DIGITALSIGN – CERTIFICADORA DIGITAL, SA.

CERTIFICATION PRACTICE STATEMENT

VERSION 2.1 – 16/10/2026

[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	Edition nr	Content
18/01/2021	0.0	Initial draft
27/01/2021	1.0	Review and publication subsequent to the creation of the CAs
24/02/2021	1.1	Revision
08/04/2021	1.2	Revision
29/04/2021	1.3	Revision
15/09/2021	1.4	Revision
18/05/2022	1.5	Revision
27/04/2023	1.6	Revision
30/10/2023	1.7	Revision
30/01/2024	1.8	Revision
06/12/2024	1.9	Revision
28/03/2025	1.10	Revision
16/07/2025	1.11	Revision
15/07/2026	2.0	Review and update in accordance with Regulation (EU) 2024/1183 (eIDAS 2)
16/10/2026	2.1	Section 6.3.2: separated the maximum validity periods of qualified electronic signature certificates and S/MIME certificates Section 1.1: updated references to the CA/Browser Forum documents

RELATED DOCUMENTS

Document Details	Author(s)
Certification Profile List	DigitalSign
PKI Disclosure Statement	DigitalSign
Timestamp Policy and TSA Practice Statement	DigitalSign
Signature Validation Service Policy and Practice Statement	DigitalSign
Preservation Service Policy and Practice Statement	DigitalSign
Remote QSCD Management Service Policy and Practice Statement	DigitalSign
Qualified Electronic Attribute Attestation Service Policy and Practice Statement	DigitalSign

AUTHORIZATIONS

Created by	Approved by

LEGAL NOTICE

Copyright © DigitalSign – Certificadora Digital, SA. All rights reserved.
DigitalSign is a registered trademark of DigitalSign - Certificadora Digital, SA. All other brands, trademarks and service marks are the property of their respective owners. Any question or request for information regarding the content of this document should be directed to suporte@digitalsign.pt.

CONTENT

1. Introduction 11
1.1. Overview 11
1.1.1. Hierarchies 12
1.2. Document Name and Identification 19
1.3. PKI Participants 20
1.3.1. Certification Authorities 20
1.3.2. Registration Authorities 20
1.3.3. Subscribers 20
1.3.4. Relying Parties 20
1.3.5. Other Participants 20
1.4. Certificate Usage 22
1.4.1. Appropriate Certificate Uses 22
1.4.2. Prohibited Certificate Uses 22
1.5. Policy Administration 23
1.5.1. Organization Administering the Document 23
1.5.2. Contact Person 23
1.5.3. Compliance Determination 23
1.5.4. Approval Procedures 24
1.6. Definitions and Acronyms 24
2. Publication and Repository Responsibilities 25
2.1. Repositories 25
2.2. Publication of Certificate Information 25
2.3. Publication Frequency 26
2.4. Access Control on Repositories 26
3. Identification and Authentication 27
3.1. Naming 27
3.1.1. Types of Names 27
3.1.2. Need for Names to be Meaningful 27
3.1.3. Anonymity or pseudonymity of Subscribers 27
3.1.4. Rules for Interpreting Various Name Forms 28
3.1.5. Uniqueness of Names 28
3.1.6. Recognition, Authentication and Role of Trademarks 28
3.2. Initial Identity Validation 28
3.2.1. Method to Prove Possession of Private Key 28
3.2.2. Authentication of Organization Identity 29
3.2.3. Authentication of Individual Identity 30

3.2.4. Non-Verified Subscriber Information 30
3.2.5. Validation of Authority 30
3.2.6. Criteria for Interoperation 31
3.3. Identification and Authentication for Re-key Requests 31
3.3.1. Routine Re-key and Renewal for CA Certificates 31
3.3.2. Identification and Authentication for Re-key after Revocation 31
3.4. Identification and Authentication for Revocation Request 32
4. Certificate Life-Cycle Operational Requirements 33
4.1. Certificate Application 33
4.1.1. Who Can Submit a Certificate Application 33
4.1.2. Enrolment Process and Responsibilities 33
4.2. Certificate Application Processing 33
4.2.1. Performing Identification and Authentication Functions 33
4.2.2. Approval or Rejection of Certificate Applications 33
4.2.3. Time to Process Certificate Applications 34
4.3. Certificate Issuance 34
4.3.1. CA actions during Certificate Issuance 34
4.3.2. Notifications to Subscribers by the CA of Issuance of Certificate 34
4.4. Certificate Acceptance 34
4.4.1. Conduct Constituting Certificate Acceptance 34
4.4.2. Publication of the Certificate by the CA 34
4.4.3. Notification of Certificate Issuance by the CA to Other Entities 34
4.5. Key Pair and Certificate Usage 35
4.5.1. Subscriber Private Key and Certificate Usage 35
4.5.2. Relying Party Public Key and Certificate Usage 35
4.6. Certificate Renewal 36
4.7. Certificate Re-key 36
4.7.1. Circumstances for Certificate Re-key 36
4.7.2. Who May Request Certification of a New Public Key 36
4.7.3. Processing Certificate Re-key Requests 36
4.7.4. Notification of New Certificate Issuance to Subscriber 36
4.7.5. Conduct Constituting Acceptance of Modified Certificate 36
4.7.6. Publication of the Modified Certificate by the CA 36
4.7.7. Notification of Certificate Issuance by the CA to other Entities 36
4.8. Certificate Modification 36
4.9. Certificate Revocation and Suspension 37
4.9.1. Circumstances for Revocation 37

4.9.2. Who Can Request Revocation ... 38
4.9.3. Procedure for Revocation Request ... 38
4.9.4. Revocation Request Grace Period ... 38
4.9.5. Time within which CA must process the Revocation Request ... 39
4.9.6. Revocation Checking Requirements for Relying Parties ... 39
4.9.7. CRL Issuance Frequency ... 39
4.9.8. Maximum Latency for CRLs ... 39
4.9.9. On-Line Revocation/Status Checking Availability ... 39
4.9.10. On-Line Revocation Checking Requirements ... 39
4.9.11. Other Forms of Revocation Advertisements Available ... 40
4.9.12. Special Requirements Regarding Key Compromise ... 40
4.9.13. Circumstances for Suspension ... 40
4.9.14. Who Can Request Suspension ... 40
4.9.15. Procedure for Suspension Request ... 40
4.9.16. Limits on Suspension Period ... 40
4.10. Certificate Status Services ... 41
4.10.1. Operational Characteristics ... 41
4.10.2. Service Availability ... 41
4.10.3. Optional Features ... 41
4.11. End of Subscription ... 41
4.12. Key Escrow and Recovery ... 41
4.12.1. Key Escrow and Recovery Policy and Practices ... 41
4.12.2. Session Key Encapsulation and Recovery Policy and Practices ... 42
5. Management, Operational and Physical Controls ... 43
5.1. Physical Security Controls ... 43
5.1.1. Site Location and Construction ... 43
5.1.2. Physical Access ... 43
5.1.3. Power and Air Conditioning ... 43
5.1.4. Water Exposures ... 44
5.1.5. Fire Prevention and Protection ... 44
5.1.6. Media Storage ... 44
5.1.7. Waste Disposal ... 44
5.1.8. Off-Site Backup ... 44
5.2. Procedural Controls ... 44
5.2.1. Trusted Roles ... 44
5.2.2. Number of People Required per Task ... 45
5.2.3. Identification and Authentication for each Role ... 46

5.2.4. Roles Requiring Separation of Duties 46
5.3. Personnel Controls 46
5.3.1. Background, Qualifications, Experience, and Clearance Requirements 46
5.3.2. Background Check Procedures 46
5.3.3. Training Requirements 47
5.3.4. Retraining Frequency and Requirements 47
5.3.5. Job Rotation Frequency and Sequence 47
5.3.6. Sanctions for Unauthorized Actions 48
5.3.7. Contracting Personnel Requirements 48
5.3.8. Documentation Supplied to Personnel 48
5.4. Audit Logging Procedures 48
5.4.1. Types of Events Recorded 48
5.4.2. Frequency of Processing Log 49
5.4.3. Retention Period for Audit Log 49
5.4.4. Protection of Audit Log 49
5.4.5. Audit Log Backup Procedures 49
5.4.6. Audit Collection System 49
5.4.7. Notification to Event-Causing Subject 49
5.4.8. Vulnerability Assessments 50
5.5. Record Archival 50
5.5.1. Types of Events Recorded 50
5.5.2. Retention Period for Archive 50
5.5.3. Protection of Archive 50
5.5.4. Archive Backup Procedures 50
5.5.5. Requirements for Time-Stamping of Records 50
5.5.6. Archive Collection System (Internal or External) 50
5.5.7. Procedures to Obtain and Verify Archive Information 51
5.6. Key Changeover 51
5.6.1. Root CA 51
5.6.2. Subordinate CA 51
5.7. Compromise and Disaster Recovery 52
5.7.1. Incident and Compromise Handling Procedures 52
5.7.2. Computing Resources, Software, and/or Data Are Corrupted 52
5.7.3. End Private Key Compromise Procedures 52
5.7.4. Business Continuity Capabilities after a Disaster 52
5.8. CA or RA Termination 53
6. Technical Security Controls 54

6.1. Key Pair Generation and Installation 54
6.1.1. Key Pair Generation 54
6.1.2. Private Key Delivery to Entity 54
6.1.3. Public Key Delivery to Certificate Issuer 54
6.1.4. CA Public Key Delivery to Users 54
6.1.5. Key Sizes 54
6.1.6. Public Key Parameters Generation 55
6.1.7. Key Usage Purposes 55
6.2. Private Key Protection and Cryptographic Module Engineering Controls 55
6.2.1. Standards for Cryptographic Modules 55
6.2.2. Private Key (m out of n) Multi-Person Control 55
6.2.3. Private Key Escrow 55
6.2.4. Private Key Backup 55
6.2.5. Private Key Archival 56
6.2.6. Private Key Transfer into or from a Cryptographic Module 56
6.2.7. Private Key Storage on Cryptographic Module 56
6.2.8. Method of Activating Private Key 56
6.2.9. Method of Deactivating Private Key 56
6.2.10. Method of Destroying Private Key 57
6.2.11. Cryptographic Module Rating 57
6.3. Other Aspects of Key Pair Management 57
6.3.1. Public Key Archival 57
6.3.2. Usage Periods for the Public and Private Keys 57
6.4. Activation Data 58
6.4.1. Activation Data Generation and Installation 58
6.4.2. Activation Data Protection 58
6.4.3. Other Aspects of Activation Data 58
6.5. Computer Security Controls 58
6.5.1. Specific Computer Security Technical Requirements 59
6.5.2. Computer Security Rating 59
6.6. Life Cycle Technical Controls 59
6.6.1. System Development Controls 59
6.6.2. Security Management Controls 59
6.6.3. Life Cycle Security Ratings 59
6.7. Network Security Controls 59
6.8. Time-stamping 60
7. Certificate and CRL Profile 61

7.1. Certificate Profile 61
7.1.1. Version Number(s) 61
7.1.2. Certificate Extensions 61
7.1.3. Algorithm Object Identifiers 61
7.1.4. Name Forms 61
7.1.5. Name Constraints 61
7.1.6. Certificate Policy Object Identifier 61
7.1.7. Usage of Policy Constraints Extension 62
7.1.8. Policy Qualifiers Syntax and Semantics 62
7.1.9. Processing Semantics for the Critical Certificate Policy Extension 62
7.2. CRL Profile 62
7.2.1. Version Number(s) 62
7.2.2. CRL and CRL Entry Extensions 62
7.3. OCSP Profile 63
7.3.1. Version Number(s) 63
7.3.2. OCSP Extensions 63
8. Compliance Audit and Other Assessments 64
8.1. Frequency and Circumstances of Assessment 64
8.2. Identity/Qualifications of Assessor 64
8.3. Assessor's Relationship to Assessed Entity 64
8.4. Topics Covered by Assessment 64
8.5. Actions Taken as a Result of Deficiency 64
8.6. Communications of Results 65
9. Other Business & Legal Matters 66
9.1. Fees 66
9.1.1. Certificate Issuance or Renewal Fees 66
9.1.2. Certificate Access Fees 66
9.1.3. Revocation or Status Information Access Fees 66
9.1.4. Fees for Other Services Such as Policy Information 66
9.1.5. Refund Policy 66
9.2. Financial Responsibility 66
9.2.1. Insurance Coverage 66
9.2.2. Other Assets 66
9.3. Confidentiality of Business Information 67
9.3.1. Scope of Confidential Information 67
9.3.2. Information Not Within the Scope of Confidential Information 67
9.3.3. Responsibility to Protect Confidential Information 67

9.4. Privacy of Personal Information 67
9.4.1. Privacy Plan 67
9.4.2. Information Treated as Private 67
9.4.3. Information Not Deemed Private 68
9.4.4. Responsibility to Protect Private Information 68
9.4.5. Notice and Consent to Use Private Information 68
9.4.6. Disclosure to Law Enforcement Officials 68
9.4.7. Other Information Disclosure Circumstances 68
9.5. Intellectual Property Rights 68
9.6. Representations and Warranties 68
9.6.1. CA Representation and Warranties 68
9.6.2. RA Representation and Warranties 69
9.6.3. Subscriber Representation and Warranties 69
9.6.4. Relying Party Representations and Warranties 70
9.7. Disclaimers of Warranties 70
9.8. Certification Authority Limitations of Liability 70
9.9. Indemnities 70
9.10. Term and Termination 70
9.10.1. Term 70
9.10.2. Termination 70
9.11. Individual Notices and Communication 71
9.12. Amendments 71
9.12.1. Procedure for Amendment 71
9.12.2. Notification Mechanism and Period 71
9.12.3. Circumstance Under Which OID Must Be Changed 71
9.13. Dispute Resolution Provisions 71
9.13.1. Disputes Among DigitalSign and RA Customers 71
9.13.2. Disputes with End-User Subscribers or Relying Parties 71
9.14. Governing Law 72
9.15. Compliance with Applicable Law 72
9.16. Miscellaneous Provisions 72
9.16.1. Entire Agreement 72
9.16.2. Assignment 72
9.16.3. Severability 72
9.16.4. Enforcement 72
9.16.5. Force Majeure 72
9.17. Other Provisions 73

9.17.1. Management Group (Grupo de Gestão) 73
10. Appendix A – Acronyms and Definitions 74

1. INTRODUCTION

The purpose of this document is to define the practices and procedures used to support the certification activities performed by DigitalSign, and every CA under the DIGITALSIGN GLOBAL ROOT CAs (hereinafter, ROOT) hierarchies.

In addition to the terms and conditions set forth in this CPS, each type of certificate issued by DigitalSign must comply with the requirements listed in the "PKI Disclosure Statement" (PDS), as well as the requirements which can be found in the applicable "Certificate Profile List" (CP).

For matters relating to the Time Stamping, Validation, Preservation, Remote QSCD Management and Electronic Attribute Attestation services, the corresponding policy and practice statement documents, identified in the "Related Documents" section, should be consulted in conjunction with this CPS.

This CPS is in compliance with the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policies and definition of Certification Practice Statement and may undergo regular updates.

1.1. OVERVIEW

The practices for creation, signing and issuing certificates, as well as revoking invalid certificates, carried out by a Certification Authority (CA) are essential to ensure the reliability and confidence of a Public Key Infrastructure (PKI).

It respects and implements the following standards:

- RFC 3647: *Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*
- RFC 5280: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
- Regulation (EU) 910/2014, as amended by Regulation (EU) 2024/1183
- ETSI EN 319 401: *General Policy Requirements for Trust Service Providers*
- ETSI EN 319 411-1: *General requirements*
- ETSI EN 319 411-2: *Requirements for trust service providers issuing EU qualified certificates*
- ETSI EN 319 412: *Certificate Profiles*
- ETSI EN 319 412-1: *Overview and common data structures*
- ETSI EN 319 412-2: *Certificate profile for certificates issued to natural persons*
- ETSI EN 319 412-3: *Certificate profile for certificates issued to legal persons*
- ETSI EN 319 412-5: *QCStatements*
- ETSI EN 319 421: *Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*
- ETSI EN 319 422: *Time-stamping protocol and time-stamp token profiles*
- ETSI TS 119 431-1: *TSP services operating a remote QSCD / SCDev*

- CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.3.1
- CA/Browser Forum, Network and Certificate System Security Requirements, version 2.0.5
- CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.16

This CPS complies with National and European legislation applicable to qualified certificates and specifies how to implement their procedures and controls, as well as how DigitalSign reaches the specified requirements.

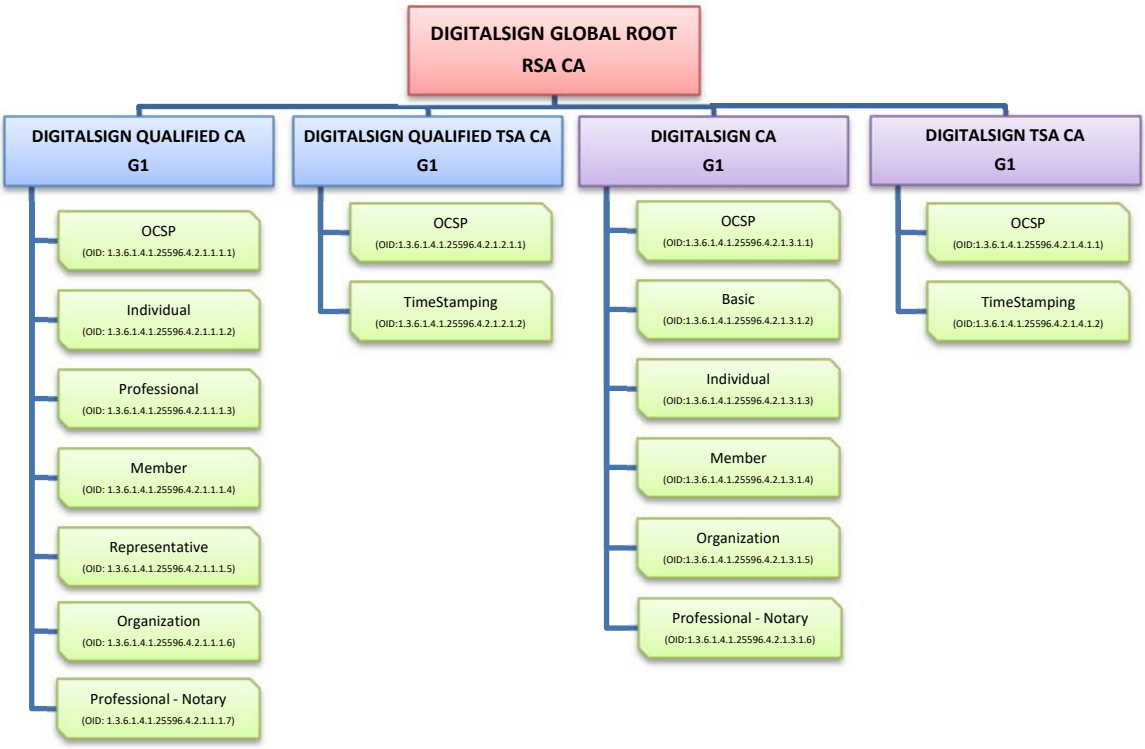
The recommendations in the technical document *CWA 14167-1 Requirements for Trustworthy Systems Managing Certificates for Digital Signatures - Part 1: System Security Requirements* have also taken into consideration.

1.1.1. HIERARCHIES

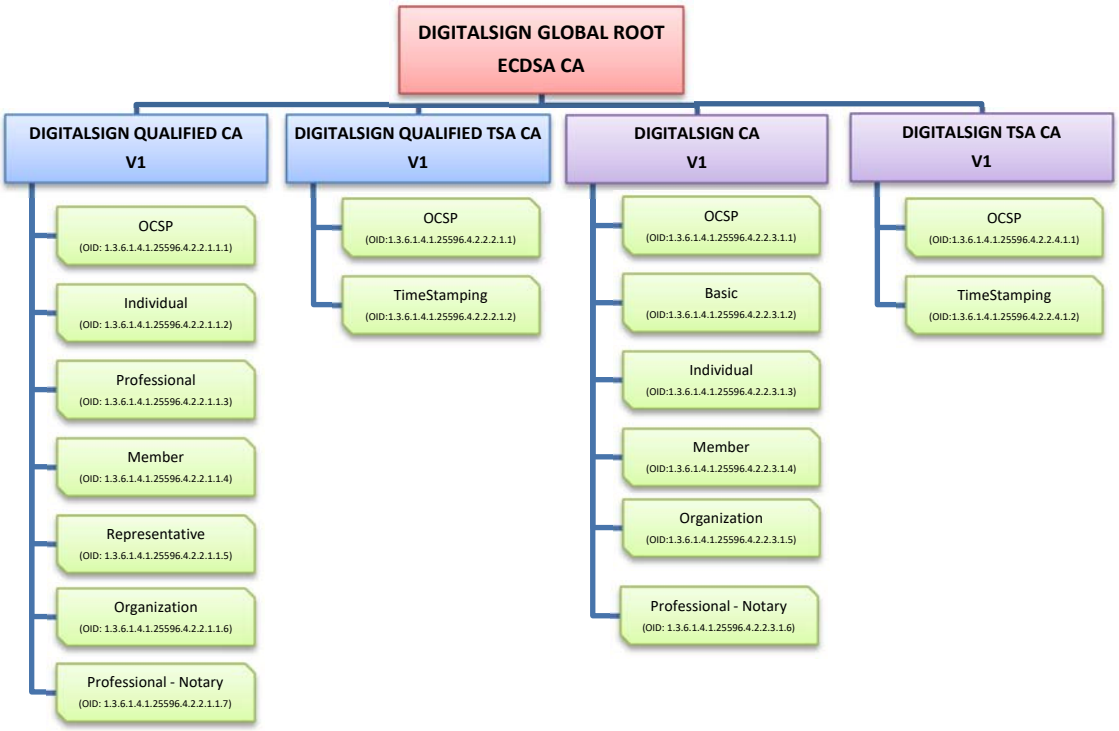
This section describes the hierarchies and Certification Authorities (hereinafter CA or CAs) that DigitalSign manages. The use of hierarchies reduces the risks involved in issuing certificates and organising them in the different CAs.

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.

RSA hierarchy:



ECDSA hierarchy:



1.1.1.1. ROOT CERTIFICATION AUTHORITIES

It is called Root Certification Authority (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 other CAs belonging to the Certification Hierarchy. The identification data of the current root CA is:

RSA hierarchy – Root CA	
CN	DIGITALSIGN GLOBAL ROOT RSA CA
Serial number	5D59C8CAAB0957F5E6B5DA2994046AFFC5D49587
SHA-256 fingerprint	82BD5D851ACF7F6E1BA7BFCBC53030D0E7BC3C21DF772D858CAB41D199BDF595
Valid from	Jan 21 10:50:34 2021 GMT
Valid to	Jan 15 10:50:34 2046 GMT
Key type	RSA 4096

ECDSA hierarchy – Root CA	
CN	DIGITALSIGN GLOBAL ROOT ECDSA CA
Serial number	362D8F7288A22827E400FF24C62DE4EBFA9DB6E1
SHA-256 fingerprint	261D7114AE5F8FF2D8C7209A9DE4289E6AFC9D717023D85450909199F1857CFE
Valid from	Jan 21 11:07:50 2021 GMT
Valid to	Jan 15 11:07:50 2046 GMT
Key type	ECDSA P384

1.1.1.2. INTERMEDIATE CERTIFICATION AUTHORITIES

It is called Intermediate or Subordinate Certification Authority the certification entity within the hierarchy that issues subsequent Intermediate Certification Authorities and its public key certificate has been digitally signed by the precedent Intermediate Certification Authority or by the Root Certification Authority.

1.1.1.3. ISSUING CERTIFICATION AUTHORITIES

It is called Issuing Certification Authorities the certification entity within the hierarchy that issues end-user certificates and its public key certificate has been digitally signed by an Intermediate Certification Authority or by the Root Certification Authority.

The identification data of the current Issuing Certification Authorities managed by DigitalSign are:

RSA hierarchy – Issuing CA (Qualified CA G1)	
CN	DIGITALSIGN QUALIFIED CA G1
Serial number	39E1A08D060E3E22CA3F6726A14984E7136F833A
SHA-256 fingerprint	27BB49D206B6DEC161EBB8EA739530E90AC68498D2EEA05A7ED9603D1DCE0FD5
Valid from	Jan 22 10:11:50 2021 GMT
Valid to	Jan 19 10:11:50 2033 GMT
Key type	RSA 4096

RSA hierarchy – Issuing CA (Qualified TSA CA G1)	
CN	DIGITALSIGN QUALIFIED TSA CA G1
Serial number	14F920B606A157F57889EF779A632E50BEBA31CF
SHA-256 fingerprint	2BB402D903E1C15743E99806D1D046CFBF45E37DDD312607566F464996E20750
Valid from	Jan 22 10:13:09 2021 GMT
Valid to	Jan 15 10:50:34 2046 GMT
Key type	RSA 4096

RSA hierarchy – Issuing CA (non-Qualified CA G1)	
CN	DIGITALSIGN CA G1
Serial number	09FF95FCF1B7680C2388FB2212DA0D6E8ADF5EFF
SHA-256 fingerprint	951B523C9B7FD59AF6FAE2E054D97F2B9371A41DF752D63295B3BB93F3C5059C
Valid from	Jan 22 10:13:40 2021 GMT
Valid to	Jan 19 10:13:40 2033 GMT
Key type	RSA 4096

RSA hierarchy – Issuing CA (non-Qualified TSA CA G1)	
CN	DIGITALSIGN TSA CA G1
Serial number	57FF5A53A0E6E06BF9DA1E417239DC14771A186C
SHA-256 fingerprint	38BD3C34D9D93D71F8F331556756CB4BE152E1C99B50EB177F8A68E8D01F5CD6
Valid from	Jan 22 10:14:11 2021 GMT
Valid to	Jan 15 10:50:34 2046 GMT
Key type	RSA 4096

ECDSA hierarchy – Issuing CA (Qualified CA V1)	
CN	DIGITALSIGN QUALIFIED CA V1
Serial number	6A246203B75AC831D5B8F4239645CC8273652B40
SHA-256 fingerprint	4A2B2B0F8429A77E23BCAB8FFA253F4C21368CB4AA2A78DBC5D417C6D1D0E105
Valid from	Jan 22 10:14:49 2021 GMT
Valid to	Jan 19 10:14:49 2033 GMT
Key type	ECDSA P384

ECDSA hierarchy – Issuing CA (Qualified TSA CA V1)	
CN	DIGITALSIGN QUALIFIED TSA CA V1
Serial number	472511C3036CD662FF8625B6DD6B09AE758EE40E
SHA-256 fingerprint	BD2318F64DCC529238BCC71C94948F7B9479A36E30DDA65A520A356F9EFB5AD9
Valid from	Jan 22 10:15:31 2021 GMT
Valid to	Jan 15 11:07:50 2046 GMT
Key type	ECDSA P384

ECDSA hierarchy – Issuing CA (non-Qualified CA V1)	
CN	DIGITALSIGN CA V1
Serial number	20142333672A6D5FF4AF267D2A9635F1B9946DF5
SHA-256 fingerprint	C18C8DE10A7B02AB2A700F3E95EE53501DC015012FAAC197B2D64BF2EE6DFE77
Valid from	Jan 22 10:16:10 2021 GMT
Valid to	Jan 19 10:16:10 2033 GMT
Key type	ECDSA P384

ECDSA hierarchy – Issuing CA (non-Qualified TSA CA V1)	
CN	DIGITALSIGN TSA CA V1
Serial number	412D3547F9713F35394C779975895AF5C5B4E0BB
SHA-256 fingerprint	C811BD06D09F43F003C496F7C28B9D5D6477EFEDFFE169B418A5B7B48B6BB9D6
Valid from	Jan 22 10:16:43 2021 GMT
Valid to	Jan 15 11:07:50 2046 GMT
Key type	ECDSA P384

1.1.1.4. END-USER CERTIFICATES

DigitalSign issues several types of digital certificates in order to meet the needs of its customers through Issuing Certification Authorities indicated in the previous section. End-user Digital Certificates issued by the DigitalSign are:

RSA hierarchy – Issuing CA (CN: DIGITALSIGN QUALIFIED CA G1)
Name: OCSP Certificate **OID**: 1.3.6.1.4.1.25596.4.2.1.1.1.1 **Usage**: Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.
Name: Individual Certificate **OID**: 1.3.6.1.4.1.25596.4.2.1.1.1.2 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual). **[0.4.0.194112.1.2 ETSI EN 319411-2 - QCP-n-qscd].**
Name: Professional Certificate **OID**: 1.3.6.1.4.1.25596.4.2.1.1.1.3 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfilment 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 319411-2 - QCP-n-qscd].**
Name: Member Certificate **OID**: 1.3.6.1.4.1.25596.4.2.1.1.1.4 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a specified organization. **[0.4.0.194112.1.2 ETSI EN 319411-2 - QCP-n-qscd].**
Name: Representative Certificate **OID**: 1.3.6.1.4.1.25596.4.2.1.1.1.5 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual) as legal representative or attorney of a specified organization. **[0.4.0.194112.1.2 ETSI EN 319411-2 - QCP-n-qscd].**
Name: Organization Certificate **OID**: 1.3.6.1.4.1.25596.4.2.1.1.1.6 **Usage**: Certificate used for eIDAS compliant qualified seal by legal persons. **[0.4.0.194112.1.3 ETSI EN 319411-2 - QCP-l-qscd].**
Name: Professional (Notary) Certificate

OID: 1.3.6.1.4.1.25596.4.2.1.1.1.7 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfilment of his/her profession. This type of certificate is issued to members of Notary professional association, where the entitlement is verified. **[0.4.0.194112.1.2 ETSI EN 319411-2 - QCP-n-qscd].**

RSA hierarchy – Issuing CA (CN: DIGITALSIGN QUALIFIED TSA CA G1)
Name: OCSP Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.2.1.1 **Usage**: Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.
Name: TimeStamp Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.2.1.2 **Usage**: Certificate used for by TimeStamping Authorities (TSA) to provide eIDAS compliant qualified timestamping services.

RSA hierarchy – Issuing CA (CN: DIGITALSIGN CA G1)
Name: OCSP Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.3.1.1 **Usage**: Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.
Name: Basic Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.3.1.2 **Usage**: Certificate used for electronic authentication/signature/encryption by natural persons or electronic seal/encryption by legal persons. This certificate profile aims to identify a natural or a legal person.
Name: Individual Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.3.1.3 **Usage**: Certificate used for electronic authentication/signature/encryption by natural persons. This certificate profile aims to identify a natural person (individual).
Name: Member Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.3.1.4 **Usage**: Certificate used for electronic authentication/signature/encryption by natural persons. This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a specified organization.
Name: Organization Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.3.1.5 **Usage**: Certificate used for electronic authentication/seal/encryption by legal persons. This certificate profile aims to identify a legal person (organization).
Name: Professional (Notary) Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.3.1.6 **Usage**: Certificate used for electronic authentication/signature/encryption by natural persons. This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfilment of his/her profession. This type of certificate is issued to members of Notary professional association, where the entitlement is verified.

RSA hierarchy – Issuing CA (CN: DIGITALSIGN TSA CA G1)
Name: OCSP Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.4.1.1 **Usage**: Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.
Name: TimeStamp Certificate
OID: 1.3.6.1.4.1.25596.4.2.1.4.1.2 **Usage**: Certificate used for by TimeStamping Authorities (TSA) to provide timestamping services.

ECDSA hierarchy – Issuing CA (CN: DIGITALSIGN QUALIFIED CA V1)
Name: OCSP Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.1.1.1 **Usage**: Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.
Name: Individual Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.1.1.2 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual). **[0.4.0.194112.1.2 ETSI EN 319411-2 - QCP-n-qscd].**
Name: Professional Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.1.1.3 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfilment 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 319411-2 - QCP-n-qscd].**
Name: Member Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.1.1.4 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a specified organization. **[0.4.0.194112.1.2 ETSI EN 319411-2 - QCP-n-qscd].**
Name: Representative Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.1.1.5 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons. This certificate profile aims to identify a natural person (individual) as legal representative or attorney of a specified organization. **[0.4.0.194112.1.2 ETSI EN 319411-2 - QCP-n-qscd].**
Name: Organization Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.1.1.6 **Usage**: Certificate used for eIDAS compliant qualified seal by legal persons. **[0.4.0.194112.1.3 ETSI EN 319411-2 - QCP-l-qscd].**
Name: Professional (Notary) Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.1.1.7 **Usage**: Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfilment of his/her profession. This type of certificate is issued to members of Notary professional association, where the entitlement is verified. **[0.4.0.194112.1.2 ETSI EN 319411-2 - QCP-n-qscd].**

ECDSA hierarchy – Issuing CA (CN: DIGITALSIGN QUALIFIED TSA CA V1)
Name: OCSP Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.2.1.1 **Usage**: Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.
Name: TimeStamp Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.2.1.2 **Usage**: Certificate used for by TimeStamping Authorities (TSA) to provide eIDAS compliant qualified timestamping services.

ECDSA hierarchy – Issuing CA (CN: DIGITALSIGN CA V1)
Name: OCSP Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.3.1.1 **Usage**: Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.
Name: Basic Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.3.1.2 **Usage**: Certificate used for electronic authentication/signature/encryption by natural persons or electronic seal/encryption by legal persons. This certificate profile aims to identify a natural or a legal person.
Name: Individual Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.3.1.3 **Usage**: Certificate used for electronic authentication/signature/encryption by natural persons. This certificate profile aims to identify a natural person (individual).
Name: Member Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.3.1.4 **Usage**: Certificate used for electronic authentication/signature/encryption by natural persons. This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a specified organization.
Name: Organization Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.3.1.5 **Usage**: Certificate used for electronic authentication/seal/encryption by legal persons. This certificate profile aims to identify a legal person (organization).
Name: Professional (Notary) Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.3.1.6 **Usage**: Certificate used for electronic authentication/signature/encryption by natural persons. This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfilment of his/her profession. This type of certificate is issued to members of Notary professional association, where the entitlement is verified.

ECDSA hierarchy – Issuing CA (CN: DIGITALSIGN TSA CA V1)
Name: OCSP Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.4.1.1 **Usage**: Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.
Name: TimeStamp Certificate
OID: 1.3.6.1.4.1.25596.4.2.2.4.1.2 **Usage**: Certificate used for by TimeStamping Authorities (TSA) to provide timestamping services.

1.2. DOCUMENT NAME AND IDENTIFICATION

Document Information	
Document Name	Certification Practices Statement (CPS)
Version/Edition	2.1
OID	1.3.6.1.4.1.25596.4.1.1
Publication Date	16/10/2026
Expiration Date	Upon publication of a newer version
Localization:	https://pki.digitalsign.pt

1.3. PKI PARTICIPANTS

1.3.1. CERTIFICATION AUTHORITIES

A Certification Authority (CA) is the entity that issues and manages digital certificates. It acts as the trusted third party between the Subscriber (Subject/Signatory) and the Relying Party in digital transactions, associating a specific public key with a person/organization. The CA has the ultimate responsibility in the provision of certification services. The CA is identified in the Issuer field of any digital certificate.

CAs are organized in hierarchies, as described in section 1.1.1.

1.3.2. REGISTRATION AUTHORITIES

A Registration Authority (RA) is the entity that performs the identification and authentication of certificate applicants for end-user certificates, initiates or forwards revocation requests, and approves applications for certificate renewal on behalf of the CA.

DigitalSign may act as an RA for certificates it issues.

Third parties, who enter into a contractual relationship with DigitalSign, may operate their own RA and authorize the issuance/renewal/revocation of certificates. Third party RAs must comply with all requirements of this CPS and the terms of their contract with DigitalSign. Third Party RAs may implement more restrictive practices based on their internal requirements.

The RA identification, when distinct from CA, must be part of the information contained in each issued digital certificate, through an "OU" identifier in the "Subject" field (**OU = ER - Entity Name**).

1.3.3. SUBSCRIBERS

Subscribers are end users of certificates issued by a CA. A subscriber is the entity named as the end-user certificate subscriber. Subscribers can be individuals, organizations or devices.

1.3.4. RELYING PARTIES

Relying parties are individuals, organizations or devices that rely on the validity of the mechanisms and procedures used in the process of association of the subscriber identity with its public key, that is, trust that the certificate corresponds in fact to whom claims to own it.

In this CPS, a relying party is considered to be one that trusts the content, validity and applicability of the issued certificate.

Relying parties may or may not hold certificates issued in DigitalSign trust hierarchies.

1.3.5. OTHER PARTICIPANTS

1.3.5.1. TRUSTED SERVICE PROVIDER (TSP)

A trusted service provider (TSP) is a natural or legal person that provides one or more trust service. TSP can be 'qualified' or 'non-qualified'.

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

The trusted services defined in eIDAS (EU Regulation 910/2014) include:

- The creation, verification and validation of electronic signatures and certificates related to those services.
- The creation, verification and validation of electronic seals and certificates related to those services.
- The creation, verification and validation of electronic timestamps and certificates related to those services.
- Electronic registered delivery services and certificates related to those services.
- The creation, verification and validation of certificates for website authentication.
- The preservation of electronic signatures, seals or certificates related to those services.

DigitalSign is a Trust Service Provider (TSP) that issues certificates compliant with Portuguese and European legislation.

DigitalSign is the issuing entity of certificates and is responsible for the life cycle and operation of the certificates during the life cycle.

RA functions may be performed by other Registration Authorities that DigitalSign has hired and trained the personnel who will perform these functions. DigitalSign also provides electronic signature and time stamping validation services, which are governed by separate policies, not included in this document

1.3.5.2. SUPERVISORY BODY

The entity responsible for carrying out the supervisory activities under EU Regulation 910/2014. In Portugal, this task is assigned to Gabinete Nacional de Segurança.

Intermediate CAs may be subject to legal frameworks in different countries or regions. In such cases, the supervisory body refers to the relevant national bodies appointed by those countries or regions.

1.3.5.3. ENTITY/ORGANIZATION

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

1.3.5.4. MANAGEMENT GROUP

The Management Group ("Grupo de Gestão"), as defined in section 9.17.1 of this document, is responsible for ensuring the effective implementation of all processes and procedures of the management system and regularly review the need to readjust them in a logic of continuous improvement, through critical analysis of its effectiveness.

1.4. CERTIFICATE USAGE

1.4.1. APPROPRIATE CERTIFICATE USES

The certificates issued by any CA under the DigitalSign hierarchies are used by the various systems, applications, protocols and mechanisms, in order to ensure the following security services:

- Access control
- Electronic signature / Electronic seal
- Integrity
- Authentication
- Non repudiation
- Confidentiality (asymmetric or mixed encryption)

These services are obtained using public key cryptography, through their use in the trusting infrastructure that the DigitalSign Certification Hierarchy offers.

The use of a specific key is determined by the key usage extension in the X.509 Certificate. Private Keys corresponding to Root or Intermediate CAs certificates must not be used to sign other certificates except in the following cases:

- Self-signed certificates to represent the Root CA itself;
- Certificates for Intermediate CAs, Issuing CAs and cross-certificates;
- Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates); and
- Certificates for OCSP response verification.

1.4.2. PROHIBITED CERTIFICATE USES

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 authorized 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 subscribers is considered illegal, and the CA is exempt from any liability due to the subscriber 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 subscriber is consequently responsible for the data for which the certificate is used. The subscriber 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 subscribers, 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 mandatory.

1.5. POLICY ADMINISTRATION

1.5.1. ORGANIZATION ADMINISTERING THE DOCUMENT

DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal

1.5.2. CONTACT PERSON

Álvaro Matos
DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: suporte@digitalsign.pt
Phone: +351 253560650

REVOCATION REPORTING CONTACT PERSON
Álvaro Matos
DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: suporte@digitalsign.pt
Phone: +351 253560650

For anyone listed in section 4.9.2 of this CPS and the CA/Browser Baseline Requirements that needs assistance with revocation or an investigative report, proceed according to section 4.9.3 or section 4.9.12, or please contact suporte@digitalsign.pt.
Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. DigitalSign or an RA will authenticate and log each revocation request according to Section 4.9.

1.5.3. COMPLIANCE DETERMINATION

The management group of this policy evaluates the compliance and internal applicability of this CPS (and/or their respective CPs), submitting it to the approval of DigitalSign's

Administration, which is the competent body to determine its suitability to the applicable legislation.

1.5.4. APPROVAL PROCEDURES

The internal approval of this CPS (and/or their respective CPs) and following fixes and/or updates are made by DigitalSign's Administration.

After internal approval, should be assessed their compliance, as described in the previous paragraph.

Corrections and/or updates shall be published in the form of new versions of the CPS (and/or their respective CPs), replacing any previous version.

1.6. DEFINITIONS AND ACRONYMS

See Appendix A.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

DigitalSign is responsible for the repository.

DigitalSign issues Certificate Revocation Lists (CRLs) under the provisions of this CPS.

Online Certificate Status Protocol (OCSP) may also be provided under the provisions of this CPS.

2.2. PUBLICATION OF CERTIFICATE INFORMATION

DigitalSign maintains a Web-based repository, which allows the relying parties to make online enquires regarding revocations and other information about the status of the certificates. DigitalSign provides information to relying parties on how to find the appropriate repository to check the status of certificates and, if the Online Certificate Status Protocol (OCSP) is available, how to find the corresponding OSCP.

DigitalSign always publishes, at least, the following public information online:

- Electronic copy of this CPS and other related documentation: https://pki.digitalsign.pt
- CAs certificates and certificate chain
  - DIGITALSIGN GLOBAL ROOT RSA CA: https://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.p7b
    - DIGITALSIGN QUALIFIED CA G1: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b
    - DIGITALSIGN QUALIFIED TSA CA G1: https://qtsa-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAG1.p7b
    - DIGITALSIGN CA G1: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.p7b
    - DIGITALSIGN TSA CA G1: https://advtsa-g1.digitalsign.pt/DIGITALSIGNTSACAG1.p7b
  - DIGITALSIGN GLOBAL ROOT ECDSA CA: https://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.p7b
    - DIGITALSIGN QUALIFIED CA V1: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.p7b
    - DIGITALSIGN QUALIFIED TSA CA V1: https://qtsa-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAV1.p7b
    - DIGITALSIGN CA V1: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.p7b
    - DIGITALSIGN TSA CA V1: https://advtsa-v1.digitalsign.pt/DIGITALSIGNTSACAV1.p7b
- CRLs:
  - Certificates issued by "DIGITALSIGN GLOBAL ROOT RSA CA": https://root-rsa.digitalsign.pt/DIGITALSIGNGLOBALROOTRSACA.crl
    - Certificates issued by "DIGITALSIGN QUALIFIED CA G1": https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl

- Certificates issued by "DIGITALSIGN QUALIFIED TSA CA G1": https://qtsa-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAG1.crl
- Certificates issued by "DIGITALSIGN CA G1": https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.crl
- Certificates issued by "DIGITALSIGN TSA CA G1": https://advtsa-g1.digitalsign.pt/DIGITALSIGNTSACAG1.crl

- Certificates issued by "DIGITALSIGN GLOBAL ROOT ECDSA CA": https://root-ecdsa.digitalsign.pt/DIGITALSIGNGLOBALROOTECDSACA.crl
  - Certificates issued by "DIGITALSIGN QUALIFIED CA V1": https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.crl
  - Certificates issued by "DIGITALSIGN QUALIFIED TSA CA V1": https://qtsa-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAV1.crl
  - Certificates issued by "DIGITALSIGN CA V1": https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.crl
  - Certificates issued by "DIGITALSIGN TSA CA V1": https://advtsa-v1.digitalsign.pt/DIGITALSIGNTSACAV1.crl

2.3. PUBLICATION FREQUENCY

Updates to this CPS and related documents are immediately published after approval.

Certificates are published after issuance.

Root CAs and Intermediate CAs CRLs are published at least every year, or immediately after a subordinated CA is revoked.

Issuing CAs CRLs are published daily.

Additional information about the status of the certificate is published in accordance with the provisions of this CPS.

2.4. ACCESS CONTROL ON REPOSITORIES

The information published in the DigitalSign repository is publicly available being guaranteed unrestricted access to read.

DigitalSign implemented measures regarding logical and physical security to prevent unauthorized persons from adding, erasing or modifying entries from the repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. TYPES OF NAMES

The certificates issued by DigitalSign or any CA under the DigitalSign Certification Hierarchy are identified by a unique name in the Issuer and Subject fields, called Distinguished Name - DN, according to the X.501 standard.

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 of the subscriber (where applicable)
Organizational Unit – **"OU"**	Digital certificates can contain attributes OU, according to the corresponding PC
State or Province – **"S"**	The State or Province of the subscriber, or unused
Locality – **"L"**	The Locality of the subscriber, or unused
Common Name – **"CN"**	Name of the subscriber
Email Address – **"E"**	Email address of the subscriber (where applicable)
First Name (Given Name) – **"G"**	First name(s) of the subscriber, when issued to natural persons, or unused
Last Name (Surname) – **"SN"**	Last name(s) of the subscriber, when issued to natural persons, or unused
ID – **"SERIALNUMBER"**	ID of the subscriber, when issued to natural persons, according to ETSI EN 319 512-1, or unused
ID (Organization Identifier) – **"OID 2.5.4.97"**	ID of the organization, according to ETSI EN 319 512-1, or unused
Title – **"T"**	Professional title or another used by the subscriber

3.1.2. NEED FOR NAMES TO BE MEANINGFUL

DigitalSign will ensure that:

- The uniqueness of the information contained in the DN.
- All data included in the DN field is properly validated and authenticated, and are easily identifiable by the humans, allowing unequivocal determination of the respective holder.

3.1.3. ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

Certificate subscribers can use pseudonyms (names other than their real name). In this case, an indication that a pseudonym is being used will be indicated in the "Observations" field.

Anonymity is not authorized.

Only when the technical constraints inherent to maximum sizes defined for each field are limiting to contain all of the information, may be authorized abbreviations, provided that they are easily identifiable by humans.

3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

No stipulation.

3.1.5. UNIQUENESS OF NAMES

DigitalSign ensures that the data in the DN are unique within their CA through automated components in the process of subscriber registration. It is possible for an owner to have two or more certificates with the same DN.

However, a certain DN cannot be transmissible between different entities.

3.1.6. RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

Entities requesting certificates must demonstrate the right to use of the requested name. The designations used on the certificates issued by any CA under the DigitalSign Certification Hierarchy can not infringe intellectual property rights of others.

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

DigitalSign does not arbitrate, mediate, or otherwise resolve any dispute relating to the ownership of any name or tag. DigitalSign reserves the right, without liability to any certificate subscriber, to reject any order due to such disputes.

For certificates issued to natural or legal persons, the subject distinguished name used in the certificate can't be re-assigned to another subject.

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.

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.

c) Keys created by DigitalSign in a remote QSCD (remote signature/seal service):

The keys are generated by DigitalSign, acting as Server Signing Application Service Provider (SSASP), in a certified remote qualified signature/seal creation device (QSCD), on behalf and at the request of the Subject/Signatory, in accordance with the "Remote QSCD Management Service Policy and Practice Statement". The private key is generated and used exclusively within the QSCD and is not delivered to the Signatory; instead, the Signatory is provided with sole control over its use through the signature activation mechanism described in that document and section 4.12 of this CPS. Proof of possession is ensured by the generation of the key pair within the QSCD managed by DigitalSign and by the protected link between the signing key, the Signatory and the corresponding public key submitted for certification; the SSAS provides the registration service with proof of possession or an assertion of the Signatory's authentication linked to the private key.

3.2.2. AUTHENTICATION OF ORGANIZATION IDENTITY

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

DigitalSign verifies an organization's right to use or control an email address to be contained in a certificate by sending an email message containing Random Information to the email address to be used in the certificate. This Random Information is required to complete the certificate issuance process.

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

3.2.2.1. CA CERTIFICATES

These certificates are intended to be used by CAs to issue subordinate CAs or end user certificates. 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. 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.

3.2.2.3. TIMESTAMPING CERTIFICATES

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

3.2.2.4. LEGAL PERSON (ORGANIZATION) 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. In the vetting process is request the commercial registration, or similar, of

the organization and a form duly signed by the legal representative taking responsibility for the certificate.

Instead of the signed form, the legal representative may be identified through remote means (attended or unattended), eID means or use of digital signature with certificate, according to ETSI TS 119 461.

3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY

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.

This can be achieved by:

a) in person at DigitalSign (or authorized RA); or

b) consulting a database provided by an entity that has collected identity information in the physical presence or equivalent of the owner; or

c) presentation of supporting documents which required physical presence to obtain, as is the case of ID or CC (Cartão de Cidadão) documents, complemented with appropriate signature recognition by Notary (or equivalent entity according to the law);

d) through remote means (attended or unattended);

e) use of eID means; or

f) use of digital signature with certificate..

g) for non-qualified certificates, submission of supporting documentation and respective signature, or through an equivalent process, is accepted, i.e., it is not required the physical presence of the subscriber.

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

DigitalSign verifies an individual's right to use or control an email address to be contained in a certificate by sending an email message containing Random Information to the email address to be used in the certificate. This Random Information is required to complete the certificate issuance process.

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.

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

3.2.6. CRITERIA FOR INTEROPERATION

DigitalSign may provide services allowing for another CA to operate within, or interoperate with, its PKI. Such interoperation may include cross-certification, unilateral certification, or other forms of operation. DigitalSign reserves the right to provide interoperation services and to interoperate with other CAs. The terms and criteria of which are to be set forth in the applicable agreement.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

Prior to the expiration of an existing certificate it is necessary to renew that certificate so that the holder maintains the continuity of its use.

DigitalSign requires for this purpose the creation of a new key pair to replace the expiring key pair (technically defined as "re-key", but in this document identified as 'renewal').

The process of creating a new key pair can be driven internally by DigitalSign, or directly by the owner (or representative) of the certificate, being guaranteed the creation of the same approved cryptographic device. In this case it is also required knowledge of user credentials defined by the holder during the initial request.

Verification of identity and other data contained in the DN is always checked by the validation services from DigitalSign in accordance with the following:

- If the information on the renewal process is identical to the information in the process of initial authentication, and that authentication has been performed less than two years ago, the request is automatically approved without submission of additional documentation or proof of identity.
- If the information on the renewal process is not identical to the information in the initial authentication process, or that authentication has been performed more than two years ago, the process is treated as an initial request and shall be applicable all authentication and validation rules described in section 3.2.

3.3.1. ROUTINE RE-KEY AND RENEWAL FOR CA CERTIFICATES

Specified in the corresponding Certificate Policy.

3.3.2. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

It is not possible to renew a certificate after it has been revoked, being always applied the rules of authentication and validation described in section 3.2.

However, the documents and information contained in the initial request may be used for that purpose, as long as they remain valid.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Prior to the revocation of a Certificate, DigitalSign verifies that the revocation was requested by the certificate holder or by the entity that approved the request.

Revocation requests can be made through customer area in the website (if available), or by filling and signing a revocation request.

Additionally, DigitalSign may proceed with the revocation of any certificate, if it is aware (after verification) that the information contained in the DN does not reflect the current reality.

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. ENROLMENT PROCESS AND RESPONSIBILITIES

All end-user certificates must agree with the terms of the "Subscriber Agreement", which contains representations and warranties described in section 9.6.3. and undergo an enrolment process that consists of completing an application form and provide true and correct information, and all supporting documents required for the validation of the information contained in the certificate.

For renewal processes, it can:

- Create a key pair in an approved cryptographic device (as defined in section 3.3)
- Submit its public key using the tools provided by RA
- Demonstrate ownership and / or exclusive control of the private key corresponding to the public key delivered

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The 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.

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 by any 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 process by the RA.

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

4.3.2. NOTIFICATIONS TO SUBSCRIBERS BY THE CA OF ISSUANCE OF CERTIFICATE

Notification of issuance and / or renewal is made via email, which also includes installation instructions.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The acceptance process is completed if the holder does not object to the certificate or its content.

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

DigitalSign publishes the certificates issued in a publicly accessible repository.

4.4.3. NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA 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 as a condition of trust in the certificate.

Before any act of trust, relying parties should independently evaluate:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. DigitalSign is not responsible for assessing the appropriateness of the use of a certificate.
- that the certificate is being used as specified in the "KeyUsage" and "extendedKeyUsage" included in the certificate (eg, if the digital signature is not enabled, then the certificate cannot be trusted to validate the signature of the holder).
- the status of the certificate and all the CAs in the chain that issued the certificate. If any of the certificates in the certificate chain is revoked, the Relying Party is solely responsible for evaluating whether it is reasonable to trust a certificate before the date of revocation. Any such reliance is made solely at the risk of the Relying party.
- Have knowledge and understand the use and functionality provided by public key cryptography and certificates.
- Read and understand the terms and conditions described in the certification practices.

Assuming the use of the certificate is appropriate, relying parties must use the software and / or the appropriate hardware to perform electronic signature or electronic seal verification or other cryptographic operations that they wish to carry on the condition of trust certificates in connection with such operations. Such operations include identifying a Certificate Chain and verifying the digital signature on all certificates in the certificate chain.

4.6. CERTIFICATE RENEWAL

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

4.7. CERTIFICATE RE-KEY

DigitalSign requires for this purpose the creation of a new key pair to replace the expiring key pair (technically defined as "re-key", but in this document identified as 'renewal').

4.7.1. CIRCUMSTANCES 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 e 4.2.

4.7.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See section 4.3.2.

4.7.5. CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

See section 4.4.1.

4.7.6. PUBLICATION OF THE MODIFIED 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

This is a practice not supported by DigitalSign.
If any data contained in a certain certificate needs to be modified, the RA shall revoke the old certificate and issue a new one.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

Revocation or suspension of certificate is only applicable if made within the period of validity of the certificate, meaning that it loses its operability.

The revoked certificates cannot be reactivated, i.e., be valid again.

DigitalSign does not support the certificate suspension.

4.9.1. CIRCUMSTANCES FOR REVOCATION

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

- the subscriber indicates that the original certificate request was not authorized and does not retroactively grant authorization;
- the CA operator obtains reasonable evidence that the subscriber's private key (corresponding to the public key in the certificate) has been compromised or is suspected of compromise;
- the CA operator obtains reasonable evidence that the certificate has been used for a purpose outside of that indicated in the certificate or in the CA operator's subscriber agreement;
- the CA operator receives notice or otherwise becomes aware that a subscriber has violated one or more of its material obligations under the subscriber agreement;
- the CA operator receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted;
- the CA operator receives notice or otherwise becomes aware of a material change in the information contained in the certificate;
- a determination that the certificate was not issued in accordance with the CA operator's Certificate Policy or Certification Practice Statement;
- the CA operator determines that any of the information appearing in the certificate is not accurate;
- the CA operator ceases operations for any reason and has not arranged for another CA operator to provide revocation support for the certificate;
- the CA private key used in issuing the certificate is suspected to have been compromised;
- such additional revocation events as the CA operator publishes in its policy documentation; or
- the certificate was issued in violation of the then-current version of these requirements.

Other circumstances:

- Termination of the Certification Authority's service, in accordance with the corresponding section of this CPS;
- Failure to pay for the certificate;

- The relationship is terminated between the Certification Authority and the Signatory or person/entity responsible for the certificate;
- 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.

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
- A third party that presents proof that the private key has been compromised

4.9.3. PROCEDURE FOR REVOCATION REQUEST

All requests must be made:

- Via the online Revocation Service (if available), by entering the Revocation Code;
- By physically going to the RA's offices during opening hours and signing the revocation form;
- By providing a signed document requesting certificate revocation; or
- By providing prove of key compromise, according to section 4.9.12.

DigitalSign (or RA) shall treat such requests as a priority (maximum period of 8 working hours).

DigitalSign stores all the information relating to certificate revocation processes.

4.9.4. REVOCATION REQUEST GRACE PERIOD

Revocation requests must be submitted as soon as possible. After being performed all procedures and it is verified that the request is valid, the request cannot be canceled.

4.9.5. TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

Updating the revocation status will be performed automatically and immediately after verifying the procedure described in point 4.9.3.

4.9.6. REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Relying Parties must check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL published by the CA that issued the Certificate on which the Relying Party wishes to rely.

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 every 24 hours with a validity of 48 hours by CAs issuing end-user certificates.

The CRL is issued at least annually by Intermediate and Root CAs, but also whenever a CA is revoked.

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

In addition to publishing the CRL, DigitalSign provides information on the status of the certificate through query functions in the DigitalSign repository.

DigitalSign also provides OCSP services. Customers who have contracted these services should check the status of the certificate by using OCSP. The URL for OCSP is communicated to the customer or available in the certificate.

OCSP responses conform to RFC6960 and/or RFC5019. OCSP responses are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

OCSP signing Certificates contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. ON-LINE REVOCATION CHECKING REQUIREMENTS

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

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

DigitalSign supports an OCSP capability using the GET method for certificates issued. OCSP Responders will not respond with a "good" status for a certificate that has not been issued.

For the status of Subscriber Certificates and Subordinate CA Certificates:

- OCSP responses have a validity interval of 8 (eight) hours;
- The information provided via an Online Certificate Status Protocol is updated every 10 (ten) minutes.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder does not respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with this CPS, the responder does not respond with a "good" status for such requests.

DigitalSign may monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

4.9.11. OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No stipulation.

4.9.12. SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE

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 also notify all root store operators that have accepted DigitalSign certificate hierarchies in their root stores as trust anchors.

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 24x7 without any scheduled interruption.

4.10.3. OPTIONAL FEATURES

The OSCP is an optional service that needs to be specifically enabled.

4.11. END OF SUBSCRIPTION

A subscriber may end a subscription of a certificate by:

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

4.12. KEY ESCROW AND RECOVERY

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 through the DigitalSign remote signature solution.

In this case, the Signatory's private key is generated in a certified remote qualified signature/seal creation device (QSCD) operated by DigitalSign as Server Signing Application Service Provider (SSASP), in accordance with the "Remote QSCD Management Service Policy and Practice Statement". The private key is stored encrypted at all times and only ever exists in clear form within the tamper-protected environment of the QSCD, where all signing operations take place; it cannot be used outside that device. Any use of the private key requires the prior authentication of the Signatory and his/her explicit approval of the signing operation, through the Signature Activation Protocol (SAP) verified by the certified Signature Activation Module (SAM), ensuring that the key is used under the sole control of the Signatory, at Sole Control Assurance Level 2 (SCAL2) as defined in EN 419 241-1. DigitalSign is not able to access or use the Signatory's private key.

4.12.1. KEY ESCROW AND RECOVERY POLICY AND PRACTICES

CAs private key are generated and is stored on Hardware Security Module (HSM) duly approved, being their protection guaranteed (backup) in identical device.

4.12.2. SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1. PHYSICAL SECURITY CONTROLS

DigitalSign has implemented a Security Policy, which supports the security requirements of this CPS. The adequacy with these policies is included in the requirements for independent audits. DigitalSign Security Policy contains sensitive security information and is only available through agreements with DigitalSign. An overview of the requirements is described below.

5.1.1. SITE LOCATION AND CONSTRUCTION

The operations DigitalSign's CA and RA are conducted within physically secure environments that dissuade, detect and prevent the use of unauthorized access or disclosure of sensitive information, whether hidden or evident.

5.1.2. PHYSICAL ACCESS

DigitalSign systems are protected by a minimum of four hierarchical levels of physical security, with access requirements to access to the lower level before having access to the level in question.

Progressively restrictive physical access privileges control access to each level. The sensitive operational activities of the CA occur within very restricted access levels. Access to each level requires the use of a proximity card. Physical access is automatically logged and recorded in video. Additional levels require individual access controlled through the use of two authentication factors including biometrics. Personnel without escort, including non-accredited staff or visitors are not allowed in such security areas.

The physical security system includes additional tiers for key management security, which serves to protect both online and offline storage of Cryptographic Signing Units (CSUs) and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two-factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Access to CSUs and keying material is restricted in accordance with segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

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 EXPOSURES

DigitalSign took precautions to minimize the impact of exposure to water, including flood detectors.

5.1.5. FIRE PREVENTION AND PROTECTION

DigitalSign has taken the necessary precautions to prevent and extinguish fires or other exposure to flames or smoke that can be destructive. Preventive measures and protection of fires of DigitalSign are designed to comply with local safety regulations for fire.

5.1.6. MEDIA STORAGE

All media containing production software and data, audit, archive or supporting information, are stored within the facility to control appropriate physical and logical access, designed to limit access to authorized personnel and protect such media information from possible accidental damage (eg, water, fire, and electromagnetic).

5.1.7. WASTE DISPOSAL

Documents and paper materials containing sensitive information are shredded before disposal.

Electronic media and equipments used to collect, store and transmission of sensitive data are securely formatted or physically destroyed, according to the manufacturer's instructions.

Other wastes are treated according to the rules defined internally by DigitalSign.

5.1.8. OFF-SITE BACKUP

Backups of critical data and routine audit logs are made.

All off-premises backups are stored in safe environments.

5.2. PROCEDURAL CONTROLS

5.2.1. TRUSTED ROLES

Trusted Persons are defined as all employees, collaborators, contractors and consultants who have access to or control authentication or coding operations, which may 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.

Established Trusted Roles include, but are not limited to:

- Security Officers: maintain the overall responsibility for the administration and implementation of policies and safety procedures.
- Registration Officers: responsible for the approval, issue, suspension and revocation of End Entity certificates, as well as verification of appropriate web authentication certificates.
- Revocation Officers: responsible for making changes to the status of a certificate.
- System Administrators: authorized to make changes to the system configuration, but without access to its data.
- System Operators: responsible for the day-to-day management of the system (monitoring, backups, recovery ...)
- System Auditors: authorized to access the system logs and verify the procedures performed on it.
- CA Operator - Certification Operator: responsible for activating the keys of the CA in the online environment, for the certificate signing processes and CRLs in the Offline Root environment.

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 control procedures are designed to ensure that at a minimum of 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 certificates, require the participation of at least two Trusted Persons, or a combination of at least one trusted person and an automated process for validation and issuance.

Any CA certificate life cycle management task requires at least two persons with trusted roles to perform such task.

5.2.3. IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

For all personnel seeking to become Trusted Persons, verification of identity is performed through the physical presence by Human Resources Department and checking of well recognized forms of identification (e.g., passports and driver's licenses). 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.
- Creation, destruction or issuance of a CA Certificate.

Systems Management staff may not carry out any task related to Auditing or Certification.

5.3. PERSONNEL CONTROLS

Anyone who seeks to be a trusted person shall provide evidence of the requirements, qualifications and experience necessary to perform their possible liability tasks competently and satisfactorily.

5.3.1. BACKGROUND, QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

DigitalSign requires that staff try to be a Trusted Person, must provide evidence of background, qualifications, experience and clearance necessary to perform their possible liability tasks, competently and satisfactorily.

5.3.2. BACKGROUND CHECK PROCEDURES

Before granting the status of trusted person DigitalSign conducts background checks, which include but are not imitated to the following:

- Arrests for criminal offenses or criminal penalties associated with the nature of the job. As an example, crimes involving financial fraud (ie, embezzlement, theft, diversion).
- 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 have an academic degree without ever obtained it, or inflating the level of the degree that actually has, such as claiming to be have of a Master's 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 liable to be rejected of candidates for Trusting Positions or for taking actions against existing trusted person generally include (but are not limited to) the following:

- False information given 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 considering 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.

5.3.3. 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 (QMS). DigitalSign periodically review and amend its program of training, if necessary.

5.3.4. RETRAINING FREQUENCY AND REQUIREMENTS

DigitalSign provides refresher training and updates to its staff, to the extent and frequency required to ensure that staff maintain proficiency levels required to perform their duties with responsibility, competence and satisfaction. 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 UNAUTHORIZED ACTIONS

Appropriate disciplinary sanctions are carried out due to unauthorized actions or other violations of the policies and procedures of DigitalSign. Disciplinary sanctions may include measures such as the end of the contract and are proportional to the frequency and severity of the unauthorized actions.

5.3.7. CONTRACTING PERSONNEL REQUIREMENTS

In exceptional situations, contractors or consultants may be used to fill positions of trust. To these subcontractors or consultants will be required the same security criteria that an employee of DigitalSign in equivalent role.

Subcontractors and independent consultants, who have not completed or passed the background check procedures specified in this CPS in section 5.3.2, only have access to the security facilities of DigitalSign in the extent they are escorted and directly supervised at all times by Trusted Persons.

5.3.8. DOCUMENTATION SUPPLIED TO PERSONNEL

DigitalSign provides to its employees required training and other documents necessary to perform their work with responsibility and competence.

In addition, to help carry out their duties competently documentation required by personnel will be provided at any time.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. TYPES OF EVENTS RECORDED

DigitalSign, manually or automatically records the following types of significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events
- CA and End User certificate life cycle management events, including:
  - Certificate request, renewal and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of certificates and CRLs
- Events related to security, including:
  - Attempts to access the PKI system, with or without success
  - Actions in the PKI and security systems performed by personnel of DigitalSign
  - Security sensitive files or records read, written or deleted

- Changes to the security profiles
- System and hardware failures and other anomalies
- Activity of the firewall and routers
- Entry and exit of visitors in the premises

Log entries include include the following:

- Date and time of entry
- Serial number or sequence of entry, for automatic daily entries
- Identity of the entity making the daily intake
- Input Type

5.4.2. FREQUENCY OF PROCESSING LOG

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, DigitalSign reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3. RETENTION PERIOD FOR AUDIT LOG

Audit records are kept available until at least two months after the procedure and then filed in accordance with section 5.5.2.

5.4.4. PROTECTION OF AUDIT LOG

Audit logs are protected by physical and logical access controls that include mechanisms to protect log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5. AUDIT LOG BACKUP PROCEDURES

Incremental backups are created daily and full backups are performed weekly.

5.4.6. AUDIT COLLECTION SYSTEM

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by DigitalSign personnel.

5.4.7. NOTIFICATION TO EVENT-CAUSING SUBJECT

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

5.4.8. VULNERABILITY ASSESSMENTS

Part of the audit records are used to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, as well as reviewed and analyzed.

The LSVAs are based on real-time automated records on a daily, monthly and annual basis.

5.5. RECORD ARCHIVAL

5.5.1. TYPES OF EVENTS RECORDED

It is stored at least:

- All audit records collected under section 5.4
- Information on the life cycle of certificates, including requests and supporting documents

5.5.2. RETENTION PERIOD FOR ARCHIVE

Archived data is retained for a period of time defined by applicable law and standards, which is currently set at seven (7) years after any certificate based on these records ceases to be valid.

5.5.3. PROTECTION OF ARCHIVE

DigitalSign protects its archived records so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storing them in a trustworthy system. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archived data can be accessed for the time period set forth in this CPS.

5.5.4. ARCHIVE BACKUP PROCEDURES

Incremental backups are created daily and full backups are performed weekly.

5.5.5. REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Some entries contain information about the time and date. Such information is not generated in the cryptographic equipment.

5.5.6. ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The data file collection system is internal except for RA customers. DigitalSign supports its RA customers in the preservation of an audit record. This file collection system is therefore external.

5.5.7. PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Only authorized Trusted Persons can access the file. The integrity of the information is verified when it is restored.

5.6. KEY CHANGEOVER

5.6.1. ROOT CA

Before the certificate of the Root CA expires a change of key (rekeying) will be made and, if appropriate, changes will be made to the content of the certificate to fit better with current legislation, the current state of DigitalSign and the market. The old CA and its private key will only be used for signing CRLs while there are active certificates issued by the former CA. A new CA will be generated with a new private key. The technical and security documentation of the CA details the CA rekeying process.

5.6.2. SUBORDINATE CA

In the case of subordinate CAs, certificate renovation can be carried out with or without rekeying. The procedure described in the previous point will only be applied in the case of rekeying.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES

The following backups should be maintained in outdoor installations, and available, in case of a compromise or disaster: Certification Application data, audit data and database records for all Certificates issued.

Backup copies of the CA private key shall be generated in accordance with Section 6.2.4.

DigitalSign will keep backup copies of the necessary data for the operation of the CA, as well as for the operation of the RAs.

A contingency plan was made, which is detailed in DigitalSign's Security Policy.

5.7.2. COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

In the event of the corruption of computing resources, software, and/or data, such occurrences are reported to DigitalSign Security Team, and applicable procedures are activated. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, DigitalSign's key compromise and/or disaster recovery procedures are activated.

5.7.3. END PRIVATE KEY COMPROMISE PROCEDURES

Upon suspicion or evidence of compromise of the CA private key, the necessary actions will be taken in response to the incident.

If it is necessary the revocation of the CA certificate, it is set the following procedure:

- It is communicated to the relying parties the revocation status of the certificate through the repository, according to this CPS.
- There will be made commercially reasonable efforts to provide additional notification about the revocation to all affected DigitalSign Certification Hierarchy participants.
- Notify all root store operators that have accepted DigitalSign certificate hierarchies in their root stores as trust anchors.
- Revoke, within the period agreed with the national supervisor, the certificates issued by this CA, applying, if applicable, any of the procedures provided in the Plan of Cessation or the Continuity Plan.

5.7.4. BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

DigitalSign offers redundant secondary facilities, capable of reactivating the essential operations of DigitalSign's Certification Hierarchy after disaster.

The recovery plan in case of disaster is regularly tested, verified and updated to be operational in case of any occurrence.

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, root stores that have included DigitalSign's certificates in their root stores, 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 Gabinete 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 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 keys for CAs is made by authorized personnel, 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 140-2 Level 3 or Common Criteria EAL 4+.

The keys for end users are generated in qualified signature creation devices, duly approved.

6.1.2. PRIVATE KEY DELIVERY TO ENTITY

See Section 3.2.1.

6.1.3. PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The public keys are submitted to DigitalSign for certification issuance through the use of a PKCS#10 Certificate Signing Request (CSR).

6.1.4. CA PUBLIC KEY DELIVERY TO USERS

The CA certificate will be available to users on the website of DigitalSign.

6.1.5. KEY SIZES

The minimum length of the key pairs are:

RSA hierarchy	Key size
Root CA	4096 bits
Intermediate CAs	4096 bits
Issuing CAs	4096 bits
End User certificates	2048 bits

ECDSA hierarchy	Key size
Root CA	384 bits
Intermediate CAs	384 bits
Issuing CAs	384 bits
End User certificates	256 bits

6.1.6. PUBLIC KEY PARAMETERS GENERATION

No stipulation.

6.1.7. KEY USAGE PURPOSES

According to to section 7.1.2.

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. STANDARDS FOR CRYPTOGRAPHIC MODULES

For the creation and storage of the DigitalSign private key is used hardware security modules that are certified or meet, at least, the requirements FIPS 140-2 Level 3 or Common Criteria EAL4+.

Where applicable ([QCP-n-qscd] and [QCP-l-qscd]), end-users private key are generated in a qualified signature creation device (QSCD). QSCD certification status is monitored until the end of the validity period of the issued certificates, and appropriate measures are taken in case of modification of this status.

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

DigitalSign has implemented technical and procedural mechanisms that require the participation of several trusted employees to perform cryptographic operations of the CA. DigitalSign uses 'secret sharing' to share the information needed for the activation of the private key into separate parts, known as "secret shares", which are held by trained and trustworthy individuals, called 'Key Holders'. The limit number of Secret Shares (m), of a total number of Key Holders created and distributed for particular hardware cryptographic module (n), is required to enable the private key stored in the module.

The Secret Shares are protected in accordance with this CPS in Section 6.4.2.

6.2.3. PRIVATE KEY ESCROW

The escrow of CA, RA and end-user private keys is not permitted under this CPS.
Regarding the Signatory's private keys generated and managed by DigitalSign in the remote signature/seal service - which does not constitute key escrow - see section 4.12.

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 with trusted roles 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 6.2.3.

6.2.5. PRIVATE KEY ARCHIVAL

See section 4.12.

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

For certificates whose private key is held by the Signatory (on a smartcard/USB token or in software), the private key is accessed via an activation key (e.g. PIN), which only the Signatory knows.

For private keys held in the DigitalSign remote signature/seal service, the private key is activated through the signature activation mechanism (SAP/SAM) described in the "Remote QSCD Management Service Policy and Practice Statement", upon two-factor authentication of the Signatory and his/her explicit approval of the signing operation (see section 4.12).

CAs private keys are activated as defined in section 6.2.2. After the private key is activated, it can remain active indefinitely until being deactivated.

6.2.9. METHOD OF DEACTIVATING PRIVATE KEY

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

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

For private keys held in the remote signature/seal service, the private key is deactivated automatically upon completion of the authorized signing operation(s), and in any case at the end of the signature session.

The CAs private keys are deactivated following the steps described in the cryptographic device administrator's manual, or when the CA system is shut down.

6.2.10. METHOD OF DESTROYING PRIVATE KEY

When necessary, DigitalSign may destroy the CA private key. DigitalSign ensures formatting (zeroisation) of its cryptographic modules and other appropriate means to ensure the complete destruction of keys. When implemented, the key destruction activities are recorded.

Also, when the cryptographic module is substituted, all keys must be destroyed before the replacement occurs.

All the copies of the CA's keys must be destroyed at the end of the cryptographic life cycle.

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

Backup copies are made and all issued certificates are stored, as part of the routine procedures of DigitalSign.

6.3.2. USAGE PERIODS FOR THE PUBLIC AND PRIVATE KEYS

The usage period of a certificate expires upon its expiration or revocation. The usage period of the key pair is the same as the period defined for the associated certificates, except:

- Private keys can still be used to decode
- Public keys can still be used for signature verification

Certificates issued by any CA have a validity period not superior to its own certificate.

Furthermore, DigitalSign stops issuing new certificates at an appropriate date prior to the expiration of the CA's certificate, so that no certificate issued expires after the expiration of any chained CA.

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

Certificate type	Certificate maximum validity
Root CAs	25 years
Issuing CAs (S/MIME/eSignature)	12 years
Issuing CAs (TSA)	25 years
OCSP	1 year
End user (eSignature)	5 years
End user (S/MIME)	825 days
TimeStamping	25 years

S/MIME certificates are issued only under dedicated certificate profiles that comply with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, including the corresponding CA/Browser Forum reserved certificate policy identifier. Certificates of the Legacy generation are not issued.

6.4. ACTIVATION DATA

6.4.1. ACTIVATION DATA GENERATION AND INSTALLATION

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

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

On the smartcards or usb tokens used by DigitalSign, keys are generated protected with a random-calculated PIN and PUK. The Subject has software to change their card's PIN and PUK.

When in software, it's required to be the enduser to generate the private key – the issued certificate is provider in a standardized base64 ou binary encoded.

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

6.4.2. ACTIVATION DATA PROTECTION

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

Activation data are stored in secure vaults.

When end-user 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 performs all CA and RA functions using reliable systems that meet the requirements stipulated by DigitalSign. DigitalSign recommends that its RA clients follow the same guidelines.

DigitalSign implements requirements specified by the CA/Browser Forum, Network and Certificate System Security Requirements, and other relevant requirements to meet best practices.

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.

6.5.2. COMPUTER SECURITY RATING

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. SYSTEM DEVELOPMENT CONTROLS

The applications are developed and implemented by DigitalSign or others, according to systems development and maintenance change management standards. DigitalSign also provides software to its customers to perform RA functions.

The developed software, when loaded, provides methods to verify that the software has not been changed before installation and is the correct version to be used.

6.6.2. SECURITY MANAGEMENT CONTROLS

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 system.

6.6.3. LIFE CYCLE SECURITY RATINGS

Update and maintenance operations of systems and products follows the same controls as the original equipment and is performed by authorized personnel with proper training to do so by following the procedures defined.

6.7. NETWORK SECURITY CONTROLS

DigitalSign performs all its CA and RA functions using secure networks, to prevent unauthorized access and other malicious activity. DigitalSign protects communication of sensitive information through the use of digital signatures and encryption.

DigitalSign implements requirements specified by the CA/Browser Forum, Network and Certificate System Security Requirements, and other relevant requirements to meet best practices.

6.8. TIME-STAMPING

Certificates, CRLs, and other revocation data contain information on the date and time. Such information is not based on cryptographic mechanisms.

7. CERTIFICATE AND CRL PROFILE

7.1. CERTIFICATE PROFILE

Certificates issued by DigitalSign in accordance to this document comply with:

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

The certificate profiles may be consulted in Certificate Profile List document associated with this CPS.

7.1.1. VERSION NUMBER(S)

All certificates issued by DigitalSign CAs are in compliance with version 3 (three) of the X.509 format.

7.1.2. CERTIFICATE EXTENSIONS

The certificate extensions are in compliance with RFC 5280.

7.1.3. ALGORITHM OBJECT IDENTIFIERS

Allowed signature algorithm object identifiers:

- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption
- 1.2.840.113549.1.1.13 - sha512WithRSAEncryption
- 1.2.840.10045.4.3.2 - ecdsa-with-SHA256
- 1.2.840.10045.4.3.3 - ecdsa-with-SHA384
- 1.2.840.10045.4.3.4 - ecdsa-with-SHA512

7.1.4. NAME FORMS

As defined in section 3.1.

7.1.5. NAME CONSTRAINTS

No stipulation.

7.1.6. CERTIFICATE POLICY OBJECT IDENTIFIER

Where this extension is used, certificates contain "policyQualiflierID: 1.3.6.1.5.5.7.2.1" and "CPSuri", which point to the URI where the Certification Practices Statement with the OID identified by the "policyIdentifier" can be found.

Other certificate policy object identifiers can be also included, depending on the type of certificate, as described in document Certificate Profiles List.

7.1.7. USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation.

7.1.8. POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9. PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

No stipulation.

7.2. CRL PROFILE

7.2.1. VERSION NUMBER(S)

It is used the version 2 (two) format for X.509 CRLs as RFC 5280, and include the following fields:

Field	Value
Version	2
Signature Algorithm	Identification of the algorithm used to sign the CRL. Allowed signature algorithm are: • 1.2.840.113549.1.1.13 - sha512WithRSAEncryption • 1.2.840.10045.4.3.3 - ecdsa-with-SHA384 • 1.2.840.10045.4.3.4 - ecdsa-with-SHA512
Issuer	DN f the CA issuing the CRL
Effective 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 defined in section 4.4.7.
Revoked Certificates	List of revoked certificates, including the serial number and date of revocation.

7.2.2. CRL AND CRL ENTRY EXTENSIONS

The CRLs issued by DigitalSign have the following extensions:

Field	Value
Authority Key Identifier	Identifier of the CA issuing the CRL.
CRL Number	Sequential CRL number.
expiredCertsOnCrl (OID: 2.5.29.60)	Indicates that CRL also contains expired entries.

7.3. OCSP PROFILE

The OCSP protocol (Online Certificate Status Protocol) is a form of DigitalSign giving information about the revocation status of a particular certificate.

The OCSP Responders are as set forth in RFC 6960.

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

7.3.1. VERSION NUMBER(S)

It is used the version one (1) from OCSP specification according RFC 6960.

7.3.2. OCSP EXTENSIONS

The OCSP responses issued by DigitalSign have the following extensions:

Field	Value
OCSP Archive Cutoff	Indicates that OCSP responder also replies for expired certificates.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

It is performed an annual audit by an accredited entity for the DigitalSign operations and Key Management operations, which support service management of DigitalSign CAs.

Beyond compliance assessments and audits, DigitalSign is responsible for performing other reviews and investigations to ensure the reliability of its PKI infrastructure which includes but is not limited to the following:

- DigitalSign or its authorized representative is responsible, within its sole discretion, to play at any time, an audit or investigation to a RA client, provided there is reason to believe that the audited entity has failed to compliance with the standards of the DigitalSign Certification Hierarchy, has suffered an incident, acted or failed to act for the entity did not fail, which could potentially threaten the security or integrity of the DigitalSign Certification Hierarchy.
- DigitalSign or its authorized representative is responsible for evaluating the Risk Management to RA clients in the fulfillment of their usual ordinary course of business.

DigitalSign, or their legal representatives, may delegate the performance of these audits, reviews or investigations to a third party auditor duly accredited by the authority. Entities that are subject to audits, reviews or investigations should establish cooperation with DigitalSign and the personnel carrying out the audit, evaluation or investigation.

8.1. FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

Audits are conducted at least on an annual basis.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

Audits to the DigitalSign should be performed by appropriately accredited auditor, in accordance with applicable local laws.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Audit operations to DigitalSign are performed by an independent auditor.

8.4. TOPICS COVERED BY ASSESSMENT

The scope of audits and other assessment includes compliance with applicable law, with this CPS, and other rules, procedures and processes (especially those related to key management operations, resources, management and operation controls and life cycle certificate management).

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, 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. COMMUNICATIONS 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 & LEGAL MATTERS

9.1. FEES

9.1.1. CERTIFICATE ISSUANCE OR RENEWAL FEES

Fees may be charged for issuing procedures, and / or renewal of certificates.

9.1.2. CERTIFICATE ACCESS FEES

It will not be charged any fees for the certificates available in the repository.

9.1.3. REVOCATION OR STATUS INFORMATION ACCESS FEES

It will not be charged any fees for the availability of the CRL in the repository, in accordance with the stipulations of this CPS.

Customized CRL issuance, OCSP services, or other value added service for status information or revocation of certificates will be subject to the charge of contracted fees.

9.1.4. FEES FOR OTHER SERVICES SUCH AS POLICY INFORMATION

Consultation of this CPS and other documents relating to policies, practices and procedures is not subject to any charging fees.

Ownership rights of this information must be guaranteed.

9.1.5. REFUND POLICY

No refunds are provided for any actions of certificate revocation.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. INSURANCE COVERAGE

DigitalSign maintains insurance coverage for errors and omissions performed within the scope of its activity, through liability insurance with a capital fixed in law of 125,000 €.

9.2.2. OTHER ASSETS

Registration Authority customers must have sufficient financial resources to maintain their operations and perform their duties should bear the liability risks to its subscribers and relying parties.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. SCOPE OF CONFIDENTIAL INFORMATION

The following records must be kept confidential and private, according to Section 9.3.2:

- Registration of requests for issuing certificates
- DigitalSign private keys, and other related security features
- Transactional records (both full records and traces)
- Any information concerning security parameters
- Audit reports performed by DigitalSign or its auditors (whether internal or external)
- Contingency planning and disaster recovery
- Security measures for monitoring the operations of hardware and software from DigitalSign and certification service management.

9.3.2. INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Certificates, certificate revocation and other status information, DigitalSign's repository and information contained therein are not considered Confidential / Private Information.

Information that is not expressly considered Confidential / Private Information, under section 9.3.1, shall not be considered confidential or private. This section is subject to applicable privacy laws.

9.3.3. RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

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

9.4. 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 DigitalSign Certification Hierarchy 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 TO LAW ENFORCEMENT OFFICIALS

All DigitalSign 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

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

The assignment of intellectual property rights among participants of the DigitalSign Certification Hierarchy domain, except end users and relying parties, is determined by the contracts applicable to these participants.

All intellectual property rights, including certificates, CRL, OIDs, CPS and key pair belong, unless explicitly agreed, to DigitalSign.

Holders certificate key pairs are owned by the holder, as well as the names and other information in the DN.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA REPRESENTATION AND WARRANTIES

DigitalSign warrant:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate.
- That issued certificates meet all the requirements of this CPS
- The revocation services and use of a repository conform to this CPS in all material aspects.

9.6.2. RA REPRESENTATION AND WARRANTIES

Digitalsign contracts with RAs warrant:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate.
- That issued certificates meet all the requirements of this CPS.
- The revocation services and use of a repository conform to this CPS in all material aspects.

9.6.3. SUBSCRIBER REPRESENTATION AND WARRANTIES

DigitalSign contracts with subscribers ensure that:

- Accept and are obliged to fulfill the contract of issued digital certificate.
- Are obliged to respect the rules of use of the digital certificate (and respective private key) and ensure that they will not modify in any way, its technical configuration
- Ensure the confidentiality of the process of obtaining and using the respective digital certificate and private key
- Declare that they know what are the legal effects attributed to the use of digital certificate and digital signature
- Declare that they are liable for any use that is given to the digital certificate (and corresponding private key) and the resulting consequences
- Declare that they are obliged to revoke or inform DigitalSign immediately on suspicion or loss of control of the private key or incorrectness or alteration of information on the certificate, while valid
- Declare that from the certificate revocation or the expiry of its validity, it is prohibited to use the respective signature creation data to generate an electronic signature.

9.6.4. RELYING PARTY REPRESENTATIONS AND WARRANTIES

Relying Third Party Charters require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in this CPS.

9.7. DISCLAIMERS OF WARRANTIES

DigitalSign refuse all warranties that are not linked to obligations established in this CPS.

9.8. CERTIFICATION AUTHORITY 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

DigitalSign assumes its responsibility with respect to any compensation from accordance with applicable law.

9.10. TERM AND TERMINATION

9.10.1. TERM

All documents related to the CA activity, including this CPS and any subsequent amendments become effective after publication in the repository.

9.10.2. TERMINATION

All documents related to the CA activity, including this CPS and any subsequent amendments shall remain in effect until publication of a new version or change.

9.11. INDIVIDUAL NOTICES AND COMMUNICATION

Unless otherwise specified by agreement between the parties, DigitalSign Subdomain 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

9.12.1. PROCEDURE FOR AMENDMENT

To ensure the update of this CPS, DigitalSign's administration meets with intervals not exceeding one (1) year, with the Operations Director and Technical Services Director for evaluation of possible needs for improvement and change.

Changes to this CPS shall be approved by the administration. Changes must be made through documents, containing the amended form of the CPS or an update.

Changes, corrections and / or updates shall be published in the form of new versions of the CPS (and / or their respective CPs), replacing any previous version.

9.12.2. NOTIFICATION MECHANISM AND PERIOD

DigitalSign reserves the right to correct these CPS without notice to corrections which are not materially relevant according to the criteria of DigitalSign, including but not limited to errors writing URLs changes, contact changes, etc

In cases where the alterations or amendments may affect the acceptability of certificates for the purposes that they have been issued, it will be tried the notification to interested parties that a change or correction was made.

9.12.3. CIRCUMSTANCE 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 PROVISIONS

9.13.1. DISPUTES AMONG DIGITALSIGN AND RA CUSTOMERS

These conflicts must be resolved by the provisions of the contract between the parties.

9.13.2. DISPUTES WITH END-USER SUBSCRIBERS OR RELYING PARTIES

Upon what is allowed by law, all contracts must contain a clause for conflict resolution.

9.14. GOVERNING LAW

Subject to any limitations imposed by law, the Portuguese law should exercise authority, construction, interpretation and validity of this CPS, regardless of the choice of contract or other legal provision. This choice of law is made to ensure uniform procedures and interpretations to all participants of DigitalSign's hierarchy, no matter their location.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to the laws, rules, regulations, ordinances, edicts, or other, whether national, state, local or foreign, including but not limited to, restrictions in the import or export of software, hardware or technical information.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. ENTIRE AGREEMENT

No stipulation.

9.16.2. ASSIGNMENT

No stipulation.

9.16.3. SEVERABILITY

No stipulation.

9.16.4. ENFORCEMENT

No stipulation.

9.16.5. FORCE MAJEURE

No stipulation.

9.17. OTHER PROVISIONS

9.17.1. MANAGEMENT GROUP (GRUPO DE GESTÃO)

The management group is constituted by:

- Administrator
- CEO
- Quality Director
- Systems' Administrator
- Systems' Operator
- Security Administrator
- Systems' Auditor
- External Consultant (by invitation)

The duties, responsibilities and objectives of this management group are defined in the CA internal documents.

10. APPENDIX A – ACRONYMS AND DEFINITIONS

CA	Certifying Authority
CP	Certificate Policies
CPS	Certification Practices Statement
CRL	Certificate Revocation List
eIDAS	Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183
EC DIGITALSIGN	DigitalSign – Certificadora Digital, SA Certification Authority
FIPS	United State Federal Information Processing Standards
HSM	Hardware Security Module
LSVA	Logical Security Vulnerability Assessment.
OCSP	Online Status Certificate Protocol
OID	Unique number of "object identifier"
OTP	One Time Password
PIN	Personal Identification Code
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PUK	Pin Unlock Key
QSCD	Qualified Electronic Signature/Seal Creation Device
RA	Registry Authority
RFC	Request for comment
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCAL2	Sole Control Assurance Level 2, as defined in CEN EN 419 241-1
SCU	Signing Cryptographic Units
SSAS	Server Signing Application Service
SSASP	Server Signing Application Service Provider
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Sockets Layer