CERTIFICATION PRACTICE STATEMENT (CPS)

DIGITALSIGN

VERSION 1.4

Language: English
Date: 29/04/2021

Control changes

Version	Date	Changes
1.0	25/11/2015	Initial CPS version
1.1	20/07/2017	Revision to include additional 2nd level CAs
1.2	01/02/2019	Revision
1.3	01/02/2020	Revision
1.4	29/04/2021	Revision

TABLE OF CONTENTS

1 INTRODUCTION 9
1.1 Overview 9
1.1.1 Hierarchies 10
1.2 Document Name and Identification 12
1.3 PKI Participants 12
1.3.1 Certification Authority (CA) 12
1.3.2 Registration Authority (RA) 13
1.3.3 Signatory/Subscriber 13
1.3.4 Relaying Parties 13
1.3.5 Other Participants 13
1.4 Certificate Usage 14
1.4.1 Appropriate Certificate Uses 14
1.4.2 Prohibited and Unauthorized Use 14
1.5 Policy Administration 15
1.5.1 Organization Administering the Document 15
1.5.2 Contact Person 15
1.5.3 Person Determining CPS Suitability For The Policy 15
1.5.4 CPS Approval Procedures 15
1.6 Definitions and Acronyms 16
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 17
2.1 Repository 17
2.2 Publication of Certificate Information 17
2.2.1 Certification Policies and Practices 17
2.2.2 Terms and Conditions 17
2.2.3 Distribution of the Certificates 17
2.3 Publication Frequency 17
2.4 Access Control 17
3 IDENTIFICATION AND AUTHENTICATION 18
3.1 Naming 18
3.1.1 Types of Names 18
3.1.2 Need for Names to be Meaningful 18
3.1.3 Pseudonyms 18
3.1.4 Rules Used to Interpret Several Name Formats 18
3.1.5 Uniqueness of Names 18
3.1.6 Recognition, Authentication and Role of Trademarks and Other Distinctive Symbols 18
3.1.7 Name Dispute Resolution Procedure 18
3.2 Initial Identity Validation 19
3.2.1 Methods to prove ownership of private key 19
3.2.2 Authentication of Organization Identity 19
3.2.3 Authentication of the Identity of an individual, the entity and their relationship 20
3.2.4 Non-verified Subscriber Information 20
3.2.5 Validation of Authority 20
3.2.6 Criteria for interoperation 20
3.3 Identification and Authentication for Re-Key Requests 20
3.3.1 Identification and Authentication for Re-Key After Revocation 21
3.4 Identification and Authentication for Revocation Request 21

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 22
4.1 Certificate Application 22
4.1.1 Who Can Submit a Certificate Application 22
4.1.2 Enrollment Process and Responsibilities 22
4.2 Certificate Application Processing 22
4.2.1 Performing Identification and Authentication Functions 22
4.2.2 Approval or Rejection of Certificate Applications 22
4.2.3 Time to Process Certificate Applications 23
4.3 Certificate Issuance 23
4.3.1 CA Actions During Certificate Issuance 23
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 23
4.4 Certificate Acceptance 23
4.4.1 Conduct Constituting Certificate Acceptance 23
4.4.2 Publication of the Certificate by the CA 24
4.4.3 Notification of the Issuance to Other Entities 24
4.5 Key Pair and Certificate Usage 24
4.5.1 Subscriber Private Key and Certificate Usage 24
4.5.2 Relying Party Public Key and Certificate Usage 24
4.6 Certificate Renewal 24
4.7 Certificate Re-Key 24
4.7.1 Circumstance for Certificate Re-Key 24
4.7.2 Who May Request Certification of a New Public Key 24
4.7.3 Processing Certificate Re-Key Requests 24
4.7.4 Notification of New Certificate Issuance to Subscriber 24
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 25
4.7.6 Publication of the Re-Keyed Certificate by the CA 25
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 25
4.8 Certificate Modification 25
4.9 Certificate Revocation and Suspension 25
4.9.1 Circumstances for Revocation 25
4.9.2 Who Can Request Revocation 26
4.9.3 Procedure for Revocation Request 27
4.9.4 Revocation Request Grace Period 27
4.9.5 Time Within Which CA Must Process the Revocation Request 27
4.9.6 Revocation Checking Requirement for Relying Parties 27
4.9.7 CRL issuance frequency 27
4.9.8 Maximum Latency for CRLs 27
4.9.9 On-line Revocation/Status Checking Availability 27
4.9.10 On-line Revocation Checking Requirements 28
4.9.11 Other Methods of Disclosing Revocation Information 28
4.9.12 Special Revocation Requirements due to Compromised Key Security 28
4.9.13 Circumstances for Suspension 28
4.9.14 Who Can Request Suspension 28
4.9.15 Procedure for Suspension Request 28
4.9.16 Limits on Suspension Period 28
4.10 Certificate Status Services 28
4.10.1 Operational Characteristics 28
4.10.2 Service Availability 28
4.10.3 Optional Features 28
4.11 End of Subscription 29
4.12 Key Escrow and Recovery 29

4.12.1 Key Escrow and Recovery Policy and Practices 29
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 29

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 30
5.1 Physical Security Controls 30
5.1.1 Site Location and Construction 30
5.1.2 Physical access 30
5.1.3 Power and Air Conditioning 31
5.1.4 Water Exposure 31
5.1.5 Fire Prevention and Protection 31
5.1.6 Media Storage 31
5.1.7 Waste Disposal 31
5.1.8 Off-Site Backup 31
5.2 Procedural controls 31
5.2.1 Trust Roles 31
5.2.2 Number of People Required per Task 31
5.2.3 Identification and Authentication for Each Role 31
5.2.4 Roles requiring separation of duties 32
5.3 Personnel Controls 32
5.3.1 Background, Qualifications, Experience and Clearance Requirements 32
5.3.2 Background Check Procedures 32
5.3.3 Training Requirements 32
5.3.4 Retraining Frequency and Requirements 32
5.3.5 Job Rotation frequency and Sequence 32
5.3.6 Sanctions for Unauthorized Actions 32
5.3.7 Contract Personnel Requirements 32
5.3.8 Documentation Supplied to Personnel 32
5.4 Audit Logging Procedures 33
5.4.1 Types of Events Recorded 33
5.4.2 Frequency of Processing Log 33
5.4.3 Retention Period for Audit Log 33
5.4.4 Protection of Audit Log 33
5.4.5 Audit Log Backup Procedures 34
5.4.6 Audit Collection System 34
5.4.7 Notification to Event-Causing Subject 34
5.4.8 Vulnerability Assessments 34
5.5 Records Archival 34
5.5.1 Type of Records Archived 34
5.5.2 Retention Period for Archive 34
5.5.3 Protection of Archive 34
5.5.4 Archive Backup procedures 35
5.5.5 Requirements for Time-stamping of Records 35
5.5.6 Archive Collection System (Internal or External) 35
5.5.7 Procedures to Obtain and Verify Archive Information 35
5.6 Key Changeover 35
5.7 Compromise and Disaster Recovery 35
5.7.1 Incident and Compromise Handling Procedures 35
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 35
5.7.3 Entity Private Key Compromise Procedures 36
5.7.4 Business Continuity Capabilities After a Disaster 36
5.8 CA or RA Termination 36

6 TECHNICAL SECURITY CONTROLS 37

6.1 Key Pair Generation and Installation 37
6.1.1 Key Pair Generation 37
6.1.2 Private Key Delivery to Subscriber 37
6.1.3 Public Key Delivery to Certificate Issuer 37
6.1.4 CA Public Key Delivery to Relaying Parties 37
6.1.5 Key Sizes 37
6.1.6 Public Key Parameters Generation and Quality Checking 37
6.1.7 Key Usage Purposes 37
6.2 Private Key Protection and Cryptographic Module Engineering Controls 38
6.2.1 Cryptographic Module Standards and Controls 38
6.2.2 Private Key (n out of m) Multi-Person Control Key 39
6.2.3 Private Key Escrow 39
6.2.4 Private Key Backup 39
6.2.5 Private Key Archival 39
6.2.6 Private Key Transfer Into or From a Cryptographic Module 39
6.2.7 Private key Storage on Cryptographic Module 39
6.2.8 Method of Activating Private Key 39
6.2.9 Method of Deactivating Private Key 40
6.2.10 Method of Destroing Private Key 40
6.2.11 Cryptographic Module Rating 40
6.3 Other Aspects of Key Pair Management 40
6.3.1 Public Key Archival 40
6.3.2 Certificate operational periods and key pair usage periods 40
6.4 Activation Data 40
6.4.1 Activation Data Generation and Installation 40
6.4.2 Activation Data Protection 41
6.4.3 Other Aspects of Activation Data 41
6.5 Computer security controls 41
6.5.1 Specific Computer Security Technical Requirements 41
6.5.2 Computer Security Rating 42
6.6 Life Cycle Technical Controls 42
6.6.1 System Development Controls 42
6.6.2 Security management controls 42
6.6.3 Life cycle security evaluation 44
6.7 Network Security Controls 44
6.8 Time-Stamping 44
7 CERTIFICATE AND CRL PROFILE 45
7.1 Certificate Profile 45
7.1.1 Version number 45
7.1.2 Certificate extensions 45
7.1.3 Algorithm object identifiers (OID) 48
7.1.4 Name Format 48
7.1.5 Name restrictions 48
7.1.6 Certification Policy (OID) object identifier 48
7.1.7 Usage of Policy Constraints extension 48
7.1.8 Policy qualifiers syntax and semantics 49
7.1.9 Processing semantics for the critical Certificate Policies extension 49
7.2 CRL Profile 49
7.2.1 Version number 49
7.2.2 CRL and extensions 49

7.3 OCSP Profile 49
7.3.1 OCSP responder certificate profile 49
7.3.2 Version number 49
7.3.3 Name formats 49
7.3.4 Certification Policy Object Identifier (OID) 50
7.3.5 OCSP Certificate extensions and fields 50
7.3.6 OCSP request format 50
7.3.7 Response format 50

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 52
8.1 Frequency and Circumstances of Assessment 52
8.2 Identity/Qualifications of Assessor 52
8.3 Assessor's Relationship to Assessed Entity 52
8.4 Topics Covered by Assessment 52
8.5 Actions Taken as a Result of Deficiency 52
8.6 Communication of Results 53

9 OTHER BUSINESS AND LEGAL MATTERS 54
9.1 Fees 54
9.1.1 Certificate Issuance or Renewal fees 54
9.1.2 Certificate Access Fees 54
9.1.3 Revocation or Status Information Access Fees 54
9.1.4 Fees for Other Services 54
9.1.5 Refund policy 54

9.2 Financial Responsibility 54
9.2.1 Insurance Coverage 54
9.2.2 Other Assets 54
9.2.3 Insurance or Warranty Coverage for End-Entities 54

9.3 Confidentiality of Business Information 55
9.3.1 Scope of Business Information 55
9.3.2 Information Not Within the Scope of Confidential Information 55
9.3.3 Responsibility to Protect Confidential Information 55

9.4 Privacy of Personal Information 55
9.4.1 Privacy Plan 55
9.4.2 Information Treated as Private 55
9.4.3 Information not Deemed Private 55
9.4.4 Responsibility to Protect Private Information 56
9.4.5 Notice and Consent to Use Private Information 56
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 56
9.4.7 Other Information Disclosure Circumstances 56

9.5 Intellectual Property Rights 56
9.6 Representations and Warranties 56
9.6.1 CA Representations and Warranties 56
9.6.2 RA Representations and Warranties 57
9.6.3 Subscriber Representations and Warranties 57
9.6.4 Relying Party Representations and Warranties 57
9.6.5 Representations and Warranties of Other Participants 57

9.7 Disclaimers of Warranties 58
9.8 Limitations of Liability 58
9.9 Indemnities 59
9.10 Term and Termination 59
9.10.1 Term 59
9.10.2 Termination 59

9.10.3 Effect of Termination and Survival 59
9.11 Individual Notices and Communications With Participants 59
9.12 Amendments 59
9.12.1 Procedures for Amendments 59
9.12.2 Notification Mechanism and Period 59
9.12.3 Circumstances Under Which OID Must be Changed 60
9.13 Dispute Resolution Procedure 60
9.14 Governing Law 60
9.15 Compliance With Applicable Law 60
9.16 Miscellaneous Provisions 60
9.16.1 Entire Agreement 60
9.16.2 Assignment 60
9.16.3 Severability 60
9.16.4 Enforcement 60
9.16.5 Force Majeure 60
9.17 Other provisions 61
9.17.1 Publication and Copy of the policy 61
9.17.2 CPS Approval Procedures 61

1 INTRODUCTION

1.1 Overview

Given that there is no specific definition of the concepts of Certification Practice Statement and Certification Policies, and due to some confusion that has arisen, DIGITALSIGN would like to explain its stance in relation to these concepts.

Certification Policy (CP): a set of rules defining the applicability of a certificate in a community and/or in an application, with common security and usage requirements. In other words, a Certification Policy must generally define the applicability of certificate types for certain applications that establish the same security and usage requirements.

Certification Practice Statement (CPS): defined as a set of practices adopted by a Certification Authority for the issue of certificates. It usually contains detailed information on its certificate security, support, administration and issuing system, as well as the trust relationship between the Signatory/Subscriber or Trusting Third Party and the Certification Authority. These may be completely comprehensible and robust documents which provide an accurate description of the services offered, detailed certificate life cycle management procedures, and so on.

These Certification Policies and Certification Practice Statement concepts are different, although they are still closely interrelated.

A detailed Certification Practice Statement is not an acceptable basis for the interoperability of Certification Authorities. On the whole, Certification Policies are a better basis for common security standards and criteria.

In summary, a Policy defines "what" security requirements are required for the issue of certificates. The Certification Practice Statement defines "how" the security requirements established in the Policy are fulfilled.

In order to simplify the documentation and ease of understanding, the Certificate Policies are integrated in this Certification Practice Statement document.

This document specifies the Certification Practice Statement (hereinafter, CPS) and the Certificate Policies that DIGITALSIGN has established for the issue of certificates and is based on the following standards specification:

- RCF 3647 – Internet X. 509 Public Key Infrastructure Certificate Policy, de IETF,
- RFC 3739 3039 of IETF Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.
- RFC 5280, RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL).
- ETSI TS 101 456 VI.2.1 Policy requirements for certification authorities issuing qualified certificate
- ETSI TS 102 042 VI. 1.1 Policy requirements for certification authorities issuing public key certificate
- ETSI TS 102 023 VI.2.1 Policy requirements for time-stamping authorities. Technically equivalent to RFC 3628
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates VI
- CA/Browser Forum EV SSL Certificate Guidelines V 1.3

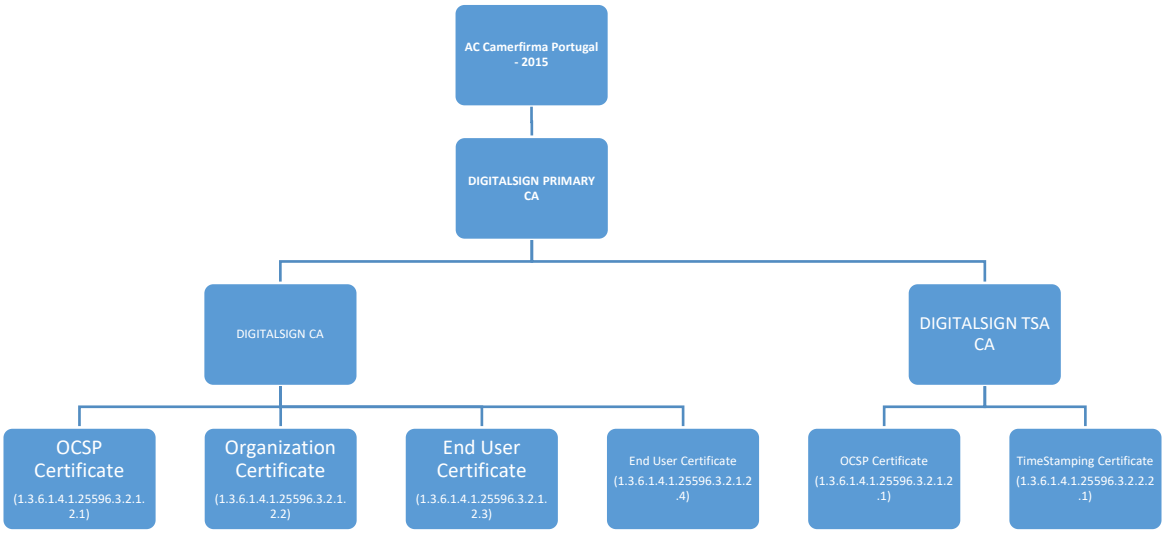
The recommendations in the technical document Security CWA 14167-1 Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

This CPS contains the Certification Policies for the different certificates that DIGITALSIGN issues, which are established in section 1.1.1 of this CPS.

1.1.1 Hierarchies

This section describes the hierarchies that DIGITALSIGN manages and is governed by this CPS.

DIGITALSIGN is part of the certification hierarchy of Spanish Certification Authority AC Camerfirma SA, which is composed of several Certification Authorities.



1.1.1.1 Root Certification Authority

It is called Root Certification Authority (CA or Root) the Certification entity within the hierarchy that issues certificates to other Certification Authorities, whose public key certificate was self-signed. Its function is to sign the certificate to the other AC belonging to the Certification Hierarchy. The identification data of the current root CA is detailed next:

- CN: *Global Chambersign Root - 2008*
- SHA1 hash: *4ABD EEEC 950D 359C 89AE C752 A12C 5B29 F6D6 AA0C*
- SHA256
- Valid from: *August 01st, 2008*
- Valid until: *July 31st, 2038*
- RSA key length: *4096 bits*

In the present case, the Root Certification Authority hierarchy includes a sub-CA of AC Camerfirma SA that issued the Level 1 Intermediate Certification Authority, as detailed next:

- CN: *AC Camerfirma Portugal - 2015*
- SHA1 hash: *A7C1 5282 FCC6 CD5A 12A2 2002 030E 2AB6 3C6A 9188*
- SHA256

- Valid from: *November 17th, 2015*
- Valid until: *November 21st, 2037*
- RSA key length: *4096 bits*

This hierarchy (Chambersign Global ROOT (JCS) 1.3.6.1.4.1.17326.10.1.1 and AC Camerfirma Portugal) is created by AC Camerfirma SA to issue certificates on specific projects with entities such as DIGITALSIGN.

1.1.1.2 Level 1 Intermediate Certification Authority

It is called Level 1 Intermediate or Subordinate Certification Authority the Certification entity within the hierarchy that issues Level 2 Intermediate Certificates and its public key certificate has been digitally signed by the Root Certification Authority.

In the present case, the identification data of the current Level 1 Intermediate Certificate managed by AC Camerfirma SA through which issues Level 2 Intermediate Certificates are detailed next:

- CN: *DIGITALSIGN PRIMARY CA*
- SHA1 hash: *9723 B18A 9F6F E78E 675D 726B 9558 5458 5641 4622*
- SHA512
- Valid from: *November 25th, 2015*
- Valid until: *November 9th, 2037*
- RSA key length: 4096 *bits*

1.1.1.3 Level 2 Intermediate Certification Authority

It is called Level 2 Intermediate or Subordinate Certification Authority the Certification entity within the hierarchy that issues end-user entity certificates and its public key certificate has been digitally signed by the Level 1 Intermediate Certification Authority mentioned above.

DIGITALSIGN PRIMARY CA, covered by this CPS, has two Level 2 Intermediates Certification Authorities, which the most relevant information are:

Level 2 Intermediate 1

- CN: DIGITALSIGN CA
- SHA1 hash: *F3B9 A546 D300 6FBA 67C9 F271 6F39 4AB7 B05C DC18*
- SHA512
- Valid from: *November 25th, 2015*
- Valid until: *October 30th, 2037*
- RSA key length: 4096 *bits*

Level 2 Intermediate 2

- CN: DIGITALSIGN TSA CA
- SHA1 hash: *2214 7178 FE6E F569 BC0D A584 15CA FEB7 15D4 4157*
- SHA512
- Valid from: *November 25th, 2015*
- Valid until: *October 30th, 2037*
- RSA key length: 4096 *bits*

DIGITALSIGN PRIMARY CA may have additional Level 2 Intermediate Certification Authorities governed by specific CPS.

1.1.1.4 End-user certificates

DIGITALSIGN issues a series of digital certificates in order to meet the needs of its customers, according to their business lines through their Level 2 Intermediates Certification Authorities indicated in the previous section. End-user Digital Certificates issued by the DIGITALSIGN are:

Level 2 Intermediate 1 (CN: *DIGITALSIGN CA)* issued certificates:

OCSP Certificate - OID: 1.3.6.1.4.1.25596.3.2.1.2.1
Certificate to be used by OCSP Responder

Organization Certificate - OID: 1.3.6.1.4.1.25596.3.2.1.2.2
Certificate to be used for signature by organizations

End User Certificate - OID: 1.3.6.1.4.1.25596.3.2.1.2.3
End-user issued certificates

End User Certificate - OID: 1.3.6.1.4.1.25596.3.2.1.2.4
End-user issued certificates

Level 2 Intermediate 2 (CN: *DIGITALSIGN TSA CA)* issued certificates:

OCSP Certificate - OID: 1.3.6.1.4.1.25596.3.2.1.2.1
Certificate to be used by OCSP Responder

TimeStamp Certificate - OID: 1.3.6.1.4.1.25596.3.2.2.2.1
Certificate to be used by TimeStamping Authorities (TSA)

As regards the contents of this CPS, it is assumed the reader is familiar with the basic concepts of PKI, certification and digital signing. Should the reader not be familiar with these concepts, he/she is advised to gain some background knowledge on these concepts. The DIGITALSIGN web site http://www.digitalsign.pt provides general information about using digital signatures and digital certificates.

1.2 Document Name and Identification

Document name:	Certification Practices Statement (CPS)
Version:	1.4
OID:	1.3.6.1.4.1.25596.3.1.1
Issue date:	29/04/2021
Expiration date:	Non-applicable
Localization:	http://www.digitalsign.pt/repository/
Web site	http://www.digitalsign.pt

1.3 PKI Participants

1.3.1 Certification Authority (CA)

This is the entity responsible for issuing and managing digital certificates. It acts as the trusted third party between the Signatory (Subscriber) and the trusting third party in electronic transactions, linking a specific public key with a person.

For the purpose of this CPS, the Certification Authority is managed by AC Camerfirma SA while Level 2 Intermediate Certification Authorities are managed by DIGITALSIGN.

Information related to the CA is available on Camerfirma's web site http://www.camerfirma.com and on the DIGITALSIGN's web site indicated in section 1.2.

1.3.2 Registration Authority (RA)

A Registration Authority (RA) is responsible for managing the requests, identification and registration of Certificate applicants, and any specific responsibilities established in this CPS. RAs are authorities delegated by the CSP, although the CSP is ultimately responsible for the service. The CSP can carry out the RA's work at any time.

For the purpose of this CPS, the following can act as RAs:

- The Certification Service Provider (DIGITALSIGN).
- Any national or international agent who has a contractual relationship with the CSP and has passed the registration and audit processes established by the CSP.

1.3.3 Signatory/Subscriber

Signatory/Subscriber refers to the certificate holder, whether this is an individual or company. When it is issued in the name of a hardware device or software application, the individual/company requesting the issued certificate will be considered the Signatory/Subscriber.

Before the certificate is issued, the signatory/subscriber is considered the applicant.

1.3.4 Relaying Parties

In this CPS, the Relaying Party (Trusting Third Party) or user is the person receiving an electronic transaction carried out with any of the certificate issued by DIGITALSIGN and who voluntarily trusts the Certificate that this CA issues.

1.3.5 Other Participants

1.3.5.1 Certification Service Provider (CSP)

This CPS defines a Certification Service Provider (CSP) as an entity that provides the specific services relating to the certificate life cycle and can manage one or more Certification Authorities and related services, such as issuing time stamps, providing signature devices or validation services.

For the purpose of this CPS, DIGITALSIGN is the CSP.

1.3.5.2 Entity

The Entity is the company or organization with which the Signatory/Subscriber has a certain relationship, as defined in the ORGANIZATION field in each certificate. And so:

- In Individual relationship certificates, the Entity is linked to the Signatory/Subscriber via a contractual relationship (labour, mercantile, as a member of professional body, etc.).
- In Powers of Representation certificates, the Entity is represented by the Signatory/Subscriber who has broad powers of representation.
- In Special Power of Attorney certificates, the Entity is represented by the Signatory/Subscriber in specific procedures.
- In Electronic invoicing certificates, the Entity authorizes the Signatory/Subscriber to issue electronic invoices.
- In Secure Server/Corporate Digital Seal certificates, the Entity owns the Internet domain or software for which the certificate has been requested.

- In CodeSign certificates, the entity linked to the procedure for which the signature is given.

As a general rule, the Entity is identified in the organization field in the certificate and its tax identification number is entered in a field for this purpose in the certificate.

1.3.5.3 Applicant

Applicant refers to the individual requesting the Certificate from the DIGITALSIGN CSP, either directly or via an authorized representative. Once the certificate has been issued, the applicant is considered the Signatory/Subscriber.

1.3.5.4 Person Responsible for Certificates

This CPS considers the certificate holder (the signatory/subscriber) to be the person responsible for certificates issued to individuals.

The CPS considers the individual making the request (the applicant) to be responsible for certificates issued to companies. This person must be identified in the certificate, even if the request is made via a third party. For certificates that contain powers of representation, this CPS considers both the Signatory/Subscriber and the represented person/Company to be the responsible party.

For component certificates, this CPS considers the individual making the request on their own behalf or via a third party to be the responsible party.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

This CPS fulfils and includes the Certification Policies described in section 1.1.1 of this CPS.

DIGITALSIGN certificates can be used in accordance with Portuguese legislation and this CPS. In particular, the certificates can only be used for the purposes for which they were issued and subject to the certificate standard fields “key usage” and “extended key usage” and whenever they not violate the prohibited and unauthorized use.

1.4.2 Prohibited and Unauthorized Use

The certificates can only be used for the purposes for which they were issued and are subject to the established limits defined in the Certification Policies included in this CPS.

The use of digital certificates in transactions that contravene the Certification Policies applicable to each of the Certificates, the CPS or the Contracts that the CAs sign with the RAs or Signatories/Subscribers will be considered illegal, and the CA will be exempt from any liability due to the signatory or third party’s misuse of the certificates in accordance with current law.

DIGITALSIGN does not have access to the data for which a certificate is used. Therefore, due to lack of access to the message contents, DIGITALSIGN cannot issue any appraisal regarding these contents and the signatory is consequently responsible for the data for which the certificate is used. The signatory will also be responsible for the consequences of any use of this data in breach of the limitations and terms and conditions established in the Certification Policies applicable to each Certificate, the CPS and the contracts the CAs sign with the Signatories, as well as any misuse thereof in accordance with this paragraph or which could be interpreted as such by virtue of current law.

DIGITALSIGN includes information in the certificate regarding usage restrictions, either in standard fields, under “key usage” and “basic constraints”, highlighted as critical in the certificate and therefore binding on any application using it, or via text included in the field such as “user notice”, which is “not critical” but binding on the certificate holder and user.

1.5 Policy Administration

DIGITALSIGN is obliged to fulfil the requirements established within current Portuguese law as the trading company providing digital certification services (hereinafter, regulations or current law).

The Certification Authority's activity may be subject to inspection by the Policy Authority (PA) or anyone appointed by it.

1.5.1 Organization Administering the Document

For the hierarchies described herein, the Policy Authority falls to DIGITALSIGN's legal department.

DIGITALSIGN's legal department therefore constitutes the Policy Authority for the Hierarchies and Certification Authorities described above and is responsible for managing the CPS.

You can contact the Policy Authority (PA) at:

Name:	Legal department of DIGITALSIGN
e-Mail:	cps@digitalsign.pt
Address:	Largo Padre Bernardino Ribeiro Fernandes, 26 4835-489 Nespereira GMR PORTUGAL
Telephone:	+351 253560650
Fax:	+351 253560639
URL	https://www.digitalsign.pt

1.5.2 Contact Person

This CPS is managed by the Policy Authority as described and can be contacted by the ways exposed there.

Additionally, you may contact the Technical Department for those technical issues regarding the management of the certificates that can not been solved by the Policy Authority.

Name:	Technical department of DIGITALSIGN
e-Mail:	dsi@digitalsign.pt
Address:	Largo Padre Bernardino Ribeiro Fernandes, 26 4835-489 Nespereira GMR PORTUGAL
Telephone:	+351 253560650
Fax:	+351 253560639
URL	http://www.digitalsign.pt

1.5.3 Person Determining CPS Suitability For The Policy

The legal department of DIGITALSIGN is therefore constituted in the Policy Authority (PA) of the Hierarchies and Certification Authorities described above being responsible for the administration of the CPS.

1.5.4 CPS Approval Procedures

The publication of the revisions of this CPS must be approved by the Management of DIGITALSIGN.

DIGITALSIGN publishes every new version on its website. The CPS is published in PDF format.

1.6 Definitions and Acronyms

CA	Certification Authority
DIGITALSIGN	DigitalSign – Certificadora Digital, SA
CPS	Certification Practices Statement
CP	Certificate Policies
PKI	Public Key Infrastructure
OID	Unique number of "object identifier"
RA	Registration Authority
CRL	Certificate Revocation List
OCSP	Online Status Certificate Protocol
FIPS	United State Federal Information Processing Standards
HSM	Hardware Security Module
PKCS	Public-Key Cryptography Standard
RFC	Request for comment
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Sockets Layer

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repository

This CPS that includes the Certificate Policies is available to the public on the DIGITALSIGN web site indicated in section 1.2.

2.2 Publication of Certificate Information

DIGITALSIGN provides a service for consulting issued certificates and revocation lists. These services are available to the public on its web site.

This information is stored in a relational database with integrity and access measures to ensure it is stored in accordance with the Certification Policy requirements.

DIGITALSIGN publishes the issued certificates, revocation lists, and certification policies and practices at no cost.

2.2.1 Certification Policies and Practices

This CPS that includes the Certificate Policies is available to the public on the DIGITALSIGN web site indicated in section 1.2.

2.2.2 Terms and Conditions

Users can find the service terms and conditions in DIGITALSIGN either via the physical contract in the certificate issuing process or in its web site indicated in section 1.2.

2.2.3 Distribution of the Certificates

The issued certificates can be accessed as long as the Signatories/Subscribers provide their consent on the web site indicated in section 1.2.

The Root keys and the Level 1 Intermediate keys in the Camerfirma hierarchies can be downloaded from http://www.camerfirma.com. The Level 2 Intermediate keys can be downloaded from the DIGITALSIGN web site indicated in section 1.2.

The end-user certificates can be viewed from a secure web site through the customer area or similar. This consultation service is therefore not free-of-charge, and the mass download of certificates is prohibited.

2.3 Publication Frequency

DIGITALSIGN publishes the certificates immediately after they have been issued, provided the Signatories/Subscribers have given their approval.

DIGITALSIGN immediately publishes any changes to the Policies and CPS on its web site indicated in section 1.2, where it maintains a version log.

2.4 Access Control

DIGITALSIGN publishes certificates and CRLs on its web site. It is required authentication to access the certificate directory to eliminate the possibility of mass searches and downloads.

Access to revocation information and certificates issued by DIGITALSIGN is free-of-charge.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The naming follows the applicable law. For certificates issued to individuals and organizations it is assigned its real name.

3.1.1 Types of Names

The Signatory/Subscriber is described in the certificates by a DN (distinguished name) in accordance with the X.500 standard.

3.1.2 Need for Names to be Meaningful

All Distinguished Names must be meaningful, and the identification the attributes associated to the subscriber should be in a human readable form.

3.1.3 Pseudonyms

The acceptance or not of pseudonyms is dealt with in each certification policy as described in section 3.1.1. If they are allowed, DIGITALSIGN will use the Pseudonym with the CN attribute of the Signatory/Subscriber's name, keeping the Signatory/Subscriber's real identity confidential.

The calculation of the pseudonym in certificates in which it is allowed is done so that it unmistakably identifies the real certificate holder, attaching an organization acronym to the certificate serial number.

3.1.4 Rules Used to Interpret Several Name Formats

DIGITALSIGN complies with the ISO/IEC 9594 X.500 standard.

3.1.5 Uniqueness of Names

The DN attribute is constructed such that it is not possible for two subscribers to have the same DN. Thus it is not possible to assign a DN to a different existing subscriber.

3.1.6 Recognition, Authentication and Role of Trademarks and Other Distinctive Symbols

Entities requesting certificates must demonstrate the right to use of the requested name. The designations used on the certificates issued by DIGITALSIGN can not infringe intellectual property rights of others.

In the procedure of identification and authentication of the certificate holder, prior to the issuing of the same, the entity requesting the certificate will have to present legal documents that demonstrate the right to the use of the requested name.

3.1.7 Name Dispute Resolution Procedure

DIGITALSIGN is not liable in the case of name dispute settlement. In any case, names will be assigned in accordance with the order in which they are input and after checking the documentation required for each type of certificate.

DIGITALSIGN shall not arbitrate this type of dispute, which the parties must settle directly between themselves.

3.2 Initial Identity Validation

3.2.1 Methods to prove ownership of private key

DIGITALSIGN uses various circuits for the issue of certificates in which the private key is managed differently. Either the user or the CA can create the private key.

The key creation method used is shown in the certificate, through the Policy ID and the Description attribute in the certificate DN field. These codes are described in the Policies.

Keys created by DIGITALSIGN

In the case that the keys are generated by DIGITALSIGN, mechanisms to ensure that only the Subscriber is in possession of the private key are used.

In the event that keys are generated in a secure sign cryptographic device (SSCD), private keys can not be removed from the cryptographic chip and the card is protected by PIN owned by the subscriber.

Keys created by Subscriber

In those cases where the subscriber generates its key pair, it is considered that the subscriber has a key generation mechanism either software or hardware, Proof of ownership of the private key in this case is the request that DIGITALSIGN receives in PKCS#10 format. (Public key signed by the private key).

When the subscriber creates its own keys in a cryptographic device and asks DIGITALSIGN to issue a digital certificate with a key creation policy on a hardware device, it is ensured (through technical process or an auditor declaration) that the keys actually have been generated in a hardware device as the issued certificate will tell.

DIGITALSIGN reserves the right to consider the external auditor's guarantee as valid, or to reject it.

3.2.2 Authentication of Organization Identity

The process of authenticating the identity of a legal person shall ensure that the legal person who is going to be issued the certificate exists, and this verification is carried out by consulting the official documentation.

Any additional information included in the DN is verified and authenticated by the validation services.

To properly identify the identity of the organization, DIGITALSIGN establishes some requirements:

OCSP Certificate – OID: 1.3.6.1.4.1.25596.3.2.1.2.1

These certificates are intended to be used by OCSP responder applications. In the vetting process is request the commercial registration of the company and a form duly signed by the general manager taking responsibility for the certificate.

Organization Certificate – OID: 1.3.6.1.4.1.25596.3.2.1.2.2

These certificates are intended to be used by organization applications. In the vetting process is request the commercial registration of the company and a form duly signed by the general manager taking responsibility for the certificate.

TimeStamp Certificate – OID: 1.3.6.1.4.1.25596.3.2.2.2.1

These certificates are intended to be used by TimeStamp Authorities applications (TSA). In the vetting process is request the commercial registration of the company and a form duly signed by the general manager taking responsibility for the certificate.

3.2.3 Authentication of the Identity of an individual, the entity and their relationship

To properly identify the identity of the Applicant, DIGITALSIGN establishes some requirements:

End User Certificate – OID: 1.3.6.1.4.1.25596.3.2.1.2.3

Every issued certificate requires identity verification of the certificate owner. The vetting process is:

i. Enroll in the website to request a certificate
ii. Fill a form with their personal data
iii. Print the form and sign it
iv. Recognize the signature on a notary, lawyer or similar
v. Send the notarize document by mail
vi. The cryptographic keys and certificate are issued and stored inside the HSM
vii. End user will be sent the credentials that allows him to activate/use the certificate for each signature performed

Alternatively, this vetting process can be achieved through online ID checking.

End User Certificate – OID: 1.3.6.1.4.1.25596.3.2.1.2.4

The identity of the certificate owner is verified by consulting a database provided by an entity that has collected that information in the physical presence or equivalent of the owner.

This verification can be done automatically or by a RA agent.

3.2.4 Non-verified Subscriber Information

All the information included in the DN is checked and authenticated by the validation services

3.2.5 Validation of Authority

All information relating to powers of attorney and / or affiliation of an individual to the corresponding company or organization is verified.

3.2.6 Criteria for interoperation

DIGITALSIGN does not provide interoperation services that permit an external CA to interoperate with the CAs governed by this CPS by unilaterally certifying that CA.

The interoperability between CAs governed by this CPS is guaranteed by its own trust hierarchy, being the root automatically available by the overwhelming majority of browsers, equipment and other software existing globally.

3.3 Identification and Authentication for Re-Key Requests

Identification and Authentication for Routine Re-Key DIGITALSIGN always issues new keys to renew certificates. The process is therefore the same as the one followed to make a new request.

DIGITALSIGN notifies, via email or other means, the subscriber that the certificate is about the expire, suggesting renewal thereof. If the active certificate to be renewed expires before the renewal takes place, a new certificate must be issued.

The renewal process can be initiated from the DIGITALSIGN web site.

The application allows the subscriber to change the email address assigned to the certificate. If other information included in the certificate has changed, the certificate must be revoked and a new one issued.

3.3.1 Identification and Authentication for Re-Key After Revocation

Once a certificate has been rendered invalid, it cannot be renewed automatically. The applicant must start a new issuance procedure.

When the renewal takes place due to certificate replacement or an issuing error, renewal is possible following a revocation. As long as the current situation is shown, the supporting documentation submitted to issue the replaced certificate will be reused and the physical presence will no longer be required, if this were necessary due to the type of certificate.

3.4 Identification and Authentication for Revocation Request

Revocation requests can be performed through customer area in the website, or by filling and signing a revocation request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Requests for Certificates Applications may be submitted by:

- An individual who is the holder of the certificate
- A representative of the certificate holder, duly authorized and empowered to the effect
- A legal person who is the holder of the certificate
- A representative of DIGITALSIGN
- An authorized representative of an RA

4.1.2 Enrollment Process and Responsibilities

Certificate requests are submitted via the application forms at website.

The web site contains the forms required to request each type of certificate that DIGITALSIGN distributes in different format and the signature creation devices, if necessary.

When the applicant creates the keys, the certificates are requested by submitting a standard PKCS#11 or CSR certificate issuance request together with the additional request information.

For each type of certificate, the subscriber must accept the terms and conditions of use between the subscriber, the registration authority and the certification authority. This is carried out by signing a contract or accepting the terms and conditions displayed on a web site before creating and downloading the certificate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

DIGITALSIGN, or a RA, must perform the identification and authentication of all requests, in accordance with Section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

DIGITALSIGN, or a RA , will approve the certificate requests if the following criteria are met:

- Successful identification and authentication of all information, in accordance with Section 3.2
- Once the payment is made or approved.

DIGITALSIGN, or a RA, reject the request for a certificate if any of the following situations occur:

- The identification and authentication, in accordance with Section 3.2, is not complete
- The subscriber does not deliver any supporting documentation requested
- The subscriber does not respond to notification within a specified time
- Payment is not received/approved
- The RA believes that issuing a certificate to the subscriber may bring discredit to the PKI chain and DigitalSign itself.

4.2.3 Time to Process Certificate Applications

DIGITALSIGN begins processing requests after receipt of the required documentation. There is no stipulated time to complete the process, unless otherwise is stated in the relevant subscriber agreement, CPS or other agreement between the participants. A request remains active until it is rejected.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

A certificate is created and issued following the approval of a certificate request for any of the RA. DigitalSign creates and sends, or makes it available in the used application, to the certificate applicant (or his representative) a certificate based on the information received, supported in legal documents and following the approval by the RA.

Each issued certificate begins its term (validity) at the time of issue.

Certificates may also be requested in batch processes. These batches are delivered to the RA, and are then entered into the management platform. Once the RA operator has compiled the documentation and checked the identity, he/she validates the certificates one-by-one or in batches.

For technical certificates (Corporate Seal, Secure Server and Code Sign) no physical presence is required for issuance. The documentation just needs to be sent to the RA office. Once the documentation has been checked and payment approved, if applicable, DIGITALSIGN issues a certificate.

In accordance with the specific policies for EV secure server certificates, these certificates require the physical presence of the applicant or an approved third party. The RA manager verifies the service payment, the related documentation and the Signatory/Subscriber's identity.

Certification policies for issuing SSL EV certificates to which this CPS is subject ("CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates") require that each EV certificate issue request be approved by two different people.

The subscriber can use their own resources to create the keys in cryptographic device and deliver the request to DIGITALSIGN in PKCS10 format to issue the certificate. This process can be used for any type of certificate, although it is common in secure server certificate requests where a file is usually submitted in PKCS#10 or CSR format.

If the subscriber creates the key, he/she will give DIGITALSIGN a standard PKCS#10 request and DIGITALSIGN will send the user a certificate in PKCS#7 format. In this case, confirmation that the keys have been created in a hardware environment is guaranteed through technical process or an auditor declaration, before DIGITALSIGN issues the certificate, otherwise DIGITALSIGN will consider the certificate issued via software.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

A notification is sent by email to the applicant indicating the approval or denial of the request.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Once the certificate has been delivered or downloaded, the user has seven days to check it works properly.

If the certificate has not been issued correctly due to technical problems, the certificate will be revoked and a new one issued.

4.4.2 Publication of the Certificate by the CA

DIGITALSIGN publishes the certificates issued in a publicly accessible repository.

4.4.3 Notification of the Issuance to Other Entities

RA may receive notice of the issuance of certificates approved by them.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The use of the private key corresponding to the public key in the certificate, should be allowed only when the holder agree to the subscriber agreement and accept the certificate. This should be used lawfully, in accordance with the subscriber agreement of DIGITALSIGN under this CPS.

The certificate holders will use their private key only for the purpose for which they are intended (as stated in the certificate field “keyUsage” and “extendedKeyUsage”) and always for legal purposes.

Holders should protect their private key against unauthorized use and must discontinue use of the private key following the expiration or revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties must agree to the terms stated in this CPS and in the relevant certification policy as a condition of trust in the certificate.

4.6 Certificate Renewal

The renewal of a certificate using the same key pair is not acceptable by DIGITALSIGN.

4.7 Certificate Re-Key

This is the usual procedure for renewing certificates, by which all the processes described in this section refer to this renewal method.

DIGITALSIGN does not allow certificate renewal without key renewal.

4.7.1 Circumstance for Certificate Re-Key

Prior to the expiration of an existing certificate, it is necessary to renew that certificate in order to the holder (or his representative) maintain the continuity of its use.

A certificate may be renewed after its expiration.

4.7.2 Who May Request Certification of a New Public Key

See section 4.1.1.

4.7.3 Processing Certificate Re-Key Requests

See section 4.1.2 and 4.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

4.8 Certificate Modification

Any need for modification to certificates requires a new application. The certificate is revoked and a new one issued with the corrected data.

4.9 Certificate Revocation and Suspension

Revocation refers to any change in a certificate's status caused by being rendered invalid due to any reason other than its expiry.

Suspension, on the other hand, refers to revocation with cause for suspension (i.e. a specific revocation case), in other words, a certificate is revoked temporarily until it is decided whether it should be revoked definitively or activated.

Rendering an electronic certificate invalid due to a cause for revocation or suspension will become effective for third parties as soon as notice of the termination has been given in the certification service provider's certificate validity consultation service (publication of a list of revoked certificates or consultation in OCSP service).

The reasons for suspending a certificate are defined in the specific certification policy.

DIGITALSIGN maintains the certificates on the revocation list until the end of their validity. When this occurs, they are removed from the list of revoked certificates.

4.9.1 Circumstances for Revocation

The reasons for revoking a certificate are defined in the specific certification policy.

As a general rule, a certificate will be revoked where:

- There are circumstances affecting the information contained in the certificate.
    - Any of the details contained in the certificate are amended.
    - Errors are detected in the data submitted in the certificate request or there are changes to the verified circumstances for the issue of the certificate.
    - An error is detected in any of the details contained in the certificate.
- There are circumstances affecting key or certificate security.
    - The private key or infrastructures or systems belonging to the Certification Authority that issued the certificate are compromised, whenever this incident affects the accuracy of the issued certificates.
    - The Certification Authority has breached the requirements in the certificate management procedures established in this CPS.

    - The security of the key or certificate belonging to the subscriber or certificate manager is compromised or suspected of being compromised.
    - There is unauthorized third party access or use of the subscriber's or certificate manager's private key.
    - There is misuse of the certificate by the subscriber or certificate manager, or failure to keep the private key safe
- There are circumstances affecting the security of the cryptographic device
    - Security of the cryptographic device is compromised or suspected of being compromised.
    - There is loss or disablement due to damage to the cryptographic device.
    - There is unauthorized third party access to the subscriber's or certificate manager's activation details.
- There are circumstances affecting the subscriber or certificate manager.
    - The relationship is terminated between the Certification Authority and the subscriber or certificate manager.
    - There are changes to or termination of the underlying legal relationship or cause for the issuance of the certificate to the subscriber or certificate manager.
    - The applicant breaches part of the requirements established for requesting the certificate.
    - The subscriber or certificate manager breach part of their obligations, responsibility and guarantees established in the legal document or in this Certification Practices Statement.
    - The sudden incapacity or death of the subscriber or certificate manager.
    - There is a termination of the certificate subscribing company and expiry of the authorization provided by the subscriber to certificate manager, or termination of relationship between the subscriber and certificate manager.
    - The subscriber requests to revoke the certificate, in accordance with the provisions of this CPS.
- Other circumstances
    - Suspension of the digital certificate for a longer period than established in this CPS.
    - Termination of the Certification Authority's service, in accordance with the relevant section of this CPS.

In order to justify the need for the proposed revocation, the required documents must be submitted to the RA or CA, depending on the reason for the request.

The subscribers have revocation codes that they can use in the online revocation services or by calling the helplines.

4.9.2 Who Can Request Revocation

Certificate revocation can be requested by:

- The Signatory/Subscriber
- The responsible Applicant
- The Entity (via a representative)
- The RA or CA.

Anyone established in the specific certification policies.

4.9.3 Procedure for Revocation Request

All requests must be made:

- Via the online Revocation Service, by accessing the revocation service on the DIGITALSIGN web site and entering the Revocation Code.
- By filling and signing a revocation request and send it to the RA's offices.

For secure server, corporate seal or code sign certificates, this revocation can be requested by email, using the address used to request issuance of the certificate, sending the revocation request to suporte@digitalsign.pt. The DIGITALSIGN operator will confirm the request by telephone in order to process it.

The revocation management service and the consultation service are considered critical services, as specified in DIGITALSIGN's contingency plan and business continuity plan. These services will be available 24 hours a day, seven days a week. In the event of a system failure, or any other circumstance out of DIGITALSIGN's control, DIGITALSIGN will make every effort to ensure the services are not down for more than 24 hours.

If the certificate is suspended, a notice will be sent to the Signatory/Subscriber by email specifying the time of suspension and the reason.

The RA will receive an email from the system notifying that the certificate has been suspended.

If the suspension does not take place and the certificate has to be activated again, the Signatory/Subscriber will receive an email specifying the new certificate status.

4.9.4 Revocation Request Grace Period

Revocation of a certificate is performed immediately after the verification of the application for revocation after a maximum period of 24 hours at the request of the revocation and the effective revocation.

4.9.5 Time Within Which CA Must Process the Revocation Request

DIGITALSIGN will process a revocation request immediately following the procedure described in point 4.9.3.

4.9.6 Revocation Checking Requirement for Relying Parties

Trusting third parties must first check their use, the status of the certificates, and in any case must verify the last CRL issued, which can be downloaded from the URL that appears in the CRL Distribution Point on each certificate.

Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository, or OCSP responder (where available) to check revocation status.

4.9.7 CRL issuance frequency

The CRL's are published every 24 hours.

4.9.8 Maximum Latency for CRLs

After creating CRL, these are published in the repository within a very brief period. Typically this is accomplished automatically within minutes after creation.

4.9.9 On-line Revocation/Status Checking Availability

Revocations and other information about the status of the certificates are available through the web-based repository and, where provided, through the OCSP service. In addition to publishing the CRL,

DIGITALSIGN provides information on the status of the certificate through query functions in the repository.

DIGITALSIGN also provides OCSP services. Customers who have contracted these services should check the status of the certificate by using OCSP.

URLs for CRL Distribution Point and OCSP Service are enclosed in the issued certificates.

4.9.10 On-line Revocation Checking Requirements

Relying parties must have software / hardware able to access the information provided about the revocation status of certificates.

4.9.11 Other Methods of Disclosing Revocation Information

No stipulation.

4.9.12 Special Revocation Requirements due to Compromised Key Security

DigitalSign will use all commercially reasonable efforts to notify potential relying parties if it discovers, or have reason to believe that the private key of its own CA is compromised. DigitalSign will transition any revocation reason code in a CRL to “key compromise” upon discovery of such reason.

Reports to DigitalSign of key compromise must include a proof of key compromise in either of the following formats:

- A CSR signed by the compromised private key with the Common Name “Proof of Key Compromise for DigitalSign”; or
- The private key itself.

4.9.13 Circumstances for Suspension

No stipulation.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of public certificates is publicly available through the CRL and via OCSP respond (where available).

4.10.2 Service Availability

The certificate status services are available 24 x 7 without any scheduled interruption.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

A subscriber may end a subscription of a certificate by:

- Allowing the certificate to expire, without renewing it.
- Revoking the certificate before the certificate expires, without replacing it.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The escrow of CA, RA and end-user private keys is not permitted under this CPS.

DIGITALSIGN does not in any way store or archive a Signatory's private key to create electronic signature/seal, except in the case of remote certification of a certificate through the DigitalSign remote signature solution.

In this case, the private key is generated in certified hardware device (HSM) and encrypted in a reliable environment. The key encryption relies on a AES symmetric key (128 bits) wrapping key created by the HSM and derived from the HSM master wrapping key and the first authentication factor created/defined by the Signatory, which ensures that only he/she can access that private key.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

DIGITALSIGN is subject to the annual validations established by AC Camerfirma SA, which regulates the establishment of suitable processes to ensure proper security management in information systems necessary to provide the service as CA.

5.1 Physical Security Controls

DIGITALSIGN has established physical and environmental security controls to protect resources in the buildings where the systems and equipment used for the transactions are stored.

The physical and environmental security policy applicable to the certificate creation services provides protection against:

- Unauthorized physical access
- Natural disasters
- Fires
- Failure in supporting systems (electricity, telecommunications, etc.).
- Building collapse.
- Flooding
- Theft
- Unauthorized withdrawal of equipment, information, devices and applications related to the components used for the Certification Service Provider's services

The facilities have preventive and corrective maintenance services with 24h/365 assistance and assistance during the 24 hours following notice.

5.1.1 Site Location and Construction

DIGITALSIGN's facilities are built from materials that guarantee protection against brute force attacks and are located in an area with a low risk of natural disasters and with quick access.

The room where encryption activities take place is a security facility, with fire detection and extinguishing system, damp proof system, dual cooling system and dual power supply system.

5.1.2 Physical access

Physical access to DIGITALSIGN offices where encryption processes are undertaken is limited and protected by a combination of physical and procedural measures.

Access is limited to expressly authorized personnel, and there are CCTV cameras film and record any activity.

The facilities include presence detectors at every vulnerable point as well as intruder alarm systems that send a warning via alternative channels.

The rooms are accessed by ID card scanners, and biometric (when applicable) which are managed by a software system that maintains an automatic log of comings and goings.

The most critical system elements are accessed through three different zones with increasingly limited access.

5.1.3 Power and Air Conditioning

DIGITALSIGN's facilities have voltage stabilizers and with an electric generator.

The rooms in which computer equipment is stored have temperature control systems with dual air conditioning units.

5.1.4 Water Exposure

DIGITALSIGN facilities are in an area with a low flooding risk. The rooms in which computer equipment is stored have a humidity detection system.

5.1.5 Fire Prevention and Protection

The rooms in which computer equipment is stored have automatic fire detection and extinguishing systems.

5.1.6 Media Storage

Each dismountable storage device (tapes, cartridges, disks, etc.) is only accessible by authorized personnel.

5.1.7 Waste Disposal

Once sensitive information is no longer of use, it is destroyed using suitable means for the device containing it.

- Printed matter and paper: Shredders or waste bins provided for this purposes, later destroyed via controlled means.
- Storage devices: Before being thrown away or reused they must be processed for deletion by being physically destroyed or the contained data made illegible.

5.1.8 Off-Site Backup

DIGITALSIGN uses encrypted external backups for sensitive data.

5.2 Procedural controls

5.2.1 Trust Roles

Roles of trust are implemented, guaranteeing the distribution of duties to share out control and limit internal fraud and avoid one person controlling the entire certification process from start to finish.

5.2.2 Number of People Required per Task

DIGITALSIGN guarantees that at least two people will carry out the tasks described in this CPS, mainly handling the Root CA and intermediate CA key storage device.

5.2.3 Identification and Authentication for Each Role

The people assigned to each role are identified by the internal auditor who must ensure that each person carries out the procedures to which he/she is assigned.

Each person only controls the assets that are required for his/her role, thereby ensuring that nobody accesses unassigned resources.

Depending on the asset, resources are accessed via cryptographic cards and activation codes.

5.2.4 Roles requiring separation of duties

Roles requiring separation of duties include, but are not limited to:

- Validation of information in requests for issuing certificates, requests for renewal or revocation, or renewal of information.
- Issuance and revocation of certificates, including staff with access to restricted parts of the repository.
- handling information or requests from the subscriber.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Clearance Requirements

All personnel are qualified and have been trained in the procedures to which they have been assigned.

DIGITALSIGN ensures that registration personnel or RA Administrators are trustworthy to undertake registration work. RA Administrators must have taken a training course for request validation duties.

In general, DIGITALSIGN will take away an employee's trust roles if it discovers that person has committed any criminal act that could affect the performance of his/her duties.

5.3.2 Background Check Procedures

DIGITALSIGN HR procedures include conducting the necessary investigations before hiring anyone.

5.3.3 Training Requirements

Personnel undertaking duties of trust must have been trained in accordance with this CPS.

5.3.4 Retraining Frequency and Requirements

DIGITALSIGN undertakes the required updating procedures to ensure certification duties are undertaken properly, especially when they are modified substantially.

5.3.5 Job Rotation frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

DIGITALSIGN has established an internal penalty system, which is described in its HR policy, to be applied when an employee undertakes unauthorized actions, which includes the possibility of dismissal.

5.3.7 Contract Personnel Requirements

Employees hired to undertake duties of trust must sign the confidentiality clauses and operational requirements that DIGITALSIGN uses. Any action compromising the security of the accepted processes could lead to termination of the employee's contract, once evaluated.

5.3.8 Documentation Supplied to Personnel

DIGITALSIGN provides all personnel with documentation describing the assigned duties, with special emphasis on security regulations and the CPS.

Any documentation that employees require will also be supplied at any given time so that they can perform their duties competently.

5.4 Audit Logging Procedures

DIGITALSIGN is subject to the annual validations of AC Camerfirma SA to ensure proper management of security in information systems necessary to provide the service as CA.

5.4.1 Types of Events Recorded

DIGITALSIGN records and saves the logs of every event relating to the CA's security system

The following events will be recorded:

- System switching on and off.
- Creation, deletion and setting up of passwords or changed privileges.
- Attempts to log in and out.
- Attempts at unauthorized access to CA's system online.
- Attempts at unauthorized access to file system.
- Physical access to logs.
- Changes to system settings and maintenance.
- CA application logs.
- CA application switching on and off.
- Changes to the CA's details and/or its passwords.
- Changes to the creation of certificate policies.
- Creation of own passwords.
- Certificate creation and revocation.
- Logs of destruction of devices containing activation keys and data

5.4.2 Frequency of Processing Log

DIGITALSIGN checks the logs when there is a system alert due to an incident.

DIGITALSIGN maintains a system that guarantees:

- Sufficient space to store logs
- That the log files are not overwritten.
- That the saved information includes at least the following: Event type, date and time, user executing the event and result of the process.

The log files are saved in structured files that can be included in a database for data mining later on.

5.4.3 Retention Period for Audit Log

DIGITALSIGN stores the log data for at least five years.

5.4.4 Protection of Audit Log

The system logs are protected from being manipulated via signatures in the files that contain them.

They are stored in fireproof devices.

Availability is ensured by storing them in buildings outside the CA's workplace.

The log files can only be accessed by authorized persons.

The devices are always handled by authorized personnel

There is an internal procedure that specifies the procedure to manage devices containing audit log data.

5.4.5 Audit Log Backup Procedures

DIGITALSIGN uses a suitable backup system to ensure that, in the event important files are lost or destroyed, the log backups are available for a short period of time.

5.4.6 Audit Collection System

Event audit information is collected internally and automatically by the operating system and certificate management software.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The analysis of vulnerabilities is covered by the DIGITALSIGN audit processes. The risk and vulnerability management processes are reviewed once a year and are included in the Risk analysis document. This document specifies the controls implemented to guarantee the required security objectives.

The system audit data is stored so that it can be used to investigate any incident and locate vulnerabilities.

5.5 Records Archival

5.5.1 Type of Records Archived

The following documents that are part of the certificate's life cycle are stored by the CA or RAs:

- Any system audit data.
- Any data related to certificates, including contracts with signatories and their identification details.
- Requests to issue and revoke certificates.
- Any issued or published certificates.
- Issued CRLs or logs of the status of created certificates.
- Log of created keys.
- Communications between PKI elements
- Certification Policies and Practices

DIGITALSIGN is responsible for properly filing all this material.

5.5.2 Retention Period for Archive

Archived data is retained for a period of time defined by applicable law, which is currently set at twenty (20) years.

5.5.3 Protection of Archive

DIGITALSIGN ensures files are protected.

5.5.4 Archive Backup procedures

DIGITALSIGN has internal procedures to ensure the availability of electronic file backups. The physical documents are stored in secure places restricted to authorized personnel.

5.5.5 Requirements for Time-stamping of Records

The logs are dated with a reliable source via NTP from the OAL, GPS and radio synchronization systems.

5.5.6 Archive Collection System (Internal or External)

DIGITALSIGN has a data collection system for activity on devices involved in the certificate management service.

5.5.7 Procedures to Obtain and Verify Archive Information

DIGITALSIGN has a software security document that describes the process for checking that the filed information is correct and accessible.

5.6 Key Changeover

The CA private key will be changed before it expires. The old CA and private key will only be used to sign CRLs while there are active certificates issued by the old CA. A new CA will be created with a new private key and a new DN.

The subscriber's keys are changed by starting a new issuance procedure (see the corresponding section of this CPS).

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

DIGITALSIGN has developed a Contingency plan to retrieve critical systems, if an alternative data center were necessary.

If the root key security is compromised, this must be considered a separate case in the contingency and business continuity plans. If the keys are replaced, this incident affects recognition by the different applications and private and public services. Recovering the validity of keys in business terms will mainly depend on the duration of these processes. The contingency and business continuity plans will only deal with operational aspects to ensure the new keys are available, which is not the case for recognition by third parties.

Any failure to meet the targets set by this contingency plan will be considered unavoidable unless there is a breach of obligations on DIGITALSIGN's part in implementing these processes.

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

Any failure to meet the targets set by this contingency plan is considered reasonably unavoidable unless there is a breach of obligations on DigitalSign's part in implementing these processes.

A part of the implementation of its ISO27001 system, DigitalSign has developed plans and procedures for continuous improvement in a way that systematically reinforces all experiences covered in the management of incidents and avoids their repetition.

5.7.3 Entity Private Key Compromise Procedures

The DIGITALSIGN contingency plan considers any situation where the compromised security of the CA's private key is a disaster.

If the security of a root key is compromised:

- All the Signatories/Subscribers, Trusting Third Parties and other CAs with which agreements or other relationships regarding a breach of security have been established will be informed.
- They will be informed that the certificates and information relating to the revocation status that are signed using this key are not valid.

5.7.4 Business Continuity Capabilities After a Disaster

DIGITALSIGN will reinstate the critical services (revocation and publication of revocations) in accordance with the contingency and business continuity plans.

5.8 CA or RA Termination

Before the DIGITALSIGN ceases its activity, it will:

- Provide the required funds (via a public liability insurance policy) to complete the revocation processes.
- Inform all the Signatories/Subscribers, Trusting Third Parties and other CAs with which it has agreements or other types of relationships regarding termination of activity at least six months in advance.
- Revoke any authorization from subcontracted entities to act on behalf of the CA in the certificate issuance procedure.
- Pass on its obligations related to keeping log data for the established time period to the subscribers and users.
- The CA's private keys will be destroyed or disabled.
- DIGITALSIGN will keep any activate certificates and the verification and revocation system until all the issued certificates have expired.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

A cryptographic device (HSM) is used to create the CA's keys, which complies with the requirements established in FIPS 140-2, level 3 and/or EAL4+.

The CA keys were created in a secure environment with dual control mechanisms and fully documented to ensure the security of the process.

6.1.1.1 Creating the subscriber's key pair

Signatories/Subscribers can create their own keys using DIGITALSIGN-authorized hardware or software devices or DIGITALSIGN can create them in PKCS#12 software format. The keys are created using the RSA public key algorithm. The keys have a minimum length of 2048 bits.

If subscribers create the keys on their own cryptographic device, DIGITALSIGN verifies through technical process or an auditor declaration before a certificate with keys created on a hardware device is issued, otherwise DIGITALSIGN will only be able to issue a certificate classified as keys created on a software device.

DIGITALSIGN has controls to ensure that generated keys are aligned with the Certification Policies, and can not issuing them otherwise.

6.1.2 Private Key Delivery to Subscriber

See section 3.2.1.

6.1.3 Public Key Delivery to Certificate Issuer

The public key will be given to DIGITALSIGN to create the certificate when the circuit requires in a standard format, preferably self-signed PKCS#10 or X509 format.

6.1.4 CA Public Key Delivery to Relaying Parties

The CA certificates are available to the users in the DIGITALSIGN website indicated in this document.

6.1.5 Key Sizes

The Signatory/Subscriber's private keys are based on the RSA algorithm with a minimum length of 2048 bits. The period of use for the public and private key varies depending on the certificate type.

6.1.6 Public Key Parameters Generation and Quality Checking

The public key for the Root CA and Subordinate CA and for subscriber certificates is encrypted in accordance with RFC 3280 and PKCS#1. The algorithm for creating keys is the RSA.

The certification issuing systems have security controls that verify the keys in order to check the Certification Policy quality parameters.

6.1.7 Key Usage Purposes

The chart below describes the key uses for different issued certificates. The solution adopted to differentiate between uses is:

- Certificates for DS bit authentication (can be combined with other uses).
- Certificates for DS + NR bit electronic signature (can be combined with other uses)

- Exclusive NR bit recognized signature certificates (CANNOT be combined with other uses)

CA:	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
AC ROOT- Chambersign Global Root						✔	✔		
AC Camerfirma Portugal						✔	✔		
DIGITALSIGN PRIMARY CA						✔	✔		
AC DIGITALSIGN						✔	✔		
OCSP Certificate	✔								
Organization Certificate	✔	✔							
End User Certificate	✔	✔	✔						
AC DIGITALSIGN TSA						✔	✔		
TimeStamp Certificate	✔								
OCSP Certificate	✔								

DS: Digital Signature
NR: Non Repudiation, “ContentCommitment”
KE: Key Encryption
DE: Data Encryption
KA: Key Agreement
KCS: Certificate Signing
CRL: CRL Signing
EO: Encryption Only
DO: Deciphering Only
(*)Although technically possible, DIGITALSIGN does not accept responsibility for its use for these purposes

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

6.2.1.1 The CA's Private Key

The CA's private key is kept and used in a secure cryptographic device that complies with FIPS 140-2 level three and/or EAL4+ requirements.

When the CA key is outside the device it is kept encrypted and shared between various devices. A backup is made of the CA private key which is stored and only retrieved by authorized personnel in accordance with the roles of trust, using at least dual control on a secure physical device. The CA private key backups are stored securely.

6.2.1.2 The Signatory’s Private Key

The subscriber's private key can be stored in a software or hardware device.

When it is stored in software format, DIGITALSIGN will provide the configuration instructions for secure use in recognized applications.

As regards cryptographic devices with certificates for advanced electronic signing, suitable as secure signature creation devices, these comply with security level CC EAL4+ and support the PKCS#11 and CSP standards.

DIGITALSIGN uses the cryptographic means allowed in its registration application and which guarantee the creation of recognized electronic signature.

Information on the type of key creation and custody is included in the digital certificate, allowing the Trusting Third Party to act accordingly.

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

Multi-person control is required for activation of the CA's private key. In accordance with this CPS, there is a policy of two of four people to activate keys.

6.2.3 Private Key Escrow

Private key escrow is not used by DigitalSign.

DigitalSign does not in any way store or archive a Signatory's private key to create electronic signature/seal, except in the case of remote certification of a certificate through the DigitalSign remote signature solution.

In this case, the private key is generated in certified hardware device (HSM) and encrypted in a reliable environment. The key encryption relies on a AES symmetric key (128 bits) wrapping key created by the HSM and derived from the HSM master wrapping key and the first authentication factor created/defined by the Signatory, which ensures that only he/she can access that private key.

6.2.4 Private Key Backup

DIGITALSIGN makes backups of CA private keys to allow their retrieval in the event of natural disaster, loss or damage. At least two people are required to create the copy and retrieve it.

DIGITALSIGN keeps minutes on CA private key management processes.

6.2.5 Private Key Archival

CA private keys are filed for at least 10 years after the last certificate has been issued. At least two people will be required to retrieve the CA private key from the initial cryptographic device. DIGITALSIGN keeps minutes on CA private key management processes.

Subscribers can store keys delivered on software for the certificate duration period at least, but must then destroy them and ensure they have no information encrypted with the public key.

Subscribers can only store the private key for as long as they deem appropriate in the case of encryption certificates.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CA keys are created inside cryptographic devices in a process fully documented. At least two people will be required to enter the key in the cryptographic module.

DIGITALSIGN keeps minutes on CA private key management processes.

Keys created on subscriber software are created in DIGITALSIGN's systems and are delivered to the end subscriber in a PKCS#12 software device.

Keys created on subscriber hardware are created inside the cryptographic device delivered by the CA.

Keys linked to subscribers cannot be transferred.

6.2.7 Private key Storage on Cryptographic Module

The CA private key is stored in the cryptographic module in in encrypted form.

6.2.8 Method of Activating Private Key

Intermediate CA private key activation is managed by the management application.

The subscriber's private key is accessed via an activation key, which only the subscriber knows and must avoid writing down.

The CA's keys are activated via an m out of n process. See section 6.2.2

DIGITALSIGN keeps minutes on CA private key management processes.

6.2.9 Method of Deactivating Private Key

The subscriber's private key will be deactivated once the cryptographic device used to create the signature is taken out of the reader.

When the key is stored in software, it can be deactivated by deleting the keys from the application in which they are installed.

The CA's private keys are deactivated following the steps described in the cryptographic device administrator's manual.

DIGITALSIGN keeps minutes on CA private key management processes.

6.2.10 Method of Destroing Private Key

Before the keys are destroyed, a revocation of the certificate of linked public keys will be issued.

Devices that have any part of the private keys belonging to the Hierarchy CAs will be destroyed or restarted at a low level. The steps described in the cryptographic device administrator's manual are followed to eliminate them.

Backups will be destroyed securely.

The subscriber's keys stored on software can be destroyed by deleting them in accordance with instructions from the application on which they are stored.

The subscriber's keys on hardware can be destroyed using special software at the Registration points or the CA's facilities.

DIGITALSIGN keeps minutes on CA private key management processes.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA will keep its files for a minimum period of fifteen (15) years provided that technology at the time allows this. The documentation to be kept includes public key certificates issued to subscribers and proprietary public key certificates.

6.3.2 Certificate operational periods and key pair usage periods

A public or private key certificate must not be used once its validity period has expired. A private key can only be used outside the period established by the digital certificate to retrieve the encrypted data.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used for protection of cryptographic modules that contain the CA private key, are created in accordance with the requirements of section 6.2.2 and specifications for key generation ceremony. The creation and distribution of shared secrets is appropriately registered.

The activation data of the user’s private key is generated differently depending on the type of certificate.

On the smartcards or usb tokens used by DigitalSign, keys are generated protected with a random-calculated PIN and PUK. This information is sent by the management platform to the Subject via the

email address associated with the digital certificate. The Subject has software to change their card's PIN and PUK.

On a third party hardware devices, DigitalSign accredits third-party devices, even though they are managed separately.

The private keys stored on a HSM for remote signature/seal, the activation data is created/defined by the Signatory.

6.4.2 Activation Data Protection

It is required to holders of Secret Shares, to safeguard data and sign an agreement acknowledging their responsibilities.

Activation data are stored in secure vaults.

End-user private keys are protected through the use of secure-signature-creation-devices, and PIN (Personal Identification Number). In case of remote signature solution, two authentication factors are required.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer security controls

DIGITALSIGN uses reliable systems to provide certification services.

DIGITALSIGN has undertaken IT controls and audits to manage its IT assets with the security level required for managing electronic certification systems.

In relation to information security, AC Camerfirma SA audits annually DIGITALSIGN to ensure the adequate security controls.

The computers used are initially configured with the appropriate security profiles by DIGITALSIGN system personnel:

- Operating system security settings.
- Application security settings.
- Correct system dimensioning.
- User and permission settings.
- Log event settings.
- Backup and retrieval plan.
- Antivirus settings.
- Network traffic requirements

6.5.1 Specific Computer Security Technical Requirements

Each DIGITALSIGN server includes the following functions:

- access control to CA services and privilege management
- separation of tasks for managing privileges
- identification and authentication of roles related to identities
- subscriber's and CA's log file and audit data

- audit of security events
- self-diagnosis of security related to CA services
- Key and CA system retrieval mechanisms

The functions described above are carried out via a combination of operating system, PKI software, physical protection and procedures.

6.5.2 Computer Security Rating

Computer security is shown in an initial risk analysis, such that the security measures applied are a response to the probability of a group of threats breaching security and their impact.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

DIGITALSIGN has established a procedure to control changes to operating system and application versions that involve upgrades to security functions or solve any detected vulnerability.

6.6.2 Security management controls

6.6.2.1 Security Management

DIGITALSIGN organizes the required training and awareness activities for employees in the field of security. The training materials used and the process descriptions are updated once approved by a security management group.

DIGITALSIGN establishes the equivalent security measures for any external provider involved in certification work in contracts.

6.6.2.2 Data and Asset Classification and Management

DIGITALSIGN maintains an inventory of assets and documentation and a procedure to manage this material to guarantee its use.

DIGITALSIGN's security policy describes the information management procedures, classifying them according to level of confidentiality.

6.6.2.3 Management Procedures

DIGITALSIGN has established an incident management and response procedure via an alert and periodical reporting system. DIGITALSIGN's security document describes the incident management process in detail.

DIGITALSIGN records the entire procedure relating to the functions and responsibilities of the personnel involved in controlling and handling elements of the certification process.

Processing devices and security

All devices are processed securely in accordance with information classification requirements. Devices containing sensitive data are destroyed securely if they are no longer required.

System planning

DIGITALSIGN's Systems department maintains a log of equipment capacity. Together with the resource control application, each system can be re-dimensioned.

Incident reporting and response

DIGITALSIGN has established a procedure to monitor incidents and solve them, including recording of the responses and an economic evaluation of the incident solution.

Operating procedures and responsibilities

DIGITALSIGN defines activities, assigned to people with a role of trust other than the people responsible for carrying out daily activities that are not confidential.

6.6.2.4 Access System Management

DIGITALSIGN makes every effort to ensure access is limited to authorized personnel.

In particular:

General CA

- There are controls based on firewalls, antivirus and IDS.
- Sensitive data is protected via cryptographic methods or strict identification access controls.
- DIGITALSIGN has established a documented procedure to process user registrations and cancellations and a detailed access policy in its security policy.
- DIGITALSIGN has implemented procedures to ensure tasks are undertaken in accordance with the roles policy.
- Each person is assigned a role to carry out certification procedures.
- DIGITALSIGN employees are responsible for their actions in accordance with the confidentiality agreement signed with the company

Creating the certificate

- Authentication for the issuance process is via an m out of n operators system to activate the CA's private key.

Revocation management

- Revocation will take place via strict card-based authentication of an authorized administrator's applications. The log systems will generate evidence that guarantee non-repudiation of the action taken by the CA administrator.

Revocation status

- The revocation status application includes access control based on authentication via certificates to prevent attempts to change the revocation status information.

6.6.2.5 Managing the Cryptographic Hardware Life Cycle

DIGITALSIGN makes sure that the cryptographic hardware used to sign certificates is not manipulated during transport, by inspecting the delivered material.

Cryptographic hardware is transported using means designed to prevent any manipulation.

DIGITALSIGN records all of the important information contained in the device to add to the assets catalogue.

At least two trusted employees are required to use certificate signature cryptographic hardware.

DIGITALSIGN runs regular tests to ensure the device is in perfect working order.

The cryptographic hardware device is only handled by trustworthy personnel.

The CA's private signature key stored in the cryptographic hardware will be deleted once the device has been taken away.

The CA's system settings and any modifications and updates are recorded and controlled.

DIGITALSIGN has established a device maintenance contract. Any changes or updates are authorized by the security manager and recorded in the minutes. These configurations will be carried out by at least two trustworthy employees.

6.6.3 Life cycle security evaluation

No stipulation.

6.7 Network Security Controls

DIGITALSIGN protects physical access to network management devices and has an architecture that sorts traffic based on its security characteristics, creating clearly-defined network sections. These sections are divided by firewalls.

Confidential information transferred via insecure networks is encrypted using SSL protocols.

6.8 Time-Stamping

DIGITALSIGN has established a time synchronization procedure in coordination with the Observatório Astronómico de Lisboa via NTP. It also obtains a reliable source via GPS synchronization.

7 CERTIFICATE AND CRL PROFILE

7.1 Certificate Profile

Certificate profiles comply with RFC 5280.

All certificates issued in accordance with this policy comply with standard X.509 version 3, and RFC 3739 and the different profiles described in the EN 319 412 standard .

The common profile for all the certificates are:

Field	Description
Version	V3 (x509 standard)
Serial	Serial number of certificate. Unique code.
Issuer	Distinguish name of the level 2 intermediate that issues the certificate
not Before	Initial validity
not After	Final validity
Subject	Distinguish name of the subscriber
Extensions	Extensions of the certificate

7.1.1 Version number

DIGITALSIGN issues X.509 certificates Version 3

7.1.2 Certificate extensions

Certificate extensions of each certificate are described below:

7.1.2.1 Organization Certificate:

Extension		Value / Description
Version		V3
Serial Number (certificate)		<Unique serial number of the certificate>
signatureAlgorithm		Sha256RSA
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity. Initial validity + 3 years>
Subject	CN	<Application Name>
	O	<Organization>
	OU (0 or more)	<Project or other relevant information about subscriber / organization>
	L (optional)	<Locality of the organization>
	S (optional)	<State of the organization>
	C	<Country of the organization>
Basic Constraints (Critical)		CA=False
Key Usage (Critical)		Digital Signature, Non Repudiation
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Subject Public Key Info		RSA (2048)
Subject Key Identifier		Subject Public Key SHA-1
Authority Key Identifier		Issuer Public Key SHA-1
Certificate Policies		[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.1.2.2 [1,1]Policy Qualifier Info:

	Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/
CRL Distribution Points	[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNCA.crl
Authority Information Access	AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNCA.p7b

7.1.2.2 End User Certificate:

Extension		Value / Description
Version		V3
Serial Number (certificate)		<Unique serial number of the certificate>
signatureAlgorithm		Sha256RSA
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity. Initial validity + ≤ 5 years>
Subject	CN	<Name and Surname of the subscriber>
	E	<Email of the subscriber>
	O (optional)	<Organization>
	T (optional)	<Title of the subscriber>
	OU (0 or more)	<Project or other relevant information about subscriber>
	L (optional)	<Locality of the subscriber>
	S (optional)	<State of the subscriber>
	C	<Country of the subscriber>
Basic Constraints (Critical)		CA=False
Key Usage (Critical)		Digital Signature, Non Repudiation, Key Encipherment
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Subject Alternative Name (0 or more)		Email / Principal Name
Subject Public Key Info		RSA (2048)
Subject Key Identifier		Subject Public Key SHA-1
Authority Key Identifier		Issuer Public Key SHA-1
Certificate Policies		[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.1.2.3 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/
CRL Distribution Points		[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNCA.crl
Authority Information Access		AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/ DIGITALSIGNCA.p7b

7.1.2.3 End User Certificate:

Extension		Value / Description
Version		V3
Serial Number (certificate)		<Unique serial number of the certificate>
signatureAlgorithm		Sha256RSA
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity. Initial validity + ≤ 5 years>
Subject	CN	<Name and Surname of the subscriber>
	E	<Email of the subscriber>
	O (optional)	<Organization>
	T (optional)	<Title of the subscriber>
	OU (0 or more)	<Project or other relevant information about subscriber>
	L (optional)	<Locality of the subscriber>
	S (optional)	<State of the subscriber>
	C	<Country of the subscriber>
Basic Constraints (Critical)		CA=False
Key Usage (Critical)		Digital Signature, Non Repudiation, Key Encipherment
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Subject Alternative Name (0 or more)		Email / Principal Name
Subject Public Key Info		RSA (2048)
Subject Key Identifier		Subject Public Key SHA-1
Authority Key Identifier		Issuer Public Key SHA-1
Certificate Policies		[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.1.2.4 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/
CRL Distribution Points		[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNCA.crl
Authority Information Access		AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNCA.p7b

7.1.2.4 TimeStamp Certificate:

Extension		Value / Description
Version		V3
Serial Number (certificate)		<Unique serial number of the certificate>
signatureAlgorithm		Sha256RSA
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity. 2nd level CA validity>
Subject	CN	<Application Name> Timestamping Service

	O	<Organization>
	OU (0 or more)	<Project or other relevant information about subscriber / organization>
	L (optional)	<Locality of the subscriber / organization>
	S (optional)	<State of the subscriber / organization>
	C	<Country of the subscriber / Organization>
Basic Constraints (Critical)		CA=False
Key Usage (Critical)		Digital Signature
Extended Key Usage (Critical)		Timestamping (1.3.6.1.5.5.7.48.3)
Subject Public Key Info		RSA (2048)
Subject Key Identifier		Subject Public Key SHA-1
Authority Key Identifier		Issuer Public Key SHA-1
Certificate Policies		[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.2.2.1 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/
CRL Distribution Points		[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNTSACA.crl
Authority Information Access		AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNTSACA.p7b

7.1.3 Algorithm object identifiers (OID)

The public key algorithm object identifier is 1.2.840.113549.1.1.11: SHA256 with RSA Encryption

The public key algorithm object identifier is 1.2.840.113549.1.1.1: rsaEncryption

7.1.4 Name Format

See 7.1.2.

7.1.5 Name restrictions

The names contained in the certificates are restricted to 'Distinguished Names' X.500, which are unique and unambiguous.

7.1.6 Certification Policy (OID) object identifier

Every certificate has a policy identifier in accordance with the following model:

Certificate	Policy OID
OCSP Certificate	1.3.6.1.4.1.25596.3.2.1.2.1
Organization Certificate	1.3.6.1.4.1.25596.3.2.1.2.2
End User Certificate	1.3.6.1.4.1.25596.3.2.1.2.3
End User Certificate	1.3.6.1.4.1.25596.3.2.1.2.4
TimeStamp Certificate	1.3.6.1.4.1.25596.3.2.2.2.1

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

The "Certificate Policy" extension identifies the policy that defines the practices that DigitalSign explicitly associates with the certificate. The extension may contain a qualifier from the policy. See 7.1.6.

7.2 CRL Profile

The CRL profile matches the one proposed in the relevant certification policies. The CRLs are signed by the CA that issued the certificates

7.2.1 Version number

The CRLs issued by DIGITALSIGN are version 2.

7.2.2 CRL and extensions

Extension	Value / Description
Version	V2
Issuer	<2nd level CA DN>
signatureAlgorithm	Sha256withRSA
Last Update	<The issue date of this CRL>
Next Update	<The date by which the next CRL will be issued. Last Update + 1 days. Note: The next CRL will be issued the next day or when a certificate revocation occurs, and so it will be issued before this limit date >
Authority Key Identifier	Issuer Public Key SHA-1
CRL Number	Sequential CRL number

7.3 OCSP Profile

In accordance with the RFC 6960 standard.

7.3.1 OCSP responder certificate profile

OCSP responder certificates shall be issued by the corresponding subordinate CA of DIGITALSIGN

The validity period of the same will be no more than 3 years. As described in RFC 6960, the OCSP responder status can be checked by using CRL Distribution Points.

7.3.2 Version number

OCSP Responder certificates will use standard X.509 version 3 (X.509 v3).

7.3.3 Name formats

OCSP Responder certificates issued by an DIGITALSIGN shall contain the distinguished name X.500 of the certificate issuer and subscriber in the issuer name and subject name fields, respectively.

Names contained in the certificates are restricted to 'Distinguished Names' X.500, which are unique and non-ambiguous.

The DN for these certificates will be composed of the following elements: CN, O and C

7.3.4 Certification Policy Object Identifier (OID)

1.3.6.1.4.1.25596.3.2.1.2.1

7.3.5 OCSP Certificate extensions and fields

The profile of the OCSP responder certificate that issues the DIGITALSIGN is described below:

Extension		Value / Description
Version		V3
Serial Number (certificate)		<Unique serial number of the certificate>
signatureAlgorithm		Sha256RSA
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity. Initial validity + 3 years>
Subject	CN	<Application Name> OCSP Service
	O	<Organization>
	OU (0 or more)	<Project or other relevant information about subscriber / organization>
	L (optional)	<Locality of the subscriber / organization>
	S (optional)	<State of the subscriber / organization>
	C	<Country of the subscriber / Organization>
Basic Constraints (Critical)		CA=False
Key Usage (Critical)		Digital Signature
Extended Key Usage		OCSP Signing (1.3.6.1.5.5.7.3.9)
Subject Public Key Info		RSA (2048)
Subject Key Identifier		Subject Public Key SHA-1
Authority Key Identifier		Issuer Public Key SHA-1
Certificate Policies		[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.1.2.1 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/
CRL Distribution Points		[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/<CA-CRL>
Authority Information Access		AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/<CA-CERTIFICATEt>
'No Check' extension		

7.3.6 OCSP request format

All OCSP request must be in accordance with the RFC 6960 standard.

7.3.7 Response format

The OCSP responder of the validation service is able, at least, to generate id-pkix-ocsp-basic type responses.

Regarding the state of certificates, it must respond as:

- "Revoked", for those certificates issued by the DIGITALSIGN and which are recorded in the CRLs.
- "Good", for those certificates issued by the DIGITALSIGN and which are not recorded in the CRLs and were issued by the DIGITALSIGN.
- "Unknown" if the request corresponds to an unknown issuer CA or the certificate was not issued by DIGITALSIGN.

Note: Semantics of the fields thisUpdate, nextupdate and producedAt.

- “producedAt” must contain the moment of time in which the OCSP responder generates and signs the response.
- “thisUpdate” must to indicate the moment at which it is known that the status indicated in the response is correct. In the case of revoked certificates, they must contain the “this Update” field of the CRL that was used. In all other cases, the local date will be used.
- “nextUpdate” must indicate the moment in time in which new revocation information will be available. In the case of revoked certificates, it must contain the “nextUpdate” field of the CRL that was used, except when the “nextUpdate” date is prior to the local date. In the rest of cases, the nextUpdate field will not be set, which is equivalent according to RFC6960 to indicating that it is possible to obtain new revocation information at any time, so it is the responsibility of the client to consult it again when they consider it convenient.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Both AC Camerfirma SA and DIGITALSIGN are committed to the security and quality of its services.

AC Camerfirma SA objectives in relation to security and quality have essentially involved receiving the ISO/IEC 27001:2005, ISO/IEC 20000-1:2011 certificates. Also is subject to regular audits, with the WEBTRUST for CA and WEBTRUST EV seal, which guarantees that the policy documents and CPS have the appropriate format and scope and are fully aligned.

DIGITALSIGN, by being within the hierarchy of AC Camerfirma SA as mentioned in section 1.1.1, is subjected to periodical Audits to ensure that their CPS and Policy Certificates are aligned with the Camerfirma's CPS and the international good practices and that certificates are managed according to it, ensuring compliance with internal procedures.

8.1 Frequency and Circumstances of Assessment

The frequency of audits to which it is subjected DIGITALSIGN is annual.

8.2 Identity/Qualifications of Assessor

The audits are conducted by audit firms specialized in PKI and in prestige in such audits. Thus, auditors have the appropriate qualifications for the proper performance of such audits.

8.3 Assessor's Relationship to Assessed Entity

The audit companies used are reputed companies with specialized departments in conducting audits in the field of PKI, which rules out any conflict of interest that could affect their work with the CA.

8.4 Topics Covered by Assessment

The audit checks:

- That DIGITALSIGN complies with the requirements of the Certification Policies that regulate the issuing of the different digital certificates.
- That the CPS is in keeping with the provisions of the Policies, with that agreed by the Authority that approves the Policy and as established under current law.
- That DIGITALSIGN properly manages its information systems in order to meet the CPS and Certification Policies.

8.5 Actions Taken as a Result of Deficiency

Regarding the results of conformity assessments or audits, exceptions or significant deficiencies identified will result in the determination of actions to be taken.

This determination is made by DigitalSign Administration, together with the leaders of the concerned areas. DigitalSign Administration is responsible for developing and implementing the corrective action plan. If DigitalSign determines that such exceptions or deficiencies may pose an immediate threat to the security or integrity of the CAs, this plan must be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies,

DigitalSign management will assess the implications of such occurrences and will determine the appropriate course of action.

8.6 Communication of Results

The results of audits and evaluations of compliance must be delivered to DigitalSign within the contractually stipulated deadlines.

The information about the corrective actions performed and / or to be performed shall be sent to the competent authority in the shortest time possible (when applicable).

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal fees

The prices for certification services or any other related services are available and updated on the DIGITALSIGN web site.

The specific price is published for each type of certificate.

9.1.2 Certificate Access Fees

Access to certificates is free-of-charge; although DIGITALSIGN applies controls to avoid mass certificate downloads. Any other situation that DIGITALSIGN deems must be considered in this respect will be published on the DIGITALSIGN web site.

9.1.3 Revocation or Status Information Access Fees

DIGITALSIGN provides free access to information relating to the status of certificates or revoked certificates via Certificate Revocation Lists (CRL) or via its web site.

DIGITALSIGN may offer the OCSP. The prices of these services will be published at website.

9.1.4 Fees for Other Services

Access to the content of this CPS is free-of-charge, on the DIGITALSIGN web site indicated in section 1.2.

9.1.5 Refund policy

DIGITALSIGN does not have a specific refund policy, and adheres to general current regulations.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DIGITALSIGN, in its role as a CSP, has a public liability insurance policy that covers its liabilities to pay compensation for damages and losses caused to the users of its services: the Signatory/Subscriber and the Trusting Third Party, and to third parties, amounting to a total of €125,000.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

See section 9.2.1.

9.3 Confidentiality of Business Information

9.3.1 Scope of Business Information

DIGITALSIGN considers any information not classified as public to be confidential. Information declared confidential is not distributed without express written consent from the entity or organization that classified it confidential, unless established by law.

DIGITALSIGN has established a policy for the processing of information and forms which anyone accessing confidential information must sign.

DIGITALSIGN strictly complies with data protection law. This document is valid as a security document in accordance with Law Decreto-Lei 290-D/99 and complementary Laws on Digital Signatures.

9.3.2 Information Not Within the Scope of Confidential Information

DIGITALSIGN considers the following information not confidential:

- The contents of this CPS that includes the Certification Policies
- The information contained in the certificates provided the Signatory/Subscriber has given consent.
- Information regarding the status of certificates (valid, suspended or revoked)
- Any information that must be published by law.

9.3.3 Responsibility to Protect Confidential Information

DIGITALSIGN ensures security of confidential information, avoiding that can be discovered or compromised by third parties.

9.3.3.1 Disclosure of Information About Certificate Revocation/Suspension

DIGITALSIGN distributes information on the suspension or revocation of a certificate by publishing it regularly on the CRLs.

DIGITALSIGN provides a CRL and Certificate consultation service on the following web site indicated in section 1.2.

9.3.3.2 Sending Information to the Competent Authority

DIGITALSIGN will provide the information that the competent authority requests in compliance with current law.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

DigitalSign repository keeps its Privacy Policy.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the contents of issued certificates, directory of certificates and CRL is treated as private.

9.4.3 Information not Deemed Private

Subject to any applicable legislation, all information made public in a certificate is not considered private.

9.4.4 Responsibility to Protect Private Information

All participants receiving private information must prevent it from being compromised or unveiled to third parties, and shall comply with all applicable privacy laws.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, in the Privacy Policy or applicable contract, the private information will not be used without the consent of the party to whom the information applies. This section is subjected to the application of privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

All DigitalSign subdomain participants should recognize that DigitalSign is forced to reveal Confidential / Private information if, in good faith, DigitalSign considers it release necessary in response to subpoenas and court orders.

9.4.7 Other Information Disclosure Circumstances

Personal data will not be transferred to third parties except legal obligation.

9.5 Intellectual Property Rights

Camerfirma / DIGITALSIGN owns the intellectual property rights for this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

In accordance with the stipulations of the Certification Policies and this CPS, and in accordance with current law regarding certification service provision, DIGITALSIGN undertakes to:

- Adhere to the provisions of this CPS and the included Certification Policies.
- Protect its private keys and keep them secure.
- Issue certificates in accordance with this CPS, the Certification Policies and the applicable technical standards.
- Issue certificates in accordance with the information in its possession and which do not contain errors.
- Issue certificates with the minimum content defined by current law for qualified or recognized certificates.
- Publish issued certificates in a directory, respecting any legal provisions regarding data protection.
- Suspend and revoke certificates in accordance with this Policy and publish the revocations in the CRL.
- Inform Signatories/Subscribers about the revocation or suspension of their certificates, as and when due, in accordance with current law.
- Publish this CPS and the Certification Policies on its web site.
- Report any amendments to this CPS to the Signatories/Subscribers and the RAs involved.
- Not to store or copy the data used to create the Signatory/Subscriber's signature, except for the encryption certificates.

- Protect the data used to create the signature while they are in its safekeeping, as necessary.
- Establish the data creation and custody systems in the aforementioned activities, protecting this data from being lost, destroyed or forged.
- Keep the data relating to the issued certificate for the minimum period required by current law.

9.6.2 RA Representations and Warranties

RAs are entities that DIGITALSIGN appointed to carry out tasks concerning subscriber registration in the certification issuing context. The RAs also undertake the obligations defined in the Certification Practices for issuing certificates, and in particular to:

- Adhere to the provisions of this CPS and the included Certification Policies.
- Protect their private keys.
- Check the identity of the Signatories/Subscribers and Applicants of the certificates.
- Check the accuracy and authenticity of the information provided by the Applicant.
- Keep the documents provided by the applicant or subscriber on file for the period required by current law.
- Respect the provisions of the contracts signed with DIGITALSIGN and with the Signatory/Subscriber.
- Inform DIGITALSIGN about the causes for revocation, when these are known.

9.6.3 Subscriber Representations and Warranties

The Signatory/Subscriber undertakes to comply with legal provisions and to:

- Use the certificate in accordance with this CPS and the applicable Certification Policies.
- Respect the provisions established in the documents signed with DIGITALSIGN and the RA.
- Report any cause for suspension/revocation as soon as possible.
- Report any changes to the data provided to create the certificate during its validity period.
- Not to use the private key or certificate once DIGITALSIGN requests or reports the suspension or revocation thereof, or once the certificate validity period has expired.

9.6.4 Relying Party Representations and Warranties

The Trusting Third Party undertakes to comply with legal provisions and to:

- Check the validity of the certificates before undertaking any transaction based on them. DIGITALSIGN has established various channels for this verification, such as access to revocation lists or online consultation services such as OCSP, all of which are described on DIGITALSIGN web site indicated in section 1.2.
- Become familiar with and adhere to the guarantees, limitations and responsibilities regarding the acceptance and use of the trusted certificates, and agree to be subject to them

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

In accordance with current law, the responsibility assumed by DIGITALSIGN and the RA does not apply in cases in which certificate misuse is caused by actions attributable to the Signatory and the Trusting Third Party due to:

- Not having provided the right information, initially or later as a result of changes to the circumstances described in the electronic certificate, when the Certification Service Provider has not been able to detect the inaccuracy of the data.
- Having acted negligently in terms of storing the data used to create the signature and keeping it confidential;
- Not having requested the suspension or revocation of the electronic certificate data in the event of doubts raised over their storage or confidentiality;
- Having used the signature once the electronic certificate has expired;
- Exceeding the limits established in the electronic certificate.
- Actions attributable to the Trusting Third Party, if this party acts negligently, that is, when it does not check or heed the restrictions established in the certificate in relation to allowed use and limited amount of transactions, or when it does not consider the certificate's validity situation.
- Damages caused to the signatory or trusting third parties due to the inaccuracy of the data contained in the electronic certificate, if this has been proven via a public document registered in a public register, if required.

DIGITALSIGN and the RAs shall neither be held responsible, under any circumstances, in the following situation:

- Warfare, natural disasters or any other case of Force Majeure.
- The use of certificates in breach of current law and the Certification Policies.
- The misuse or fraudulent use of the certificates or CRLs issued by the CA.
- Use of the information contained in the Certificate or CRL.
- Fraud in the documentation submitted by the Applicant
- Damages caused during verification of the causes for revocation/suspension.
- Due to the contents of messages or documents signed or encrypted digitally.
- Failure to comply with the obligations established for the Signer / Subscriber or third parties who rely on the rules in force in the applicable Certification Policies or this CPS
- Failure to retrieve encrypted documents with the Signatory's public key

9.8 Limitations of Liability

DigitalSign guarantees damages or losses caused to end users and relying parties resulting from their activity, according to applicable legislation.

DigitalSign is not liable for any loss or damage resulting from abusive use or outside the scope of the contract with users and / relying parties.

DigitalSign assumes no liability in the event of service failure related causes of Force Majeure such as natural disasters, war or other similar.

9.9 Indemnities

See section 9.2 and 9.6.1.

9.10 Term and Termination

9.10.1 Term

See section 5.8.

9.10.2 Termination

See section 5.8.

9.10.3 Effect of Termination and Survival

See section 5.8.

9.11 Individual Notices and Communications With Participants

Unless otherwise specified by agreement between the parties, participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

As stated in section **Error! Reference source not found.**, DIGITALSIGN's legal department sets up the policy authority (PA) and is responsible for managing the Policies and CPS.

9.12.1 Procedures for Amendments

This CPS will be amended when any significant changes are made to certificate management, for any type of certificate to which it applies. Yearly reviews will take place should no changes have been made in that time. These reviews will be included in the version table at the start of the document.

Changes that can be made to this CPS do not require notification unless they directly affect the certificate Signatory/Subscribers' rights, in which case notice must be given any comments can be submitted to the policy management organization within 15 days following publication of that notice.

9.12.2 Notification Mechanism and Period

9.12.2.1 List of aspects

Any aspect of this CPS can be changed without notice.

9.12.2.2 Notification Method

Any proposed changes to this policy will be published immediately on DIGITALSIGN's web site indicated in section 1.2.

This document contains a section on changes and versions, specifying the changes that occurred since it was created and the dates of those changes.

9.12.2.3 Period for Comments

The affected Signatories/Subscribers and Trusted Third Parties can submit their comments to the policy management organization within 15 days following receipt of notice. The Policies state 15 days.

9.12.2.4 Comment Processing System

Any action taken as a result of comments is at the PA's discretion.

9.12.3 Circumstances Under Which OID Must be Changed

If DigitalSign determines that the amendment to the identifier (OID) of the certificate policy is required, the amendment shall contain the new identifiers. Otherwise, the amendments should not require a change in the policy certificate identifier.

9.13 Dispute Resolution Procedure

Any dispute or conflict arising from this document shall be definitively resolved by means of arbitration administered by the Portuguese Court Arbitration in accordance with its Regulations and Statutes, entrusted with the administration of the arbitration and the nomination of the arbitrator or arbitrators. The parties undertake to comply with the decision reached.

9.14 Governing Law

The enforcement, interpretation, amendment or validity of this CPS shall be subject to current Portuguese law.

9.15 Compliance With Applicable Law

See section 9.14.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The Signers and third parties that rely on the Certificates assume in their entirety the content of this Certification Practices and Policy Statement.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of DIGITALSIGN.

9.16.3 Severability

Should individual provisions of this CPS prove to be ineffective or incomplete, this shall be without prejudice to the effectiveness of all other provisions.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

Force Majeure clauses, if existing, are included in the “Subscriber Agreement”.

9.17 Other provisions

9.17.1 Publication and Copy of the policy

A copy of this CPS will be available in electronic format at the Internet address indicated in section 1.2.

9.17.2 CPS Approval Procedures

The publication of the revisions of this CPS must be approved by the Management of DIGITALSIGN.