Certification Practice Statement

Validated ID

Always be yourself

General information

Documentary control

Security classification:	Public
Version:	1.1
Edition date:	22/11/2023
Code:	VALIDATEDID_DPC_EN_VID_v1.1

Formal state

Prepared by:	Reviewed by:	Approved by:
Name: Andrea Vargas Date: 22/11/2023	Name: Fernando Pino Date:	Name: Santi Casas Date:

Versions control

Version	Changes	Description of change	Author of change	Date of change
1.0	Original	Document creation	AGB	31/05/2022
1.1	3.1.4	Clarification of the attributes of certificates for the identification of the persons concerned with public administrations.	APV	07/08/2023
Typo error	1.4.15	OID error	FPS	22/11/2023

Index

GENERAL INFORMATION 2

DOCUMENTARY CONTROL 2
FORMAL STATE 2
VERSIONS CONTROL 3

INDEX 4

1. INTRODUCTION 12

1.1. PRESENTATION 12
1.2. DOCUMENT NAME AND IDENTIFICATION 14
1.2.1. Certificates´ identifiers 14
1.3. PARTICIPANTS IN THE CERTIFICATION SERVICES 16
1.3.1. Trust service Provider 16
1.3.1.1. Validated ID Root CA 16
1.3.1.2. Validated ID Subordinate CA 01 17
1.3.2. Registration Authority 17
1.3.3. End entities 18
1.3.3.1. Subscribers of the certification services 18
1.3.3.2. Signers 19
1.3.3.3. Relying parties 20
1.3.4. Public Key Infrastructure Provider 20
1.4. USE OF CERTIFICATES 21
1.4.1. Uses permitted for certificates 21
1.4.1.1. Qualified Certificate for Natural Person issued on software 21
1.4.1.2. Qualified Certificate for Natural Person on HSM centralized 22
1.4.1.3. Qualified Certificate for Natural Person issued on QSCD centralized 23
1.4.1.4. Qualified certificate for Natural Person belonging in Software 24
1.4.1.5. Qualified certificate for Natural Person belonging in HSM centralized 24
1.4.1.6. Qualified certificate for Natural Person belonging in QSCD centralized 25
1.4.1.7. Qualified certificate for Natural Person member on software 26
1.4.1.8. Qualified certificate for Natural Person member on HSM centralized 27
1.4.1.9. Qualified certificate for Natural Person member on QSCD centralized 28
1.4.1.10. Qualified Certificate of signature for Natural Person Representative on software 28
1.4.1.11. Qualified certificate of signature for Natural Person Representative on HSM centralized 29
1.4.1.12. Qualified certificate of signature for Natural Person Representative on QSCD centralized 30
1.4.1.13. Qualified certificate for natural person Representative of Entity with the administrations on software 31
1.4.1.14. Qualified certificate for natural person Representative of Entity with the administrations on HSM centralized 32
1.4.1.15. Qualified certificate for natural person Representative of Entity with the administrations on centralized QSCD 32

1.4.1.16. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on software 33
1.4.1.17. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on HSM centralized 34
1.4.1.18. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on QSCD centralized 35
1.4.1.19. Qualified certificate for Electronic Seal on software 36
1.4.1.20. Qualified certificate for Electronic Seal on HSM centralized 36
1.4.1.21. Qualified certificate for Electronic Seal on QSCD centralized 37
1.4.1.22. Qualified certificate for electronic timestamping 37
1.4.2. Limits and forbidden uses of certificates 38
1.5. POLICY MANAGEMENT 40
1.5.1. Organization that administers the document 40
1.5.2. Contact information of the organization 40
1.5.3. Document management procedures 40

2. PUBLICATION OF INFORMATION AND DEPOSITO OF CERTIFICATES 41

2.1. DEPOSIT(S) OF CERTIFICATES 41
2.2. PUBLICATION OF INFORMATION OF THE CERTIFICATION SERVICES PROVIDER 41
2.3. FREQUENCY OF PUBLICATION 41
2.4. ACCESS CONTROL 42

3. IDENTIFICATION AND AUTHENTICATION 43

3.1. INITIAL REGISTRATION 43
3.1.1. Type of names 43
3.1.1.1. Qualified Certificate for Natural Person on software 43
3.1.1.2. Qualified Certificate for Natural Person on HSM centralized 43
3.1.1.3. Qualified Certificate for Natural Person issued on QSCD centralized 44
3.1.1.4. Qualified certificate for Natural Person belonging in Software 44
3.1.1.5. Qualified certificate for Natural Person belonging in HSM centralized 45
3.1.1.6. Qualified certificate for Natural Person belonging in QSCD centralized 46
3.1.1.7. Qualified certificate for Natural Person member on software 47
3.1.1.8. Qualified certificate for Natural Person member on HSM centralized 47
3.1.1.9. Qualified certificate for Natural Person member on QSCD centralized 48
3.1.1.10. Qualified Certificate of signature for Natural Person Representative on software 49
3.1.1.11. Qualified certificate of signature for Natural Person Representative on HSM centralized 49
3.1.1.12. Qualified certificate of signature for Natural Person Representative on centralized QSCD 50
3.1.1.13. Qualified certificate for natural person Representative of Entity with the administrations on software 50
3.1.1.14. Qualified certificate for natural person Representative of Entity with the administrations on HSM centralized 51
3.1.1.15. Qualified certificate for natural person Representative of Entity with the administrations on centralized QSCD 52
3.1.1.16. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on software 52

3.1.1.17. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on HSM centralized 53
3.1.1.18. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on QSCD centralized 53
3.1.1.19. Qualified certificate for Electronic Seal on software 54
3.1.1.20. Qualified certificate for Electronic Seal on HSM centralized 54
3.1.1.21. Qualified certificate for Electronic Seal on QSCD centralized 55
3.1.1.22. Qualified certificate for electronic timestamping 55
3.1.2. Meaning of the names 56
3.1.2.1. Issuance of certificates of the set of tests and certificates of tests in general 56
3.1.3. Use of anonymous and pseudonymous 56
3.1.4. Interpretation of name formats 56
3.1.5. Uniqueness of names 57
3.1.6. Resolution of name conflicts 57
3.2. INITIAL IDENTITY VALIDATION 59
3.2.1. Proof of possession of private key 59
3.2.2. Identity Validation 59
3.2.3. Authenticate the identity of an organization, company, or entity by proxy 60
3.2.4. Authentication of natural person identity 63
3.2.4.1. In the certificates 63
3.2.4.2. Identity validation 64
3.2.4.3. Entail of the natural person 65
3.2.5. Subscriber´s not verified information 65
3.2.6. Autentication of te identity of a RA and its operators 65
3.3. IDENTIFICATION AND AUTHENTICATION OF RENEWAL REQUESTS 67
3.3.1. Validation for certificates routine renewal 67
3.3.2. Identification and authentication of revocation request 67
3.4. IDENTIFICATION AND AUTHENTICATION OF REVOCATION, SUSPENSION OR REACTIVATION REQUEST 68

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 69

4.1. CERTIFICATE ISSUANCE REQUEST 69
4.1.1. Legitimation to apply for the issuance 69
4.1.2. Registration procedure and responsibilities 69
4.2. PROCESSING THE CERTIFICATION REQUEST 70
4.2.1. Implementation of identification and authentication fuctions 70
4.2.2. Approval or rejection of request 70
4.2.3. Time to process certificate requests 71
4.3. CERTIFICATE ISSUANCE 71
4.3.1. CA actions during certificate issuance 71
4.3.2. Notification to the certificate issuance applicant 72
4.4. CERTIFICATE DELIVERY AND ACCEPTANCE 72
4.4.1. CA Responsabilities 72
4.4.2. Way in which the certificate is accepted 73

4.4.3. Publication of the certificate ... 73
4.4.4. Notification of the certificate issuance to third parties ... 73
4.5. KEY PAIR AND CERTIFICATE USAGE ... 73
4.5.1. Use by the signer ... 73
4.5.2. Use by the subscriber ... 74
4.5.2.1. Obligations of the certificate subscriber ... 74
4.5.2.2. Civil liability of the certificat´s subscriber ... 75
4.5.3. Use by the relying third party in certificates ... 76
4.5.3.1. Obligations of the relying third parties in certificates ... 76
4.5.3.2. Civil liability of the relying third parties in certificates ... 76
4.6. CERTIFICATE RENEWAL ... 77
4.7. KEY AND CERTIFICATE RENEWAL ... 77
4.7.1. Circumstances for certificate and key renewal ... 77
4.7.2. Online renewal process ... 77
4.7.2.1. Circumstances for online renewal ... 77
4.7.2.2. Who can request an online renewal certificate ... 78
4.7.2.3. Approval or rejection of the request ... 78
4.7.2.4. Procedure for online renewal request ... 78
4.7.2.5. Notification of the renewed certificate issuance ... 79
4.7.2.6. Way in which the certificate is accepted ... 79
4.7.2.7. Publication of the certificate ... 79
4.7.2.8. Notification of the certificate issuance to third parties ... 79
4.8. CERTIFICATE MODIFICATION ... 79
4.9. REVOCATION, SUSPENSION OR REACTIVATION OF CERTIFICATES ... 80
4.9.1. Causes os certificate revocation ... 80
4.9.2. Reasons for suspension of certificates ... 81
4.9.3. Reason for reactivation of certificates ... 82
4.9.4. Who can request the revocation, suspension or reaction of a certificate ... 82
4.9.5. Procedures for revocation, suspension or reactivation request ... 82
4.9.6. Temporary revocation, suspension or reactivation application ... 83
4.9.7. Temporary period of revocation, suspension or reactiviation application processing ... 83
4.9.8. Obligation to consult certificate revocation or suspension information ... 84
4.9.9. Frequency of issuance of certificate revocation lists (CRLs) ... 84
4.9.10. Maximum period of publication of CRLs ... 84
4.9.11. Availability of the service checking in line with the state of the certificates ... 85
4.9.12. Obligation to check the consultation certificate status service ... 85
4.9.13. Special requirements in case of compromise of the private key ... 85
4.9.14. Maximum period os suspension of digital certificate ... 86
4.10. COMPLETION OF THE SUBSCRIPTION ... 86
4.11. DEPOSIT AND RECOVERY OF KEYS ... 86
4.11.1. Policies and practices of deposit and key recovery ... 86
4.11.2. Policy and practices of encapsulation and recovery of key session ... 86
5. PHYSICAL SECURITY CONTROLS, MANAGEMENT AND OPERATIONS ... 87

5.1. PHYSICAL SECURITY CONTROLS 87
5.1.1. Location and construction of facilities 87
5.1.2. Physical access 88
5.1.3. Electrical power and air conditioning 88
5.1.4. Exposer to water 88
5.1.5. Fire prevention and protection 89
5.1.6. Backup storage 89
5.1.7. Waste management 89
5.1.8. Offsite backup 89
5.2. PROCEDURE CONTROLS 89
5.2.1. Reliable features 90
5.2.2. Number of individuals per task 90
5.2.3. Identification and authentication for each role 91
5.2.4. Roles requiring separation of tasks 91
5.2.5. PKI management system 91
5.3. PERSONNEL CONTROLS 92
5.3.1. History, qualification, experience and authorisation requirements 92
5.3.2. Procedures of history investigation 93
5.3.3. Training requirements 93
5.3.4. Retraining frequency and requirements 94
5.3.5. Job rotations frequency and sequence 94
5.3.6. Sections and unauthorized actions 94
5.3.7. Professionals contracting requirements 94
5.3.8. Documentation supplied to personnel 94
5.4. SECURITY AUDIT PROCEDURES 95
5.4.1. Types of recorded events 95
5.4.2. Frecuency of processing audit logs 96
5.4.3. Period of retention of audit logs 96
5.4.4. Audit logs protection 97
5.4.5. Audit log backup procedures 97
5.4.6. Location of the audit logs storage system 97
5.4.7. Notification of the audit event to the subect that caused the event 97
5.4.8. Vulnerabily analysis 98
5.5. INFORMATION FILES 99
5.5.1. Types of records archived 99
5.5.2. Retention period for the files 100
5.5.3. Protection of the file 100
5.5.4. File backup procedures 100
5.5.5. Requirements of timestamping 100
5.5.6. Location of the file system 101
5.5.7. Procedures to obtain and verify file information 101
5.6. KEYS RENEWAL 101

5.7. COMPROMISED KEY AND RECOVERY OF DISASTER 102
5.7.1. Management procedures of incidents and commitments 102
5.7.2. Resources, applications or data corruption 102
5.7.3. Compromised privated key of the entity 102
5.7.4. Business continuaty capabilities after a disaster 102
5.8. SERVICE TERMINATION 103

6. TECHNICAL SECURITY CONTROLS 105

6.1. GENERATION AND INSTALLATION OF THE PAIRO F KEYS 105
6.1.1. Generation of the pair of keys 105
6.1.1.1. Generation of the key pair from the signer 105
6.1.2. Sending the private key to the signer 106
6.1.3. Sending of the public key to the certificate issuer 106
6.1.4. Public key distribution of the certification services provider 106
6.1.5. Key sizes 107
6.1.6. Generation of public key parameters 107
6.1.7. Quality check of the public key parameters 107
6.1.8. Key generation in IT applications or in equipment goods 107
6.1.9. Key usage purposes 107
6.2. PRIVATE KEY PROTECTION 108
6.2.1. Cryptographic modules standars 108
6.2.2. Private key multi-person (n-m) control 108
6.2.3. Private key deposit 108
6.2.4. Private key backup 108
6.2.5. Private key storage 109
6.2.6. Private key transfer into a cryptographic module 109
6.2.7. Method of activating the private key 109
6.2.8. Method of deactivating private key 110
6.2.9. Method of destroying the private key 110
6.2.10. Cryptographic modules clasification 110
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT 110
6.3.1. Public key file 110
6.3.2. Public and private key usage periods 110
6.4. ACTIVATION DATA 111
6.4.1. Activation data generation and instalation 111
6.4.2. Activation data protection 111
6.5. COMPUTER SECURITY CONTROLS 111
6.5.1. Specific computer security technical requirements 112
6.5.2. Computer security rating 112
6.6. LIFE CYCLE TECHNICAL CONTROLS 112
6.6.1. System development controls 112
6.6.2. Security management controls 113

6.6.2.1. Classification and management of information and goods 113
6.6.2.2. Management operations 113
6.6.2.3. Treatment of supports and safety 114
Planning system 114
Reports of incidents and response 114
Operational procedures and responsibilities 114
6.6.2.4. Access system management 114
CA General 114
Certificate generation 115
Revocation management 115
Revocation management 115
6.6.2.5. Gestión del ciclo de vida del hardware criptográfico 115
6.7. NETWORK SECURITY CONTROLS 116
6.8. ENGINEERING CONTROLS OF CRYPTOGRAPHIC MODULES 117
6.9. TIME SOURCE 117
6.10. CHANGING THE STATUS OF A SECURE SIGNATURE CREATION DEVICE (QSCD) 117

7. CERTIFICATES PROFILES AND CRLS 119

7.1. CERTIFICATE PROFILE 119
7.1.1. Version number 119
7.1.2. Certificate extensions 119
7.1.3. Object identifier (OID) of algorithms 119
7.1.4. Names format 119
7.1.5. Names restriction 120
7.1.6. Object identifiers (OID) of certificates types 120
7.2. CRL PROFILE 120
7.2.1. Version number 120
7.2.2. OCSP profile 120

8. COMPLIANCE AUDIT 121

8.1. FREQUENCY OF COMPLIANCE AUDIT 121
8.2. FREQUENCY OF COMPLIANCE AUDIT 121
8.3. AUDITOR RELATIONSHIP TO AUDITED ENTITY 121
8.4. TOPICS COVERED BY AUDIT 121
8.5. ACTIONS TAKEN AS A RESULT OF LACK OF CONFORMITY 122
8.6. TREATMENT OF AUDIT REPORTS 123

9. BUSINESS AND LEGAL REQUIREMENTS 124

9.1. FEES 124
9.1.1. Certidicate issuance or renewal fees 124
9.1.2. Certificate access fees 124
9.1.3. Certificate status information access fees 124
9.1.4. Fees for other service 124
9.1.5. Refund policy 124

9.2. FINANCIAL CAPACITY 124
9.2.1. Insurance coverage 125
9.2.2. Other assets 125
9.2.3. Insurance coverge for subscribers and relaying third parties in certificates 125
9.3. CONFIDENTIALITY 125
9.3.1. Confidential information 125
9.3.2. Non confidential information 125
9.3.3. Information disclosure of suspension and revocation 126
9.3.4. Legal disclosure of information 126
9.3.5. Information disclosure on request of owner 127
9.3.6. Other information disclosure cirmstances 127
9.4. PERSONAL DATA PROTECTION 127
9.5. INTELLECTUAL PROPERTY RIGHTS 130
9.5.1. Property of certificates and revocation information 130
9.5.2. Property of the Certification Practice Statement 131
9.5.3. Property of information relating to names 131
9.5.4. Property of keys 131
9.6. OBLIGATIONS AND CIVIL LIABILITY 132
9.6.1. VALIDATED ID obligations 132
9.6.2. Guarantees offered to subscribers and relaying third parties in certidicates 133
9.6.3. Rejection of other guarantees 134
9.6.4. Limitation of liability 134
9.6.5. Indemnity clauses 135
9.6.5.1. Subscriber indemnity clause 135
9.6.5.2. Relaying third person in the certificate indemnity clause 135
9.6.6. Fortuitous event and force majeure 135
9.6.7. Applicable law 136
9.6.8. Severability, survival, entire agreement and notification clauses 136
9.6.9. Competent jurisdiction clause 137
9.6.10. Resolution of conflicts 137

10. ANNEX I - ACRONYMS 138

1. Introduction

1.1. Presentation

This document declares the Certification Practice of the digital signature of Validated ID, S.L., on the following "VALIDATED ID".

Los certificados que se emiten son los siguientes:

- **Natural Person**
  - Qualified certificate for Natural Person on software
  - Qualified certificate for Natural Person on HSM centralized
  - Qualified certificate for Natural Person on QSCD centralized
  - Qualified certificate for Natural Person belonging in Software
  - Qualified certificate for Natural Person belonging in HSM centralized
  - Qualified certificate for Natural Person belonging in QSCD centralized
  - Qualified certificate for Natural Person member in Software
  - Qualified certificate for Natural Person member in HSM centralized
  - Qualified certificate for Natural Person member en QSCD centralized

- **Entity Representative**
  - Qualified certificate for Natural Person Representative on software
  - Qualified certificate for Natural Person Representative signature on HSM centralized
  - Qualified certificate for Natural Person Representative signature on QSCD centralized

- **Representative of Legal Person with the Public Administrations**
  - Qualified certificate for natural person Representative of Legal Person with the administrations on software
  - Qualified certificate for natural person Representative of Legal Person with the administrations on HSM centralized
  - Qualified certificate for natural person Representative of Legal Person with the administrations on QSCD centralized

- **Representative of Entity without Legal Personality with the Public Administrations**
    - Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on software
    - Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on HSM centralized
    - Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on QSCD centralized

- **Company Seal**
    - Qualified certificate for Electronic Seal on software
    - Qualified certificate for Electronic Seal on HSM centralized
    - Qualified certificate for Electronic Seal on QSCD centralized

- **Timestamping**
    - Qualified certificate for electronic timestamping

1.2. Document name and identification

This document establishes the Declaration of Certification Practices dedicated to the issuance of electronic certificates of VALIDATED ID.

1.2.1. Certificates´ identifiers

VALIDATED ID has assigned an object identifier (OID) to each certificate policy, for their identification by requests.

Number OID	Type of certificates
	Natural Person
1.3.6.1.4.1.54932.2.1.1	*Qualified Certificate for Natural Person on software*
1.3.6.1.4.1.54932.2.1.2	*Qualified certificate for Natural Person on HSM centralized*
1.3.6.1.4.1.54932.2.1.3	*Qualified certificate for Natural Person on QSCD centralized*
1.3.6.1.4.1.54932.2.2.1	Qualified certificate for Natural Person belonging in Software
1.3.6.1.4.1.54932.2.2.2	Qualified certificate for Natural Person belonging in HSM centralized
1.3.6.1.4.1.54932.2.2.3	Qualified certificate for Natural Person belonging in QSCD centralized
1.3.6.1.4.1.54932.2.3.1	Qualified certificate for Natural Person member on software
1.3.6.1.4.1.54932.2.3.2	Qualified certificate for Natural Person member on HSM centralized
1.3.6.1.4.1.54932.2.3.3	Qualified certificate for Natural Person member on QSCD centralized
	Entity Representative
1.3.6.1.4.1.54932.2.4.1	Qualified certificate for Natural Person Representative on software
1.3.6.1.4.1.54932.2.4.2	Qualified certificate for Natural Person Representative signature on HSM centralized
1.3.6.1.4.1.54932.2.4.3	Qualified certificate for Natural Person Representative signature on QSCD centralized
	Representative of Legal Person with Public Admin.
1.3.6.1.4.1.54932.2.5.1	Qualified certificate for natural person Representative of Entity with the administrations on software

1.3.6.1.4.1.54932.2.5.2	Qualified certificate for natural person Representative of Entity with the administrations on HSM centralized
1.3.6.1.4.1.54932.2.5.3	Qualified certificate for natural person Representative of Entity with the administrations on QSCD centralized
1.3.6.1.4.1.54932.2.6.1	Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on software
1.3.6.1.4.1.54932.2.6.2	Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on HSM centralized
1.3.6.1.4.1.54932.2.6.3	Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on QSCD centralized
	Electronic Seal
1.3.6.1.4.1.54932.2.8.1	Qualified certificate for Electronic Seal on software
1.3.6.1.4.1.54932.2.8.2	Qualified certificate for Electronic Seal on HSM centralized
1.3.6.1.4.1.54932.2.8.3	Qualified certificate for Electronic Seal on QSCD centralized
	Time Stamp Certificate
1.3.6.1.4.1.54932.3.10	Qualified certificate for electronic timestamping

In case of contradiction between this Certification Practice Statement and other documents of practices and procedures, the established in this Practice Statement shall prevail.

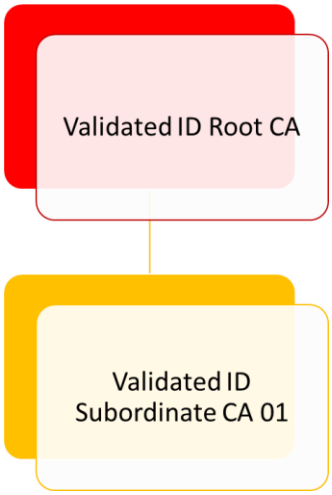
1.3. Participants in the certification services

1.3.1. Trust service Provider

The electronic certification service provider is the natural or legal person that issues and manages certificates of end entities, using a Certification authority, or provides other services relate to the electronic signature.

VALIDATED ID is a trust service provider, acting in accordance with Regulation (EU) 910/2014 OF THE EUROPEAN PARLAMENT AND BOARD of 23rd July of 2014 related to the electronic identification and to the relying services for electronic transactions within the domestic market and repealing Directive 1999/93/CE, as well as the technical rules of the ETSI applicable to the issuance and management of qualified certificates, mainly the 319 411-1 and EN 319 411-2, in order to facilitate the legal requirements and international recognition of his services.

To provide certification services, VALIDATED ID has established a hierarchy of certification entities:



1.3.1.1. Validated ID Root CA

This is the Root Certification Authority of the hierarchy that issues certificates to other certification authorities, and whose public key certificate has been self-signed.

Identification data:

CN:	Validated ID Root CA
Digital fingerprint:	16faee503d28fd8a508e84b6848cfbbeef4eeec2
Valid from:	Friday 21 October 2021
Valid until:	Sunday, 21 de October 2046
RSA key length:	4.096 bits

1.3.1.2. Validated ID Subordinate CA 01

This is a Certification Authority of the hierarchy that issues certificates to other end entities of certification and whose public key certificate has been self-signed by VALIDATED ID ROOT.

Identification data:

CN:	Validated ID Subordinate CA 01
Digital fingerprint:	0ade43e51b41f739848fe23c07fc384c1fc0d1ff
Valid from:	jueves, 21 de octubre de 2021
Valid until:	sábado, 21 de octubre de 2034
RSA key length:	4.096 bits

1.3.2. Registration Authority

A Registration Authority by VALIDATED ID is the entity in charge of:

- Processing the certificate applications.
- Identify the applicant and verify that complies with the requirements needed for the certificate applications.
- Validating the personal conditions of the signatory of the certificate.
- Managing the key generation and the issuing of the certificate.
- Delivering the certificate to the subscriber or to the means for its generation.
- Custody of the documentation related to the identification and registry of the signers and /or subscribers and management of the life cycle of the certificates.

They will be able to act as RA of VALIDATED ID:

- Any entity authorized by VALIDATED ID.
- VALIDATED ID directly.

VALIDATED ID contractually will formalize the relations between itself and each of the entities that act as Registration Authority of VALIDATED ID.

The entity acting as a Registration Authority by VALIDATED ID will be able to authorize to one or more persons as Trader of the RA to operate with the emission certificates system of VALIDATED ID on behalf of the Registration Authority.

The Registration Authority will be able to delegate the identification functions of the subscribers and /or signers, prior agreement for the delegation of these functions. VALIDATED ID will need to expressly authorize the collaboration agreement.

In addition, the appointed units for this function will be able to be Registry Authorities according to the Practice Declaration Certification, by the certificate subscribers, such as a personal department, as they provide authentic records with regard to the relationship between the signers and the subscriber.

1.3.3. End entities

The end entities are the persons and the organizations receiving the services of the issuance, management and use of digital certificates, for identification and electronic signature.

The end entities of VALIDATED ID of certification services will be the following:

1. Subscribers of the certification service
2. Signers
3. Relying parties

1.3.3.1. Subscribers of the certification services

The subscribers of the certification services are:

- Companies, entities, corporations and organizations that acquire them from VALIDATED ID (directly or through a third party) for its use in its business or organizational corporate level and which have been identified in the certificates.
- Natural persons that acquire the certificates for themselves and they have been identified in the certificates.

The subscriber of the certification service acquires a license to use the certificate, for his own use, or in order to facilitate the certification of the identity of a specific person duly authorized for various actions in the organizational scope of the subscriber. In the latter case, this person is identified on the certificate.

The subscriber of the relying electronic service, is therefore, the client of the certification services provider, according to the commercial legislation, and has the rights and obligations defined by the certification services provider, which are additional and do not prejudice the rights and obligations of the signers, as it is authorized and regulated in the European technical standards applicable to the issuance of qualified electronic certificates.

1.3.3.2. Signers

The signers are natural people, who possess exclusively the digital signature keys of their identification and/or advance electronic signature or qualified; being typically the employees, legal representatives or volunteers, as well as other persons linked to the subscribers; including Public Administrations employees, to the public employee certificates.

The signers are properly authorized by the subscriber and properly identified in the certificate through their name, last name and their VAT number valid in the jurisdiction, without being possible, in general, the use of pseudonyms.

The private key of a signer cannot be recovered or deducted by the relying electronic services provider, so the natural persons identified in the relevant certificates are the sole responsible for their protection and should consider the implications of losing a private key.

Given the existence of certificates for different use of the electronic signature, such as authentication, the more generic term 'identified natural person in the certificate', is also used, with full respect to the compliance the electronic signature legislation in relation with the signer's rights and obligations.

1.3.3.3. Relying parties

The relying parties are the persons and organizations that receive digital signatures and digital certificates.

To trust certificates, the relying parties must verify them, as it is established in the certification practice statement and in the corresponding instructions available in the web page of the Certification Authority.

1.3.4. Public Key Infrastructure Provider

VALIDATED ID and Uanataca, S.A. (hereinafter UANATACA) have signed a contract for the provision of technology services in which UANATACA will provide the public key infrastructure (PKI) that support VALIDATED ID's trust services. Likewise, UANATACA provides VALIDATED ID with the technical staff necessary for the proper performance of the trustworthy functions of a Trust Service Provider.

That said, UANATACA is configured as the provider of infrastructure services for certification services, provides its technological services to VALIDATED ID so that it can carry out the services inherent to a Trusted Service Provider, ensuring at all times the continuity of services in the conditions and under the requirements of the regulations.

Also, it is informed that UANATACA is a relying electronic certification service provider, acting in accordance with Regulation (EU) 910/2014 OF THE EUROPEAN PARLAMENT AND BOARD of 23rd July of 2014 related to the electronic identification and to the relying services for electronic transactions within the domestic market and repealing Directive 1999/93/CE, as well as the technical rules of the ETSI applicable to the issuance and management of qualified certificates, mainly the 319 411-1 and EN 319 411-2, in order to facilitate the legal requirements and international recognition of his services.

UANATACA's PKI undergoes annual audits for conformity assessment of qualified trust service providers in accordance with the applicable regulations, under the standards:

a) ISO/IEC 17065:2012

b) ETSI EN 319 403

c) ETSI EN 319 421

d) ETSI EN 319 401

e) ETSI EN 319 411-2

f) ETSI EN 319 411-1

UANATACA's PKI also undergoes annual audits under security standards:

a) ISO 9001:2015

b) ISO/IEC 27001:2014

1.4. Use of certificates

This section lists the requests for which each type of certificate can be used, sets limitations to certain requests and prohibits certain requests of certificates.

1.4.1. Uses permitted for certificates

The permitted used specified in the various fields of the certificate profiles should be taken into consideration, available on the webpage https://www.validatedid.com/

1.4.1.1. Qualified Certificate for Natural Person issued on software

This certificate has the OID 1.3.6.1.4.1.54932.2.1.1. It is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 eIDAS, which is issued for the electronic signature and authentication, in accordance to the certification statement QCP-n with OID 0.4.0.194112.1.0.

Natural person certificates, issued on software do not guarantee their correct functionality as intended with the qualified signature creation devices, as referred to Articles 29 and 51 of the Regulation (EU) 910/2014.

These certificates guarantee the identity of the subscriber and the person named on the certificate, and they allow the generation of the 'advance electronic signature based on a qualified electronic certificate'.

The certificates can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure e-mail
c) Other digital signature requests, in accordance with the agreements between the interested parties or with legal rules applicable in each individual case.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.2. Qualified Certificate for Natural Person on HSM centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.1.2. It is a qualified certificate that it is issued for the advance electronic signature and authentication, according to QCP-n with the OID 0.4.0.194112.1.0. The natural person certificates on HSM centralized are qualified certificates in accordance with Articles 24 and 28 Of the Regulation (EU) 910/2014.

It guarantees the identity of the subscriber and the indicated person on the certificate, and allows the generation of the 'advance electronic signature based on the qualified electronic certificate'.

The certificates can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure e-mail
c) Other digital signature requests, in accordance with the agreements between the interested parties or with legal rules applicable in each individual case.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature

c. Key Encipherment

1.4.1.3. Qualified Certificate for Natural Person issued on QSCD centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.1.3. It is a qualified certificate that is issued for the qualified electronic signature and authentication, in accordance with the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2. This certificate issued on centralized QSCD, is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 eIDAS.

It works with the qualified signature creation devices, in accordance with Articles 29 and 51 of the Regulation (EU) 910/2014, and which comply with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

It guarantees the identity of the signer and his entail with the subscriber of the relying electronic service and allow the generation of the 'qualified electronic signature'; that is, the advance electronic signature that is based on a qualified certificate and it has been generated using a qualified device, therefore it is compared to the handwritten signature by legal effect, without having to meet any additional requirement.
They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email.
b) Other digital signature requests.

The information of uses in the certificate's profile indicates the following:
The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.4. Qualified certificate for Natural Person belonging in Software

The certificate has the OID 1.3.6.1.4.1.54932.2.2.1. It is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 eIDAS, which is issued for the electronic signature and authentication, in accordance to the certification statement QCP-n with OID 0.4.0.194112.1.0.

Natural person certificates, issued on software do not guarantee their correct functionality as intended with the qualified signature creation devices, as referred to Articles 29 and 51 of the Regulation (EU) 910/2014.

These certificates guarantee the identity of the subscriber and the signer, as well as a relationship between the signer and an entity, company or organisation described in the "O" (organisation) field, allowing the generation of the "qualified electronic certificate-based advanced electronic signature".

The certificates can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure e-mail
c) Other digital signature requests, in accordance with the agreements between the interested parties or with legal rules applicable in each individual case.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.5. Qualified certificate for Natural Person belonging in HSM centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.2.2. It is a qualified certificate that it is issued for the advance electronic signature and authentication, according to QCP-n with the OID 0.4.0.194112.1.0. The natural person certificates on HSM centralized are qualified certificates in accordance with Articles 24 and 28 Of the Regulation (EU) 910/2014.

These certificates guarantee the identity of the subscriber and the signer, as well as a relationship between the signer and an entity, company or organisation described in the "O" (organisation) field, allowing the generation of the "qualified electronic certificate-based advanced electronic signature".

The certificates can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure e-mail
c) Other digital signature requests, in accordance with the agreements between the interested parties or with legal rules applicable in each individual case.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.6. Qualified certificate for Natural Person belonging in QSCD centralized

The certificate has the OID 1.3.6.1.4.1.54932.2.2.3. It is a qualified certificate issued for the qualified electronic signature, in accordance with the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2, as stated in the certificate. This certificate is issued on centralized QSCD, and it is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 eIDAS.

Natural person qualified certificates, issued on QSCD, work with the signature creation device in accordance with Articles 29 and 51 of the Regulation (EU) 910/2014, and which comply with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

It guarantees the identity of the signer and his entail with the subscriber of the relying electronic service, and allows the generation of the 'qualified electronic signature', that is, the advance electronic signature that is based on a qualified certificate, and it has been

generated using a qualified device, therefore it is compared to the handwritten signature by legal effect, without having to meet any additional requirement.

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email.
b) Other digital signature requests.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.7. Qualified certificate for Natural Person member on software

This certificate has the OID 1.3.6.1.4.1.54932.2.3.1. It is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 eIDAS, which is issued for the electronic signature and authentication, in accordance to the certification statement QCP-n with OID 0.4.0.194112.1.0.

Natural person certificates, issued on software do not guarantee their correct functionality as intended with the qualified signature creation devices, as referred to Articles 29 and 51 of the Regulation (EU) 910/2014.

These certificates guarantee the identity of the subscriber and the signer, as well as a relationship between the signer and a professional body or association described in the "O" (organisation) field, allowing the generation of the "advanced electronic signature based on a qualified electronic certificate".

The certificates can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure e-mail

c) Other digital signature requests, in accordance with the agreements between the interested parties or with legal rules applicable in each individual case.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.8. Qualified certificate for Natural Person member on HSM centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.3.2. It is a qualified certificate that it is issued for the advance electronic signature and authentication, according to QCP-n with the OID 0.4.0.194112.1.0. The natural person certificates on HSM centralized are qualified certificates in accordance with Articles 24 and 28 Of the Regulation (EU) 910/2014.

These certificates guarantee the identity of the subscriber and the signer, as well as a relationship between the signer and a professional body or association described in the "O" (organisation) field, allowing the generation of the "advanced electronic signature based on a qualified electronic certificate".

The certificates can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure e-mail
c) Other digital signature requests, in accordance with the agreements between the interested parties or with legal rules applicable in each individual case.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.9. Qualified certificate for Natural Person member on QSCD centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.3.3 It is a qualified certificate that is issued for the qualified electronic signature and authentication, in accordance with the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2. This certificate issued on centralized QSCD, is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 eIDAS.

It works with the qualified signature creation devices, in accordance with Articles 29 and 51 of the Regulation (EU) 910/2014, and which comply with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

These certificates guarantee the identity of the subscriber and the signer, as well as a relationship between the signer and a professional body or association described in the "O" (organisation) field, allowing the generation of the "qualified electronic signature", i.e. the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, thus equating it to a written signature for legal effect, without the need to fulfil any additional requirements.

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email.
b) Other digital signature requests.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.10. Qualified Certificate of signature for Natural Person Representative on software

This certificate has the OID 1.3.6.1.4.1.54932.2.4.1 It is a qualified certificate, and it is issued for the advance electronic signature and authentication, in accordance to the

certification statement QCP-n with the OID 0.4.0.194112.1.0., of natural person representative of the entity issued on software in accordance to Article 28 of the Regulation (EU) 910/2014 eIDAS, and which comply with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

They guarantee the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organisation described in the "O" (Organisation) field, and allow the generation of the "qualified electronic certificate-based advanced electronic signature".
The representative certificates issued on software can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure e-mail

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Content commitment, to perform the e-signature function

1.4.1.11. Qualified certificate of signature for Natural Person Representative on HSM centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.4.2. It is a qualified certificate that it is issued for the qualified electronic signature, in accordance to the certification statement QCP-n con el OID 0.4.0.194112.1.0. This certificate of representative issued on Centralized HSM, it is a qualified certificate in accordance to Article 28 of the Regulation (EU) 910/2014 eIDAS.

They guarantee the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organisation described in the "O" (Organisation) field, and allow the generation of the "qualified electronic certificate-based advanced electronic signature".

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email.

b) Other digital signature requests.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Content commitment, to perform the e-signature function

1.4.1.12. Qualified certificate of signature for Natural Person Representative on QSCD centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.4.3. It is a qualified certificate that it is issued for the qualified electronic signature, in accordance to the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2. This certificate of representative issued on centralized QSCD, it is a qualified certificate in accordance to Article 28 of the Regulation (EU) 910/2014 eIDAS.

It works with the qualified signature creation devices, in accordance with Articles 29 and 51 of the Regulation (EU) 910/2014, and which comply with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signer, and a legal representation or a general empowerment between the signer and the entity company or organization described in the field 'O' (Organization), and allows the generation of an 'advance electronic signature' that is the advance electronic signature is based on a qualified electronic certificate and it has been generated using a qualified device, therefore it is compared to the handwritten signature by legal effect, without having to meet any additional requirement.

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email.
b) Other digital signature requests.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions activated and therefore allows us to perform the following functions:

a. Content commitment (to perform the electronic signature function).

1.4.1.13. Qualified certificate for natural person Representative of Entity with the administrations on software

This certificate has the OID 1.3.6.1.4.1.54932.2.5.1. It is a qualified certificate issued for the advanced electronic signature and authentication, in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0.

This certificate issued on software, is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 elDAS, and which complies with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signer, and a legal representation or a general empowerment between the signer and the entity company or organization described in the field 'O' (Organization) and allows the generation of an 'advance electronic signature based on a qualified electronic'.

On the other hand, the representative certificates issued on software can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other electronic signature requests

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment

1.4.1.14. Qualified certificate for natural person Representative of Entity with the administrations on HSM centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.5.2. It is a qualified certificate issued for the advance electronic signature and authentication, in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0, which it is stated in the certificate.

It is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 eIDAS and which complies with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signer, and a legal representation or a general empowerment between the signer and the entity company or organization described in the field 'O' (Organization), and allows the generation of the 'advance electronic signature based on a qualified electronic certificate'.

On the other hand, the certificates can be used in other requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other electronic signature requests

The information of uses in the certificate's profile indicates the following:
The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment

1.4.1.15. Qualified certificate for natural person Representative of Entity with the administrations on centralized QSCD

This certificate has the OID 1.3.6.1.4.1.54932.2.5.2.7.6. It is a qualified certificate issued for the qualified electronic signature and authentication, in accordance with the

certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2, which it is stated in the certificate.

This certificate issued on centralized QSCD, is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 eIDAS. It works with qualified signature creation device, in accordance with Articles 29 and 51 of the Regulation (EU) 910/2014, and which complies with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signer, and a legal representation or a general empowerment between the signer and the entity company or organization described in the field 'O' (Organization), and allows the generation of the 'qualified electronic signature', that is the advance electronic signature is based on a qualified certificate and it has been generated using a qualified device, therefore it is compared to the handwritten signature by legal effect, without having to meet any additional requirement.

It can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, such as the applications listed below:

a) Signature of secure email
b) Other electronic signature request

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment

1.4.1.16. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on software

This certificate has the OID 1.3.6.1.4.1.54932.2.6.1. It is a qualified certificate issued for the advance electronic signature and authentication, in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0, which it is stated in the certificate.

It is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 elDAS and which complies with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signer, and a legal representation or a general empowerment between the signer and the entity Company or organization described in the field 'O' (Organization), and allows the generation of the 'advance electronic signature based on a qualified electronic certificate'.

On the other hand, this certificate can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other electronic signature requests

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment

1.4.1.17. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on HSM centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.6.2. It is a qualified certificate issued for the advance qualified electronic signature and authentication, in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0.

It is a qualified certificate in accordance with Article 28 of the Regulation (EU) 910/2014 elDAS and which complies with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signer, and a legal representation or a general empowerment between the signer and the entity Company or organization

described in the field 'O' (Organization), and allows the generation of the 'advance electronic signature based on a qualified electronic certificate'.

On the other hand, this certificate can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other electronic signature requests

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment

1.4.1.18. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on QSCD centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.6.3. It is a qualified certificate issued for the qualified electronic signature and authentication, in accordance with the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2, which it is stated in the certificate. This certificate is issued on QSCD, it is a qualified certificate as stated in Article 28 of the Regulation (UE) 910/2014 eIDAS.

This certificate issued on centralized QSCD works with a qualified signature creation device, in accordance with Articles 29 and 51 of the Regulation (EU) 910/2014, and which complies with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2.
It guarantees the identity of the subscriber and the signer, and a legal representation or a general empowerment between the signer and the entity company or organization described in the field 'O' (Organization), and allows the generation of the 'qualified electronic signature', that is, the advance electronic signature is based on a qualified certificate and it has been generated using a qualified device, therefore it is compared to the handwritten signature by legal effect, without having to meet any additional requirement.

It can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, such as the applications listed below:

a) Signature of secure email
b) Other electronic signature request

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment

1.4.1.19. Qualified certificate for Electronic Seal on software

The certificated has the OID 1.3.6.1.4.1.54932.2.8.1. This qualified certificate is issued in accordance with the certification statement QCP-l with the OID 0.4.0.194112.1.1. The certificates of electronic seal are qualified certificates issued as stated in Article 38 of the Regulation (EU) 910/2014 eIDAS.

These certificates guarantee the identity of the subscribing entity, and where relevant, the responsible person who manage the seal. The information of uses in the certificate's profile indicates the following:

The "key usage" field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.20. Qualified certificate for Electronic Seal on HSM centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.8.2,.It is a certificate issued in according with the certification statement QCP-l with the OID 0.4.0.194112.1.1. The electronic seal certificates are qualified certificates issued as stated in Article 38 of the Regulation (EU) 910/2014 eIDAS.

These certificates guarantee the identity of the subscribing entity, and where relevant, the responsible person who manage the seal. The information of uses in the certificate's profile indicates the following:

The "key usage" field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.21. Qualified certificate for Electronic Seal on QSCD centralized

This certificate has the OID 1.3.6.1.4.1.54932.2.8.3. It is a qualified certificate, which it is issued in accordance with the certification statement QCP-l-qscd with the OID 0.4.0.194112.1.3. The electronic seal certificates are qualified and issued as stated in Article 38 of the Regulation (EU) 910/2014 eIDAS.

The electronic seal certificates on centralized QSCD guarantee the identity of the organization included in the certificate.

These certificates guarantee the identity of the subscribing entity, and where relevant, the responsible person who manage the seal. The information of uses in the certificate's profile indicates the following:

The "key usage" field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4.1.22. Qualified certificate for electronic timestamping

This certificate has the OID 1.3.6.1.4.1.54932.3.10, and it is issued in accordance with the certification statement QCP-l-qscd with the OID 0.4.0.194112.1.3.

The qualified electronic timestamping certificates are certificates issued for the timestamping authorities for signing the timestamps that they produce.

These certificates allow signing the timestamps issued, from the moment they have got a valid timestamping certificate, while it is in force.

The synchronization of the times in VALIDATED ID is done with a timeserver NTP stratum 1.

This server, a Meinberg Lantime M300/GPS, with TCXO high stability, GPS receiver, is comprised of an internal GPS card to synchronize simultaneously with the satellites having visibility at all times (between 3 to 8), and anti-Ray protection.

1.4.2. Limits and forbidden uses of certificates

Certificates are used for their own function and the established purpose, not being able to be used for other functions or other purposes.

Likewise, certificates must be used only in accordance with the applicable law, especially taking into consideration the import and export restrictions prevailing at any given time.

Certificates cannot be used to sign public key certificates of any type, nor Certificate Revocation List (CRL).

The certificates have not been designed, cannot be assigned and its use or resale as control equipment for dangerous situations is not authorized nor for uses that require fail-safe actions, as the operation of nuclear installation, navigation systems or air communications, or weapons control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

There must be taken into account the limits indicated in the various fields of the certificates profiles, visible in the web of Validated ID.

The use of the digital certificates in operations that violate this Certification Practice Statement, the binding legal documents with each certificate, or the contracts with the Registration Authorities or their signers/subscribers, is considered to misuse the legal purposes, exempting therefore to VALIDATED ID, according to the current legislation, of any liability for this misuse of the certificates made by the signer or any third party.

Validated ID does not have any access to the data on which the use of the certificate can be applied. Therefore, as a result of this technical impossibility to access to the content of the message, VALIDATED ID can't issue any evaluation about the mentioned content, the subscriber, the signer or the person responsible of the custody, is the one who will assume any responsibility arising from the content rigged to the use of a certificate.

Likewise, any responsibility that could result from the use of the custody out of the limits and conditions of use included in this Certification Practice Statement, the binding legal documents with each certificate, or the contracts or agreements with the registration authorities or with their subscribers, and any other misuse thereof derived from this section or may be interpreted as such according to the law, will be attributable to the subscriber, signer or the responsible of it.

1.5. Policy management

1.5.1. Organization that administers the document

VALIDATED ID S.L.

Carrer de Sepúlveda 143 P.4

08011 Barcelona

1.5.2. Contact information of the organization

VALIDATED ID S.L.

Carrer de Sepúlveda 143 P.4

08011 Barcelona

tsp@validateid.com

1.5.3. Document management procedures

The documental and organization system of VALIDATED ID guarantees, according to the existence and request of the corresponding procedures, the correct maintenance of this document and the specification of the service related to itself.

2. Publication of information and deposito of certificates

2.1. Deposit(s) of certificates

Validated ID has a Deposit of certificates, in which the information related to the certification services is published.

That service is available 24 hours, 7 days per week and, in case of the system failure was under Validated ID's control, it will make its best efforts to ensure that the service is back available within the prescribed time in the section 5.7.4 of this Certification Practice Statement.

2.2. Publication of information of the certification services provider

Validated ID publishes the following information, in its Deposit:

- Revoked certificates list and other information about the status if the certificates revocation.
- Applicable certificate policies.
- Certification Practice Statement.
- Policy Disclosure Statements - PDS, at least in Spanish and English.

2.3. Frequency of publication

The information of the certification services provides, including the policies and the Certification Practice Statement, is published when available.

Changes to the Statement of Certification Practices are governed by section 1.5 of this document.

Certificate revocation status information is published in accordance with this Statement of Certification Practices.

2.4. Access control

Validated ID does not limit the read access to the information established in the section 2.2, but establishes controls to prevent non-authorized people to add, modify or delete registrations of the Deposit, to protect the integrity and authenticity of the information, especially information about the revocation status.

Validated ID uses reliable systems for the Deposit, in such a way that:

- Only authorized persons could do annotations and modifications.
- The authenticity of the information could be verified.
- Any technical change affecting the security requirements could be detected.

3. Identification and authentication

3.1. Initial registration

3.1.1. Type of names

All certificates contain a distinguished name (DN or distinguished name) according to the X.509 standard in the Subject field, including a Common Name (CN =) component, related to the identity of the subscriber and the natural person identified in the certificate, as well as various additional identity information in the SubjectAlternativeName field.

3.1.1.1. Qualified Certificate for Natural Person on software

Campo	Descripción	Obligación
Country (C)	State[1]	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	Name and surname of the signer	Sí

3.1.1.2. Qualified Certificate for Natural Person on HSM centralized

Campo	Descripción	Obligación
Country (C)	State[2]	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí

[1] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

[2] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	Name and surname of the signer	Sí

3.1.1.3. Qualified Certificate for Natural Person issued on QSCD centralized

Campo	Descripción	Obligación
Country (C)	State[3]	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	Name and surname of the signer	Sí

3.1.1.4. Qualified certificate for Natural Person belonging in Software

Campo	Descripción	Obligación
Country (C)	State[4]	Sí
Organization (O)	Organization to which the signer is bound	Sí
Organization Unit (OU)	Organization Unit to which the signer is bound	No
Organization Identifier	Taxpayer Identification Number of the Organization to which the signer is bound	Sí
Title	Title or specialty of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí

[3] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

[4] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	Name and surname of the signer	Sí

3.1.1.5. Qualified certificate for Natural Person belonging in HSM centralized

Campo	Descripción	Obligación
Country (C)	State[5]	Sí
Organization (O)	Organization to which the signer is bound	Sí
Organization Unit (OU)	Organization Unit to which the signer is bound	No
Organization Identifier	Taxpayer Identification Number of the Organization to which the signer is bound	Sí
Title	Title or specialty of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	Name and surname of the signer	Sí

[5] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

3.1.1.6. Qualified certificate for Natural Person belonging in QSCD centralized

Campo	Descripción	Obligación
Country (C)	State[6]	Sí
Organization (O)	Organization to which the signer is bound	Sí
Organization Unit (OU)	Organization Unit to which the signer is bound	No
Organization Identifier	Taxpayer Identification Number of the Organization to which the signer is bound	Sí
Title	Title or specialty of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	Name and surname of the signer	Sí

[6] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

3.1.1.7. Qualified certificate for Natural Person member on software

Campo	Descripción	Obligación
Country (C)	State [7]	Sí
Organization (O)	Organization to which the signer is bound	Sí
Organization Unit (OU)	Specify in general "Member" or "Profession" + "Member number".	Sí
Organization Identifier	Tax Identification Number of the Organization to which the signer is bound	Sí
Title	Title or specialty of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / Tax Identification Number / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	First Name and Surname of the signer, followed by their member number	Sí

3.1.1.8. Qualified certificate for Natural Person member on HSM centralized

Campo	Descripción	Obligación
Country (C)	State [8]	Sí
Organization (O)	Organization to which the signer is bound	Sí
Organization Unit (OU)	Specify in general "Member" or "Profession" + "Member number".	Sí
Organization Identifier	Tax Identification Number of the Organization to which the signer is bound	Sí
Title	Title or specialty of the signer	Sí

[7] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

[8] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / Tax Identification Number / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	First Name and Surname of the signer, followed by their member number	Sí

3.1.1.9. Qualified certificate for Natural Person member on QSCD centralized

Campo	Descripción	Obligación
Country (C)	State [9]	Sí
Organization (O)	Organization to which the signer is bound	Sí
Organization Unit (OU)	Specify in general "Member" or "Profession" + "Member number".	Sí
Organization Identifier	Tax Identification Number of the Organization to which the signer is bound	Sí
Title	Title or specialty of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / Tax Identification Number / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	First Name and Surname of the signer, followed by their member number	Sí

[9] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

3.1.1.10. Qualified Certificate of signature for Natural Person Representative on software

Campo	Descripción	Obligación
Country (C)	State [10]	Sí
Organization (O)	Organization to which represents the signer	Sí
Organization Unit (OU)	Organization to which the signer is bound	No
Organization Identifier	Tax Identification Number of the Organization to which the signer is bound	Sí
Title	Type of representation	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	Name and surname of the signer	Sí

3.1.1.11. Qualified certificate of signature for Natural Person Representative on HSM centralized

Campo	Descripción	Obligación
Country (C)	State [11]	Sí
Organization (O)	Organization to which represents the signer	Sí
Organization Unit (OU)	Organization to which the signer is bound	No
Organization Identifier	Tax Identification Number of the Organization to which the signer is bound	Sí
Title	Type of representation	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí

[10] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link), regardless the nationality of the employee.

[11] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link), regardless the nationality of the employee.

Common Name (CN)	Nombre y apellidos del firmante	Sí

3.1.1.12. Qualified certificate of signature for Natural Person Representative on centralized QSCD

Campo	Descripción	Obligación
Country (C)	State [12]	Sí
Organization (O)	Organization to which represents the signer	Sí
Organization Unit (OU)	Organization to which the signer is bound	No
Organization Identifier	Tax Identification Number of the Organization to which the signer is bound	Sí
Title	Type of representation	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognized by law	Sí
Common Name (CN)	Name and surname of the signer	Sí

3.1.1.13. Qualified certificate for natural person Representative of Entity with the administrations on software

Campo	Descripción	Obligación
Country (C)	State	Sí
Organization (O)	Organization represented by the signer	Sí
Organization Unit (OU)	Organization unit to which the signer belongs	No
Organization Identifier	Tax Identification Number of the Organization which represents the signer	Sí
Title	Name of the representation of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	National Identity Card/NIE of the signer	Sí

[12] The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link), regardless the nationality of the employee.

Common Name (CN)	National Identity Card/NIE, first name and surname of the signer and Tax Identification Number of the organization	Sí
Description	Information about the representation concession of the registration	Sí

3.1.1.14. Qualified certificate for natural person Representative of Entity with the administrations on HSM centralized

Campo	Descripción	Obligación
Country (C)	State	Sí
Organization (O)	Organization represented by the signer	Sí
Organization Unit (OU)	Organization unit to which the signer belongs	No
Organization Identifier	Tax Identification Number of the Organization which represents the signer	Sí
Title	Name of the representation of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	National Identity Card/NIE of the signer	Sí
Common Name (CN)	National Identity Card/NIE, first name and surname of the signer and Tax Identification Number of the organization	Sí
Description	Information about the representation concession of the registration	Sí

3.1.1.15. Qualified certificate for natural person Representative of Entity with the administrations on centralized QSCD

Campo	Descripción	Obligación
Country (C)	State	Sí
Organization (O)	Organization represented by the signer	Sí
Organization Unit (OU)	Organization unit to which the signer belongs	No
Organization Identifier	Tax Identification Number of the Organization which represents the signer	Sí
Title	Name of the representation of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	National Identity Card/NIE of the signer	Sí
Common Name (CN)	National Identity Card/NIE, first name and surname of the signer and Tax Identification Number of the organization	Sí
Description	Information about the representation concession of the registration	Sí

3.1.1.16. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on software

Campo	Descripción	Obligación
Country (C)	State	Sí
Organization (O)	Organization represented by the signer	Sí
Organization Unit (OU)	Organization unit to which the signer belongs	No
Organization Identifier	Tax Identification Number of the Organization which represents the signer	Sí
Title	Name of the representation of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	National Identity Card/NIE of the signer	Sí

Common Name (CN)	National Identity Card/NIE, first name and surname of the signer and Tax Identification Number of the organization	Sí
Description	Information about the representation concession of the registration	Sí

3.1.1.17. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on HSM centralized

Campo	Descripción	Obligación
Country (C)	State	Sí
Organization (O)	Organization represented by the signer	Sí
Organization Unit (OU)	Organization unit to which the signer belongs	No
Organization Identifier	Tax Identification Number of the Organization which represents the signer	Sí
Title	Name of the representation of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	National Identity Card/NIE of the signer	Sí
Common Name (CN)	National Identity Card/NIE, first name and surname of the signer and Tax Identification Number of the organization	Sí
Description	Information about the representation concession of the registration	Sí

3.1.1.18. Qualified certificate for natural person Representative of Entity without Legal Personality with the administrations on QSCD centralized

Campo	Descripción	Obligación
Country (C)	State	Sí
Organization (O)	Organization represented by the signer	Sí
Organization Unit (OU)	Organization unit to which the signer belongs	No

Organization Identifier	Tax Identification Number of the Organization which represents the signer	Sí
Title	Name of the representation of the signer	Sí
Surname	Signer's Surname	Sí
Given Name	Signer's First Name	Sí
Serial Number	National Identity Card/NIE of the signer	Sí
Common Name (CN)	National Identity Card/NIE, first name and surname of the signer and Tax Identification Number of the organization	Sí
Description	Information about the representation concession of the registration	Sí

3.1.1.19. Qualified certificate for Electronic Seal on software

Campo	Descripción	Obligación
Country (C)	State where the entity has registered the Organization	Sí
Organization (O)	Name of the Organization	Sí
Organization Unit (OU)	Shows the nature of the certificate	No
Organization Identifier	Tax Identification Number of the Organization under to which the electronic seal is bound	Sí
Serial Number	Surname of the responsible person of the certificate	Sí
Common Name (CN)	First Name of the responsible person of the certificate	Sí

3.1.1.20. Qualified certificate for Electronic Seal on HSM centralized

Campo	Descripción	Obligación
Country (C)	State where the entity has registered the Organization	Sí
Organization (O)	Name of the Organization	Sí
Organization Unit (OU)	Shows the nature of the certificate	No

Organization Identifier	Tax Identification Number of the Organization under to which the electronic seal is bound	Sí
Serial Number	Surname of the responsible person of the certificate	Sí
Common Name (CN)	First Name of the responsible person of the certificate	Sí

3.1.1.21. Qualified certificate for Electronic Seal on QSCD centralized

Campo	Descripción	Obligación
Country (C)	State where the entity has registered the Organization	Sí
Organization (O)	Name of the Organization	Sí
Organization Unit (OU)	Shows the nature of the certificate	No
Organization Identifier	Tax Identification Number of the Organization under to which the electronic seal is bound	Sí
Serial Number	Surname of the responsible person of the certificate	Sí
Common Name (CN)	First Name of the responsible person of the certificate	Sí

3.1.1.22. Qualified certificate for electronic timestamping

Campo	Descripción	Obligación
Country (C)	State from where the service is provided	Sí
Locality (L)	Name of the Organization	Sí
Organization (O)	Locality of the Organization	Sí
Organization Unit (OU)	Tax Identification Number of the Organization	Sí
Organization Identifier	Name of the Service	Sí
Common Name (CN)	Unit providing the service	Sí

3.1.2. Meaning of the names

The names in the fields of the certificates *SubjectName* and *SubjectAlternativeName* are understandable in natural language, in accordance with the provisions of the previous section.

3.1.2.1. Issuance of certificates of the set of tests and certificates of tests in general

In case the provided data in the DN or Subject were fictitious (e.g. 'Test Organization', 'Test First Name', Surname1') or expressly stated words indicating its invalidity (e.g. 'TEST' 'EVIDENCE' OR 'INVALID'), the certificate will be considered as legally invalid and therefore with no responsibility for VALIDATED ID. Theses certificates are issued to take interoperability tests and allow the regulatory body its assessment.

3.1.3. Use of anonymous and pseudonymous

Under no circumstances can the pseudonymous be used for identifying an entity, company, organization or signer. Likewise, under no circumstances can anonymous certificates be issued.

3.1.4. Interpretation of name formats

Name formats will be interpreted in accordance with the law of the country in which the subscriber is established, on its own terms.

The field 'country' or 'state' will be the subscriber's.

The certificates show the relation between a natural person and the legal person, entity or organization to which is bound, regardless the nationality of the natural person.

The "serial number" field must include the signer's Identity Card Number, NIE, Passport or any other identification number recognized by law.

Without prejudice to the foregoing, any type of qualified electronic certificate, when issued for the identification of the interested parties before the Public Administrations,

must contain as attributes their name and surname and their National Identity Document number, Foreigner's Identification Number or Tax Identification Number in an unequivocal manner, as appropriate.

3.1.5. Uniqueness of names

The names of the subscribers of certificates will be unique, for each certification policy of VALIDATED ID.

It won't be possible to assign a subscriber's name that already has been used, to a different subscriber, situation that, in theory, at first shouldn't happen, thanks to the tax identification number, or equivalent, in the names' scheme.

A subscriber can request more than one certificate whenever the combination of the following existing values in the request was different from a valid certificate:

- Tax Identification Number or other valid legal identifier of the natural person.
- Tax Identification Number or other valid legal identifier of the subscriber.
- Type of Certificate (Description of the certificate field).
- Support of the certificate (QSCD, software, HSM centralized, QSCD centralized)

As an exception, this CPS allows to issue a certificate when there is an overlap with the Tax Identification Number of the subscriber or the signer, Type of certificate, Support of the certificate, with an active certificate, as long as there is a differentiating element between them, in the title and/or Organizational Unit fields.

3.1.6. Resolution of name conflicts

Certificate applicants won't include names in requests that may involve infringement, by the future subscriber, of third party rights.

VALIDATED ID won't be required to first determine that an applicant of certificates has industrial property rights on the name of a certificate request, but at first will proceed to certify it.

Furthermore, it won't act as arbitrator or mediator, or in any other way to resolve any dispute concerning the property of names of persons or organizations, web domains, brands or commercial names.

However, in case of receiving a notification concerning a name conflict, according to the legislation of the subscriber's country, it may take appropriate actions to block or withdraw the certificate issued.

In any case, the certification services provider reserves the right to reject the certification request due to names conflict.

Any controversy or dispute arising out of this document will be solved definitively, by the arbitration law of an arbitrator within the framework of the Spanish Court of Arbitration, in accordance with its Regulation and Statute, to which the administration of the arbitration and the designation of the arbitrator or the arbitral court is entrusted.
The parties state their commitment to comply with the award rendered in the contractual document that formalizes the service.

3.2. Initial identity validation

The identity of the certificate subscribers is established at the time of signing the contract between VALIDATED ID and the subscriber, at which time the existence of the subscriber is verified by means of their official identity document or the corresponding deeds, as well as the powers of attorney. performance of the person presenting as representative, if applicable. For this verification, public or notarial documentation may be used, or direct consultation with the corresponding public records.

The identity of the natural persons identified in the certificates is validated through the corporative records of the entity, Company or organization of public or private law, subscribers to the certificates. The subscriber will produce a certification of the necessary data, and will send it to VALIDATED ID, through these methods it will enable, for registering the identity of the signers.

3.2.1. Proof of possession of private key

The possession of the private key is demonstrated under the reliable process of delivery and acceptance of the certificate by the subscriber, for seal certificates, and by the signer, for signature certificates.

3.2.2. Identity Validation

For the request of certificates, the VALIDATED ID Registration Authority Operators will verify the identity of the signatory to whom the certificate is issued (see the natural person or authorized representative of the legal person), as well as any specific attribute of the natural or legal person with whom it has a relationship or link.

Verification shall be done directly or through a third party in accordance with national law, in accordance with the following methods:

A) In the presence of the natural person or an authorized representative of the legal person. Personation may be dispensed with when the application for the issue of a qualified certificate has been legitimized in the presence of a notary, or

B) At a distance, using means and electronic identification, for which the presence of the natural person of an authorized representative of the legal person has been

guaranteed prior to the issuance of the qualified certificate and which meet the requirements set out in Article 8 of the eIDAS Regulation with regard to "substantial" or "high" security levels, or

C) By means of a certificate of a qualified electronic signature or a qualified electronic seal issued in accordance with point (a) or (b), or

D) Through the electronic identification procedure through the VALIDATED ID remote identification video identification system, in accordance with the identification methods recognized at national level by Order ETD/465/2021, of May 6, which regulates the methods of remote identification by video for the issuance of qualified electronic certificates.

Notwithstanding the foregoing, the validation of the identity will not be required when the identity or other permanent circumstances of the signatories to whom the certificates are issued, are already recorded in VALIDATED ID by virtue of a pre-existing relationship, as long as a method of face-to-face identification has been used to identify the signatory and no more than 5 years have passed.

3.2.3. Authenticate the identity of an organization, company, or entity by proxy

Natural persons with the capacity to act on behalf of legal persons or entities without legal personality, public or private, that are subscribers of certificates, may act as representatives of the same, if there is a prior situation of legal or voluntary representation between the natural person and the organization in question, that requires its recognition by VALIDATED ID, which will be carried out through the following procedure:

1. The subscriber's representative must prove his identity by one of the identification methods specified in section 3.2.2., in such a way that:
    - (i) If you identify in person before an operator or authorized person of a VALIDATED ID Registration Authority:
        - Showing your Identity Document, passport or other suitable means recognized in law for the identification of the representative.
        - Accrediting the character and faculties that it claims to possess.

- (ii) If you are identified electronically through VALIDATED ID's remote video identification system:
  - Showing your Identity Document, passport or other suitable means recognized in law for the identification of the representative.
  - Providing proof of life through the use of technical means of capturing images and video using facial biometric cryptography algorithms and artificial intelligence for the unequivocal comparison of the identity of the applicant and the verification of the proof of life of the latter, as well as the authenticity of the identity document exhibited.
  - Accrediting the character and faculties that it claims to possess.

2. The representative shall provide the following information and its corresponding supporting supports:

- Your identification data, as a representative:
  - Name and surname
  - Place and date of birth
  - Document: Identity document, passport or other suitable means recognized in law for the identification of the representative

- The identification data of the subscriber it represents:
  - Name or company name.
  - All existing registration information, including data related to the constitution and legal personality and the extension and validity of the applicant's powers of representation.
  - Document: NIF or document proving the entity's tax identification.
  - Document: Public documents that serve to prove the aforementioned points in a reliable manner and their registration in the corresponding public registry if required. The aforementioned verification may also be carried out by consultation in the public registry in which the documents of constitution and power of attorney are registered, being able to use the telematic means provided by the aforementioned public registries.

- The data relative to the representation or the capacity for action that holds:
  - The validity of the representation or the ability to act (the start and end date) if applicable.

- The field and the limits, in its case, of the representation or the capacity of action:
  - TOTAL. Representation or total capacity. This checking will be able to be made through a tele-consultation to the public registry stating the inscribed representation.
  - PARTIAL. Representation or partial capacity. This checking will be able to be made through an authentic electronic copy of the notarial empowerment deed, under the terms of the notarial law.

3. The operator or authorized personnel of the VALIDATED ID Registration Authority will verify the identity of the representative acting as follows:

- When the identification has been carried out in person, through the review of:
  - Identity document provided.
  - Documentation proving your representation.

- When the identification has been made through the method of electronic identification through video identification of VALIDATED ID by:
  - Review of the videos and images captured from the identification document provided and the applicant himself.
  - Review of the applicant's proof of life, through the results provided by the remote video identification system.
  - Review of the comparison produced by the remote video identification system of the photograph of the identity document with the images and video obtained during the registration of the applicant.
  - Review produced by the remote video identification system, through artificial intelligence for the detection of false identity documents.
  - Documentation proving your representation.

4. The operator or authorized personnel of the VALIDATED ID Registration Authority will verify the information provided for authentication and will return the original documentation provided when appropriate.

5. Alternatively, it will be possible to legitimize by legal process the signature in the form, and be delivered to VALIDATED ID by certified post, in which case steps 3 and 4 above won't be necessary.

The digital certification service provision is formalized through the appropriate contract between VALIDATED ID and the subscriber, duly represented.

3.2.4. Authentication of natural person identity

This section describes the testing methods of the identity of a natural person identify in the certificate.

3.2.4.1. In the certificates

The identity of the signatory natural persons identified in the certificates is validated through the identification methods specified in section 3.2.2., In such a way that:

- (i) If you identify yourself in person before an operator or authorized person of a VALIDATED ID Registration Authority:
  - Showing your Identity Document, passport or other suitable means recognized in law.

- (ii) If you identify yourself electronically through VALIDATED ID's remote video identification system:
  - Showing your Identity Document, passport or other suitable means recognized in law.
  - Providing proof of life through the use of technical means of capturing images and video using facial biometric cryptography algorithms and artificial intelligence for the unequivocal comparison of the applicant's identity and the verification of the applicant's proof of life, as well as the authenticity of the identity document displayed.

The information of the identification of the natural persons identified in the certificates when the subscriber is an entity with or without legal personality, the information will be validated comparing the information of the request with the registrations of the entity,

company or organization of public or private law to which is bound, ensuring the correctness of the information to be certified.

The identification information of the natural person identified in the certificates whose subscriber is an entity with or without legal personality may be validated by comparing the information in the application with the records of the entity, company or organization under public or private law to which it is linked, or with the documentation that it has provided on the natural person it identifies as the signer, ensuring the correctness of the information to be certified.

3.2.4.2. Identity validation

To request certificates, the operator or authorized personnel of the VALIDATED ID Registration Authority will verify the identity of the natural person identified in the certificate request, acting as follows:

- When the identification has been carried out in person, through the review of:
  - Identity document provided.
- When the identification has been made through the electronic identification method through video identification of VALIDATED ID through:
  - Review of the videos and images captured from the identification document provided and the applicant himself.
  - Review of the applicant's proof of life, through the results provided by the remote video identification system.
  - Review of the comparison produced by the remote identification video system of the photograph of the identity document with the images and video obtained during the registration of the applicant.
  - Review produced by the remote video identification system, through artificial intelligence for the detection of false identity documents.

For the application of certificates whose subscriber is a legal person, direct physical presence is not required, due to the relationship already accredited between the natural person and entity, company or organization of public or private law to which it is linked, provided that no more than five (5) years have elapsed since the identification. However, before the delivery of a certificate, the underwriting entity, company or organization under public or private law, through its certification officer, if it has one, or another

designated member, must verify the identity of the natural person identified in the certificate through one of the procedures described in the previous paragraph.

During this proceeding the identity of the natural person identified in the certificate is appropriately confirmed. Therefore, in all cases in which a certificate is issued the identity of the signer is verified in person.

The Registration Authority will verify through the production of documents or through its own sources of information, the remaining data and features that need to be included in the certificate, keeping the supporting information that proves the validity of them.

3.2.4.3. Entail of the natural person

Documentary evidence of the entail of a natural person identified in a certificate with an entity, Company or organization of public or private law will be proven by the persistence in the internal records (employee contract, commercial contract or records where his position is indicated, or the request as a member of the organization) of each public or private persons to which is bound.

3.2.5. Subscriber´s not verified information

VALIDATED ID doesn´t include any unverified subscriber information in the certificates except for the email of the subscriber or signer.

3.2.6. Autentication of te identity of a RA and its operators

For the construction of a new Registration Authority, VALIDATED ID performs the necessary checks in order to confirm the existence of the identity or organization involved. For that purpose, VALIDATED ID will be able to use the production of documents or use its own information sources.

Likewise, VALIDATED ID, directly or through its Registration Authority, verifies and validates the operator's identity of the Registration Authorities, and they send VALIDATED ID the relevant identification documentation of the new operator, together with its authorization to act in such capacity.

VALIDATED ID is assured that the operators of the Registration Authority receive the proper training for the performance of their duties, which is verified with a relevant assessment. The Registration Authority previously approved by VALIDATED ID can execute such training and assessment.

For the delivery of services, VALIDATED ID ensures that the operators of the Registration Authority have access to the system via strong authentication with digital certificate.

3.3. Identification and authentication of renewal requests

3.3.1. Validation for certificates routine renewal

Before renewing a certificate, the operator or the authorized personnel of VALIDATED ID's Registration Authority verifies that the information used to verify the identity and the remaining subscriber data and the natural person identified in the certificate remain valid.

The acceptable methods for such verifications are:

- The use of the code 'CRE' or 'ERC' related to the previous certificate, or other methods of personal authentication, that consist in information that only the natural person identified in the certificate knows, and allows in an automatic way the renewal of the certificate, as long as the deadline legally established hasn't exceed.
- The use of the current certificate for its renewal as long as it has not exceeded the deadline legally established for this possibility.

If any information of the subscriber or natural person identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section 3.2.

3.3.2. Identification and authentication of revocation request

Before generating a certificate to a subscriber whose certificate was renewed, the operator or the authorized personnel of VALIDATED ID's Registration Authority will verify that the information used that day to verify the identity and the rest of the data of the subscriber and the natural person identified in the certificate are still valid, in which case previous section shall apply.

The renewal of the certificates after their revocation will not be possible in the following cases:

- The certificate was revoked by erroneous issuance to a person different than the one identified in the certificate.
- The certificate was revoked by a non-authorized issuance by the natural person identified in the certificate.
- The certificate revoked may contain misleading or fake information.

If any information of the subscriber or natural person identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section **¡Error! No se encuentra el origen de la referencia.**.

3.4. Identification and authentication of revocation, suspension or reactivation request

VALIDATED ID or operator or authorized personnel of the Registration Authority authenticate the requests and reports relative to revocation, suspension or reactivation of a certificate verifying that they come from an authorized person.

The identification of the subscribers and/or signers during the process of revocation suspension or reactivation of the certificates can be performed by:

- The subscriber and/or signer:
    - Identifying and authenticating through the Revocation Code (ERC o ERC) via VALIDATED ID's web page in 24x7 schedule.
    - Other media, as telephone, e-mail, etc. when there is reasonable assurance of the identity of the applicant for suspension or revocation in the judgement of VALIDATED ID and/or Registration Authorities.

- VALIDATED ID's registration authorities: they must identify the signer upon a revocation, suspension or reactivation request using the methods they consider appropriate.

When the subscriber would want to initiate a revocation request, and there were doubts for its identification, during office hours, his certificate would go onto suspension status.

4. Certificate life-cycle operational requirements

4.1. Certificate issuance request

4.1.1. Legitimation to apply for the issuance

The requester of the certificate, a natural or legal person, must sign a certification services provision contract with VALIDATED ID.

Likewise, before the issuance and delivery of a certificate, there must exist a request of a certificate either in the same contract, in a specific certificate request form or in the face of the Registration Authority.

When the applicant is a different person than the subscriber, there must be an authorization from the subscriber to allow the applicant to proceed with the request, which is legally implemented by a certificate request form subscribed by that applicant on behalf of the entity, Company or organization of public or private law.

4.1.2. Registration procedure and responsibilities

VALIDATED ID receives certificates' request, made by persons, entities, Companies or organizations of public or private law.

The requests are implemented by a document in paper or electronic format, individually or in batches, through external databases or interface of *Web Services* whose addressee is VALIDATED ID. When the subscriber of the certificates is filled by an entity, Company or organization of public or private law that acts as a Registration Authority of VALIDATED ID, the request will be carried out accessing directly to VALIDATED ID's information systems and produce the relevant certificates for the entity, Company or organization itself or for its members.

The request will go together with the supporting documentation of the identity and other circumstances of the natural person identified in the certificate, in accordance with the established in the section **¡Error! No se encuentra el origen de la referencia.**4. Also, an

address or other data that will allow contacting the natural person identified in the certificate.

4.2. Processing the certification request

4.2.1. Implementation of identification and authentication fuctions

Once the certificate applicant has been received, VALIDATED ID ensures that the certificates' requests will be completed, precise and duly authorized, before processing them.

If so, VALIDATED ID verifies the information provided, verifying the aspects described in section **¡Error! No se encuentra el origen de la referencia.**

In case of a qualified certificate, the supporting documentation of the approval of the request must be preserved and properly registered with guarantees of security and integrity during 15 years from the expiration of the certificate, even in case of early loss effective for renovation.

4.2.2. Approval or rejection of request

In case the data is correctly verified, VALIDATED ID should approve the request of the certificate and proceed with its issuance and delivery.

If the verification indicates that the information is not correct, or if it is suspected that it is not correct or it may affect the reputation of the Certification Authority, the Registration Authority or the subscribers, VALIDATED ID will deny the request, or will stop its approval up to having made the additional checks that it considers appropriate.

VALIDATED ID will definitely deny the request in case the additional checks won't help to correct the information to verify.

VALIDATED ID notifies the approval or denial of the request to the applicant.

4.2.3. Time to process certificate requests

VALIDATED ID attends to the certificates' requests in order of arrival, in a reasonable time, being possible to specify a guarantee can specify a maximum guarantee in the contract certificate issuance.

Requests remain active until its approval or rejection.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

After approving the certification request, the CA proceeds to issue the certificate in a safe way and make it available to the signer for its acceptance.

The established procedures in this section are applicable in case of certification renewal, taking into consideration that the same involves the issuance of a new certificate.

During the process, VALIDATED ID:

- Protects the confidentiality and integrity of the registration data that owns.
- Uses reliable systems and products that are protected against every disturbance and guarantee the technical security and, in its case, cryptographic security of the processes of certification to which they support.
- Generates a pair of keys, through a procedure of generation of certificates bound in a safe way with the procedure of generation of keys.
- Uses a procedure of generation of certificates that links in a safe way the certificate with the registration information, including the certified public key.
- It ensures that the certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the mentioned keys.
- Indicates the date and hour in which a certificate was issued.
- It ensures the exclusive control of the keys by the user, and VALIDATED ID or its Registration Authorities cannot deduce or use them in any way.

4.3.2. Notification to the certificate issuance applicant

VALIDATED ID notifies the issuance of the certificate to the subscriber and/or the natural person identified in the certificate and method for production/download.

4.4. Certificate delivery and acceptance

4.4.1. CA Responsabilities

During this process, the operator or authorized personnel of the VALIDATED ID'S Registration Authority must perform the following actions:

- Definitely confirm the identity of the natural person identified in the certificate, in accordance with the established in the sections 3.2.4 and **¡Error! No se encuentra el origen de la referencia.**.
- To have the Trust Services Provision Contract duly signed by the Subscriber.
- Deliver to the natural person identified in the certificate the sheet delivery and acceptance of the certificate with the following minimum contents:
    - Basic information about the use of the certificate, especially including information about the certification services provider and the applicable Certification Practice Statement, as his obligations, faculties and responsibilities.
    - Information about the certificate.
    - Recognition, from the signer, of receiving the certificate and/or the procedures for its creation/download and the acceptance of the mentioned elements.
    - Signer liability regime.
    - Responsibility of the signer.
    - Imputation method exclusive to the signer, of its private key and its certificate activation data, in accordance with the established in the sections 6.2 and 6.4.
    - The date of the act of delivery and acceptance.

  All this information may be included in the Trust Services Provision Contract. In this sense, the delivery and acceptance of the certificate will take place the Subscriber signs the Trust Services Provision Contract.
- To obtain the signature of the person identified in the certificate.

The Registration Authority collaborates in these processes, having to register the previous acts, and preserves the mentioned original ones (delivery and acceptance sheets), referring to VALIDATED ID the electronic copy as well as the original when VALIDATED ID required access to them.

4.4.2. Way in which the certificate is accepted

When the acceptance sheet is delivered, the acceptance of the certificate by the natural person identified in the certificate occurs when signing the delivery and acceptance sheet.

When the generation and delivery of the certificate is carried out through the automated procedure defined by VALIDATED ID, the acceptance of the certificate by the natural person identified in it, it is produced by signing the Trust Services Provision Contract using the certificate itself.

4.4.3. Publication of the certificate

VALIDATED ID publishes the certificate in the Deposit referred in section 2.1, with the proper safety controls and whenever VALIDATED ID had the authorization of the natural person identified in the certificate.

4.4.4. Notification of the certificate issuance to third parties

VALIDATED ID does not notify any issuance to third parties.

4.5. Key pair and certificate usage

4.5.1. Use by the signer

VALIDATED ID forces him to:

- Provide to VALIDATED ID complete and proper information, in accordance with the requirements of this Certification Practice Statement, especially on the registering procedure.
- Express his consent prior the certificate issuance and delivery.

- Use the certificate in accordance with the established in the section 4.5.2.
- When the certificate works together with a SSCD, recognize its capacity to produce qualified electronic signatures; that is, equivalent to handwritten signatures, as well as other types of electronic signatures and information encryption mechanisms.
- Be especially diligent in the custody his private key, in order to prevent unauthorized uses.
- Communicate to VALIDATED ID, Registration Authorities and anyone who believes may trust the certificate, without unjustifiable delays:
    - The loss, theft or potential compromise of his private key.
    - The loss of control over his private key, due to the compromise of the activation data (i.e. PIN) or any other reason.
    - The inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
- Stop using the private key once the period specified in the section 6.3.2 has elapsed.

VALIDATED ID forces the signer to take responsibility to ensure:

- All the information in the certificate provided by the signer is correct.
- The certificate is used exclusively for legal and authorized uses, in accordance with the Certification Practice Statement.
- No unauthorized person has ever had access to the private key of the certificate, and that he is the sole responsible for any damage caused by his infringement of protecting the private key.
- The signer is an end entity and not a certification services provider and will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification services provider title, nor any other case.

4.5.2. Use by the subscriber

4.5.2.1. Obligations of the certificate subscriber

VALIDATED ID contractually forces the subscriber to:

- Provide complete and appropriate information to the Certification Authority, in accordance with the requirements of this Certification Practice Statement, especially on the registering procedure.
- Express his consent prior to the certificate issuance and delivery.
- Use the certificate in accordance with the established in the section 4.5.2
- Communicate to VALIDATED ID, Registration Authorities and anyone who the subscriber believes may trust the certificate, without unjustifiable delays:
    - The loss, theft or potential compromise of his private key.
    - The loss of control over his private key, due to the compromise of the activation data (i.e. PIN) or any other reason.
    - The inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
    - When there is a loss, alteration, unauthorized use, theft or compromise of the card.
- Communicate to the natural persons identified in the certificate the compliance of the specific obligations of them, and establish mechanisms to guarantee the proper compliance of them.
- Not to monitor, manipulate or perform reverse engineer acts on the technical implantation of the certification services of VALIDATED ID, without previous written permission.
- Not to compromise the safety of the certification services of the certification services provider of VALIDATED ID.

4.5.2.2. Civil liability of the certificat´s subscriber

VALIDATED ID contractually forces the subscriber to take responsibility to ensure:

- All the statements in the request are correct.
- All the information provided by the subscriber that is in the certificate is correct.
- The certificate is exclusively used for legal and authorized uses, in accordance with the Certification Practice Statement.
- No unauthorized person has ever had access to the private key of the certificate, and that he is the sole responsible for any damage caused by his infringement of protecting the private key.

- The subscriber is an end entity and not a certification services provider, and will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification services provider title, nor any other case.

4.5.3. Use by the relying third party in certificates

4.5.3.1. Obligations of the relying third parties in certificates

VALIDATED ID informs the relying third party in certificate of the following obligations he must assume:

- Consulting if the certificate is appropriate for the intending use, in an independent way.
- Verify the validity, suspension or revocation of the issued certificates, for which certificates status information will be used.
- Verify all certificates of the certificates hierarchy, before trusting the digital signature or any of the certificates of the hierarchy.
- Recognize that the verified electronic signatures, produced on a qualified signature creation device (SSCD) have the legal consideration of qualified electronic signatures; that is, equivalent to handwritten signatures, as well as the certificate allows the creation of other types of electronic signatures and encryption mechanisms.
- Remember any limitation on the use of the certificate, regardless of whether in the own certificate or in the relying third party in certificates contract.
- Remember any caution established in a contract or other instrument, regardless of its legal nature.
- Not to monitor, manipulate or perform reverse engineer acts about the technical implementation of the certification services of VALIDATED ID, without previous written permission.
- Not compromise the safety of the certification services of VALIDATED ID.

4.5.3.2. Civil liability of the relying third parties in certificates

VALIDATED ID informs to the relying third party in certificates that he must assume the following responsibilities:

- He has enough information to make an informed decision in order to trust or not the certificate.
- He is the sole responsible for trusting or not the information of the certificate.
- He will be the sole responsible if he breaches his obligations as a third party that trust the certificate.

4.6. Certificate renewal

The certificates renewal requires the renewal of keys, so that must comply with the established in section 4.7

4.7. Key and certificate renewal

4.7.1. Circumstances for certificate and key renewal

The existing certificates can be renewed through a specific and simplified procedure of request, in order to keep the continuity of the certification service.

There are at least two ways for certificate renewal:

a) Face to face renewal process – it will be carried out the same way as a new certificate issuance.

b) Online renewal process (via internet) – as detail below.

4.7.2. Online renewal process

4.7.2.1. Circumstances for online renewal

The online renewal of the certificate will take place only if the following conditions are executed:

- The Registration Authority and/or VALIDATED ID have access to the online renewal service.
- The certificate that is used for the renewal is valid, in other words, it is not expired, revoked or suspended.

- No more than 5 years have passed since the last accreditation of identity with an identification operator when obtaining a certificate.

4.7.2.2. Who can request an online renewal certificate

Any signer will be able to request an online renewal certificate if all the circumstances described in the previous point are fulfilled.

The signer will be able to formalize his request by accessing the online renewal service certificate in VALIDATED ID's website.

4.7.2.3. Approval or rejection of the request

In case the data is correctly verified, VALIDATED ID should approve the request of the certificate and proceed with its issuance and delivery.

VALIDATED ID notifies the approval or denial of the request to the applicant.

VALIDATED ID will be able to automate the verification procedures of the information correction that will be in the certificates, and the approval of the requests.

4.7.2.4. Procedure for online renewal request

The renewal request of a certificate will be carried performed according to the following:

- When the digital certificate of the user is about to expire, VALIDATED ID will be able to send one or more notifications over time, requesting the renewal to the user.
- The signer will connect to the renewal service in VALIDATED ID's webpage and he will proceed with the renewal request.
- The signer will sign his valid certificate renewal.
- Creation of a new pair of keys and generation and import of the certificate taking into account the following constrains:
    - Protects the confidentiality and integrity of the registration data that owns.

- Uses reliable systems and products that are protected against every disturbance and guarantee the technical security and, in its case, cryptographic security of the processes of certification to which they support.
- Generates a pair of keys, through a procedure of generation of certificates bound in a safe way with the procedure of generation of keys.
- Uses a procedure of generation of certificates that links in a safe way the certificate with the registration information, including the certified public key.
- It ensures that the certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the mentioned keys.
- Indicates the date and hour in which a certificate was issued.
- It ensures the exclusive control of the keys by the user, and VALIDATED ID or its Registration Authorities cannot deduce or use them in any way.

4.7.2.5. Notification of the renewed certificate issuance

VALIDATED ID notifies the certificate issuance to the subscriber and the natural person identified in the certificate.

4.7.2.6. Way in which the certificate is accepted

The acceptance of the certificate occurs when signing the renewal electronically.

4.7.2.7. Publication of the certificate

VALIDATED ID publishes the renewed certificate in the Deposit to which refers in the section 2.1, with the proper safety controls.

4.7.2.8. Notification of the certificate issuance to third parties

VALIDATED ID does not make any notification of the issuance to third entities.

4.8. Certificate modification

The modification of certificates, except the modification of the certified public key, which is considered renewal, will be treated as a new issue of certificate applied as described in sections **¡Error! No se encuentra el origen de la referencia.**, 4.2, 4.3 and 4.4.

4.9. Revocation, suspension or reactivation of certificates

The revocation of a certificate means the definitive withdrawal of the certificate and it is irrevocable.

The suspension (or temporal revocation) of a certificate means the temporal withdrawal of it and it is reversible. Only end entity certificates will be able to be stopped.

The reactivation of a certificate is the transition from a hold status to an active state.

4.9.1. Causes os certificate revocation

VALIDATED ID revokes a certificate when any of the following causes occur:

1) Circumstances affecting the information contained in the certificate:
   a) Modification of any of the data contained in the certificate, after the corresponding issue of the certificate including amendments.
   b) Discovery that any of the data contained in the certificate application is incorrect.
   c) Discovery that any of the data contained in the certificate is incorrect.

2) Circumstances affecting the security of the key or certificate:
   a) Compromise of the private key, infrastructure or systems certification service provider that issued the certificate, provided that it affects the reliability of the certificates issued from that incident.
   b) Infringement, by VALIDATED ID, of the requirements of the certificate management procedures established in this Certification Practice Statement.
   c) Commitment or suspected compromise of the security key or certificate issued.
   d) Unauthorized access or use, by a third party private key corresponding to the public key contained in the certificate.

e) Irregular use of the certificate by the natural person identified in the certificate or lack of diligence in the custody of the private key.

3) Circumstances affecting the subscriber or the natural person identified in the certificate:
   a) Completion of the legal relationship between VALIDATED ID provision of services and the subscriber.
   b) Modification or termination of the underlying legal relationship or what caused the issuance of the certificate to the natural person identified in the certificate.
   c) Infringement by the certificate applicant of the present requirements for the application thereof.
   d) Violation by the subscriber or by the person identified in the certificate, of their obligations, responsibility and guarantees established in the relevant legal document.
   e) Incapacity or death of key owner.
   f) The termination of the legal certificate underwriter _ and authorization to the holder by the subscriber key or termination of the relationship between subscriber and identified in the certificate.
   g) Request by the subscriber for certificate revocation in accordance with the provisions of section **¡Error! No se encuentra el origen de la referencia.**.

4) Other circumstances:
   a) Termination of Certification Service Certification Entity VALIDATED ID.
   b) The use of the certificate that is harmful and continued to VALIDATED ID. In this case, it is considered that a use is harmful in terms of the following criteria:
      - The nature and number of complaints received.
      - The identity of the entities filing complaints.
      - The relevant legislation in force at all times.
      - The response of the subscriber or of the person identified in the certificate to complaints received.

4.9.2. Reasons for suspension of certificates

VALIDATED ID certificates may be suspended from the following causes:

- When so requested by the subscriber or the person identified in the certificate.
- When the documentation required in the request for revocation is sufficient but cannot reasonably identify the subscriber or the person identified in the certificate.
- The lack of use of the certificate for an extended period of time, previously known.
- If the key is suspected to have been compromised until it is confirmed. In this case, VALIDATED ID will have to make sure that the certificate is not suspended for longer than necessary to confirm their commitment.

4.9.3. Reason for reactivation of certificates

VALIDATED ID certificates may be reactivated from the following causes:

- When the certificate is in suspended status.
- When so requested by the subscriber or the natural person identified in the certificate.

4.9.4. Who can request the revocation, suspension or reaction of a certificate

The certificate may be requested to be revoked, suspended or reactivated by:

- The person identified in the certificate.
- The subscriber of the certificate through a responsible certification service.
- Administrative or legal Authority using a binding resolution.

4.9.5. Procedures for revocation, suspension or reactivation request

The entity required to revoke, suspend or reactivate a certificate must apply to VALIDATED ID or the Registration Authority of the subscriber or doing it himself via the online service available in the VALIDATED ID's website. The revocation, suspension or reactivation request shall include the following information:

- Date of application for the revocation, suspension or reactivation.
- Identity of the Subscriber.

- Name and title of the person requesting the revocation, suspension or reactivation.
- Contact information for the person requesting the revocation, suspension or reactivation.
- Detailed reason for the revocation.

The application must be authenticated by VALIDATED ID, in accordance with the requirements of section **¡Error! No se encuentra el origen de la referencia.** of this policy, prior to the revocation, suspension or reactivation.

The revocation, suspension or reactivation service can be found in the VALIDATED ID website at: https://www.validatedid.com/

If the recipient of a request for revocation, suspension or reactivation by a natural person identified in the certificate is outside the subscribing entity, once authenticated the application must submit a request to that effect to VALIDATED ID.

The revocation, suspension or reactivation request will be processed upon receipt, and inform the subscriber and, where appropriate, physical person identified in the certificate about the change of status of the certificate.

Both, the revocation, suspension or reactivation management service as consultation service are considered critical services and thus contained in the Plan contingency and business continuity planning of VALIDATED ID.

4.9.6. Temporary revocation, suspension or reactivation application

Revocation, suspension or reactivation requests shall be sent immediately when knowledge of the cause of revocation is known.

4.9.7. Temporary period of revocation, suspension or reactiviation application processing

The revocation, suspension or reactivation will occur immediately when received. If it takes place with an operator, it will be executed within the regular hours of operation

VALIDATED ID or the Registration Authority. If it is carried out via the online service, it will happen immediately.
In any case, the requests will be managed in a time period no longer than 24 hours from the reception of the request.

4.9.8. Obligation to consult certificate revocation or suspension information

Third parties must check the status of those certificates they want to trust.

A method by which you can check the certificate status is by consulting the latest Certificate Revocation List issued by the VALIDATED ID Certification Authority.

The Certificate Revocation Lists are published in the Deposit of the Certification Authority, as well as the following web addresses indicated in certificates:

- Validated ID Subordinate CA 01
  http://crl1.validatedid.com/tsp/crl/validatedid.crl
  http://crl2.validatedid.com/tsp/crl/validatedid.crl

The status of the certificate validity can also be checked by the OCSP protocol.

- http://ocsp1.validatedid.com/tsp/ocsp/
- http://ocsp2.validatedid.com/tsp/ocsp/

4.9.9. Frequency of issuance of certificate revocation lists (CRLs)

VALIDATED ID issues an LRC at least every 24 hours.

The LRC indicates the scheduled time of issuance of a new LRC, although it may issue an LRC before the deadline stated in the previous LRC, to reflect revocations.

The LRC is obliged to maintain the revoked or suspended certificate until it expires.

4.9.10. Maximum period of publication of CRLs

CRLs are published in the Repository within a reasonable period immediately after their generation, which in no case exceeds a few minutes.

4.9.11. Availability of the service checking in line with the state of the certificates

Alternatively, third parties who rely on certificates may consult VALIDATED ID deposit certificates, which is available 24 hours 7 days a week on VALIDATED ID website.

- To check the latest CRL issued in each CA, the following may be downloaded:

- *Certification Authority (CA) ROOT - Validated ID Root CA:*
  - http://crl1.validatedid.com/tsp/crl/arl_validatedid.crl
  - http://crl2.validatedid.com/tsp/crl/arl_validatedid.crl

- *Subordinate Certification Authority - Validated ID Subordinate CA 01:*
  - http://crl1.validatedid.com/tsp/crl/validatedid.crl
  - http://crl2.validatedid.com/tsp/crl/validatedid.crl

In case of failure of systems checking certificate status for reasons beyond the control of VALIDATED ID, it must make its best efforts to ensure that this service remains inactive for the minimum possible time, which may not exceed one day.

VALIDATED ID provides information to third parties who rely on certificates on the operation of the service certificate status information.

4.9.12. Obligation to check the consultation certificate status service

It is mandatory to check the status of certificates before relying on them.

4.9.13. Special requirements in case of compromise of the private key

The compromise of the private key VALIDATED ID is notified to all participants in certification services, as far as possible, by posting this in the website VALIDATED ID and, if deemed necessary, in other media, even on paper.

4.9.14. Maximum period os suspension of digital certificate

The maximum period of a digital certificate in suspended status shall be ninety (90) days from the time the SUBSCRIBER or SIGNER requests the suspension. Once the maximum period has elapsed without it being reactivated, Validated ID will proceed to directly revoke it.

If, during the suspension period, the digital certificate expires or its revocation is requested, its validity shall expire under the same conditions as a valid digital certificate.

Notwithstanding the above, the maximum period of ninety (90) days may be altered due to an investigation procedure by Validated ID or due to an ongoing judicial or administrative procedure. In such cases, the digital certificate shall be suspended for the required period of time, after which it shall be definitively revoked. Under no circumstances may the period of suspension of the digital certificate exceed the period of validity of the certificate.

4.10. Completion of the subscription

After the period of validity of the certificate, the service subscription ends.

As an exception, the subscriber can maintain the existing service, requesting certificate renewal, in time determined by this Certification Practice Statement.

VALIDATED ID can officially issue a new certificate, while subscribers maintain that state.

4.11. Deposit and recovery of keys

4.11.1. Policies and practices of deposit and key recovery

VALIDATED ID does not provide deposit services and key recovery.

4.11.2. Policy and practices of encapsulation and recovery of key session

No stipulation.

5. Physical security controls, management and operations

5.1. Physical security controls

Physical and environmental security controls have been implemented to protect the resources of the facilities where the systems, the systems themselves and the equipment used for operations of the provision of relying electronic services.

Specifically, the security policy applicable to the relying electronic services has established requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Protective measures against fires.
- Failure of the support systems (electronic energy, telecommunications, etc.)
- Collapse of the building.
- Flooding.
- Antitheft protection.
- Unauthorized removal of equipment, information, media and applications relating to components used for the services of the service provider certification.

These measures are applicable to installations where the certificates are produced, which lends from its both mainstream and, where appropriate, operating in contingency high security installations that are properly audited periodically.

Facilities include preventive and corrective maintenance systems with assistance 24/7 all year round with assistance in the following 24 hours notice.

5.1.1. Location and construction of facilities

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and strength of building materials facility ensures adequate levels of protection against intrusion by brute force and located in an area of low risk of disasters and allows quick access.

The room where the cryptographic operations are performed in the Data Processing Centre has redundancy in its infrastructure, as well as several alternative sources of power and cooling in an emergency.

It has facilities to physically protect the provision of services approval of applications for certificates and revocation management, compromise caused by unauthorized access to systems or data access and disclosure thereof.

5.1.2. Physical access

It has three levels of physical security (building entrance where the CPD is found, access to the room of the CPD and access to the rack) for service of protecting the certificate generation, and must be accessed from the lower to the upper levels.

Physical access to the premises where certification is processed, is limited and protected by a combination of physical and procedural measures are carried out as such:

- Limited to expressly authorized persons, with identification at the time of access and registration thereof, including filming by CCTV.
- Access to the rooms is done with ID card readers and managed by a computer system that keeps a log of inputs and outputs automatically.
- To access the rack where the cryptographic processes are located, prior authorization from administrators hosting service is necessary to have the key to open the cage.

5.1.3. Electrical power and air conditioning

The facilities have current-stabilising equipment and power system doubled with generator equipment.

The rooms housing IT equipment have temperature control systems with air conditioners.

5.1.4. Exposer to water

The facilities are in an area of low risk of flooding.

The rooms where computers are housed have a moisture detection system.

5.1.5. Fire prevention and protection

The facilities and assets have automatic detection and fire fighting systems.

5.1.6. Backup storage

Only authorized individuals have access to support storage.

The most highly classified information is stored in a safe offsite Data Processing Centre.

5.1.7. Waste management

The elimination of media, both paper and magnetic, is made by mechanisms that guarantee the impossibility of retrieving information.

In the case of magnetic media, it proceeds to formatting, permanent deletion, or physical destruction of the support. For paper documents, paper shredders or specially arranged bins for later destruction are used, under supervision.

5.1.8. Offsite backup

It is used a secure external storage for the safekeeping of documents, magnetic and electronic devices that are independent of the operations center.

5.2. Procedure controls

It is guaranteed that its systems are operated safely, for which it has establish and implemented procedures for the functions which affect the supply of its services.

The staff runs the administrative and management procedures according to the security policy procedures.

5.2.1. Reliable features

Roles have been identified, according with its security policy, the following reliable functions and roles

- **Internal Auditor**: Responsible for compliance with operating procedures. This is an external person to the Department of Information Systems. The tasks of Internal Auditor are incompatible in time with tasks and incompatible with Certification Systems. These functions will be subordinate to the head of operations, reporting both this technical direction.
- **System Administrator**: Responsible for the proper functioning of hardware and software support platform certification
- **Certification Authority Administrator**: Responsible for the actions to be executed with the cryptographic material, or performing any function involving the activation of private keys of certification authorities described in this document, or any of its elements.
- **Certification Authority Operator**: Necessary to be responsible, in conjunction with CA Manager, of the custody of material activation of cryptographic keys, and responsibility for backup operations and maintenance of AC.
- **Register Administrator**: Person responsible for approving the certification requests made by the subscriber and issuing digital certificates.
- **Revocation officer**: Person responsible for making the changes in the status of a certificate, mainly proceed with the suspension and revocation of the same.
- **Security Manager**: Responsible for coordinating, monitoring and enforcing security measures as defined by the security policies of VALIDATED ID. This individual should be responsible for aspects related to information security: logic, physics, networking, organization, etc.

Persons holding previous posts are subject to procedures of investigation and specific control. Additionally, it is applied policy criteria for the segregation of duties, as preventive measure to fraudulent activities.

5.2.2. Number of individuals per task

It is guaranteed at least two people to perform tasks related to the generation, recovery and back up of the private key of the Certification Authorities. Same criteria applies to the

implementation of issuance tasks and activation of the certificates and private keys of the Certification Authorities and in general in handling the device custody of the keys of the Authority root and intermediate certification.

5.2.3. Identification and authentication for each role

The individuals assigned for each role are identified by the internal auditor will ensure that each person performs the operations for which they are assigned.

Each person only controls the assets required for its role, ensuring that no person access unallocated resources.

Access to resources is performed depending on the asset through cryptographic cards and activation codes.

5.2.4. Roles requiring separation of tasks

The following tasks are performed by at least two people:

- The tasks of the Auditor role will be incompatible with the operation and management of systems, and in general, with those roles related to the direct provision of relying electronic services.
- Issuance and revocation of certificates will be incompatible tasks with the Management and systems operation.
- The management and systems operation and the Certification Authorities will be mutually incompatible.

5.2.5. PKI management system

The PKI system is composed of the following modules:

- Component/module for Subordinate Certificate Authority management.
- Component/module for Registration Authority management.
- Component/module for solicitation management
- Component/module for key management (HSM)
- Component/module for databases

- Component/module for CRL management.
- Component/module for OCSP service management.

5.3. Personnel controls

5.3.1. History, qualification, experience and authorisation requirements

All staff is qualified and has been properly instructed to perform operations that they have been assigned.

Staff in positions of trust has no personal interests that conflict with the development of the role that has been entrusted.

It is ensured that personnel record is reliable for registration tasks. The Registration Manager has completed a course of preparation for the tasks of validation requests.

In general, it is withdrawn an employee from their duties when knowledge of the existence of the commission of any criminal act that could affect the performance of its functions.

The person who is not suitable for the position is not assigned, especially for having been convicted of a crime or minor affecting their suitability for the position. For this reason, a previous investigation, **to the extent permitted by applicable law**, on the following is done:

- Studies, including alleged degree.
- Previous work up to five years, including professional references.
- Professional references.

In any case, the Registration Authorities will be able to establish checking procedures of different backgrounds, always preserving VALIDATED ID's policies, who remains responsible for the actions of the persons who authorize the operations.

5.3.2. Procedures of history investigation

Before hiring a person or before that person has access to the job, performs the following checks:

- References of the past years jobs
- Professional references
- Studies, including qualifications

Validated ID obtains the unequivocal consent of the affected to such previous research, and processes and protects all his personal data in accordance with the regulations in force regarding the protection of personal data, reflected in the General Data Protection Regulation (EU) 2016/679 and in general any applicable national regulations.

All checks are made up to be allowed by the applicable law. The reasons that may lead the candidate rejection of a job are the followings:

- Falsehoods on the job application, done by the candidate.
- Very negative professional references or not very reliable.

5.3.3. Training requirements

The personnel is trained in reliable and management jobs, until they reach the required qualification, keeping reports of the training.
Training programs are updated and improved periodically and they are updated and improved periodically.

Training includes, at least, the following contents:

- Principles and mechanisms of security of the certification hierarchy, and the user environment of the person to train.
- Tasks the person must do.
- Policies and security procedures. Use and operation of machinery and installed applications.
- Management and processing of incidents and security commitments.
- Procedures of business continuity and emergency.
- Process management and security regarding the processing of personal data.

5.3.4. Retraining frequency and requirements

The staff is updated on their training in accordance with the needs, and with enough frequency to comply their functions in a competent and satisfactory way, especially when doing the substantial modifications in the certification tasks.

5.3.5. Job rotations frequency and sequence

Not applicable.

5.3.6. Sections and unauthorized actions

It has a disciplinary system, to debug the responsibilities arising from unauthorized actions, appropriate to the applicable labor legislation.

Disciplinary actions include suspension and loss of employment of the person responsible for the harmful action, proportionate to the gravity of the unauthorized action.

5.3.7. Professionals contracting requirements

The staff hired to perform reliable tasks sign a previous confidentially agreement and the operational requirements. Any action that may compromise the security of the accepted processes could, once evaluated, lead to the termination of the employment contract.

In case all or part of the certification services were performed by a third party, the previsions and controls performed in this section, or other parts of the Certification Practice Statement, will be applied and complied by the third party who performs the operation functions of the certification services, notwithstanding, the certification authority will be responsible in any case for the effective implementation. These aspects are concretized in the legal instrument used to arrange the certification services provision by a third party.

5.3.8. Documentation supplied to personnel

The certification services provider will provide the documentation strictly needed by the staff at any moment, to perform their job in a competent and satisfactory form.

5.4. Security Audit procedures

5.4.1. Types of recorded events

It is produced and registered at least, of the following events related to the entity security:

- Booting and shutting down of systems.
- Attempts to create, delete, set passwords or change privileges.
- Attempts to login and logout.
- Unauthorized attempts to enter the CA network.
- Unauthorized attempts to access system files.
- Physical access to logs.
- System configuration maintenance and changes.
- Records of the CA applications.
- Booting and shutting down of CA application.
- Changes of the CA and/or keys details.
- Changes in certificate issuing policies.
- Generation of own keys.
- Creation and revocation of certificates.
- Records of destruction of materials containing key information or activation data.
- Events related to the certificate's lifecycle of the cryptographic module, as lobby, use and uninstalling of it.
- Generation keys ceremony and keys management databases.
- Physical access records.
- System configuration maintenance and changes.
- Staff changes.
- Commitments and disagreements reports.
- Records of destruction of materials containing key information, activation data or personal information of the subscriber, in case of individuals certificates, or the natural person identified in the certificate, in case of organization certificates.
- Possession of activation information for operations with the private key of the certification Authority.

- Complete reports of the physical intrusion attempts in the infrastructures that support the certificates issuance and management.

Log entries include the following elements:

- Login date and time.
- Serial number or entry sequence, in the automatic records.
- Identity of the entity entering in the register.
- Type of entrance.

5.4.2. Frecuency of processing audit logs

Logs are reviewed when a system alert motivated by the existence of any incident occurs.

Processing audit logs is a review of the records including the verification that confirm they have not been tampered, a brief inspection of all log entries and a deeper investigation of any alert or irregularities in the logs. The actions from the audit review are documented.

A system is kept that guarantees:

- Enough space for logs storage.
- Logs files are not rewritten.
- Information held includes, at least: type of event, date and time, user running the event and result of the operation.
- Logs files will be held in structured files susceptible to incorporate into a DB for further exploration.

5.4.3. Period of retention of audit logs

The logs information is held for a period of between 1 and 15 years, depending on the type of information recorded.
Audit registers related to the life cycle management of the digital certificates will be preserved for 15 years.

5.4.4. Audit logs protection

The systems logs:

- Are protected from manipulation by signing the files that contain them.
- Are stored in fireproof devices.
- Availability is protected through its storage in facilities out of the center where the CA is located.

Access to logs files is reserved only to authorized persons. Also, devices are handled at all times by authorized personnel.

There is an internal procedure where management processes devices containing the data of the audit logs are detailed.

5.4.5. Audit log backup procedures

A proper backup procedure is avaliable so that, in case of loss or destruction of relevant files, were available in a short period of time the corresponding logs backup.

It has been implemented a secure backup procedure of audit logs, making a copy of all logs weekly in an external source. Additionally, a copy is held in a custody external center.

5.4.6. Location of the audit logs storage system

The information of the audit events is collected internally and in an automated way by the operating system, network communications and software certificate management, in addition to the data generated manually, will be stored by the authorized personnel. All this composes the storage system of audit logs.

5.4.7. Notification of the audit event to the subect that caused the event

When the log audit accumulation system records an event, it is not necessary to send a notification to the individual, organization, device or application that caused the event.

5.4.8. Vulnerabily analysis

The audit processes of VALIDATED ID cover vulnerability analysis.

Vulnerability analysis must be run, reviewed and revised by an examination of these monitored events. This analysis must be run periodically in accordance with the internal procedure intended for this purpose.

Audit data systems are stored in order to be used in the investigation of any incident and to locate vulnerabilities.

5.5. Information files

It is guaranteed that all information relating to the certificates is held for an appropriate period of time as established in section **¡Error! No se encuentra el origen de la referencia.** of this policy.

5.5.1. Types of records archived

The following documents involved in the life cycle of the certificate are stored by VALIDATED ID (or registration authorities):

- All audit data system.
- All data relating to certificates, including contracts with the signers and the data relating to their certification and location.
- Requests of issuance and revocation of certificates.
- Type of document presented in the certificate request.
- Identity of the Registration Authority that accepts the certificate request.
- Unique identification number provided by the previous document.
- All certificates issued or published.
- CRLs issued or logs of the status of the generated certificates.
- The history of generated keys.
- Communications between the elements of the PKI.
- Policies and Practices Certification.
- All audit data identified in section **¡Error! No se encuentra el origen de la referencia.**.
- Information of requests certification.
- Documentation provided to justify the certification requests.
- Life cycle certificate information.

VALIDATED ID and/or the Registration Authorities accordingly are responsible for the correct file of all this material.

5.5.2. Retention period for the files

The logs are saved for at least 15 years, or the period defined in the current law.

In particular, the records of revoked certificates shall be accessible for free consultation for at least 15 years or the period established by the legislation in force since their change of status.

5.5.3. Protection of the file

The file is protected so only the duly authorized persons can access to it. The file is protected against visualization, modification erased or any other manipulation through its storage in a reliable system.

It is ensured the proper protection of the files by assigning qualified personnel for its treatment and its storage in secure fireproof boxes and external facilities.

5.5.4. File backup procedures

A external storage center is provided in order to ensure the availability of the file backups of electronic files. The physical documents are stored in safe places restricted to authorized personnel.

Incremental daily backups are performed of support of all its electronic documents and weekly full backups for data recovery cases.

In addition, (the organizations that make the registration functions) keep a copy of the paper documents in a safe place different from the own Certification Authority.

5.5.5. Requirements of timestamping

Records are dated with a reliable source via NTP.

There is no need to sign this information digitally.

5.5.6. Location of the file system

A centralized system of gathering information of the activity of the equipment involved in the certificate management service is available.

5.5.7. Procedures to obtain and verify file information

A procedure where describes the process to verify that the stored information is correct and reachable is available. It provides the information and means of verification to the auditor.

5.6. Keys renewal

The CA keys will be changed before the use of the private key expires. The former CA and its private key will only be used for signing CRLs while there are active certificates issued by that CA. A new CA will be generated with a new private key and a new DN. The key change of the subscriber is done by a new issuing process.

Alternatively, in the case of the subordinated Certification Authorities, you will be able to renew the certificate with or without key change, not applying the procedure described earlier.

5.7. Compromised key and recovery of disaster

5.7.1. Management procedures of incidents and commitments

Security policies and business continuity have been developed, which allows the management and backup of the systems in case of compromise or disaster of its operations, ensuring critical services of revocation and publication of the condition of the certificates.

5.7.2. Resources, applications or data corruption

When resources, applications or data corruption events happen, the incidences will be communicated to security, and the proper management procedures will begin, which contemplate scaling, investigation and response to the incident. Procedures of commitment of the keys or disaster recovery of VALIDATED ID will begin, if necessary.

5.7.3. Compromised privated key of the entity

In case of suspicion or knowledge of the commitment of VALIDATED ID, key commitment procedures will be activated in accordance to the security policies, incident management and business continuity, which allow the recovery of the critical systems, and if necessary in an alternative data center.

5.7.4. Business continuaty capabilities after a disaster

Critical services will be restored (suspension and revocation, and publication of the information of the certificates status) in accordance with the contingency and business continuity plan restoring the normal operation of the previous services within 24 hours of the disaster.

An alternative center for the operation of Certification schemes described in the business conitunity plan is avaliable.

5.8. Service termination

It is ensured that potential disruptions to subscribers and third parties are minimized as a result of the cessation of the service provider's services. In this regard, continuous maintenance of the records defined in section 5.5.1 is ensured for the defined in section 5.5.1, for the time established in section 5.5.2 of this Certification Practice Statement.

Notwithstanding the above, where appropriate, all necessary actions shall be taken to transfer to a third party or to a notarial depository, the obligations for the maintenance of the specified records during the relevant period according to this Certification Practice Statement or the relevant legal provision.

Before the services cessation, a termination plan is developed, with the following provisions:

- To provide the necessary funds (by civil liability insurance) to continue the completion of revocation activities.
- To inform all Signers/Subscribers, relying third parties and other CA's with which it has agreements or another type of relation of the cessation with a minimum of 6 months.
- To revoke any authorization to outsourced entities to act on behalf of the CA in the process of certificates issuance.
- To transfer its obligations regarding the maintenance of the registry information and logs for the period of time indicated to subscribers and users.
- To destroy or disable for use the private keys of the CA.
- To keep active the certificates and verification system to extinction and revocation of all certificates issued.
- To run all necessary tasks to transfer the maintenance obligations of registration information and the files of events log during the respective time periods indicated to the subscriber and relying third parties in certificates.
- To communicate the Ministry of Energy, Tourism, and Digital Agenda, no later than 2 months before, the cessation of activity and destination of the certificates specifying if the management is transferred and to whom or if the validity will be extinguished.

- To communicate, also to the Ministry of Energy, Tourism and Digital Agenda, the opening of any bankruptcy process against VALIDATED ID, as well as any other relevant circumstance that can prevent the continuation of activity.

6. Technical security controls

Reliable systems and products are used, protected against any alteration and guarantee the technical and cryptographic security of the certification, which are used as support.

6.1. Generation and installation of the pairo f keys

6.1.1. Generation of the pair of keys

The pair of keys of the intermediate Certification Authority "Validated ID Subordinate CA 01" are created by the Root Certification authority by the Validated ID Root CA in accordance with the Validated ID ceremony procedures, within the high security perimeter set aside for this task.

The activities performed during the keys generation ceremony have been registered, dated and signed for all the individuals participating in it, with the presence of an Auditor CISA. Such records are guarded to the effects of audit and follow-up during an appropriate period determined by VALIDATED ID.

For the certification authorities root and intermediate key generation, devices with the certification FIPS 140-2 level 3 and Common Criteria EAL4+ are used.

Validated ID Root CA	4.096 bits	25 años
Validated ID Subordinate CA 01	4.096 bits	13 year
- End entity Certificates	2.048 bits	Up to 5 years
- Certificates of the Timestamping unit	2.048 bits	Up to 5 years

The PKI Disclosure Statement (PDS) of all the electronic certificate profiles indicated in this document, are accessible under the link: https://www.validatedid.com/.

6.1.1.1. Generation of the key pair from the signer

The signer can create the signer keys through hardware and/or software devices authorized by Validated ID. The keys that have not being created on a QSCD will be

created by the signer. Validated ID never creates a key outside of a QSCD to be sent to the signer.

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

6.1.2. Sending the private key to the signer

In certificates, the private key of the qualified signature creation device is created and stored, properly protected, in the interior of such a qualified device.

In the software certificate the private key of the signer is created and stored in the computer system that this signer uses when requesting the certification so the sending of the private key does not exist, ensuring the exclusive control of the key by the user.

In certificates HSM centralized and QSCD centralized, the private key of the signer is created in a private area of the signer on a distant HSM. The signatory enters the login information to the private key, and it is not stored, or susceptible to powers of deduction or interception by the generation system and remote custody. The private key is not sent to the signer, in other words, never leaves the security environment that guarantees the exclusive control of the private key by the signer.

6.1.3. Sending of the public key to the certificate issuer

The method of remission of the public key to the relying electronic certification services provider is PKCS#10, other equivalent cryptographic test or any other method approved by Validated ID.

6.1.4. Public key distribution of the certification services provider

Validated ID's keys are communicated to third parties who trust in certificates, ensuring the integrity of the key and authenticating its origin, through its publication in the Deposit.

Users can access to the Deposit to obtain the public keys, and additionally, in applications S/MIME, the data message may contain a chain of certificates, which are distributed to the users in this way.

The certificate of the CA root and subordinated will be available on the Validated ID web page.

6.1.5. Key sizes

- The length of the Certification Authority root keys is 4096 bits.
- The length of the Certification Authority subordinated keys is 4096 bits.
- The length of the end Entity Certificates keys are 2048 bits.

6.1.6. Generation of public key parameters

The CA Root, CA subordinated and the subscriber certificates public key are encrypted in accordance with RFC 5280.

6.1.7. Quality check of the public key parameters

- Module Length= 4096 bits
- Algorithm of keys generation: rsagen1
- Cryptographic functions of Summary: SHA256.

6.1.8. Key generation in IT applications or in equipment goods

All keys are generated in equipment goods, in accordance with the indicated in section 6.1.1.

6.1.9. Key usage purposes

Key usage for the CA certificates is exclusively for signing certificates and CRLs.

Key usage for the end entity is exclusively for the digital signature, non-repudiation and data encryption.

6.2. Private key protection

6.2.1. Cryptographic modules standars

In relation to the modules that manage the keys of Validated ID and the subscribers of the electronic signature certificates, the required level by the standards indicated in the above sections is ensured.

6.2.2. Private key multi-person (n-m) control

A multi-person control is required for activating the private key of the AC. In case of this Certification Practice Statement, in detail there is a policy of **3 of 6** people for the keys activation.

Cryptographic devices are physically protected, as determined in this document.

6.2.3. Private key deposit

Validated ID doesn't store usable copies by proper means of the private key of the signers.

6.2.4. Private key backup

Validated ID makes backup copy of the CA private key that makes their recovery in case of disaster, loss or deterioration thereof. Both generation of the copy and the recovery thereof need at least two people participation.

These recovery files are stored in fireproof cabinets and in the external custody center.

Keys generated on software device: Validated ID cannot make keys backups, since no longer have access to them. The signer may make a backup.

Keys generated on QSCD: Backups are not possible, since the export from the QSCD is not possible.

Keys generated on HSM centralized and QSCD centralized: Only it is possible to make backups of an encrypted blob with Security World key of the HSM used and it is impossible

to decrypt it without the use of the credentials that only the owner of the certificate knows.

6.2.5. Private key storage

The CA private keys are archived for a period of **10 years** after the issuance of the last certificate. They will be stored in secure fireproof files and in the external custody center. At least the collaboration of two people will be needed to recover the CA private key in the initial cryptographic device.

The subscriber can store the private key during the time he thinks appropriate, just in case of encrypted certificates. In this case Validated ID also keep a copy of the private key associated to the encrypted certificate.

Validated ID does not generate or archive certificate keys, issued on software.

6.2.6. Private key transfer into a cryptographic module

Private keys are directly generated in the cryptographic modules of production of de Validated ID.

The Certification Authority private keys are encrypted stored in the cryptographic modules of Validated ID production.

6.2.7. Method of activating the private key

The Validated ID private key is activated by the running of the corresponding secure start procedure of the cryptographic module, by the persons indicated in section 6.2.2. authorized in accordance with this Certification Practice Statement.

The CA keys are activated by a process m of n (3 of 6).

The activation of the private keys of the Intermediate CA is managed with the same process of m of n of the CA keys.

6.2.8. Method of deactivating private key

For deactivation of Validated ID private key, the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

6.2.9. Method of destroying the private key

Prior to the destruction of the keys, a revocation of the certificate of the public keys associated with them will be issued.

Devices that have stored any part of Validated ID's private keys will be physically destroyed or rebooted at a low level. For the elimination, the steps described in the cryptographic equipment administrator's manual will be followed.

Finally, the backups will be destroyed in a safety way.

Regarding the private keys of the signatories, the procedure will be in accordance with those established in the termination plan.

6.2.10. Cryptographic modules clasification

See Section 6.2.1

6.3. Other aspects of key pair management

6.3.1. Public key file

Validated ID archives its public keys routinely, according to the established in section 5.5 this document.

6.3.2. Public and private key usage periods

Periods of use of the keys are determined by the duration of the certificate, after which they cannot continue to be used.

As an exception, the private key of decryption can continue being used even after the expiration of the certificate.

6.4. Activation data

6.4.1. Activation data generation and instalation

Activation data of the devices that protect Validated ID private keys are generated in accordance with the established in section **¡Error! No se encuentra el origen de la referencia.** and key procedures ceremony.

The creation and distribution of such devices is recorded.

Likewise, Validated ID generates the activation data in a safe way.

6.4.2. Activation data protection

Activation data devices that protect the private keys of the Certification Authority root and subordinated, are protected by the holders of cards managers of the cryptographic modules, as stated in the document of the keys ceremony.

The certificate signer is responsible for protecting his private key, with a password as complete and complex as possible. The signer must remember the password(s).

6.5. Computer security controls

Reliable systems are used to provide certification services. Controls and computer audits have been made to establish its proper computer activity management with the level of security required in the system management of electronic certification.

Regarding the information security, Validated ID applies the certification scheme controls on management systems ISO 27001.

Used equipment's are initially configured with appropriate security profiles of Validated ID staff system, in the following aspects:

- Setting up the operating system.
- Setting up the application security.
- Correct sizing of the system.
- User and permissions settings.
- Setting event Log.
- Backup and recovery plan.
- Antivirus settings.
- Requirements of network traffic.

6.5.1. Specific computer security technical requirements

Each server includes the following functionalities:

- Access control of the subordinate CA services and privilege management.
- Imposition of separation of duties for managing privileges.
- Identification and authentication of roles associated to identities.
- Archive of the subscriber and subordinate CA history and audit data.
- Audit events related to security.
- Self-diagnosis of safety related with the subordinate CA services.
- Recovery mechanisms of keys and subordinate CA system.

The stated functionalities are performed through a combination of operating system, PKI software, physical protection and procedures.

6.5.2. Computer security rating

The CA and RA applications used by Validated ID are reliable.

6.6. Life cycle technical controls

6.6.1. System development controls

The applications are developed and implemented in accordance with the development and change control standards.

The applications have methods for verifying the integrity and authenticity, as well as the correction of the version to use.

6.6.2. Security management controls

The necessary activities are carried out to train and raise employee awareness of safety issues. Training materials and process descriptions are updated after approval by a safety management group. An annual training plan is in place for this function.

Equivalent security measures are contractually required of any external supplier involved in the work of trusted e-services.

6.6.2.1. Classification and management of information and goods

An inventory of assets and documentation and a procedure for the management of this material is maintained to ensure its use.

The security policy details the information management procedures where it is classified according to its level of confidentiality.

Documents are catalogued in three levels: UNCLASSIFIED, INTERNAL USE and CONFIDENTIAL.

6.6.2.2. Management operations

An adequate incident management and response procedure is in place, through the implementation of an alert system and the generation of periodic reports.

The security document develops in detail the incident management process.

The entire procedure relating to the functions and responsibilities of personnel involved in the control and handling of elements contained in the certification process is documented.

6.6.2.3. Treatment of supports and safety

All supports are treated safely in accordance with the requirements of the classification of information. The supports that contain sensitive information are destroyed safely if they are not going to be required again.

Planning system

The Systems department keeps track of the capabilities of the equipment. In conjunction with the implementation of resources control each system can provide a possible downsizing.

Reports of incidents and response

A procedure is in place for the follow-up of incidents and their resolution, where the responses and an economic evaluation of the resolution of the incident are recorded.

Operational procedures and responsibilities

Activities are defined, assigned to people with a role of trust, different from the people in charge of day-to-day operations that are not confidential.

6.6.2.4. Access system management

Every reasonable effort is made to confirm that system access is limited to authorized persons.
In particular:

CA General

- Controls based on firewalls, antivirus and IDS with high availability are in place.
- Sensitive data is protected by cryptographic techniques or access controls with strong identification.
- There is a documented procedure for managing user registrations and cancellations and an access policy detailed in its security policy.
- Procedures are in place to ensure that operations are carried out in compliance with the role policy.
- Each person has an associated role to perform certification operations.
- Personnel are responsible for their actions through the confidentiality commitment signed with the company.

Certificate generation

Authentication for Issuance process is performed through a system of m of n operators for activating Validated ID private key.

Revocation management

Revocation will be performed by strong authentication to the applications of an authorized administrator. Logs systems will generate the tests that guarantee non-repudiation of the action taken by Validated ID administrator.

Revocation management

The revocation status application has access control based on certificate or two-factor authentication to prevent attempts to modify revocation status information.

6.6.2.5. Gestión del ciclo de vida del hardware criptográfico

Validated ID ensures that the cryptographic hardware used for signing certificates is not handled during its transport by inspecting the delivered material.

The cryptographic hardware moves on prepared supports to prevent any manipulation.

All relevant device information is recorded to add to the asset catalog.

The use of cryptographic certificate signing hardware requires the use of at least two trusted employees.

Periodic tests are performed to ensure the correct functioning of the device.

The cryptographic hardware device is only handled by trusted personnel.

The Validated ID private signing key stored in the cryptographic hardware will be deleted once the device has been removed.

La configuración del sistema de Validated ID, así como sus modificaciones y actualizaciones son documentadas y controladas.

Changes or updates are authorized by the security manager and are reflected in the corresponding working minutes. These configurations shall be performed by at least two reliable people.

6.7. Network security controls

Physical access to network management devices is protected, and it has an architecture that orders the generated traffic based on its security characteristics, creating clearly defined network sections. This division is made through the use of firewalls.

Confidential information that is transferred over unsecured networks is encrypted using SSL protocols or the VPN system with two-factor authentication.

6.8. Engineering controls of cryptographic modules

Cryptographic modules are subject to engineering controls provided in the standards indicated along this section.

The key generation algorithms used are commonly accepted for the use of the key to which they are intended.

All cryptographic operations of Validated ID are performed in modules with FIPS 140-2 level 3 certification.

6.9. Time source

There is a coordinated time synchronization procedure via NTP, which accesses two independent services:

- The first synchronization is with a service based on GPS antennas and receivers that allows a confidence level of STRATUM 1 (with two systems in high availability).
- The second has a complementary synchronization, via NTP, with the Royal Institute and Observatory of the Navy (ROA).

6.10. Changing the status of a Secure Signature Creation Device (QSCD)

Validated ID in the case of modification of the certification status of Qualified Signature Creation Devices (QSCD), will proceed as follows:

1. Validated ID has a list of several certified QSCDs, as well as a close relationship with suppliers of such devices, in order to ensure alternatives to possible loss of certification status of QSCD devices.
2. In the event of expiration of the period of validity or loss of certification, Validated ID will not use such QSCD for the issuance of new digital certificates, either in new issues or eventually in possible renewals.
3. Proceed immediately to switch to QSCD devices with valid certification.
4. In the event that a QSCD device proves to have never been a QSCD device, due to forgery or any other type of fraud, Validated ID will immediately proceed to inform

its customers and the regulatory body, revoke the digital certificates issued on these devices and replace them by issuing them on valid QSCDs.

7. Certificates profiles and CRLs

7.1. Certificate profile

All qualified certificates issued under this policy comply the X.509 standard version 3, RFC 3739 and ETSI 101 862 “Qualified Certificate Profile”. The documentation relating to the profiles of the policy EN 319 412 can be requested to Validated ID.

7.1.1. Version number

Validated ID issues certificates X.509 Version 3

7.1.2. Certificate extensions

Certificates extensions are detailed in the profiles documents, which are accessible from Validated ID’s web (https://www.validatedid.com/).

In this way, it is allowed to keep more stable versions of the Certification Practice Statement and decouple them from frequent adjustments in the profiles.

7.1.3. Object identifier (OID) of algorithms

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Names format

Certificates must contain the required information for its use, as determined by the appropriate policy.

7.1.5. Names restriction

Names contained in the certificates are restricted as “Distinguished Names” X.500, which are unique and not ambiguous.

7.1.6. Object identifiers (OID) of certificates types

All certificates include a certificate policy identifier under which they have been issued, according to the structure indicated in point 1.2.1.

7.2. CRL profile

7.2.1. Version number

CRLs issued by Validated ID are from version 2.

7.2.2. OCSP profile

According to standard IETF RFC 6960.

8. Compliance audit

Validated ID has communicated the beginning of its activity as certification services provider by the National supervisory body and when the authority deems necessary it is subjected to check controls.

8.1. Frequency of compliance audit

Validated ID conducts a compliance audit annually, in addition to internal audits carried out at its own discretion or at any time, due to a suspected breach of any security measure.

8.2. Frequency of compliance audit

The audits are performed by an external independent auditing firm that demonstrates technical competence and experience in computer security, information systems security and compliance audits of public key certification services and related elements.

8.3. Auditor relationship to audited entity

Audit firms are of renowned prestige, with specialized departments in conducting IT audits, so there is no conflict of interest that could undermine its performance in relation to Validated ID.

8.4. Topics covered by audit

The audit verifies with reference to Validated ID that:

a) The entity has a management system, which ensures the quality of service.
b) The entity complies with the requirements of the Certification Practice Statement and other documentation related to the issuance of the various digital certificates.

c) The Certification Practice Statement and other related legal documentation comply with the agreed with Validated ID and the established in the current regulation.
d) The entity properly manages its information systems.

Specially, the topics covered by audit are as follows:

a) CA, RA's and related elements processes.
b) Information systems.
c) Protection of the data processing center.
d) Documents.

8.5. Actions taken as a result of lack of conformity

Once the management has received the auditor's compliance report, the deficiencies found are analyzed with the audit entity. This report also develops and implements the corrective policies that tackle these deficiencies.

If Validated ID is unable to develop and/or implement the corrective measures or if the deficiencies found suppose an immediate threat to the system security or integrity, shall immediately inform to the Security Committee of Validated ID which can perform the following actions:

- Cease operation temporarily.
- Revoke the CA key and regenerate the infrastructure.
- Terminate the CA service.
- Other complementary actions needed.

8.6. Treatment of Audit reports

Audit reports results are delivered to the Security Committee of Validated ID within a maximum period of 15 days after completion of the audit.

9. Business and legal requirements

9.1. Fees

9.1.1. Certidicate issuance or renewal fees

Validated ID can establish a certificate issuance or renewal fee and when appropriate the subscribers will be informed in due course.

9.1.2. Certificate access fees

Validated ID hasn't established any fee for certificates access.

9.1.3. Certificate status information access fees

Validated ID hasn't established any fee for certificates status information access.

9.1.4. Fees for other service

Not stipulated.

9.1.5. Refund policy

Not stipulated.

9.2. Financial capacity

Validated ID has enough economic resources to keep its operations, to comply with its obligations and to confront the risk of liability for claim and damages, as established in ETSI EN 319 401-1 7.12 c), in relation to the management of the services finalization and termination plan.

9.2.1. Insurance coverage

Validated ID has warranty coverage of its civil liability, with an insurance of professional civil liability that complies with the current regulation applicable.

9.2.2. Other assets

Not stipulated.

9.2.3. Insurance coverge for subscribers and relaying third parties in certificates

Validated ID has a warranty coverage of its civil liability, with an insurance of professional civil liability, for relying electronic services, with the minimum insured of 2.500.000 Euros.

9.3. Confidentiality

9.3.1. Confidential information

Validated ID keeps in confidence the following information:

- Certificates request, approved or rejected, and all other personal information obtained for issuance and maintenance of certificates, except the information indicated in next section.
- Private keys generated and/or stored by the certification services provider.
- Transaction record, including full records and audit records of the transactions.
- Internal and external transactions records created and/or kept by the Certification Authority and its auditors.
- Business continuity and emergency plans.
- Security plans.
- Documentation of operations, archiving, motorization and other analogous.
- All other information identified as 'Confidential'.

9.3.2. Non confidential information

The following information is considered non-confidential:

- Certificates issued or in the process of issuance.
- Linking the subscriber to a certificate issued by the Certification Authority.

- Name and surname of the natural person identified on the certificate, as well as any other circumstance or personal information of the holder, in the event that it is important according to the purpose of the certificate.
- Email of the natural person identified on the certificate, or email assigned to the subscriber, in case it is important according to the purpose of the certificate.
- Economic uses and limits outlined in the certificate.
- Validity period of the certificate, as well as date of issue and expire date of the certificate.
- Serial number of the certificate.
- The different status or conditions of the certificate and starting date for each, specifically: pending of generation and/or delivery, valid, revoked, suspended or expired and the reason that caused the change of status.
- The Certificate Revocation Lists (CRLs), and the remaining revocation status information.
- The information contained in the certificates deposits.
- Any other information not indicated in the previous section.

9.3.3. Information disclosure of suspension and revocation

See previous section.

9.3.4. Legal disclosure of information

Validated ID only discloses the confidential information in the cases legally foreseen.

Specifically, records that support the reliability of the data contained in the certificate will be disclosed if required to prove the evidence of the certification in legal proceedings, even without the consent of the certificate subscriber.

Validated ID will indicate these circumstances in the privacy policy under section **¡Error! No se encuentra el origen de la referencia.**.

9.3.5. Information disclosure on request of owner

Validated ID includes under privacy policy Section **¡Error! No se encuentra el origen de la referencia.**, requirements to allow the disclosure of subscriber information and, when appropriate, of the natural person identified on the certificate directly allocated or to third parties.

9.3.6. Other information disclosure cirmstances

Not stipulated.

9.4. Personal data protection

Validated ID is compliance with current regulations on the protection of personal data, as reflected in the General Data Protection Regulation No. 2016/679 and in general any applicable national regulations.

In compliance with, Validated ID has documented in this Certification Practice Statement the security and organizational aspects and procedures, in order to guarantee that all the personal data to which it has access are protected against its loss, destruction, damage, forgery and illegal or unauthorized processing.

The following is a detail of all the necessary information regarding the processing of personal data made by Validated ID:
Data controller:

Validated ID, S.L.
NIF: ESB65750721
Dirección: Carrer de Sepúlveda 143 pl. 4 08011 Barcelona
Datos registrales: Registro Mercantil de Barcelona, Tomo 43051 , Folio 30, Sección 8, Hoja B 419604

Data privacy officer
Teléfono: (+34) 900828948

Correo electrónico: dpo@validatedid.com

Purposes of data processing

Validated ID treats the personal data provided to carry out the requested electronic services, specifically the issuance of electronic certificates, all in accordance with the provisions of the VALIDATED ID Certification Practices Statement (CPS), which is available at the following link: https://www.validatedid.com/

The purposes of data processing related to the SERVICE are the following:

- Identification of the subscribers and / or signers of the electronic certificates.
- Issuance and management of electronic certificates.
- Certificate life cycle management (suspension, renewal, reactivation and revocation).
- Communications related to the service.
- Custody and maintenance of the file related to the electronic certificate.
- Administrative, accounting and billing management derived from the hiring.

Lawfulness of processing

The legitimacy of the processing of personal data for the Provision of Trust Services for the issuance of electronic certificates, is based on the execution of a contract for the services requested, where the user is a party to it.

Processed data and conservation

The categories of personal data processed by Validated ID, by way of example but not limited to, include:

- Identification data: name, surname and official identity number.
- Professional data: organization, department and / or position.

- Contact information: postal address, email and telephone number.

- Data related to the identity or identification of the users: photographs and / or when the facial biometric pattern corresponds, in order to be able to carry out the Validated ID video identification process.

Personal data will be kept until the end of the contractual relationship and subsequently, during the legally required periods according to each case. As a general rule, personal data related to the SERVICE will be kept for 15 years from the revocation of the corresponding certificate.

Likewise, the proofs of the identification processes will be kept for 15 years, except for those incomplete proofs which will be kept for a minimum of 5 years.

Personal data will be stored in the secure facilities of the PKI provider located in Spain and Italy.

Data transfer

The data may be made available to third parties, within the territory of the European Union, for the provision of services contracted by the user (for example data hosting providers (CPD), identification support services, companies of the group, etc.), all under the protection of the corresponding contract for the processing of personal data, guaranteeing at all times suitable security measures that ensure the due protection of users' personal data.

Notwithstanding the foregoing, as a general rule, personal data will only be transferred to third parties under legal obligation.

As a general rule, international transfers will not be made.

User rights

Users may exercise their rights of confirmation, access, rectification, deletion, cancellation, limitation, opposition and portability.

- Confirmation. All users have the right to obtain confirmation on whether Validated ID is treating personal data that concerns them.

- Access and rectification. Users have the right to access all their personal data, as well as request the rectification of those that are inaccurate or erroneous.

- Suppression and cancellation. Users may request the deletion / cancellation of the data when, among other reasons, they are not necessary for the purposes for which they were collected.

- Limitation and opposition. The user may request the limitation of the treatment so that their personal data is not applied in the corresponding operations. In certain circumstances and for reasons related to their particular situation, the user may oppose the processing of data, Validated ID being obliged to stop processing them, except for compelling legitimate reasons, or the exercise or defense of possible claims.

- Portability. Interested parties may request that their personal data be sent to them or transmitted to another person in charge, in a structured and commonly used electronic format.

To exercise their rights, users may send a request to the e-mail address or write to the address previously identified. In such request, they must attach a copy of their identity document and clearly indicate which right they wish to exercise.

9.5. Intellectual property rights

9.5.1. Property of certificates and revocation information

Validated ID is the only one that has intellectual property rights on the certificates that issues, without any prejudice of the rights of the subscribers, key holders and third parties, to which it grants non exclusive license to reproduce and distribute certificates,

free of charge, as long as the reproduction is full and does not alter any element of the certificate, and is necessary in relation with digital signatures and/or encryption systems within the scope of the certificate use, and according to the documentation that links them.

In addition, certificates issued by Validated ID have a legal notice concerning their ownership.

The same rules are applicable to the use of the information of certificates revocation.

9.5.2. Property of the Certification Practice Statement

Validated ID is the only one that has intellectual property rights of this Certification Practice Statement.

9.5.3. Property of information relating to names

The subscriber and, if applicable, the natural person identified in the certificate retains all rights, if any, to the trademark, product or trade name contained in the certificate.

The subscriber is the owner of the distinguished name (DN) of the certificate, consisting of the information specified in section 3.1.1.

9.5.4. Property of keys

The subscribers of the certificates are the owners of the key pair.

When a key is divided in parts, all parts of the key are property of the owner of the key.

9.6. Obligations and civil liability

9.6.1. VALIDATED ID obligations

Validated ID guarantees, under full responsibility that complies with all requirements established in the Certification Practice Statement, and it is responsible for ensuring compliance with the procedures described, according to the instructions contained in this document.

Validated ID provides relying electronic services in accordance with this Certification Practice Statement.

Previous issuance and delivery of the certificate to the subscriber, Validated ID informs the subscriber of the terms and conditions related to the use of the certificate, price and use limitations, through a subscriber contract that includes by reference the disclosure texts (PDS) of each of the acquired certificates.

The disclosure text document, also known as PDS[13], meets the content of Annex A of ETSI EN 319 411-1 v1.1.1 (2016-02) this document can be transmitted by electronic media, using a sustainable communication method, and in accessible language.

Validated ID binds subscribers, key holders and third parties that trust in certificates through the disclosure text or PDS, in written and understandable language, with the minimum following contents:

- Requirements to comply with the provisions of sections **¡Error! No se encuentra el origen de la referencia.**,9.2,9.6.7, **¡Error! No se encuentra el origen de la referencia.**, **¡Error! No se encuentra el origen de la referencia.** and 9.6.10.
- Indication of the applicable policy, indicating that the certificates are not issued to the public.
- Demonstration of the information contained in the certificate is accurate, unless notification against the subscriber.

[13] "PKI Disclosure Statement".

- Consent for the publication of the certificate in the deposit and third party access.
- Consent for storing information used for the subscriber registration and the termination of such information to third parties, in case of termination of operations of the Certification Authority without revocation of valid certificates.
- Limits of use of the certificate, including those established in section **¡Error! No se encuentra el origen de la referencia.**.
- Information about how to validate a certificate, including the requirement to check the certificate status and the conditions under which it can reasonably trust the certificate, which applies when the subscriber acts as a relying third party in the certificate.
- The way in which the liability of the Certification Authority is guaranteed.
- Limitations of liability, including the uses for which the Certification Authority accepts or excludes its liability.
- Certificates request information file period.
- Audit registry file period.
- Applicable procedures of dispute settlement.
- Applicable Law and competent jurisdiction.
- If the Certification Authority has been declared in conformity with the certification policy, where appropriate, according to which system.

9.6.2. Guarantees offered to subscribers and relaying third parties in certidicates

Validated ID, establishes and rejects guarantees and applicable disclaimers in the documentation that connects the subscribers and relying third parties in certificates.

Validated ID, guarantees the subscriber, at least:

- Not factual errors in the information in the certificates, known or made by the Certification Authority.
- Not factual errors in the information in the certificates, due to lack of due diligence of the certificate request or to its creation.
- The certificates comply with all the material requirements established in the Certification Practice Statement.

- Revocation services and the use of the Deposit comply with all material requirements established in the Certification Practice Statement.

Validated ID, guarantees the third party that trusts in the certificate, at least:

- The information contained or incorporated by reference in the certificate is accurate, except when the opposite is indicated.
- In case of certificates published in the Deposit, that the certificate has been issued to the identified subscriber and the certificate has been accepted, in accordance with section **¡Error! No se encuentra el origen de la referencia.**.
- The approval of the certificate request and in the certificate issuance all the material requirement established in the Certification Practice Statement has been accomplished.
- Speed and assurance with the services provision, especially with revocation services and Deposit.

In addition, Validated ID guarantees the subscriber and the relying third party in the certificate:

- That the certificate contains the information that a qualified certificate must contain, in accordance with the provisions of Law 6/2020, of November 11.
- Confidentiality is preserved during the process if private keys are generated by the subscriber or, where appropriate, the natural person identified on the certificate.
- The responsibility of the Certification Authority, with the limits established.

9.6.3. Rejection of other guarantees

Validated ID rejects any other guarantee that is not enforceable under the laws, except the ones covered in section **¡Error! No se encuentra el origen de la referencia.**.

9.6.4. Limitation of liability

Validated ID limits its responsibility to the issuance and management of certificates and key pair of subscribers supplied by the Certification Authority.

9.6.5. Indemnity clauses

9.6.5.1. Subscriber indemnity clause

Validated ID includes in the contract with the subscriber, a clause whereby the subscriber agrees to indemnify the Certification Authority of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including judicial and legal representation that may be incurred by the publication and use of the certificate, when occurs any of the following causes:

- Falsehood or inaccurate statements committed by the certificate user.
- Certificate user error when administering enrolment request data. If there was fraud or negligence in the action or omission regarding the Certification Authority or any relying person in the certificate.
- Private key protection negligence, when using a relying system or when keeping the necessary precautions to avoid its compromise, loss, disclosure, modification or the unauthorized use.
- Use of a name (including names, email address and domain names), or other certificate information that infringes intellectual or third party industrial property of others by the subscriber.

9.6.5.2. Relaying third person in the certificate indemnity clause

Validated ID includes in the disclosure text or PDS, a clause whereby the relying on third party in the certificate agrees to indemnify the Certification Authority of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including court and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes occurs:

- Breach of the obligations of the relying on third party in the certificate.
- Reckless trust in a certificate, along with the circumstances.
- Lack of checking of the certificate status, to determine that it is not suspended or revoked.

9.6.6. Fortuitous event and force majeure

Validated ID shall not be liable in any case under situations incurring in fortuitous event and in case of force majeure.

An act of God is understood as a situation or event that is impossible to foresee, or that, if foreseen, is unavoidable with respect to its mitigation. In addition, force majeure is understood as that situation or event that is unavoidable in its circumstances, unforeseeable and extraordinary in its origin, emanating from an external and irresistible environment.

Therefore, Validated ID shall not be liable under any circumstances in case of war, natural disasters, malfunction of electrical services, networks or computer infrastructure, for reasons not attributable to Validated ID.

9.6.7. Applicable law

Validated ID establishes, in the subscriber contract and in the disclosure text or PDS, that the applicable law of services provision, including the policy and practices of certification, is the Spanish Law.

9.6.8. Severability, survival, entire agreement and notification clauses

Validated ID establishes, in the subscriber's contract and in the disclosure text or PDS, the severability, survival, entire agreement and notification clauses:

- Under the severability clause, the invalidity of a clause will not affect the rest of the contract.
- Under the survival clause, certain rules will remain in force after the completion of the regulatory service of the legal relationship between the parties. For this purpose, the Certification Authority ensures that the requirements of sections 9.6.1 (Obligations and liability), 8 (Compliance audit) and 9.3 (Confidentiality), remain in force after the termination of the service and the general conditions of issuance/use.
- Under the entire agreement clause, it is understood that the regulatory legal service contains the full will and all agreements between the parties.
- Under the notification clause, it will be established the procedure by which the parties mutually report incidents.

9.6.9. Competent jurisdiction clause

Validated ID establishes, in the subscriber's contract and in the disclosure text or PDS, a jurisdiction clause, indicating that the international jurisdiction corresponds to the Spanish judges.

The territorial and functional jurisdiction shall be determined under the regulations of international private law and procedural law that may be applied.

9.6.10. Resolution of conflicts

Validated ID establishes, in the subscriber's contract, and in the disclosure text or PDS, mediation and resolution procedures of applicable disputes.

10. Annex I - Acronyms

EBA	European Banking Authority
CA	Certification Authority.
RA	Registration Authority
CP	Certificate Policy
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
CSR	Certificate Signing Request.
DES	Data Encryption Standard.
DN	Distinguished Name.
DSA	Digital Signature Algorithm.
QSCD	Qualified Signature Creation Device.
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization.
LDAP	Lightweight Directory Access Protocol.
OCSP	On-line Certificate Status Protocol.
OID	Object Identifier.
PA	Policy Authority.
PIN	Personal Identification Number.
PKI	Public Key Infrastructure.
PSD2	Payment service directive
RSA	Rivest-Shimar-Adleman.
SHA	Secure Hash Algorithm.
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol
EBA	European Banking Authority
CA	Certification Authority.