DIGITALSIGN – CERTIFICADORA DIGITAL, SA.

CERTIFICATION PRACTICES STATEMENT

VERSION 1.4 – 29/04/2021

[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	*Edition nr*	*Content*
20/07/2017	1.0	Initial draft
29/01/2018	1.1	Revision
01/02/2019	1.2	Revision
01/02/2020	1.3	Revision
29/04/2021	1.4	Revision

LEGAL NOTICE

Any question or request for information regarding the content of this document should be directed to suporte@digitalsign.pt.

CONTENTS

1. Introduction 11
1.1. Overview 11
1.1.1 Hierarchies 13
1.2. Document Name and Identification 17
1.3. PKI Participants 18
1.3.1 Certification Authority (CA) 18
1.3.2 Registration Authority (RA) 19
1.3.3 Signatory/Subscriber 19
1.3.4 Relaying Parties 20
1.3.5 Other Participants 20
1.4. Certificate Usage 21
1.4.1 Appropriate Certificate Uses 21
1.4.2 Prohibited and Unauthorised Use 21
1.5. Policy Administration 22
1.5.1 Organization Administering the Document 22
1.5.2 Contact Person 23
1.5.3 Person Determining CPS Suitability For The Policy 23
1.5.4 CPS Approval Procedures 23
1.6. Definitions and Acronyms 23
2. Publication and repository Responsibilities 24
2.1. Repository 24
2.2. Publication of Certificate Information 24
2.2.1 Certification Policies and Practices 24
2.2.2 Terms and conditions 24
2.2.3 Distribution of the certificates 24
2.3. Publication frequency 25
2.4. Access control 25
3. Identification and Authentication 26
3.1. Naming 26
3.1.1 Types of names 26
3.1.2 Need for Names to be Meaningful 26
3.1.3 Pseudonyms 26
3.1.4 Rules used to interpret several name formats 27
3.1.5 Uniqueness of names 27

3.1.6 Recognition, Authentication and Role of Trademarks and Other Distinctive Symbols 27
3.1.7 Name dispute resolution procedure 27
3.2. Initial Identity Validation 27
3.2.1 Method to prove possession of private key 27
3.2.2 Authentication of organization identity 27
3.2.3 Authentication of the Identity of an individual, the entity and their relationship 28
3.2.4 Non-verified Subscriber Information 28
3.2.5 Validation of Authority 29
3.2.6 Criteria for interoperation 29
3.3. Identification and Authentication for Re-Key Requests 29
3.3.1 Identification and authentication for routine re-key 29
3.3.2 Identification and Authentication for Re-Key After Revocation 29
3.4. Identification and Authentication for Revocation Request 29
4. Certificate Life-Cycle Operational Requirements 30
4.1. Certificate Application 30
4.1.1 Who Can Submit a Certificate Application 30
4.1.2 Enrollment Process and Responsibilities 30
4.2. Certificate Application Processing 30
4.2.1 Performing Identification and Authentication Functions 30
4.2.2 Approval or Rejection of Certificate Applications 30
4.2.3 Time to Process Certificate Applications 31
4.3. Certificate issuance 31
4.3.1 CA Actions During Certificate Issuance 31
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 31
4.4. Certificate acceptance 31
4.4.1 Conduct Constituting Certificate Acceptance 31
4.4.2 Publication of the Certificate by the CA 31
4.4.3 Notification of the Issuance to Other Entities 32
4.5. Key Pair and Certificate Usage 32
4.5.1 Subscriber Private Key and Certificate Usage 32
4.5.2 Relying Party Public Key and Certificate Usage 32
4.6. Certificate Renewal 32
4.7. Certificate Re-Key 32
4.7.1 Circumstance for Certificate Re-Key 32

4.7.2 Who May Request Certification of a New Public Key 32
4.7.3 Processing Certificate Re-Key Requests 32
4.7.4 Notification of New Certificate Issuance to Subscriber 32
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 32
4.7.6 Publication of the Re-Keyed Certificate by the CA 33
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 33
4.8. Certificate Modification 33
4.9. Certificate Revocation and Suspension 33
4.9.1 Circumstances for Revocation 34
4.9.2 Who can request revocation 35
4.9.3 Procedure for Revocation Request 35
4.9.4 Revocation Request Grace Period 36
4.9.5 Time Within Which CA Must Process the Revocation Request 36
4.9.6 Revocation Checking Requirement for Relying Parties 36
4.9.7 CRL issuance frequency 36
4.9.8 Maximum Latency for CRLs 36
4.9.9 On-line Revocation/Status Checking Availability 36
4.9.10 On-line Revocation Checking Requirements 37
4.9.11 Other methods of disclosing revocation information 37
4.9.12 Special Revocation Requirements due to Compromised Key Security 37
4.9.13 Circumstances for Suspension 37
4.9.14 Who Can Request Suspension 37
4.9.15 Procedure for Suspension Request 37
4.9.16 Limits on Suspension Period 37
4.10. Certificate Status Services 37
4.10.1 Operational Characteristics 37
4.10.2 Service Availability 37
4.10.3 Optional Features 38
4.11. End of Subscription 38
4.12. Key Escrow and Recovery 38
4.12.1 Key Escrow and Recovery Policy and Practices 38
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 38
5. Physical, Procedural and Personnel Security Controls 39
5.1. Physical Security Controls 39
5.1.1 Site Location and Construction 39
5.1.2 Physical access 39

5.1.3 Power and air conditioning 40
5.1.4 Water exposure 40
5.1.5 Fire prevention and protection 40
5.1.6 Media Storage 40
5.1.7 Waste disposal 40
5.1.8 Off-site backup 40
5.2. Procedural controls 41
5.2.1 Trust roles 41
5.2.2 Number of people required per task 41
5.2.3 Identification and authentication for each role 42
5.2.4 Roles requiring separation of duties 42
5.3. Personnel controls 42
5.3.1 Background, qualifications, experience and clearance requirements 42
5.3.2 Background checking procedures 43
5.3.3 Training requirements 43
5.3.4 Retraining Frequency and Requirements 44
5.3.5 Job rotation frequency and sequence 44
5.3.6 Sanctions for unauthorised actions 44
5.3.7 Contract personnel requirements 44
5.3.8 Documentation supplied to personnel 44
5.4. Audit Logging Procedures 45
5.4.1 Types of events recorded 45
5.4.2 Frequency of Processing Log 46
5.4.3 Retention period for audit log 46
5.4.4 Protection of audit log 46
5.4.5 Audit Log backup procedures 46
5.4.6 Audit collection system 46
5.4.7 Notification to event-causing subject 47
5.4.8 Vulnerability assessments 47
5.5. Records Archival 47
5.5.1 Type of records archived 47
5.5.2 Retention period for archive 47
5.5.3 Protection of archive 47
5.5.4 Archive backup procedures 48
5.5.5 Requirements for timestamping of records 48
5.5.6 Archive collection cystem (internal or external) 48

5.5.7 Procedures to obtain and verify archive information 48
5.6. Key Changeover 48
5.7. Compromise and Disaster Recovery 48
5.7.1 Incident and compromise handling procedures 48
5.7.2 Computing resources, software, and/or data are corrupted 49
5.7.3 Entity private key compromise procedures 49
5.7.4 Business continuity capabilities after a disaster 49
5.8. CA or RA Termination 49
6. Technical Security Controls 51
6.1. Key pair generation and installation 51
6.1.1 Key pair generation 51
6.1.2 Private key delivery to subscriber 51
6.1.3 Public key delivery to certificate issuer 51
6.1.4 CA public key delivery to relying parties 51
6.1.5 Key Sizes 52
6.1.6 Public key parameters generation and quality checking 52
6.1.7 Key Usage Purposes 52
6.2. Private Key Protection and Cryptographic Module Engineering Controls 53
6.2.1 Cryptographic module standards and controls 53
6.2.2 Private key (n out of m) multi-person control 53
6.2.3 Private key escrow 54
6.2.4 Private key backup 54
6.2.5 Private key Archival 54
6.2.6 Private key transfer into or from a cryptographic module 54
6.2.7 Private key Storage on Cryptographic Module 54
6.2.8 Method of activating private key 54
6.2.9 Method of deactivating private key 55
6.2.10 Method of destroying private key 55
6.2.11 Cryptographic Module Rating 55
6.3. Other aspects of key pair management 55
6.3.1 Public key archival 55
6.3.2 Certificate operational periods and key pair usage periods 55
6.4. Activation data 56
6.4.1 Activation data generation and installation 56
6.4.2 Activation data protection 56
6.4.3 Other aspects of activation data 56

6.5. Computer security controls 56
6.5.1 Specific computer security technical requirements 57
6.5.2 Computer security rating 57
6.6. Lifecycle technical controls 57
6.6.1 System development controls 57
6.6.2 Security management controls 58
6.6.3 Lifecycle security evaluation 60
6.7. Network security controls 60
6.8. Time-Stamping 60
7. Certificate and CRL Profile 61
7.1. Certificate Profile 61
7.1.1 Version number 61
7.1.2 Certificate extensions 61
7.1.3 Algorithm object identifiers (OID) 69
7.1.4 Name format 69
7.1.5 Name restrictions 70
7.1.6 Certification Policy (OID) object identifier 70
7.1.7 Using the "Policy Constraints" extension 70
7.1.8 policy qualifiers syntax and semantics 70
7.1.9 Processing semantics for the critical Certificate Policies extension 70
7.2. CRL Profile 70
7.2.1 Version number 70
7.2.2 CRL and extensions 70
7.3. OCSP Profile 71
7.3.1 Version number 71
7.3.2 OCSP Extensions 71
7.3.3 Algorithm object identifiers (OID) 72
7.3.4 Name format 72
7.3.5 Name restrictions 72
7.3.6 Certification Policy (OID) object identifier 72
7.3.7 Usage of Policy Constraints extension 72
7.3.8 Policy qualifiers syntax and semantics 72
7.3.9 Processing semantics for the critical Certificate Policies extension 73
7.3.10 OCSP request format 73
7.3.11 Response format 73
8. Compliance Audit and Other Assessments 74

8.1. Frequency and Circumstances of Assessment 74
8.2. Identity/Qualifications of Assessor 74
8.3. Assessor's Relationship to Assessed Entity 74
8.4. Topics Covered by Assessment 74
8.5. Actions Taken as a Result of Deficiency 75
8.6. Communication of Results 75
9. Other Business and Legal Matters 76
9.1. Fees 76
9.1.1 Certificate Issuance or Renewal fees 76
9.1.2 Certificate Access Fees 76
9.1.3 Revocation or Status Information Access Fees 76
9.1.4 Fees for Other Services 76
9.1.5 Refund policy 76
9.2. Financial Responsibility 76
9.2.1 Insurance Coverage 76
9.2.2 Other Assets 76
9.2.3 Insurance or Warranty Coverage for End-Entities 76
9.3. Confidentiality of Business Information 77
9.3.1 Scope of Business Information 77
9.3.2 Information Not Within the Scope of Confidential Information 77
9.3.3 Responsibility to Protect Confidential Information 77
9.4. Privacy of Personal Information 77
9.4.1 Privacy Plan 77
9.4.2 Information Treated as Private 77
9.4.3 Information not Deemed Private 78
9.4.4 Responsibility to Protect Private Information 78
9.4.5 Notice and Consent to Use Private Information 78
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 78
9.4.7 Other Information Disclosure Circumstances 78
9.5. Intellectual Property Rights 78
9.6. Representations and Warranties 78
9.6.1 CA Representations and Warranties 78
9.6.2 RA Representations and Warranties 79
9.6.3 Subscriber Representations and Warranties 79
9.6.4 Relying Party Representations and Warranties 80
9.6.5 Representations and Warranties of Other Participants 80

9.7. Disclaimers of Warranties 80
9.8. Limitations of Liability 81
9.9. Indemnities 81
9.10. Term and Termination 81
9.10.1 Term 81
9.10.2 Termination 81
9.10.3 Effect of Termination and Survival 81
9.11. Individual Notices and Communications With Participants 81
9.12. Amendments 82
9.12.1 Procedures for Amendments 82
9.12.2 Notification Mechanism and Period 82
9.12.3 Circumstances Under Which OID Must be Changed 82
9.13. Dispute Resolution Procedure 82
9.14. Governing Law 83
9.15. Compliance With Applicable Law 83
9.16. Miscellaneous Provisions 83
9.16.1 Entire Agreement 83
9.16.2 Assignment 83
9.16.3 Severability 83
9.16.4 Enforcement 83
9.16.5 Force Majeure 83
9.17. Other provisions 83
9.17.1 Publication and Copy of the policy 83
9.17.2 CPS Approval Procedures 83
Appendix I. Acronyms 84
Appendix II. Definitions 86

1. INTRODUCTION

1.1. OVERVIEW

Given that there is no specific definition of the concepts of the Certification Practices and Certification Policies Statement, 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 Practices Statement (CPS): defined as a set of practices adopted by a Certification Authority for the issuance of certificates. It usually contains detailed information about its certificate security, support, administration and issuing system, as well as the trust relationship between the Subject/Signatory, the User Party and the Certification Authority. These may be completely comprehensible and robust documents that provide an accurate description of the services offered, detailed certificate lifecycle management procedures, etc.

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

A detailed Certification Practices 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 "which" security requirements are required for the issuance of certificates. The Certification Practices Statement defines "how" the security requirements established in the Policy are fulfilled.

Regulation (EU) 910/2014 of the European Parliament and Council, 23 July 2014, about digital identification and trust services for digital transactions in the internal market and amending Directive 1999/93/CE (hereinafter, eIDAS), establishes that trusted services include the following digital services normally provided in exchange for remuneration:

- the creation, verification and validation of digital signatures;
- the creation, verification and validation of digital seals;
- the creation, verification and validation of digital timestamps;
- certified digital delivery;
- the creation, verification and validation of certificates for authentication of websites;
- the preservation of digital signatures, stamps or certificates for these services.

This document specifies the Certification Practices Statement (hereinafter, CPS) that AC DigitalSign – Certificadora Digital, SA. (hereinafter, DigitalSign) has established for issuing trusted certificates and services based on the following standards:

Service	EN General	EN Scope	Profiles/Semantics
Creation, verification and validation of electronic signatures	319 401 v2.1.1: General Policy Requirements for Trust Service Providers	319 411-1 v1.1.1: General requirements 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates	319 412: Certificate Profiles - 319 412-1 v1.1.1: Overview and common data structures - 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons - 319 412-5 v2.1.1: QCStatements
Creation, verification and validation of electronic stamps, includes certificates related to these services	319 401 v2.1.1: General Policy Requirements for Trust Service Providers	319 411-1 v1.1.1: General requirements 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates	319 412: Certificate Profiles - 319 412-1 v1.1.1: Overview and common data structures - 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons - 319 412-5 v2.1.1: QCStatements
Creation, verification and validation of electronic timestamps, includes certificates related to these services	319 401 v2.1.1: General Policy Requirements for Trust Service Providers	319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	319 422 v1.1.1: Time-stamping protocol and time-stamp token profiles

Regarding the policies to be applied in accordance with EN 319 411-1 / 2, the following policy groups are described:

General policies:

- **NCP** Standardised certification policy.
- **NCP+** Standardised certification policy with secure device.
- **LCP** Light certification policy (without physical presence).
- **EVCP** Certificate policy for extended validation certificates.
- **DVCP** Certificate policy for domain validation certificates.
- **OVCP** Certificate policy for organisation validation certificates.

Policies for qualified certificates:

- **QCP-n** Policies for qualified certificates issued to natural persons. Includes the **NCP** policy requirements plus additional requirements to support the management of qualified certificates.
- **QCP-l** Policies for qualified certificates issued to legal entities. Includes the **NCP** policy requirements plus additional requirements to support the management of qualified certificates.

- **QCP-n-qscd** Policies for qualified certificates issued to natural persons with SSCD. Includes the **QCP-n (including NCP+**) policy requirements plus additional requirements to support the management of qualified certificates and the provision of secure signature creation devices.
- **QCP-l-qscd** Policies for qualified certificates issued to natural persons with SSCD. Includes the **QCP-l** (including **NCP+**) policy requirements plus additional requirements to support the management of qualified certificates and the provision of secure signature creation devices.
- **QCP-w**Policies for qualified certificates issued to web servers. When the certificate is issued to a legal entity, it includes the **OVCP** and **EVCP** policy requirements plus additional requirements to support the management of qualified certificates. When the certificate is issued to a natural person it includes the **NCP** policy requirements plus additional requirements to support the management of qualified certificates.

Additionally, the requirements established in the certification policies to which this CPS refers.

The recommendations in the technical document *CWA 14167-1 Requirements for Trustworthy Systems Managing Certificates for Digital Signatures - Part 1: System Security Requirements* have also taken into consideration.

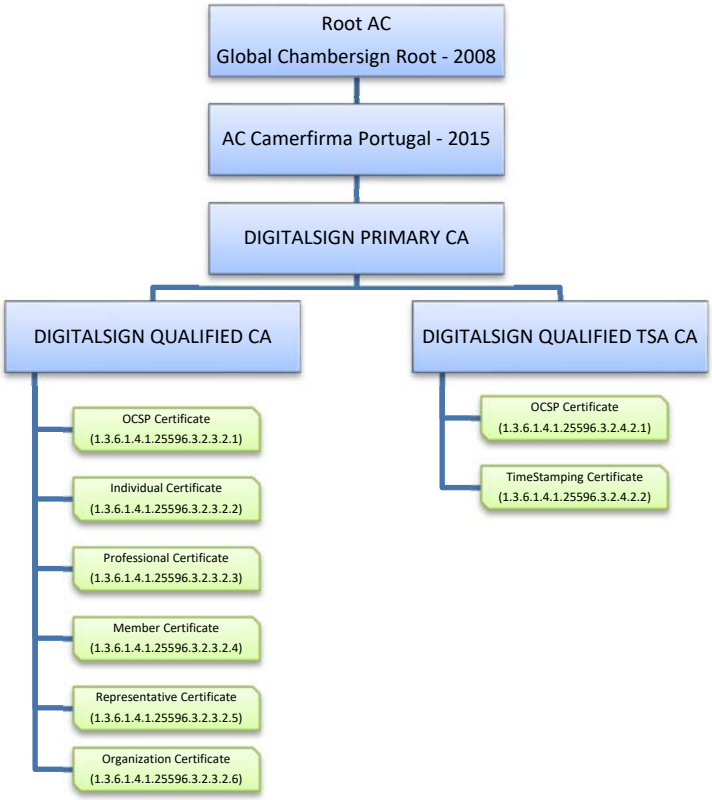
This CPS is compliant with the Certification Policies for the different certificates that DigitalSign issues, which are described in section **1.2.1** of this CPS. In the event of any conflict between both documents, the provisions of this document shall prevail.

1.1.1 HIERARCHIES

This section describes the hierarchies and Certification Authorities (hereinafter CA or CAs) that DigitalSign manages. The use of hierarchies reduces the risks involved in issuing certificates and organising them in the different CAs.

All the Certification Authorities (CAs) described can issue OCSP responder certificates. This certificate is used to sign and verify the OCSP service's responses regarding the status of the certificates issued by these CAs.

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



The certificates issued under this intermediate certification authorities acquire the recognition obtained by ROOT in commercial applications (read: Browsers such as Internet Explorer, Google Chrome, Mozilla Firefox, etc.).

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*
- 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*
- 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*
- 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, governed by this CPS, has two Level 2 Intermediates Certification Authorities, which the most relevant information are:
Level 2 Intermediate 1

- CN: DIGITALSIGN QUALIFIED CA
- SHA1 hash: *400E DF3C 7A23 36A5 F1FE AC3C F423 A917 F8C9 6308*
- Valid from: *August 30th, 2017*
- Valid until: *October 30th, 2037*
- RSA key length: 4096 *bits*

Level 2 Intermediate 2

- CN: DIGITALSIGN QUALIFIED TSA CA
- SHA1 hash: *BDFC 57D1 9675 C455 2DF8 8376 A16C 8B61 A183 2D49*
- Valid from: *August 30th, 2017*
- Valid until: *October 30th, 2037*

- RSA key length: 4096 *bits*

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 QUALIFIED CA)* issued certificates:

OCSP Certificate - OID: 1.3.6.1.4.1.25596.3.2.3.2.1
Certificate to be used by OCSP Responder

Individual Certificate - OID: 1.3.6.1.4.1.25596.3.2.3.2.2
Certificate to be used for digital signature by natural persons.
This certificate profile aims to identify a natural person (individual).
[0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]

Professional Certificate - OID: 1.3.6.1.4.1.25596.3.2.3.2.3
Certificate to be used for digital signature by natural persons.
This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfillment of his/her profession. Usually this type of certificate is issued to members of professional associations, where the entitlement should be checked with his/her association.
[0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]

Member Certificate - OID: 1.3.6.1.4.1.25596.3.2.3.2.4
Certificate to be used for digital signature by natural persons.
This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a particular organization.
[0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]

Representative Certificate - OID: 1.3.6.1.4.1.25596.3.2.3.2.5
Certificate to be used for digital signature by natural persons.
This certificate profile aims to identify a natural person (individual), as legal representative or attorney of an organization.
[0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]

Organization Certificate - OID: 1.3.6.1.4.1.25596.3.2.3.2.6
Certificate to be used for digital seal by legal persons.
[0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]

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

OCSP Certificate - OID: 1.3.6.1.4.1.25596.3.2.4.2.1
Certificate to be used by OCSP Responder

TimeStamp Certificate - OID: 1.3.6.1.4.1.25596.3.2.4.2.2
Certificate to be used by TimeStamping Authorities (TSA)
[0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]

The time-stamping authority issues certificates to intermediate entities called "Timestamping Authorities" TSA. These TSA ultimately issue the timestamps on receiving a standard request in accordance with the RFC 3161 specifications. Each of these TSA can be associated either with the service's specific technical features or exclusive client use.

The procedure for issuing the certificate is covered in the relevant section of this CPS.

AC DigitalSign issues TSA certificates on equipment accredited by AC DigitalSign. The accredited equipment may be located on the premises of the Signatory through the signature of an affidavit and compliance with the requirements associated with issuing a TSA certificate.

AC DigitalSign also issues TSA certificates for storage on third party platforms as long as these platforms:

- Are synchronised with the timestamps established by DigitalSign.
- Allow DigitalSign or an authorised third party to audit the systems.
- Allow AC DigitalSign signing applications access to their service in order to establish the appropriate controls regarding the correction of the timestamp.
- Sign a service agreement.
- Provide access to AC DigitalSign to collect information about the seals issued or submit a periodic report on the number of seals issued.
- Submit a key creation record in a safe environment as indicated by DigitalSign's TSA certification policies (HSM FIPS 140-1 Level 2 certificate) signed by a competent organisation. This record is first reviewed and signed by AC DigitalSign technical personnel before validation is given.

1.2. DOCUMENT NAME AND IDENTIFICATION

Document name:	Certification Practices Statement (CPS)
Version:	1.4
OID:	1.3.6.1.4.1.25596.3.2.3.1
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)

The component of a PKI responsible for issuing and managing digital certificates. It acts as the trusted third party between the Subject (Signatory) and the User Party in digital transactions, associating a specific public key with a person. The CA has the ultimate responsibility in the provision of certification services. The CA is identified in the Subject (Issuer) field of the digital certificate.

A CA is a type of Trusted Service Provider (TSP) that issues digital certificates.

A TSP can incorporate a CA hierarchy. This CA hierarchy is associated with a root CA. The TSP is responsible for ensuring all the CAs included in the hierarchy meet the requirements of the corresponding policies. There may be more than one intermediate CA between the root certification authority and the final-entity certificate. The number of intermediate CAs allowed is specified in the Basic Constraints (pathLenConstraint) extension of the Certification Authority's certificate.

A Certification Authority (CA) uses Registration Authorities (RA) for the purpose of testing and storage of digital certificate content documentation. The CAs can carry out the RAs' work at any time.

A CA belongs to a legal entity specified in the organisation attribute (O) of the issuer field (*Issuer*) of the associated digital certificate.

For the purpose of this CPS, the root Certification Authorities are 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.

1.3.1.1 INTERMEDIATE OR SUBORDINATE CERTIFICATION AUTHORITY

An Intermediate Certification Authority or Subordinate CA is a hierarchical object that obtains a certificate from the Root CA to issue final-entity certificates or other CA certificates.

The Subordinate CAs enable risks to be distributed in a complex hierarchical structure, which allows their keys to be managed in a more agile "online" environment, protecting the CA Root keys stored in a secure disconnected environment. A Subordinate CA enables the organisation of various types of certificates issued by the main CA.

The Subordinate CA's certificate is signed by a root CA certificate (origin root entity of the certification hierarchy) or another Subordinate CA.

A Subordinate CA may be subject to limitations by the CA on which it depends hierarchically:

a) Technically by a combination of the following parameters within the certificate: *Extended Key Usage* and *Name Constraints*
b) Contractually.

1.3.2 REGISTRATION AUTHORITY (RA)

An RA may be a natural person or a legal entity acting in accordance with this CPS and, if applicable, through an agreement with a specific CA, exercising the roles of managing the requests, identification and registration of certificate applicants, and any responsibilities established in the specific Certification Policies. RAs are authorities delegated by the CA, although the latter is ultimately responsible for the service.

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

The 'Subject' is the certificate holder and is described in the CN (Common Name) attribute of the DN (Distinguished Name) field of the certificate. The Subject may be:

- A natural person.
- A natural person associated with an organization.
- A legal entity.
- A hardware device or software application operated by or on behalf of a legal entity.

When a Signatory is the Subject of the certificate, the Signatory is directly responsible for the obligations associated with managing the certificate.

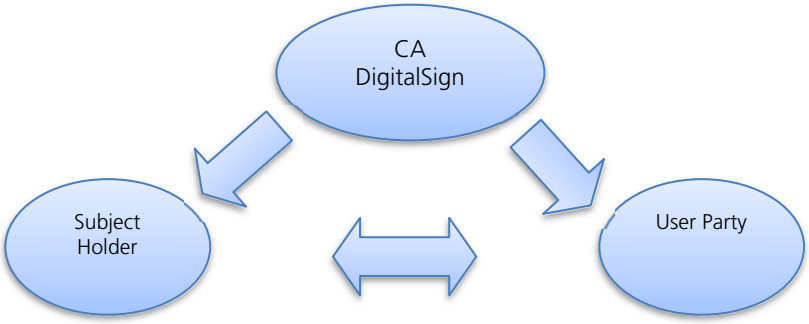
When a Signatory act on behalf of one or more Subjects to which the Signatory is associated (example: a company that requests certificates for its employees to act on behalf of the company). The connections between the Subject and the Signatory may be:

- When it is a natural person the Signatory may be:
  - The natural person
  - A natural person representing the certificate's Subject.
  - Any entity authorised to represent the legal entity for which the entity is identified in association with the certificate's organisation field (O).
- When it is a legal entity, the Creator of the Seal may be:
  - Any entity authorised to represent the legal entity.
  - A legal representative.
- When it is a device, the Signatory may be:
  - The natural person operating the device or application.
  - Any entity authorised to represent the legal entity.
  - A legal representative.

In order to avoid a conflict of interest, AC DigitalSign does not allow the Signatory and RA to be the same entity except when requesting certificates for an organisation associated with the RA or people associated with this organisation.

1.3.4 RELAYING PARTIES

In this CPS, the Relaying Party (Trusting Third Party) or user is the person receiving a digital transaction carried out with a certificate issued by any of the DigitalSign CAs and who voluntarily trusts the Certificate that this CA issues. Flow diagram.



1.3.5 OTHER PARTICIPANTS

1.3.5.1 TRUSTED SERVICE PROVIDER (TSP)

A trusted service provider (TSP) is a natural person or legal entity who provides one or more trust services, whether a qualified or unqualified trusted service provider.

A qualified trusted service provider provides one or more qualified trusted services for which the supervisory body has granted the qualification.

The trusted services defined in eIDAS include:

- The creation, verification and validation of digital signatures. Certificates relating to these services are included.
- The creation, verification and validation of digital seals. Certificates relating to these services are included.
- The creation, verification and validation of digital timestamps. Certificates relating to these services are included.
- Certified digital delivery. Certificates relating to these services are included.
- The creation, verification and validation of certificates for website authentication.
- The preservation of digital signatures, seals or certificates related to these services.

1.3.5.2 ACCREDITATION ENTITY OR SUPERVISORY BODY

The supervision authority is the corresponding management entity that accepts, accredits and supervises the TSPs within a specific geographic area. Within Portugal, this task is the responsibility of the Autoridade Nacional de Segurança, which is the competent authority depending on the Portuguese State member of the European Economic Space.

The Subordinate CAs that DigitalSign develops may be subject to legal frameworks in different countries or regions. In such cases, the accreditation entity refers to the relevant national bodies.

1.3.5.3 ENTITY/ORGANISATION

The Entity is a public or private, individual or collective organisation, recognised under the law, with which the Subject maintains a certain relationship, as defined in the ORGANISATION field (O) in each certificate.

1.3.5.4 CERTIFICATE HOLDER/KEY HOLDER

This CPS considers the certificate holder (the Subject) to be the person responsible for certificates issued to natural persons.

This CPS considers that the Signatory natural person submitting the application responsible for certificates issued to legal entities, even if the request is made via a third party, when it has knowledge of the existence of the certificate's existence.

For component certificates, this CPS considers the natural person, the Signatory submitting the application on their own behalf or via a third party to be the responsible party.

1.3.5.5 APPLICANT

Under this CPS, the Applicant is understood as the Signatory.

1.4. CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

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

DigitalSign certificates can be used in accordance with Portuguese and EU legislation and the terms and conditions set out in the Certification Policies. 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.
In general terms, certificates are issued for the following uses:

- **Authentication** based on X.509v3 certificates.
- **Electronic qualified signature**, based on X.509v3 certificates.
- **Electronic qualified seal**, based on X.509v3 certificates.
- **Asymmetric or mixed encryption**, based on X.509v3 certificates.

1.4.2 PROHIBITED AND UNAUTHORISED USE

The certificates can only be used for the purposes for which they were issued and are subject to the limits defined in the certification policies.

Certificates are not designed, may not be used and their use or resale is not authorised as control equipment for dangerous situations or for uses requiring fail-safe actions, such as

the operation of nuclear facilities, navigation systems or aerial communication or weapon control systems, where an error could directly result in death, personal injury, or severe environmental damage.

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 with the Signatory (Subjects) and/or Signatories is considered illegal, and the CA is 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 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 is also 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 Signatory (Subject), as well as any misuse thereof in accordance with this paragraph or which could be interpreted as such by virtue of current law.

In the certificate information on the limitation of use, in standardised "*key usage*" attributes, DigitalSign includes "*basic constraints*" marked as critical in the certificate fields and therefore compliance is obligatory by the applications that use it, or limitations on attributes such as "*extended key usage*", "*name constraints*" and/or by means of text included in the "*user notice*" marked "not critical" but for which the certificate holder and user's compliance are obligatory.

1.5. POLICY ADMINISTRATION

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

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 cannot 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

See Appendix I and II.

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 generally publishes the following information in its repository:

- The lists of revoked certificates and other information about the status of revoked certificates.
- The general certification policy and, where appropriate, specific policies.
- Certificate profiles and lists of revoked certificates.
- The Certification Practices Statement and the corresponding PDS (*PKI Disclosure Statement*).
- Binding legal instruments with Signatories and verifiers.

Any changes to specifications or conditions of service shall be communicated to users by the Certification Authority, through its website indicated in section 1.2.

AC DigitalSign shall not remove the previous version of the changed document, indicating that it has been replaced by the new version.

2.2.1 CERTIFICATION POLICIES AND PRACTICES

This CPS and Policies are available to the public on the following website: https://www.digitalsign.pt/repository.

2.2.2 TERMS AND CONDITIONS

Users can find the service terms and conditions in DigitalSign's certification policies and practices. The Subject/Signatory receives information on the terms and conditions in the certificate issuing process, either via the physical contract or the condition acceptance process prior to submitting the application.

When the Subject/Signatory accepts the terms and conditions on paper they must be signed in writing. If they are accepted in electronic format it is done by accepting the terms and uses in the application form.

2.2.3 DISTRIBUTION OF THE CERTIFICATES

The issued certificates can be accessed as long as the Signatory/Subject has provided consent. Prior to issuing the certificate, the applicant must accept the uses, granting DigitalSign the right to publish the certificate on the website indicated in section 1.2.

The root keys in the DigitalSign hierarchies can be downloaded from:
https://www.digitalsign.pt/repository

The certificates can be viewed from a secure website by entering the Signatory's registered credentials. After the Signatory authentication, the system displays a page with all the related certificates, whether active, expired or revoked. Therefore, the query service does not allow the mass download of certificates.

2.3. PUBLICATION FREQUENCY

AC DigitalSign publishes the final entity's certificates immediately after they have been issued, provided the Subject/Signatory has given approval.

AC DigitalSign issues and publishes revocation lists periodically in accordance with the table shown in the corresponding section of these certification practices: "CRL issuance frequency".

DigitalSign immediately publishes on its website https://www.digitalsign.pt/repository any change to the Policies and the CPS, maintaining a version log.

Older versions of documents are kept by DigitalSign and may be consulted, by request.

2.4. ACCESS CONTROL

DigitalSign publishes certificates and CRLs on its website. 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

3.1.1 TYPES OF NAMES

The Subject/Certificate holder is described by a distinguished name (DN, *distinguished name*, Subject) pursuant to the X.501 standard. The DN field descriptions are shown in each of the certificate profile sheets. It also includes a *"Common Name"* component (CN =).

The structure and content of the fields of each certificate issued by DigitalSign as well as its semantic meaning are described in each profile record in the certificates.

DN consist of, as specified in the following table:

Attribute	***Value***
Country – "C"	"PT", or other according to ISO 3166 table.
Organization – "O"	Name of organization to which belongs the signature holder (where applicable)
Organizational Unit – "OU"	Digital certificates can contain attributes OU, according to the corresponding PC
State or Province – "S"	The District of the signatory, or unused
Locality – "L"	The Location of the signatory, or unused
Common Name – "CN"	Certificate's Holder or service
Email Address – "E"	Email address associated with the signature holder (where applicable)
First Name (Given Name – "G")	Holder's first name(s), when issued to natural persons, or unused
Last Name (Surname – "SN")	Holder's last name(s), when issued to natural persons, or unused
ID (SERIALNUMBER)	Holder's ID, when issued to natural persons, or unused
ID (Organization Identifier)	Organization's ID, or unused
Title – "T"	Professional title or another used by the certificate holder

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 use of pseudonyms is allowed. DigitalSign will use the Pseudonym with the CN attribute of the Subject/Signatory's name, keeping the Subject/Signatory's real identity confidential.

The pseudonym in certificates in which it is allowed is calculated in such a way that the real certificate holder is unmistakably identified**.**

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

Within a single CA, a Subject/Signatory name that has already been taken cannot be re-assigned to a different Subject/Signatory. It is possible for an owner to have two or more certificates with the same DN.

3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS AND OTHER DISTINCTIVE SYMBOLS

DigitalSign does not assume any obligations regarding issuing certificates in relation to the use of trademarks or other distinctive symbols. DigitalSign deliberately does not allow the use of a distinctive sign on the Subject/Signatory that does not hold usage rights. However, DigitalSign is not required to seek evidence about the rights to use trademarks or other distinctive signs prior to issuing certificates.

3.1.7 NAME DISPUTE RESOLUTION PROCEDURE

DigitalSign is not liable in the case of name dispute resolution. In any case, names are assigned in accordance with the order in which they are entered.

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

3.2. INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

DigitalSign uses various circuits for issuing certificates in which the private key is managed differently. Either the user or DigitalSign 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 corresponding policies and in the certificate profile records.

a) Keys created by DigitalSign:
The keys can be delivered by DigitalSign to the Subject/Signatory, directly or through a registration authority on a qualified signature creation device (QSCD).

b) Keys created by the Signatory:
Proof of ownership of the private key in this case is the request that DigitalSign receives in **PKCS#10** format.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

These certificates are intended to be used by organization applications. The process of authenticating the identity of a legal person shall ensure that the person who is going to be issued the certificate exists, and this verification is carried out by consulting the official documentation. Verification of identity is complemented indirectly through documental

means by a notary or entity with legal authority for the recognition of signatures, in quality and empowered to act, and it's required the intervention of the persons who, in the bylaws, represent that collective person.

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

3.2.2.1 OCSP CERTIFICATES

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.

3.2.2.2 LEGAL PERSON CERTIFICATES

These certificates are intended to be used by organization applications. The process of authenticating the identity of a legal person shall ensure that the person who is going to be issued the certificate exists, and this verification is carried out by consulting the official documentation. Verification of identity is complemented indirectly through documental means by a notary or entity with legal authority for the recognition of signatures, in quality and empowered to act, and it's required the intervention of the persons who, in the bylaws, represent that collective person.

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:

3.2.3.1 NATURAL PERSON CERTIFICATES

The process of identity authentication of a natural person ensures that the person who is going to be issued the certificate is who he actually says he is, through submission of documentation as well as the signature. This can be achieved by three distinct ways:

a) presently at DigitalSign; or
b) the appropriate recognition of the signature by Notary (or equivalent entity according to the law); or
c) by a remote video conference.

The verification of the identity and powers of the representative/attorney (if applicable) is made indirectly through documental means by a notary or entity with legal authority for the recognition of signatures, in quality and empowered to act.

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

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

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

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.

3.3.2 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 website contains the forms required to apply for each type of certificate that DigitalSign distributes in different formats and the signature creation devices, if they are required.

After confirmation of the application data, the user receives an email sent to the account associated with the certificate application containing a link to confirm the application and accept the terms of use.

Once the application is confirmed, the Signatory is informed of the documentation to be submitted for this purpose and to comply with the physical identification requirement, if applicable.

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 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.

TSA and OCSP certificates are issued in a certificate issuing ceremony in a secure environment by trusted personnel.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

In the final entity certificates issued by DigitalSign, an email notification is sent to the applicant indicating the request's approval or denial.

TSA and OCSP certificates are issued in a key ceremony and subsequently delivered to the certificate holder.

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 verify that it has been issued correctly.

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

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Certification path and issued certificates are published at https://www.digitalsign.pt/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.

If it is a certificate replacement process, it is considered to be a renewal and thus counted when calculating the years of renewal without physical presence as required by law.

The certificates may be modified as renewal when the attributes of the Signatory or key holder that form part of the uniqueness control provided for this policy have not changed.

If the modification request is made within the ordinary period for renewal of the certificate, it is renewed instead of modified with prior revocation of the certificate to be modified.

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). A certificate is revoked until it is decided whether it should be revoked definitively or activated.

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

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

AC 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.

However, DigitalSign maintains the information about the status of an expired certificate in its databases and it can be accessed via the OCSP service.

Revoked certificates cannot be reinstalled under these practices.

The OCSP response for a revoked certificate when it expires maintains the revoked status and its cause.

Due to the different natures of the OCSP and CRL services, in the case of obtaining different responses for an expired certificate, the response given by the OCSP shall be maintained as a valid response.

For DigitalSign, the consultation service for the status of a primary certificate is the one offered by OCSP.

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:

- Any of the details contained in the certificate are amended.
- Errors or incomplete data detected in the data submitted in the certificate request or there are changes to the circumstances verified for issuing the certificate.
- Failure to pay for the certificate.

Due to 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 Signatory or person/entity responsible for the certificate is compromised or suspected of being compromised.
- There is unauthorised third party access or use of the private key of the Signatory or person/entity responsible for the certificate.
- There is misuse of the certificate by the Signatory or person/entity responsible for the certificate or failure to keep the private key secure.

Due to 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 unauthorised third party access to the activation details of the Signatory or person/entity responsible for the certificate.

There are circumstances that affect the Signatory or person/entity responsible for the certificate:

- The relationship is terminated between the Certification Authority and the Signatory or person/entity responsible for the certificate.
- There are changes to or termination of the underlying legal relationship or cause for issuing the certificate to the Signatory or person/entity responsible for the certificate.
- The applicant breaches part of the requirements established for requesting the certificate.

- The Signatory or person responsible for the certificate 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 Signatory or person/entity responsible for the certificate.
- There is a termination of the legal entity that is Signatory of the certificate and expiry of the authorization provided by the Signatory to the person/entity responsible for the certificate, or termination of the relationship between the Signatory and the person/entity responsible for the certificate.
- The Signatory requests revocation of the certificate in accordance with the provisions of this CPS.
- Firm resolution of the competent administrative or judicial authority.

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 corresponding section of this CPS.

In order to justify the need for the proposed revocation, 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 Subject/Signatory
- 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 DigitalSign's website and entering the Revocation Code.
- By physically going to the RA's offices during opening hours and signing the revocation form.
- By sending DigitalSign a document signed by a representative with sufficient representation powers for the entity requesting certificate revocation.

DigitalSign stores all the information relating to certificate revocation processes on its website.

The revocation management service and the query service are considered critical services, as specified in DigitalSign's contingency plan and business continuity plan. These services are 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 that services are not down longer than 24 hours.

In case of revocation due to non-payment of the issued certificate price, the RA or CA shall request by emailing the Signatory at their contact e-mail address, prior and on two successive occasions, that this situation is remedied within eight days, failing which, the certificate will be revoked immediately.

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 is issued at least once a day for end-user certificates. CRL for CA Certificates shall be issued at least annually, but also whenever a CA is revoked.

If a certificate listed in the CRL expires, it can be removed from the later-issued CRL after the expiry of the certificate.

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. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

DigitalSign is subject to the annual validations established by the UNE-ISO/IEC 27001 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems.

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:

- Unauthorised physical access
- Natural disasters
- Fires
- Failure in supporting systems (electricity, telecommunications, etc.).
- Building collapse
- Flooding
- Theft
- Unauthorised 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 day per year assistance and assistance during the 24 hours following the 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 Faraday cage protected against external radiation, with double flooring, 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's offices where encryption processes are undertaken is limited and protected by a combination of physical and procedural measures.

Access is limited to expressly authorised personnel who must show identification when they access and register, and CCTV cameras film and record any activity.

Any external person must be accompanied by a person in charge of the organisation when they are found within restricted areas for any reason.

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 which are managed by a software system that maintains an automatic audit log of comings and goings.

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

Access to the certification system is protected by four access levels.

5.1.3 POWER AND AIR CONDITIONING

DigitalSign safety facilities are equipped with:

- Electricity systems to ensure continuous, uninterrupted access to electricity
- Heating / ventilation / air conditioning to control the temperature and relative humidity.

5.1.4 WATER EXPOSURE

DigitalSign's facilities are in an area with a low flooding risk. The rooms in which computer equipment is stored have a humidity and flooding 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 demountable storage device (tapes, cartridges, CDs, disks, etc.) is only accessible by authorised personnel.

5.1.7 WASTE DISPOSAL

Once sensitive information is no longer useful, it is destroyed using the most appropriate means for the media containing it.

- Print-outs and paper: shredders or waste bins are provided for this purpose, for subsequent destruction in a controlled manner.
- Storage media: 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

Backups of critical data and routine audit logs are made. All backups are stored off-premises in safe environments.

5.2. PROCEDURAL CONTROLS

5.2.1 TRUST ROLES

Are defined as Trusted Persons all officials, employees, contractors and consultants who have access or control authentication or encryption operations, which could materially affect:

- Validation of information for certificate issuance requests.
- The acceptance, rejection, or other processes for subscription of certificates, requests for revocation or renewal, or enrollment information.
- The issuance or revocation of certificates, including personnel having access to restricted portions of the repository.
- Handling of End User information or requests.

Trusted Persons include, but are not limited to:

- Personal of customer's service.
- Cryptographic operations Personnel.
- Security personnel.
- Management and operating systems Personnel.

DigitalSign considers the categories of personnel identification in this section as Trusted Persons having Positions of Trust. People seeking to become Trusted Persons by obtaining a position of Security, must successfully complete the requirements of this CPS.

5.2.2 NUMBER OF PEOPLE REQUIRED PER TASK

DigitalSign has established and maintains a policy of strict control procedures to ensure segregation of duties, based on the responsibilities of each task, and ensuring that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold "Secret Shares" and vice versa.

Other manual operations such as the validation and issuance of qualified certificates, require the participation of at least two Trusted Persons, or a combination of at least one trusted person and automated process for validation and issuance.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing HR (or equivalent) or security functions and a check of well recognized forms of identification (e.g., id cards). Identity is further confirmed through the background checking procedures described in this CPS.

DigitalSign ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are granted access to:

- issued access devices and granted access to the required facilities.
- issued electronic credentials to access and perform specific functions on CA, RA, or other IT systems.

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.

Personnel in positions of trust must have no personal interests that conflict with undertaking the role to which they are entrusted.

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 request duties.

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

DigitalSign shall not assign a trusted or managed site to a person who is not suitable for the position, especially for having been convicted of a crime or misdemeanor affecting their suitability for the position. For this reason, an investigation will first be carried out, to the extent permitted by applicable law, on the following aspects but are not imitated to:

- Arrests for criminal offenses or criminal penalties associated with the nature of the job. As an example, crimes involving financial fraud.
- Any pattern of behavior that indicates personal irresponsibility, for example:
    - Arrests for driving under the influence of alcohol or drugs.

  - Bankruptcy declarations.
  - Recent credit problems (up to 3 years) (ie, missed mortgage or car payments).
- Any add on the resume or involving professional applications:
  - False employment statements (ie, claim to have worked for an employer particularly when it never did).
  - False statement on the academic qualifications (ie, claiming to be holder of a degree without ever having obtained it, or inflate the grade level that actually has as claiming to be the possessor of a degree having only obtained a Bachelor's degree).

To the extent that any of these requirements imposed by this section are not met due to prohibitions or limitations of local law or other circumstances, DigitalSign will use a surrogate research technique permitted by law, that provides substantially similar information, including, but not limited the respective background checks.

Factors revealed in the background check that could be considered for rejection of candidates for Trusting Positions or for developing actions against existing trusted person generally include (but are not limited to) the following:

- False presentation made by the candidate or trusted person.
- References highly adverse or unreliable.
- Certain criminal convictions.
- Indications of a lack financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, which determine the appropriate action in the light of the type, magnitude and frequency of the behavior, discovered by checking its past. Such actions may include measures covering the cancellation of offers of employment made to candidates for Trusting Positions or the end of the occupation of existing Trusted Persons.

The use of information revealed in the background check is subject to local law.

5.3.2 BACKGROUND CHECKING PROCEDURES

DigitalSign's HR procedures include conducting relevant investigations before hiring anyone.

5.3.3 TRAINING REQUIREMENTS

DigitalSign provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. DigitalSign maintains records of such trainings in its Quality Management System ISO 9001 and ISO/IEC 27001. DigitalSign periodically review and amend its program of training, if necessary.

The training programs / courses are tailored to the individual's responsibilities and include the following:

- Basic concepts of Public Key Infrastructures
- Job responsibilities
- Operational policies and safety procedures
- Use and operation of implemented hardware and software
- Report and handling incidents
- Recovery procedures and business continuity in the event of disaster

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. Periodic training of safety awareness is provided on a regular basis.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORISED ACTIONS

DigitalSign has established an internal penalty system, which is described in its HR policy, to be applied when an employee undertakes unauthorised 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.

In the event that all or part of the certification services are operated by a third party, the controls and provisions made in this section or in other parts of the CPS are applied and enforced by the third party that performs the operational functions of the certification services, and the certification authority is responsible for the actual implementation in all situations.

These aspects are specified in the legal instrument used to agree on the provision of certification services by third parties other than DigitalSign, and the third parties must be obliged to meet the requirements demanded by DigitalSign.

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.

This documentation is in an internal repository accessible by any DigitalSign employee; the repository contains a list of documents of mandatory knowledge and compliance.

Any documentation that employees require is also 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 established by the ISO/IEC 27001 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems.

5.4.1 TYPES OF EVENTS RECORDED

DigitalSign records and saves the audit logs of every event relating to the CA's security system.
The following events are recorded:

- System switching on and off.
- Creation, deletion and setting up of passwords or changed privileges.
- Attempts to log in and out.
- Attempts at unauthorised access to the CA's system made online.
- Attempts at unauthorised access to the file system.
- Physical access to audit logs.
- Changes to system settings and maintenance.
- CA application logs.
- CA application switching on and off.
- Changes to the CA's details and/or 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.
- Events related to the cryptographic module's lifecycle, such as its reception, use and uninstallation.

DigitalSign also retains the following information, either manually or digitally:

- The key generation event and key management databases.
- Physical access records.
- Maintenance and system configuration changes.
- Personnel changes.
- Reports on compromises and discrepancies.
- Records of the destruction of material containing key information, activation data or personal information about the Signatory for individual certificates or a future key holder for organisation certificates, access to the certificate.
- Possession of activation data for operations with the Certification Authority's private key.
- Complete reports on physical intrusion attempts in infrastructure that support certificate issuance and management.

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

Processing audit records involves reviewing records that include verification that they have not been tampered with, a brief inspection of all log entries and further investigation of any alerts or irregularities in the logs. The actions taken from the audit review are documented.

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 for storing audit logs.
- Audit log files are not rewritten.
- That the saved information includes at least the following: event type, date and time, user executing the event and result of the process.
- The audit log files are saved in structured files that can be included in a database for subsequent data mining.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

DigitalSign stores the information from audit logs for at least five years.

5.4.4 PROTECTION OF AUDIT LOG

The systems' audit logs are protected against manipulation via signatures in the files that contain them.

They are stored in fireproof devices.

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

Audit log files can only be accessed by authorised persons.

Devices are always handled by authorised 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 that important files are lost or destroyed, audit 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, the network and by the certificate management software, in addition to the data generated manually, which is stored by duly authorised personnel, all of which makes up the audit record accumulation system.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

When the audit log accumulation system records an event, there is no need to send a notification to the individual, organisation, device or application that caused the event.

It may be communicated whether the result of his/her action was successful or not, but the action is not audited.

5.4.8 VULNERABILITY ASSESSMENTS

The analysis of vulnerabilities is covered by the DigitalSign audit processes. Risk and vulnerability management processes are reviewed once a year in accordance with the ISO/IEC 27001 certificate and included in the risk analysis document. This document specifies the controls implemented to guarantee 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. PKI, TSA and OCSP
- Any data related to certificates, including contracts with Signatories and the RA. The data relating to their identification and location.
- Requests to issue and revoke certificates.
- Type of document submitted in the license application.
- Identity of the Registration Authority that accepts the certificate application.
- Unique identification number provided by the previous document.
- 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 correctly filing all this material.

5.5.2 RETENTION PERIOD FOR ARCHIVE

Certificates, contracts with Subjects/Signatories and any information relating to the Subject/Signatory's identification and authentication must be kept for at least 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 TIMESTAMPING OF RECORDS

Logs are dated with a reliable source via NTP from the OAL and GPS synchronization systems.

5.5.6 ARCHIVE COLLECTION CYSTEM (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 final entity's keys are changed by starting a new issuance procedure (see the corresponding section of this CPS).

In CA (Root CA, Subordinate CA). The key will be changed before the CA certificate expires. The certificate to be updated from the CA and its private key can only be used to sign CRLs while there are active certificates issued by the old CA. A new CA certificate is generated with a new private key and a CN (*common name*) other than the CA certificate to be replaced.

A CA's certificate is also changed when there is a change to cryptographic technology (algorithms, key size, etc.) that so requires it.

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 centre were necessary as part of the ISO/IEC 27001 certification.

If root key security is compromised, this must be considered a specific case in the contingency and business continuity document. If the keys are replaced, this incident affects recognition by the various private and public sector applications. Recovering the validity of keys in business terms mainly depends on the duration of these recognised processes.

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.

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 ISO 27001 and ISO 9001 systems, 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 contingency plan encompassed in DigitalSign's ISO/IEC 27001 certification considers that compromised security of the CA's private key is a disaster.
If the security of a root key is compromised:

- All Subjects/Signatories, User Parties and other CAs with which agreements or other relationships have been established must be informed.
- They are 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 critical services (revocation and publication of revocations) in accordance with the contingency and business continuity plan encompassed in the ISO/IEC 27001 certification.

5.8. CA OR RA TERMINATION

In the event it is necessary to cease operations of the CA or any of the RAs, DigitalSign shall make commercially reasonable effort to notify in advance the end-users, relying parties and other entities affected by such termination.

When required the CA termination, DigitalSign will develop a termination plan to minimize the impact to its customers, end users and relying parties. Such a plan should contain the following, as applicable:

- Report the cessation of activity
- Notify the termination of the activity to the Autoridade Nacional de Segurança for the purposes of cancellation of security clearances
- Cease all contractual relationships with third parties authorized to act on its behalf in performing functions relating to the issuance of certificates
- Provide notice to the parties affected by the term, such as end users, relying parties and customers, informing them of the status of CA
- Support the costs of such notifications
- The revocation of the certificate issued to DigitalSign
- The preservation of the file and records of CA during the imposed period in this CPS and applicable law
- Continued support services to end users and customers
- The continuation of revocation services, such as CRL issuance and maintenance of online status check service

- The revocation, if necessary, of all issued certificates that are not expired or revoked already
- Refund, if necessary, unexpired and unrevoked certificate holders which are revoked under the termination plan, or alternatively issue replacement certificates by a successor CA
- Destruction (or equivalent) of the private key of the CA and HSMs that contains them
- Plan for transition services for a successor CA, ensuring that the entity to which is transmitted all documentation undertakes its maintenance during the period of time required by law.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

The generation of cryptographic CA keys is made by authorized elements for such, at a security level 4 or higher, at a ceremony planned and audited in accordance with written procedures to perform operations, and using systems that ensure the requirements of cryptographic strength of keys. All activities developed in each key generation ceremony are recorded, dated and signed by all the elements involved. These records are retained for future audit purposes.

The cryptographic hardware used for the generation of CA keys, meets at least the requirements of FIPS 140-1 Level 3 and / or Common Criteria EAL4+.

6.1.1.1 CREATING THE SIGNATORY'S KEY PAIR

Subjects/Signatories keys of a qualified certificate for advanced electronic signature/Seal can be remotely generated in a secure environment as required by Regulation (EU) 910/2014. The keys are generated in secure signature creation devices, duly approved. The sole control of the private key is granted through the use of two factor authentication.

In the case of the key pair is generated in a smartcard or usb token by the RA, the delivery of the key pair and corresponding certificate is done in person or through registered postal mail or equivalent. The cryptographic device access codes are sent to the end user via email (to the address on the certificate) after receipt and verification of the "Statement of Reception", duly signed by the Subject/Signatory.

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.

All keys are created using the RSA public key algorithm, with a minimum length of 2048 bits.

DigitalSign has controls to ensure that generated keys are aligned with the Certification Policies, and cannot 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 is sent to DigitalSign to create the certificate when the circuit so requires. It is sent in standard PKCS#10 format.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The CA certificate are available to users on DigitalSign's web site 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 CAs and for Signatories' certificates is encrypted pursuant to RFC 3280 and PKCS#1. RSA is the key generation algorithm.

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 CA makes all reasonable efforts to confirm that the CA's signature keys are used only for the purposes of generating certificates and signing CRLs.

The key usage limitation is defined in the certificate content in the extensions: *keyUsage*, *extendedKeyUsage* and *basicConstraints*:

CA	Key Usage	Extended Key Usage	Basic Constraints
Global Chambersign Root - 2008	**critical**, keyCertSign, cRLSign	--	**critical**,CA:true, pathlen:12
AC Camerfirma Portugal - 2015	**critical**, keyCertSign, cRLSign	--	**critical**,CA:true, pathlen:3
DigitalSign Primary CA	**critical**, keyCertSign, cRLSign	--	**critical**,CA:true, pathlen:1
DigitalSign Qualified CA	**critical**, keyCertSign, cRLSign	emailProtection clientAuth	**critical**,CA:true, pathlen:0
OCSP Certificate	**critical**, digitalSignature	ocspSigning	**critical**,CA:false
Individual Certificate	**critical**, nonRepudiation	emailProtection clientAuth	**critical**,CA:false
Professional Certificate	**critical**, nonRepudiation	emailProtection clientAuth	**critical**,CA:false
Member Certificate	**critical**, nonRepudiation	emailProtection clientAuth	**critical**,CA:false
Representative Certificate	**critical**, nonRepudiation	emailProtection clientAuth	**critical**,CA:false
Organization Certificate	**critical**, nonRepudiation	emailProtection clientAuth	**critical**,CA:false

DigitalSign Qualified TSA CA	**critical**, keyCertSign, cRLSign	timeStamping	**critical**,CA:true, pathlen:0
OCSP Certificate	**critical**, digitalSignature	ocspSigning	**critical**,CA:false
TSA Certificate	**critical**, digitalSignature	**critical**, timeStamping	**critical**,CA:false

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

DigitalSign has implemented a combination of monitoring procedures to ensure physical and logical security of its private key. It also requires the subscribers, by contract, to take reasonable precautions to prevent loss, disclosure, modification or unauthorized use of their private keys.

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

6.2.1.1 THE CA'S PRIVATE KEY

The private signature key of the root CAs and Subordinate CAs are maintained in a cryptographic device that meets FIPS 140-2 level 3 and/or EAL4+ specifications.

When the CA's private key is outside the device, it is kept encrypted.

A backup is made of the CAs private keys which are 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's private key backups are stored securely. This procedure is described in detail in the DigitalSign security policies.

6.2.1.2 THE SIGNATORY'S PRIVATE KEY

The Signatory's private key are stored in cryptographic devices distributed by DigitalSign to host qualified certificates must meet all requirements of qualified secure signature creation devices and therefore are suitable for generating qualified signatures/seals.

Information regarding the key creation and custody process that DigitalSign uses is included in the digital certificate itself, in the corresponding OID, allowing the User Party to act in consequence.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

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 in order 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 qualified certificate through the DigitalSign remote signature solution.

In this case, the private key is generated in a qualified signature creation device (QSCD) and encrypted in a reliable environment. The key encryption relies on a AES symmetric key (128 bits) wrapping key created by the QSCD and derived from the QSCD 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 records on CA private key management processes.

DigitalSign does not create copies of user's private keys, except in the case referred in the previous section 6.3.2.

6.2.5 PRIVATE KEY ARCHIVAL

The CAs private keys are filed for at least 10 years after the last certificate has been issued. At least two people are required to retrieve the CA's private key from the archiving cryptographic device.

DigitalSign keeps records on CA private key management processes.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

DigitalSign creates key pairs directly in the cryptographic module in which they are used. DigitalSign makes copies of these keys with the purpose of routine recoveries and in cases of disasters.

When keys are transferred to another cryptographic module (for backup purposes), such keys are transferred between cryptographic modules in encrypted form, and according to the manufacturer's specifications.

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

The Signatory's private key is accessed via an activation key, which only the Signatory 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 records on CA private key management processes.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

For certificates on a smartcard or usb token, the Signatory's private key is deactivated once the cryptographic device used to create the signature is removed from the reader.

The private keys stored on a HSM 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 DESTROYING PRIVATE KEY

Before the keys are destroyed, a revocation of the certificate of the public key associated with them is issued.

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

Backups are destroyed securely.

The Signatory's keys on hardware can be destroyed by following the steps described in the cryptographic device administrator's manual to eliminate them.

DigitalSign keeps records 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 maintains its archives for a minimum period of twenty (20) years provided that the technology at the time allows this. The documentation to be kept includes public key certificates issued to Signatories and proprietary public key certificates.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

The private key must not be used once the validity period of the associated public key certificate has expired.

The public key or its public key certificate can be used as a mechanism for verifying encrypted data with the public key outside the temporary scope for validation work.

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 6.3.1 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

In the cases where activation data is generated by DigitalSign, it is communicated to the Subject by an independent channel. AC DigitalSign stores this information in its database. Data can be sent back to the subject at prior request to the email address associated with the certificate, and it is effective as long as the user has not previously changed it.

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 digital certification systems.

In relation to information security, the certification model on ISO/IEC 27001 information management systems is followed.

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

DigitalSign ensures systems maintaining CA activities are reliable and secure from unauthorized access. Furthermore, DigitalSign limits access to production servers only to individuals in need of such access effectively.

DigitalSign production network is logically separated from other components. This separation prevents network access except through well-defined applicational processes. DigitalSign uses firewall systems to protect the network from internal and external intrusion and limit the nature and origin of the network activities that may access production systems

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
- the Signatory'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 using 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. LIFECYCLE 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 to resolve any detected vulnerability.

In response to intrusion and vulnerability analyses, adaptations are made to systems and applications that may have security problems, and to security alerts received from managed security services contracted with third parties.

The changes are incorporated and the measures taken for acceptance, implementation or rejection of the change are documented.

In cases where the implementation of the update or correction of a problem entails a situation of vulnerability or a significant risk, it is included in the risk analysis and alternative controls are implemented until the risk level is acceptable.

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.
An annual training plan has been established for such purposes.

DigitalSign has mechanisms and / or policies to control or monitor the configuration of its CA systems. After installation and periodically DigitalSign validates the integrity of its CA systems.

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 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 LIFECYCLE 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.

The policy used to configure security systems and elements is to start from an initial state of total blocking and to open the services and ports necessary for executing the services. Reviewing accesses is one of the tasks carried out in the systems department.

Management systems and production systems are in separate environments.

6.8. TIME-STAMPING

DigitalSign has established a time synchronisation procedure in coordination with the OAL Observatório Astronómico de Lisboa via NTP. It also obtains a secure source via GPS synchronisation.

7. CERTIFICATE AND CRL PROFILE

7.1. CERTIFICATE PROFILE

Certificate profiles comply with RFC 5280.

All qualified or recognised 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.

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 [1.3.6.1.4.1.25596.3.2.3.2.2] INDIVIDUAL CERTIFICATE

This certificate profile aims to identify a natural person (individual).

Extension		Value / Description
Version		V3
Serial Number (certificate)		<Unique serial number of the certificate>
signatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity>
Subject	CN	<Signatory full name>
	OU(1)	RemoteQSCDManagement
	G	<Signatory first name(s)>
	SN	<Signatory last name(s)>
	SERIALNUMBER (optional)	<Signatory identifier, according to ETSI EN 319 412-1>
	E	<Signatory email address, or to which he/she has access>
	OU (optional)	Limitation1 - <Any limitations for use of signature (line 1)>
	OU (optional)	Limitation2 - <Any limitations for use of signature (line 2)>
	OU (optional)	Limitation3 - <Any limitations for use of signature (line 3)>
	OU (optional)	Obs1 - <Any comments (line 1)>
	OU (optional)	Obs2 - <Any comments (line 2)>
	OU (optional)	Obs3 - <Any comments (line 3)>
	OU	Certificate Profile - Qualified Certificate - Individual
	C	<Country (two-letter country code according to ISO 3166)>
Public key		RSA (2048 bits or more)

Basic Constraints (Critical)	CA=False	
Key Usage (Critical)	Non Repudiation	
Subject Key Identifier	Subject Public Key SHA-1	
Authority Key Identifier	Issuer Public Key SHA-1	
Certificate Policies	[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.3.2.2 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/ [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2	
CRL Distribution Points	[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.crl	
Authority Information Access	AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.p7b	
Enhanced 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	RFC822 Name=< Signatory email address, or to which he/she has access>	
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1]
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]	
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]	
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	Pds Locations PdsLocation= https://www.digitalsign.pt/repository/cps/ddp Language=pt PdsLocation= https://www.digitalsign.pt/repository/cps/ddp_en Language=en

(1) Only present on certificates issued for remote signature

7.1.2.2 [1.3.6.1.4.1.25596.3.2.3.2.3] PROFESSIONAL CERTIFICATE

Certificate to be used for digital signature by natural persons.
This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfillment of his/her profession. Usually this type of certificate is issued to members of professional associations, where the entitlement should be checked with his/her association.

Extension	Value / Description
Version	V3
Serial Number (certificate)	<Unique serial number of the certificate>

signatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer		<2nd level CA DN>	
not Before		<Initial validity>	
not After		<Final validity>	
Subject	CN	<Signatory full name>	
	OU(1)	RemoteQSCDManagement	
	G	<Signatory first name(s)>	
	SN	<Signatory last name(s)>	
	SERIALNUMBER (optional)	<Signatory identifier, according to ETSI EN 319 412-1>	
	E	<Signatory email address, or to which he/she has access>	
	OU	Entitlement - <Professional title verified with the Professional Order>	
	OU (optional)	Limitation1 - <Any limitations for use of signature (line 1)>	
	OU (optional)	Limitation2 - <Any limitations for use of signature (line 2)>	
	OU (optional)	Limitation3 - <Any limitations for use of signature (line 3)>	
	OU (optional)	Obs1 - <Any comments (line 1)>	
	OU (optional)	Obs2 - <Any comments (line 2)>	
	OU (optional)	Obs3 - <Any comments (line 3)>	
	OU	Certificate Profile - Qualified Certificate - Professional	
	C	<Country (two-letter country code according to ISO 3166)>	
Public key		RSA (2048 bits or more)	
Basic Constraints (Critical)		CA=False	
Key Usage (Critical)		Non Repudiation	
Subject Key Identifier		Subject Public Key SHA-1	
Authority Key Identifier		Issuer Public Key SHA-1	
Certificate Policies		[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.3.2.3 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/ [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2	
CRL Distribution Points		[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.crl	
Authority Information Access		AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.p7b	
Enhanced 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		RFC822 Name=< Signatory email address, or to which he/she has access>	
QCStatements		id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1]
		id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]	

	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]	
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	Pds Locations PdsLocation= https://www.digitalsign.pt/repository/cps/ddp Language=pt PdsLocation= https://www.digitalsign.pt/repository/cps/ddp_en Language=en

(1) Only present on certificates issued for remote signature

7.1.2.3 [1.3.6.1.4.1.25596.3.2.3.2.4] MEMBER CERTIFICATE

Certificate to be used for digital signature by natural persons.
This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfillment of his/her profession. Usually this type of certificate is issued to members of professional associations, where the entitlement should be checked with his/her association.

Extension		Value / Description
Version		V3
Serial Number (certificate)		<Unique serial number of the certificate>
signatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity>
Subject	CN	<Signatory full name>
	OU(1)	RemoteQSCDManagement
	G	<Signatory first name(s)>
	SN	<Signatory last name(s)>
	SERIALNUMBER (optional)	<Signatory identifier, according to ETSI EN 319 412-1>
	E	<Signatory email address, or to which he/she has access>
	T (optional)	<Academic degree or another title that the holder can use>
	OU	Entitlement - <Position or function that takes/plays in the organization (see field "O")>
	O	<Full name of the organization where holds/plays the position or function defined in the "OU = Entitlement"
	OrganizationIdentifier (2.5.4.97)	<Legal person identifier, according to ETSI EN 319 412-1>
	OU (optional)	Limitation1 - <Any limitations for use of signature (line 1)>
	OU (optional)	Limitation2 - <Any limitations for use of signature (line 2)>
	OU (optional)	Limitation3 - <Any limitations for use of signature (line 3)>
	OU (optional)	Obs1 - <Any comments (line 1)>
	OU (optional)	Obs2 - <Any comments (line 2)>
	OU (optional)	Obs3 - <Any comments (line 3)>
	OU	Certificate Profile - Qualified Certificate - Member

	C	<Country (two-letter country code according to ISO 3166)>
Public key		RSA (2048 bits or more)
Basic Constraints (Critical)		CA=False
Key Usage (Critical)		Non Repudiation
Subject Key Identifier		Subject Public Key SHA-1
Authority Key Identifier		Issuer Public Key SHA-1
Certificate Policies		[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.3.2.4 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/ [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2
CRL Distribution Points		[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.crl
Authority Information Access		AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.p7b
Enhanced 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		RFC822 Name=< Signatory email address, or to which he/she has access>
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1] id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]	
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]	
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	Pds Locations PdsLocation= https://www.digitalsign.pt/repository/cps/ddp Language=pt PdsLocation= https://www.digitalsign.pt/repository/cps/ddp_en Language=en

(1) Only present on certificates issued for remote signature

7.1.2.4 [1.3.6.1.4.1.25596.3.2.3.2.5] REPRESENTATIVE CERTIFICATE

Certificate to be used for digital signature by natural persons.
This certificate profile aims to identify a natural person (individual), as legal representative or attorney of an organization.

Extension	Value / Description
Version	V3
Serial Number (certificate)	<Unique serial number of the certificate>

signatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity>
Subject	CN	<Signatory full name>
	OU(1)	RemoteQSCDManagement
	G	<Signatory first name(s)>
	SN	<Signatory last name(s)>
	SERIALNUMBER (optional)	<Signatory identifier, according to ETSI EN 319 412-1>
	E	<Signatory email address, or to which he/she has access>
	T (optional)	<Academic degree or another title that the holder can use>
	OU	Entitlement - <Powers of representation that the representative/attorney hold in the organization (see field "O")>
	O	<Full name of the organization>
	OrganizationIdentifier (2.5.4.97)	<Legal person identifier, according to ETSI EN 319 412-1>
	OU (optional)	Limitation1 - <Any limitations for use of signature (line 1)>
	OU (optional)	Limitation2 - <Any limitations for use of signature (line 2)>
	OU (optional)	Limitation3 - <Any limitations for use of signature (line 3)>
	OU (optional)	Obs1 - <Any comments (line 1)>
	OU (optional)	Obs2 - <Any comments (line 2)>
	OU (optional)	Obs3 - <Any comments (line 3)>
	OU	Certificate Profile - Qualified Certificate - Representative
	C	<Country (two-letter country code according to ISO 3166)>
Public key		RSA (2048 bits or more)
Basic Constraints (Critical)		CA=False
Key Usage (Critical)		Non Repudiation
Subject Key Identifier		Subject Public Key SHA-1
Authority Key Identifier		Issuer Public Key SHA-1
Certificate Policies		[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.3.2.5 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/ [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2
CRL Distribution Points		[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.crl
Authority Information Access		AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.p7b
Enhanced 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	RFC822 Name=< Signatory email address, or to which he/she has access>	
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1] id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]	
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]	
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	Pds Locations PdsLocation= https://www.digitalsign.pt/repository/cps/ddp Language=pt PdsLocation= https://www.digitalsign.pt/repository/cps/ddp_en Language=en

(1) Only present on certificates issued for remote signature

7.1.2.5 [1.3.6.1.4.1.25596.3.2.3.2.6] ORGANIZATION CERTIFICATE

Certificate to be used for digital seal by legal persons.

Extension		Value / Description
Version		V3
Serial Number (certificate)		<Unique serial number of the certificate>
signatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		<2nd level CA DN>
not Before		<Initial validity>
not After		<Final validity>
Subject	CN	<Full name of the organization>
	OU(1)	RemoteQSCDManagement
	E	<Signatory email address, or to which Signatory has access>
	O	<Full name of the organization>
	OrganizationIdentifier (2.5.4.97)	<Legal person identifier, according to ETSI EN 319 412-1>
	OU (optional)	Limitation1 - <Any limitations for use of seal (line 1)>
	OU (optional)	Limitation2 - <Any limitations for use of seal (line 2)>
	OU (optional)	Limitation3 - <Any limitations for use of seal (line 3)>
	OU (optional)	Obs1 - <Any comments (line 1)>
	OU (optional)	Obs2 - <Any comments (line 2)>
	OU (optional)	Obs3 - <Any comments (line 3)>
	OU	Certificate Profile - Qualified Certificate - Organization
	C	<Country (two-letter country code according to ISO 3166)>
Public key		RSA (2048 bits or more)
Basic Constraints (Critical)		CA=False

Key Usage (Critical)	Non Repudiation	
Subject Key Identifier	Subject Public Key SHA-1	
Authority Key Identifier	Issuer Public Key SHA-1	
Certificate Policies	[1] Policy: Policy Identifier =1.3.6.1.4.1.25596.3.2.3.2.6 [1,1]Policy Qualifier Info: Policy qualifier id=CPS Qualifier: http://www.digitalsign.pt/repository/ [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.3	
CRL Distribution Points	[1]CRL Distribution Point DistributionPoint: fullName: URL:http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.crl	
Authority Information Access	AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDCA.p7b	
Enhanced 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	RFC822 Name=< Signatory email address, or to which he/she has access>	
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]	
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]	
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-eseal [0.4.0.1862.1.6.2]
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	Pds Locations PdsLocation= https://www.digitalsign.pt/repository/cps/ddp Language=pt PdsLocation= https://www.digitalsign.pt/repository/cps/ddp_en Language=en

(1) Only present on certificates issued for remote signature

7.1.2.6 [1.3.6.1.4.1.25596.3.2.4.2.2] TSA CERTIFICATE

Certificate to be used by TimeStamping Authorities (TSA).
For matters relating to the Time Stamping service, in conjunction with this CPS, should also be consulted the document "TimeStamp Policy and Certification Practices", which is available in the repository indicated in the section 1.2.

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>	
Subject	CN	<Application Name>	
	O	<Organization>	
	OU (0 or more)	<Project or other relevant information about subscriber / organization>	
	OrganizationIdentifier (2.5.4.97)	<Legal person identifier, according to ETSI EN 319 412-1>	
	L (optional)	<Locality of the organization>	
	S (optional)	<State of the organization>	
	C	<Country (two-letter country code according to ISO 3166)>	
Public key		RSA (2048 bits or more)	
Basic Constraints (Critical)		CA=False	
Key Usage (Critical)		Digital Signature	
Subject Key Identifier		Subject Public Key SHA-1	
Authority Key Identifier		Issuer Public Key SHA-1	
Certificate Policies		[1] Policy: Policy Identifier = 1.3.6.1.4.1.25596.3.2.4.2.2 [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/DIGITALSIGNQUALIFIEDTSACA.crl	
Authority Information Access		AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDTSACA.p7b	
Enhanced Key Usage (critical)		Time Stamping (1.3.6.1.5.5.7.3.8)	
QCStatements		id-etsi-tsts-EuQCompliance (0.4.0.19422.1.1)	
		id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]
		id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]	
		id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]	
		id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	Pds Locations PdsLocation= https://www.digitalsign.pt/repository/cps/ddp Language=pt PdsLocation= https://www.digitalsign.pt/repository/cps/ddp_en Language=en

7.1.3 ALGORITHM OBJECT IDENTIFIERS (OID)

See 7.1.2.

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

Where this extension is used, certificates contain the respective identifier as defined in the section 7.1.2.

7.1.7 USING THE "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
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<2nd level CA DN>
Efective Date	<Issue date of the CRL. The CRL are effective upon issuance>
Next Update	<Date on which the next CRL will be issued. The emission frequency of the CRL is 24 hours>

Authority Key Identifier	Issuer Public Key SHA-1
Authority Information Access	AIA: (Issuer Cert URL) http://www.digitalsign.pt/repository/DIGITALSIGNQUALIFIEDTSACA.p7b
Revoked Certificates	List of revoked certificates, including the serial number and date of revocation

7.3. OCSP PROFILE

OCSP responder These certificates are issued by each CA managed by AC DigitalSign according to the RFC 6960 standard.

The validity period of OCSP certificates will be no more than 3 years.

As described in RFC 6960, the OCSP responder status can be checked by using CRL Distribution Points.

7.3.1 VERSION NUMBER

The OCSP Responder certificates are Version 3.

7.3.2 OCSP EXTENSIONS

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>
Subject	CN	<Application Name>
	O	<Organization>
	OU (0 or more)	<Project or other relevant information about subscriber / organization>
	OrganizationIdentifier (2.5.4.97)	<Legal person identifier, according to ETSI EN 319 412-1>
	L (optional)	<Locality of the organization>
	S (optional)	<State of the organization>
	C	<Country (two-letter country code according to ISO 3166)>
Public key		RSA (2048 bits or more>
Basic Constraints (Critical)		CA=False
Key Usage (Critical)		Digital Signature
Subject Key Identifier		Subject Public Key SHA-1
Authority Key Identifier		Issuer Public Key SHA-1
Certificate Policies		[1] Policy: Policy Identifier =<policy OID – see section 7.3.3>

	[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:<CRL Distribution Point defined by the issuer CA>
Authority Information Access	AIA: (responder) <Application OCSP Responder URL> AIA: (Issuer Cert URL) <URL where issuer certificate chain can be obtained>
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)
'No Check' extension	

7.3.3 ALGORITHM OBJECT IDENTIFIERS (OID)

See 7.3.2.

7.3.4 NAME FORMAT

See 7.3.2.

7.3.5 NAME RESTRICTIONS

No stipulation.

7.3.6 CERTIFICATION POLICY (OID) OBJECT IDENTIFIER

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

Issuer	Policy OID
DigitalSign Qualified CA	1.3.6.1.4.1.25596.3.2.3.2.1
DigitalSign Qualified TSA CA	1.3.6.1.4.1.25596.3.2.4.2.1

7.3.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation.

7.3.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.3.9 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 7.3.6.

7.3.10 OCSP REQUEST FORMAT

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

7.3.11 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 **Error! Reference source not found.**, 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 **Error! Reference source not found.**.

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 **Error! Reference source not found.**.

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 **Error! Reference source not found.**.
- 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 **Error! Reference source not found.**.
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.

APPENDIX I. ACRONYMS

AES	Advanced Encryption Standard. Standard for encrypting data.
CA	Certification Authority.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List. List of revoked certificates.
CSR	Certificate Signing Request.
DES	Data Encryption Standard. Standard for encrypting data.
DN	Distinguished Name. Distinguished name in the digital certificate.
DSA	Digital Signature Algorithm. The signature's algorithm standard.
FIPS	Federal Information Processing Standard Publication.
IETF	Internet Engineering Task Force.
ISO	International Standards Organisation International Standards Organisation.
ITU	International Telecommunications Union.
LDAP	Lightweight Directory Access Protocol. Protocol for directory access.
OCSP	On-line Certificate Status Protocol. Protocol for accessing the status of certificates.
OID	Object Identifier.
PA	Policy Authority.
PC	Certification Policy.
PIN	Personal Identification Number.
PKI	Public Key Infrastructure.
QSCD	Qualified Signature Creation Device
RA	Registration Authority.
RSA	Rivest-Shimar-Adleman. Type of encryption algorithm.
SHA	Secure Hash Algorithm.

SSCD Secure Signature Creation Device

SSCDSD Secure Signature Creation Data Storage Device

SSL Secure Sockets Layer. A protocol designed by Netscape that has become standard on the Internet. It allows the transmission of encrypted information between a browser and a server.

TCP/IP Transmission Control. *Protocol/Internet Protocol*. System of protocols, as defined in the IETF framework. The TCP protocol is used to split source information into packets and then recompile it on arrival. The IP protocol is responsible for correctly directing the information to the recipient.

APPENDIX II. DEFINITIONS

Activation data	Private data such as PINs or passwords used for activating the private key.
Applicant	Within the context of this certification policy, the applicant is a natural person with special powers to carry out certain procedures on behalf of the entity.
Certificate	A file that associates the public key with some data identifying the Subject/Signatory and signed by the CA.
Certification Authority	This is the entity responsible for issuing and managing digital certificates. It acts as the trusted third party between the Subject/Signatory and the User Party, associating a specific public key with a person.
Certification Policy	A set of rules defining the applicability of a certificate in a community and/or in an application, with common security and usage requirements.
CPS	Defined as a set of practices adopted by a Certification Authority for issuing certificates in compliance with a specific certification policy.
CRL	A file containing a list of certificates that have been revoked for a certain period of time and which is signed by the CA.
Cross certification	Establishing a trust relationship between two CAs, by exchanging certificates between the two under similar levels of security.
Digital signature	The result of the transformation of a message, or any type of data, by the private key application in conjunction with known algorithms, thus ensuring: a) that the data has not been modified (integrity) b) that the person signing the data is who he/she claims (ID) c) that the person signing the data cannot deny having done so (non-repudiation at origin)
Entity	Within the context of these certification policies, a company or organisation of any type with which the applicant has any kind of relationship.
Key pair	A set consisting of a public and private key, both related to each other mathematically.

OID	A unique numeric identifier registered under the ISO standardisation and referring to a particular object or object class.
PKI	A set of hardware, software and human resources elements and procedures, etc., that a system is made up of based on the creation and management of public key certificates.
Policy authority	A person or group of people responsible for all decisions relating to the creation, management, maintenance and removal of certification and CPS policies.
Private key	A mathematical value known only to the Subject/Signatory and used for creating a digital signature or decrypting data. Also called signature creation data.
Public key	A publicly known mathematical value used for verifying a digital signature or encrypting data. Also called signature verification data. The CA's private key is to be used for signing certificates and CRLs.
Registration Authority	The entity responsible for managing applications and identification and registration of certificates.
SCDSD	*Secure Signature Creation Data Storage Device* A software or hardware element used to safeguard the Subject/Signatory's private key so that only he/she has control over it.
SSCD	Secure Signature Creation Device. A software or hardware element used by the Subject/Signatory for generating digital signatures, so that cryptographic operations are performed within the device and control is guaranteed solely by the Subject/Signatory.
Subject/Signatory	Within the context of this certification practices statement, the natural person whose public key is certified by the CA and who has a valid private key for generating digital signatures.
User Party	Within the context of this certification policy, the person who voluntarily trusts the digital certificate and uses it as a means for accrediting the authenticity and integrity of the signed document.