA.

The activation data necessary for using the private key of a Multicert PKI CA are divided in several parts (stored in the PED keys – small digital identification *tokens*, with physical USB pen format, identifying different access roles to HSM), being accessible, and at the responsibility of different

members of the Working Group. A defined number of these parts (*n*) from the total number of parts (*m*) is necessary to activate a CA's private key stored in the *hardware* cryptographic module.

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

6.2.3 Private Key Escrow

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

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

6.2.7 Private Key Storage on Cryptographic Module

The private keys of Multicert PKI CAs are stored in an enciphered way in the cryptographic *hardware* modules.

6.2.8 Method of Activating Private Key

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

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

6.2.9 Method of Deactivating Private Key

The private key of a Multicert PKI CA is deactivated when the CA's system is disconnected.

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

6.2.10 Method of Destroying Private Key

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

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

6.2.11 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 of Multicert PKI CAs is made by the members of the Working Group and remain stored after the expiry date of the corresponding certificates, to verify the signatures generated during its validity.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The period to use the keys can have up to the same validity as the certificate's validity period.

Certificates signed by a specific CA must expire before the end of that key pair's operational period.

In this sense, the validity of the various types of certificates is the following:

Certificate type	Private key usage	Maximum Certificate validity
Multicert Root CA	12 years	25 years
Sub CAs	No Stipulation	12 years and 6 months
OCSP *on-line* validation	4 months	1 year
Qualified Digital Signature	No Stipulation	4 years
Qualified Electronic Seal	No Stipulation	3 years
Electronic Seal PSD2	No Stipulation	2 years
Authentication	No Stipulation	4 years
Advanced Digital Signature	No Stipulation	3 years
Web Server Certificate (OV[2]/Wildcard)	No Stipulation	1 year
Qualified Website Authentication Certificate PSD2	No Stipulation	1 year

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

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

The private keys of Multicert PKI CAs are stored in an enciphered way in cryptographic *token*.

6.4.3 Other Aspects of Activation Data

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

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

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

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

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

6.5.2 Computer Security Rating

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

The hardware cryptographic module of Multicert PKI CAs complies with the standard EAL 4+ *Common Criteria for Information Technology Security Evaluation* and/or FIPS 140-2 level 3.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

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

6.8 Time-Stamping

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

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

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

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

Each certificate includes a unique Serial Number (within the context of the Issuer DN), which is non-sequential, greater than zero (0) and contains at least 64 bits of output from a CSPRNG.

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 certificates issued by Multicert PKI CAs is compliant with:

- ITU.T recommendation X. 509[10];
- RFC 5280[5];
- Applicable legislation, national and European;
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.

The certificate profiles can be consulted in the Certificate Profiles List document available at https://pki.multicert.com.

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

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

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

7.1.3 Algorithm Object Identifiers

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

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

7.1.4 Name Forms

As defined in section 3.1.

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

All certificates issued in Multicert PKI contain the qualifiers:

"*policyQualifIierID*: 1.3.6.1.5.5.7.2.1" and "*cPSuri*", which point to the URI where the Certification Practices Statement with the OID identified by the "*policyIdentifier*" can be found. Other certificate policy object identifiers are also included, depending on the type of certificate, according to section 1.2 of this document, and as described in document Certificate Profiles List (MULTICERT_PJ.ECRAIZ_428_en) available at https://www.pki.multicert.com.

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation.

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.[5]

The protocol X.509 defines a method of certificate revocation, which involves the periodic issuing, by the CA, of a signed data structure called a certificate revocation list (CRL). A CRL is a time stamped list identifying revoked certificates, which is signed by the CA and made freely available in a public repository. Each revoked certificate is identified in the CRL by its serial number. When an application uses a certificate (e.g., for verifying a remote user's digital signature), that application not only verifies the certificate signature and validity; it also obtains the most recent CRL and checks if the serial number of the certificate is not in it. Note that a CA issues a new CRL on a regular periodic basis.[5]

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

- ITU.T Recommendation X.509[10];
- RFC 5280[5] and;
- Applicable legislation, national and European.

7.2.1 Version Number(s)

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

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

7.2.2 CRL and CRL Entry Extensions

The CRLs issued in Multicert PKI have the following extensions:

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

7.3 OCSP Profile

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

- ITU.T recommendation X.509[10];
- RFC 6960[11] and;
- Applicable legislation, national and European.

7.3.1 Version Number(s)

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

7.3.2 OCSP Extensions

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 internal audits to this CPS and to other rules, procedures, ceremonies, and processes are performed.

Multicert PKI is subject to external audits, performed by a Conformity Assessment Body (CAB) in order to evaluate the compliance of Multicert PKI CA´s and RA`s with the National and European applicable legislation.

8.1 Frequency or Circumstances of Assessment

The compliance audits are performed periodically in annual basis. Multicert must prove, through audit reports (produced by the conformity assessment body), that it is in compliance with the applicable National and European applicable legislation.

8.2 Identity/Qualifications of Assessor

The external compliance audits are performed by a Conformity Assessment Body (CAB) duly accredited[12].

The National Accreditation Body (NAB) is responsible for the accreditation of the Conformity Assessment Bodies (CAB) on the basis of EN ISO/IEC 17065 as profiled by ETSI EN 319 403, which are qualified to carry out the conformity assessments, resulting from these evaluations a Conformity Assessment Report (CAR), which is subsequently made available to the Supervisory Body and other interested parties 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, financial, legal or organic dependency exists between the auditor and the entity subject to the audit, or any other type of dependency which may lead to conflict of interests.

8.4 Topics Covered by Assessment

The scope of audits and other assessments include the accordance with the applicable National and European legislation, 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).

[12] https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation

8.5 Actions Taken as a Result of Deficiency

If from an audit results non-conformities, the auditor proceeds as follows:

a) Documents all non-conformities found during the audit in the Conformity Assessment Report (CAR). Depending on the severity of the non-conformities:
    a. Failed if the non-conformities are severe, in this case the audited trust service is not certified conformant;
    b. Passed if the non-conformities are not severe, in this case the audited trust service have 3 months to correct the non-conformities, performing the steps above.

b) Bearing in mind the non-conformities stated on the CAR, the entity subject to the audit will send a Corrective Action Plan, where the actions, methodology and time needed for correction of the non-conformities shall be described;

c) The CAB, after analyzing this action plan takes one of the following options:
    a. Accepts the proposed actions, in this case after the actions are implemented a follow up audit is performed to verify the effective implementation of the actions;
    b. Does not accept the proposed actions, in this case the audited must proposed another action plan.

8.6 Communication of Results

The results shall always be communicated to the Supervisory Body and other interested parties.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The fees charged by Multicert are identified in its online store or 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 about certificate status or revocation (CRL and Delta-CRL) is free and open.

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

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:

- The private keys of Multicert PKI CAs;
- All information relative to auditing safety, control, and procedures parameters;
- All information of a personal nature provided to Multicert PKI during the registration process of the subscribers of certificates, unless if there is explicit authorization for its release and/or if this is not included in the content of the issued certificate;
- Business continuity and recovery plans;
- Transaction records, including complete records and auditing records of the transactions;
- Information of all the documents related with Multicert PKI (rules, policies, ceremonies, forms and processes), including organizational concepts, secret, confidential and/or privileged financial/commercial information, being the property of Multicert. These documents are entrusted to the human resources of Multicert PKI's Working Groups on the condition of not being used or released beyond the scope of its duties under the established terms, without the previous and explicit authorization from Multicert;
- All passwords, PINs and other security elements related to Multicert PKI CAs;
- The identification of the members of Multicert PKI's Working Groups;
- The location of Multicert PKI's environments and its content.

9.3.2 Information not within the Scope of Confidential Information

It is considered as information for public access:

- Certificate Policy;
- Certification Practices Statement;
- CRL;
- Delta-CRL;
- All information classified as “public” (the information not expressly considered as “public” shall be considered as confidential).

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

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

In accordance with the Portuguese and European applicable legislation.

9.4.5 Notice and Consent to Use Private Information

In accordance with the Portuguese and European applicable legislation.

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 related to Multicert PKI, belong to Multicert S.A..

The private keys and the public keys are property 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

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

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

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

c) Protect its private keys;

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

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

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

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

h) Use reliable systems to store recognized certificates, that enable proving their authenticity and prevent 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, revoked 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 4.9 of this document and publish the revoked certificates on the CRL of Multicert PKI CAs repository, with the frequency stipulated in section 2.3;

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

n) Make available the previous versions of its CPS as well as the Certificate Policies;

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

p) Collaborate with the audits performed by the Conformity Assessment Body;

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 2,

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 Supervisory Body;

u) Comply with the specifications contained in the European regulation 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 7 (seven) years after the certificate expires; and

w) Make available the certificates of Multicert PKI CAs.

9.6.2 RA Representations and Warranties

Registration Authorities are obliged to:

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

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

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

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

e) Store the certificates issued without any changes;

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

g) Collaborate with the audits performed by the Conformity Assessment Body;

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

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

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

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

l) Maintain all information and documentation relative to a recognized certificate at each moment and for for 7 (seven) years after the certificate expires.

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, General Terms and Conditions of Digital Certificate Issuance, and in section 1.4 of CPS;

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

c) Immediately request the certificate revocation in the case of having knowledge or suspicion that the private key corresponding to the public key contained in the certificate has been compromised, or other reason stated in section 4.9 occurs;

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

e) Submit to the Certification Authority (or Registration Authority) the information that they consider accurate and complete with relation to the data that these require to carry out

the registration process. The CA should be informed on any changes in this information; and

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

9.6.4 Relying Party Representations and Warranties

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

a) Limit the reliability of the certificates to the uses allowed to them in compliance with that expressed in the corresponding Certificate Policy and section 1.4 of CPS;

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

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

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

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

f) Notify any occurrence or anomalous situation related to the certificate that may be considered the cause of its revocation, using the means indicated by Multicert S.A. in its CPS.

9.6.5 Representations and Warranties of other Participants

No Stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

Multicert S.A., as a Certification Authority:

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

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

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

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

e) 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;

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

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

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

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

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

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

9.9 Indemnities

In accordance with the legislation in force.

9.10 Term and Termination

9.10.1 Term

The documents related with Multicert PKI (including this CPS) become effective immediately after they are approved by the Management Working Group.

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

This CPS remains in force while it is not expressly revoked by issuing a new version.

9.10.2 Termination

The changes are appropriately marked by an indicated minor version.

The changes become effective after the approval of the Management Working Group and the publication in the repository of a new major version.

9.10.3 Effect of Termination and Survival

The obligations and restrictions established in this CPS, regarding the compliance audits, confidential information, records archival, obligations and responsibilities, born while it is in force, shall subsist after the replacement by a new version in everything that does not oppose it.

9.11 Individual Notices and Communications with Participants

Any notification related to this CPS shall be made by digitally signed e-mail, signed forms sent by mail, or other, depending on the criticality and subject of the communication. These notifications shall be sent to the contacts indicated in section 1.5.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are carried out by the Authentication Working Group. Suggestions of changes to be included can be submitted to the Authentication Working Group, through the contacts provided in section 1.5, to be analyzed.

The Authentication Working Group records revision changes in minor versions of the CPS. When a new version of the CPS is ready for approval, the Authentication Working Group submits the document to be approved by the Management Working Group, and a major version is incremented in the CPS.

9.12.2 Notification Mechanism and Period

Amendments to the CPS are recorded in the Version History table of this document, containing the version identification, date, details of changes made, and the change author.

When a new major version of the CPS is approved by the Management Working Group, an updated version of this document is published in the Multicert`s repository.

9.12.3 Circumstances under which OID must be Changed

If the Authentication Working Group determines that a change is necessary in the OID corresponding to a CPS or CP, it proposes it to the Management Working Group. In this case, a new CPS or CP document is created with a different OID.

Otherwise, amendments shall not require a change in CPS or CP OID.

9.13 Dispute Resolution Provisions

In case of dispute, the consumer may resort to an Alternative Dispute Resolution Entity. The official list of such entities is available on the Consumer Website at www.consumidor.pt.

Without prejudice to the possibility of prior use of mediation, if no agreement is reached between the parties within the scope of such procedure as to any dispute arising from interpretation, application or execution of this document, either party may appeal to the courts, being set as competent jurisdiction for the purpose the District Court of Lisbon.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

See section 9.14.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

Parties operating under this CPS or applicable agreements cannot assign their rights or obligations without the prior written consent of Multicert.

9.16.3 Severability

If a provision of this CPS, including limitation of liability clauses, is found to be ineffective or enforceable, the remainder of this CPS should be interpreted in the sense of the parties' original intention. Any provision of this CPS which provides for a limitation of liability, is intended to be severable and independent of any other provision and should be enforced as such.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Multicert may seek indemnification and attorneys` fees from a party for damage, losses and expenses related to that party`s conduct. Multicert`s failure to enforce a provision of this CPS does not waive Multicert`s right to enforce the same provision later or right to enforce any other provisions of this CPS. To be effective any waivers must be in writing and signed by Multicert.

9.16.5 Force Majeure

Force majeure clauses are included in the General Terms and Conditions of Digital Certificate Issuance.

9.17 Other Provisions

No Stipulation.

Approval

Nuno Ponte (Management Working Group)

[Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte

Digitally signed by [Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte
Date: 2020.12.17 19:45:27 Z