Trust Practices Statement of the Digital Certification Service

Reference: IZENPE-DPC
Version no.: v7.7
Date: 08/11/2024

ZIURTAPEN ETA
ZERBITZU
ENPRESA-EMPRESA
DE CERTIFICACION
Y SERVIC

© IZENPE 2024

This document is property of IZENPE. This document may only be reproduced in its entirety.

Version History

Changes to versions prior to 7.0 can be found in the "Updates and Notifications about the Certification Practice Statement" section of www.izenpe.eus

Version	Date	Summary of changes
7.0	14/07/2021	Added change table to replace the updates document Updated section 4.9.12 of the CPD to indicate methods available for demonstrating private key commitment
7.1	13/01/2022	The following headings are updated, – 6.2.1 Standards for cryptographic modules – 9.3.3 Responsibility to protect confidential information: regulatory update. – 9.16.6: Other stipulations
7.2	01/09/2022	The following headings are updated, 1.1 1.1.1 Hierarchy CA root 2007 (CN=Izenpe.com): the value of the Qualified signature type is updated to Advanced for current OIDs in the cryptographic chip.
7.3	21/10/2022	The following headings are updated, 1.2 Hierarchy CA root 2007 (CN=Izenpe.com): the value of the policy identifier is updated to QCP-n for current OIDs in the cryptographic chip and the SSL EV certificate policy is updated to QEVCP-w
7.4	13/09/2023	1.4.1 Errors corrected 1.6.2 Errors corrected 2.3 Wording updated 6.1.2 FIPS updated 6.1.3 Distribution methods updated 7.1 Certificate profile updated

7.5	08/11/2023	Point 4.9.8 updated: Time passing between generation and publication of the CRLs Updated point 9.16.6 on prevalence of the guidelines guide
7.6	23/07/2024	Updated Introduction: regulations Updated table 1.1.1 Updated table 1.1.2 Addition of table 1.1.5 Update 1.3.1 new root CA Updated 1.4.1 test certificates Updated headquarters address 1.5.1 Updated mail 1.5.2 Updated 4.2.1 establishing the validity of an ID Updated 4.9.3 adding a specific email address Updated 5.5.2, Error corrected (issue date by end date) Updated 5.7.1 Updated 6.3.2 validity new root CA Update 9.4.4.4 of the supervisory authority in the field of data protection Updated writing 9.8.4
7.7	07/11/2024	DPC version fix in footer. ANNEX I is eliminated, and a link is included to the profiles published on the website (https://www.izenpe.eus/contenidos/informacion/doc_juridica/es_de

		f/adjuntos/Perfiles_de_Certificados.pdf) Correction of the OIDs in section 1.1.4

Table of contents

Content

1	**Introduction**	**17**
1.1	Purpose	18
1.1.1	Hierarchy CA root 2007 (CN=Izenpe.com)	19
1.1.2	Hierarchy CA root 2020 qualified (CN=ROOT CA QC IZENPE)	22
1.1.3	Hierarchy CA root 2020 non-qualified (CN=ROOT CA NQC IZENPE)	25
1.1.4	Internal SSL Root CA Hierarchy (CN=Izenpe.com)	**Error! Undefined marker.**
1.2	Document name and identification	26
1.3	Participants in the Public Key Infrastructure (PKI)	27
1.3.1	Certification Authorities	27
1.3.2	Registration Entities	28
1.3.3	Certificate Subscribers	28
1.3.4	Trusting third parties	28
1.3.5	Other participants	29
1.4	Certificate uses	29
1.4.1	Appropriate certificate uses	29
1.4.2	Prohibited certificate uses	31
1.5	Policy administration	31
1.5.1	Entity responsible for managing documentation	31
1.5.2	Contact details	31
1.5.3	In charge of adapting the Certificate Practice Statement	31
1.5.4	Procedure to approve the Certificate Practice Statement	32
1.6	Definitions and acronyms	32
1.6.1	Definitions	32

1.6.2 Acronyms 36

2 Publication and supervisors of information repository 38

2.1 Information repository 38

2.2 Publication of certification information 38

2.2.1 Publication and notification policy 38

2.2.2 Items not published in the Certification Practice Statement 38

2.3 Frequency of publication 38

2.4 Controlling access to the repository 39

3 Names 40

3.1.1 Types of names 40

3.1.2 Meaning of names 40

3.1.3 Pseudonyms 40

3.1.4 Rules for interpreting name formats 41

3.1.5 Uniqueness of names 41

3.1.6 Resolving conflicts relating to names and processing trademarks 41

3.2 Validation of identity 41

3.2.1 Methods for proving possession of the private key 41

3.2.2 Authentication of the Organisation Identity 42

3.2.3 Authentication of the identity of the natural person applicant 42

3.2.4 Unverified subscriber information 42

3.2.5 Authority validation 42

3.2.6 Interoperability criteria 42

3.3 Identification and authentication for requests to reissue keys 42

3.3.1 Routine renewal 42

3.3.2 Renewal after revocation 42

3.4 Identification and authentication for revocation requests 43

4 Operative requisites for the certificates' life cycle 44

4.1 Certificate application 44

4.1.1 Verification of application 44

4.1.2 Proceso de inscripción y responsabilidades. 44

4.2 Processing applications 45

4.2.1 Carrying out identification and authentication functions 45

4.2.2 Approve or deny applications 45

4.2.3 Application processing time 45

4.3 Certificate issuance 45

4.3.1 CA actions during issuance 45

4.3.2 Notification to the issuance subscriber 46

4.4 Certificate acceptance 46

4.4.1 Certificate acceptance process 46

4.4.2 Publication of the certificate by the CA 46

4.4.3 Notification of certificate issuance by the CA and other entities 46

4.5 Pair of keys and uses of the certificate 47

4.5.1 Subscriber's private key and use of the certificate 47

4.5.2 Use of the public key and the certificate by relying parties 48

4.6 Certificate revocation 49

4.6.1 Circumstances for certificate renewal 49

4.6.2 Who may apply for renewal 49

4.6.3 Processing certificate renewal requests 49

4.6.4 Notification to the subscriber 49

4.6.5 Renewed certificate acceptance procedure 49

4.6.6 Publishing the certificate 49

4.6.7 Notifying other entities 50

4.7 Renewal with certificate key regeneration 50

4.7.1 Circumstances to regenerate certificate keys 50

4.7.2 Who can apply 50

4.7.3 Processing renewal applications with key regeneration 50

4.7.4 Notification to the subscriber 50

4.7.5 Renewed certificate acceptance procedure 50

4.7.6 Publishing the certificate 51

4.7.7 Notifying other entities 51

4.8 Modification of the certificate 51

4.8.1 Circumstances for certificate modification 51

4.8.2 Who may apply for certificate modification? 51

4.8.3 Processing of certificate modification applications 51

4.8.4 Notification of certificate modification 51

4.8.5 Conduct constituting acceptance of the certificate modification 51

4.8.6 Publication of the modified certificate 51

4.8.7 Notification of certificate modification to other entities 51

4.9 Revocation 51

4.9.1 Circumstances for revocation 51

4.9.2 Who can request revocation 52

4.9.3 Processing revocation requests 53

4.9.4 Grace period for the revocation request 53

4.9.5 CA deadline to process the revocation 53

4.9.6 Obligation to verify revocations by relying parties 53

4.9.7 Frequency of CRL generation 53

4.9.8 Time passing between generation and publication of the CRLs 54

4.9.9 Availability of the online verification system for the status of certificates 54

4.9.10 Online revocation checking requisites 54

4.9.11 Other revocation notifications available 55

4.9.12 Special committed key requisites 55

4.9.13 Circumstances for suspension 55

4.9.14 Who can request suspension? 55

4.9.15 Procedure for requesting suspension 55

4.9.16 Limits on the period of suspension 55

4.10 Certificate status services 55

4.10.1 Operational characteristics 55

4.10.2 Service availability 56

4.10.3 Optional characteristics 56

4.11 Termination of subscription 56

4.12 Custody and recovery of keys 56

4.12.1 Key custody and recovery practices and policies 56

4.12.2 Session key protection and recovery practices and policies 56

5 Physical, procedural and personnel security controls 57

5.1 Physical security controls 57

5.1.1 Site location and construction 57

5.1.2 Physical access 57

5.1.3 Power and air conditioning 58

5.1.4 Exposure to water 58

5.1.5 Fire prevention and protection 58

5.1.6 Media storage 58

5.1.7 Waste processing 58

5.1.8 Off-site backup 58

5.2 Procedural controls 59

5.2.1 Trusted roles 59

5.2.2 Number of people per task 59

5.2.3 Identification and authentication for each role 59

5.2.4 Separating tasks into different roles 59

5.3 Personnel controls 59

5.3.1 Background, qualifications, experience, and authentication requirements 59

5.3.2 Background check procedures 60

5.3.3 Training requirements 60

5.3.4 Retraining frequency and requirements 60

5.3.5 Sequence and frequency of job rotation 60

5.3.6 Sanctions for unauthorised actions 60

5.3.7 Recruitment requirements 60

5.3.8 Provision of documentation to staff 61

5.4 Audit 61

5.4.1 Type of events recorded 61

5.4.2 Frequency of log processing 61

5.4.3 Period for audit log retention 61

5.4.4 Protecting the audit log 62

5.4.5 Audit log backup procedure 62

5.4.6 Compiling logs 62

5.4.7 Notifying the action causing the logs 62

5.4.8 Vulnerability analysis 62

5.5 Archiving of records 62

5.5.1 Type of records archived 62

5.5.2 File retention period 62

5.5.3 File protection 62

5.5.4 Archive backup procedures 63

5.5.5 Requisites for time stamping the records 63

5.5.6 Filing system 63

5.5.7 Procedures to obtain and verify the archive information 63

5.6 CA key change 63

5.7 Incident Management and Contingency Plan 63

5.7.1 Incident management procedures 63

5.7.2 Action plan to deal with corrupt data and software 65

5.7.3 Procedure in case of compromise of the CA's private key 65

5.7.4 Business continuity after a disaster 65

5.8 CA or RA termination 65

5.8.1 Certification Authority 65

5.8.2 Registration Authority 66

6 Technical security controls 67

6.1 Key pair generation and installation 67

6.1.1 Key pair generation 67

6.1.2 Private key delivery to subscriber 67

6.1.3 Public key delivery to certificate issuer 67

6.1.4 Certification Authority public key delivery to certificate users 67

6.1.5 Key sizes and algorithms used 68

6.1.6 Certificate signing algorithms **Error! Undefined marker.**

6.1.7 Supported Key Usages (KeyUsage field X.509v3) 69

6.2 Private key protection 69

6.2.1 Standards for cryptographic modules 69

6.2.2 Private key (n out of m) multi-person control 69

6.2.3 Private key custody 69

6.2.4 Private key backup 70

6.2.5 Private key archiving 70

6.2.6 Transfer of the private key to or from the cryptographic module 70

6.2.7 Storage of the private key in the cryptographic module 70

6.2.8 Private key activation method 71

6.2.9 Private key deactivation method 71

6.2.10 Private key destruction method 71

6.2.11 Qualifying the cryptographic module 71

6.3 Other aspects of key pair management 71

6.3.1 Public key archiving 71

6.3.2 Certificate operation periods and key pair use periods 71

6.4 Activation data 72

6.4.1 Generation and installation of activation data 72

6.4.2 Activation data protection 72

6.4.3 Other aspects of the activation data 72

6.5 Computer security controls 72

6.5.1 Specific technical requirements for computer security 72

6.5.2 Assessment of the level of IT security 73

6.6 Life cycle engineering controls 73

6.6.1 System development controls 73

6.6.2 Security management controls 74

6.6.3 Life cycle security controls 74

6.7 Network security controls 74

6.8 Time source 74

7 Revoked Certificate and CRL profiles 75

7.1 Certificate profile 75
7.1.1 Version number 75
7.1.2 Certificate extensions 75
7.1.3 Algorithm object identifiers 75
7.1.4 Name Formats 75
7.1.5 Name restrictions 75
7.1.6 Certificate Policy Object Identifier 75
7.1.7 Use of extension policy restrictions 76
7.1.8 Syntax and semantics of policy qualifiers 76
7.1.9 Semantic treatment for the “Certificate policy” extension 76
7.2 Certificate revocation list profile 76
7.2.1 Version number 76
7.2.2 List of certificate revocation and extensions of elements 77
7.3 OCSP profile 77
7.3.1 Version number 77
7.3.2 OCSP Extensions 77
7.3.3 Other OCSP aspects 77
8 Compliance audits 78
8.1 Audit frequency 78
8.2 Auditor qualifications 78
8.3 Relationship of the auditor with the audited company 78
8.4 Elements to be audited 78
8.5 Decision-making as the result of deficiencies 78
8.6 Communication of results 79
9 Other legal and activity matters 80
9.1 Fees 80

9.1.1 Fees for the issue or renewal of certificates 80

9.1.2 Fees for access to certificates 80

9.1.3 Certificate status information access fees 80

9.1.4 Fees for other services 80

9.1.5 Refund policy 80

9.2 Financial responsibility 80

9.2.1 Liability insurance 80

9.2.2 Other assets 80

9.2.3 Insurance and guarantees for end entities 80

9.3 Information confidentiality 81

9.3.1 Scope of confidential information 81

9.3.2 Information beyond the scope 81

9.3.3 Responsibility to protect confidential information 82

9.4 Personal data protection 82

9.4.1 Privacy Plan 82

9.4.2 Information treated as private 83

9.4.3 Information not considered private 83

9.4.4 Responsibility to protect private information 83

9.4.4.1 Data Protection Officer 83

9.4.4.2 Processing activity record 83

9.4.4.3 Rights of interested parties 84

9.4.4.4 Cooperation with the authorities 84

9.4.4.5 Security violation notifications 84

9.4.5 Notice and consent to use private information 84

9.4.6 Disclosure pursuant to judicial or administrative process 85

9.4.7 Other disclosure circumstances 85

9.5 Intellectual property rights 85

9.5.1 Property rights in certificates 85

9.5.2 Property rights in certification practice 85

9.5.3 Property rights in names 85

9.5.4 Property rights in keys and key material 85

9.6 Obligations and guarantees 85

9.6.1 Obligations of the CA 85

9.6.1.1 Obligation of providing service 85

9.6.1.2 Reliable operation obligations 86

9.6.1.3 Identification obligations 87

9.6.1.4 User information obligations 87

9.6.1.5 Obligations regarding verification programmes 88

9.6.1.6 Obligations regarding legal regulation of the certification service 88

9.6.2 Registration Authority obligations 89

9.6.3 Holder obligations 89

9.6.4 Obligations of the relying parties 90

9.6.5 Obligations of other participants 91

9.7 Waiver of guarantees 91

9.8 Liability limitation 91

9.8.1 Certification Authority liabilities 91

9.8.2 Registration authority liabilities 92

9.8.3 Subscriber liabilities 92

9.8.4 Relying party liability 93

9.9 Compensation 94

9.10 Validity period 94

9.10.1 Term 94

9.10.2 Termination 94

9.10.3 Effects of termination 94

9.11 Individual notifications and communication with participants 94

9.12 Amendments to this document 94

9.12.1 Procedure for changes 94

9.12.2 Notification period and mechanism 95

9.12.3 Circumstances under which an OID must be changed 95

9.13 Complaints and dispute resolution 95

9.14 Applicable regulations 96

9.15 Compliance with applicable legislation 96

9.16 Various stipulations 97

9.16.1 Full agreement 97

9.16.2 Allocation 97

9.16.3 Severability 97

9.16.4 Compliance 97

9.16.5 Force Majeure 97

9.16.6 Other stipulations 97

10 ANNEX I. CAS CERTIFICATE PROFILES 99

10.1 ROOT CERTIFICATION AUTHORITIES 99

10.2 SUBORDINATE CERTIFICATION AUTHORITIES 101

10.2.1 CN subCAs=Izenpe.com 101

10.2.2 CN subCAs=ROOT CA QC IZENPE 107

10.2.3 CN subCAs=ROOT CA NQC IZENPE 110

1 Introduction

The Basque public authorities, as promoters of the Information Society, and in the endeavour to guarantee full incorporation of information and communication technologies into the economic and social activities of its citizens, has set up instruments permitting citizens to relate to the different administrations, bodies and companies with a view to guaranteeing data privacy and personal privacy and protecting their rights, always with the best possible security guarantees.

With these premises, the Basque Government and the Provincial Councils, through their respective IT companies established in June 2002 the commercial company "Ziurtapen eta Zerbitzu Enpresa- Empresa de Certificación y Servicios, IZENPE, S.A." (hereinafter, IZENPE)

IZENPE was constituted as the instrument or organisation to provide Basque public administration IT companies with management in their joint interest of electronic certification, proving itself to be an ideal means of simplifying citizen/administration relations.

Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and Regulation 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation 910/2014 as regards the establishment of the European digital identity framework contemplates the possibility of establishing oneself as a Qualified Trust Service Provider.

In this regard, IZENPE is established as a Qualified Trust Service Provider, depending on Basque Administrations, whose corporate purpose is:

- To foment the use and development of electronic government based on telecommunications networks and backed by guaranteed security, confidentiality, authenticity and irrevocability of transactions.
- As well as the provision of security, technical and administrative services in communications through electronic, computer and telematic techniques and media.

The identification mechanisms offered by Izenpe are stipulated by the Commission Regulation on Execution (EU) 2015/1502 dated 8 September, 2015, on setting specifications and minimum technical procedures for security levels for electronic identification methods as stipulated in article 8, section 3, of the European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market.

Moreover, in order to develop and effectively implement these services, Izenpe has established an information security system for processes related to trust services, as per standard ISO 27001.

IZENPE follows the guidelines of ETSI (European Telecommunications Standards Institute) standards for the issuance of qualified and non-qualified certificates, for the qualified signature validation service and for the issuance of time stamps. For secure server certificates (SSLs), the guides approved by CA/Browser Forum are also followed, available at www.cabforum.org.

The technical specifications (ETSI TS) defined in these standards set out the basic requirements regarding the management and certification practices of trust service providers issuing qualified and non-qualified certificates and time stamps within the legal framework of Regulation 910/2014 and Regulation 2024/1183, EN 319 411-1 for the issuance of certificates, EN 319 411-2 for the issuance of qualified certificates and EN 319 421 for the issuance of time stamps.

In compliance with ETSI EN 319 401, which requires that all end-user products and trust services be accessible, Izenpe works to guarantee that all citizens, especially those with some sort of disability and the elderly with relation with Izenpe, can access the information and electronic services on an equal basis, regardless of their personal circumstances, resources or knowledge. To this end, Izenpe shall bear ETSI EN 301 549 recommendations in mind.

In any event, any consultation regarding accessibility of Izenpe's website, its products or its services, may be made via email at info@izenpe.com, or the form available at www.izenpe.eus.

This Certification Practice Statement (CPS) is structured based on RFC 3647.

1.1 Purpose

IZENPE operates an Infrastructure with a view to providing the following qualified services:

a) Issue of qualified electronic signature certificates
b) Issue of qualified electronic stamp certificates
c) Issue of qualified website authentication electronic certificates
d) Issue of qualified electronic time stamp service

And the following non-qualified services:

a) Issue of non-qualified electronic signature certificates
b) Issue of non-qualified website authentication electronic certificates
c) Certified electronic delivery
d) Validation of electronic signatures
e) Validation of electronic stamps

In the scope of the present Certification Practice Statement and the *Specific policy for each certificate,* IZENPE issues the following types of certificates:

1.1.1 Hierarchy CA root 2007 (CN=Izenpe.com)

CITIZEN					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signatur type eIDAS**
B@K	HSM	NCP	1.3.6.1.4.1.14777.5.2.5	Low	Basic
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	Substantial (with Giltza)	Advanced
Certificate General Public	Cryptographic chip	QCP-n	eIDAS Profile 1.3.6.1.4.1.14777.2.18.1	High	Advanced
			Profile prior to eIDAS 1.3.6.1.4.1.14777.2.6	High	Qualified
Izenpe Mobile	APP container	NCP	1.3.6.1.4.1.14777.5.2.5.4	Substantial	n/a (the BAKQ is used to sign)
NQC pseudonym	Software	NCP	1.3.6.1.4.1.14777.5.2.7.2	Substantial	Advanced

ENTITY REPRESENTATIVE					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Entity representative	HSM	QCP-n	1.3.6.1.4.1.14777.2.14	Substantial (with Giltza)	Advanced
	Cryptographic chip	QCP-n	1.3.6.1.4.1.14777.2.12	High	Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.16	Substantial	Advanced

SPJ ENTITY REPRESENTATIVE

Brief description	Media	Policy identifier	Policy OID	eIDAS identification level	Signature type eIDAS
SPJ Entity Representative	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	Substantial (with Giltza)	Advanced
	Cryptographic chip	QCP-n	1.3.6.1.4.1.14777.2.13	High	Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.17	Substantial	Advanced

PROFESSIONAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Public Entity Staff	Cryptographic chip	QCP-n	1.3.6.1.4.1.14777.4.14.1	High	Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.4.14.2	Substantial	Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Substantial (with Giltza)	Advanced
Public Entity Staff with a pseudonym	Cryptographic chip	QCP-n	**Signature** 1.3.6.1.4.1.14777.4.13.1.1	High	Advanced
		NCP+	**Authentication** 1.3.6.1.4.1.14777.4.13.1.2	High	n/a
		n/a	**Encryption** 1.3.6.1.4.1.14777.4.13.1.3	High	n/a
Qualified corporate	Cryptographic chip	QCP-n	1.3.6.1.4.1.14777.2.19.1	High	Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.19.2	Substantial	Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Substantial (with Giltza)	Advanced
Non-qualified corporate	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a (not qualified)	Advanced
Public Entity Staff (pre- eIDAS)	Cryptographic chip	QCP public + SSCD	1.3.6.1.4.1.14777.4.1	n/a	Recognised

Recognised public corporate (pre-eIDAS)	Cryptographic chip	QCP public + SSCD	1.3.6.1.4.1.14777.4.2	n/a	Recognised
Not recognised public corporate (pre-eIDAS)	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a	Advanced
Recognised private corporate (pre-eIDAS)	Cryptographic chip	QCP public + SSCD	1.3.6.1.4.1.14777.2.2	n/a	Recognised
Unrecognised private corporate (pre-eIDAS)	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.5.2.2	n/a	Advanced

ENTITY SEAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Entity seal	Izenpe software container	QCP-l	1.3.6.1.4.1.14777.2.11	Substantial	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.2.20	Substantial	Advanced

ADMINISTRATION SEAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Administration stamp	Izenpe software container	QCP-l	1.3.6.1.4.1.14777.4.11.2	Substantial	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.4.11.3	Substantial	Advanced

SECURE SERVER (SSL/TLS)			
BRIEF DESCRIPTION	**MEDIA**	**POLICY IDENTIFIER**	**POLICY OID**
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.1.2.4
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.1.2.1
Qualified SSL	Software	QEVCP-w	1.3.6.1.4.1.14777.6.1.3

APPLICATION			
BRIEF DESCRIPTION	**MEDIA**	**POLICY IDENTIFIER**	**POLICY OID**
Application	Izenpe software container	NCP	1.3.6.1.4.1.14777.1.2.2

CODE SIGNATURE			
BRIEF DESCRIPTION	**MEDIA**	**POLICY IDENTIFIER**	**POLICY OID**
Code signature	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.1.3.1

IOT DEVICE			
BRIEF DESCRIPTION	**MEDIA**	**POLICY IDENTIFIER**	**POLICY OID**
Device	Software	NCP	1.3.6.1.4.1.14777.1.3.2

1.1.2 Hierarchy CA root 2020 qualified (CN=ROOT CA QC IZENPE)

CITIZEN						
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**		**Signature type eIDAS**
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.8.1.3		Substantial (with Giltza)	Advanced
Certificate General Public	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.8.1.1	High		Qualified

ENTITY REPRESENTATIVE						
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**		**Signature type eIDAS**
Entity representative	HSM	QCP-n	1.3.6.1.4.1.14777.8.3.3		Substantial (with Giltza)	Advanced
	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.8.3.1	High		Qualified
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.8.3.2	Substantial		Advanced

SPJ ENTITY REPRESENTATIVE						
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**		**Signature type eIDAS**
SPJ Entity Representative	HSM	QCP-n	1.3.6.1.4.1.14777.8.4.3		Substantial (with Giltza)	Advanced
	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.8.4.1	High		Qualified
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.8.4.2	Substantial		Advanced

PROFESSIONAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Public Entity Staff	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.9.1.1	High	Qualified
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.9.1.2	Substantial	Advanced

	HSM	QCP-n	1.3.6.1.4.1.14777.9.1.3		Substantial (with Giltza)	Advanced
Public Entity Staff with a pseudonym	Cryptographic chip	QCP-n-qscd	**Signature** 1.3.6.1.4.1.14777.9.2.1	High		Qualified
		NCP+	**Authentication** 1.3.6.1.4.1.14777.9.2.2	High		n/a
		n/a	**Encryption** 1.3.6.1.4.1.14777.9.2.3	High		n/a
Qualified corporate	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.8.2.1	High		Qualified
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.8.2.2	Substantial		Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.8.2.3		Substantial (with Giltza)	Advanced

ENTITY SEAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Entity seal	Izenpe software container	QCP-l	1.3.6.1.4.1.14777.8.5.2	Substantial	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.8.5.3	Substantial	Advanced

ADMINISTRATION SEAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Administration stamp	Izenpe software container	QCP-l	1.3.6.1.4.1.14777.9.3.2	Substantial	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.9.3.3	Substantial	Advanced

1.1.3 Hierarchy CA root 2020 non-qualified (CN=ROOT CA NQC IZENPE)

CITIZEN					
Brief description	Media	Policy identifier	Policy OID	eIDAS identification level	Signature type eIDAS
B@K	HSM	NCP	1.3.6.1.4.1.14777.11.1.2	Low	Basic
Mobile	APP container	NCP	1.3.6.1.4.1.14777.11.3.4	Substantial	n/a (the BAKQ is used to sign)
NQC pseudonym	Software	NCP	1.3.6.1.4.1.14777.11.2.2	Substantial	Advanced

PROFESSIONAL					
Brief description	Media	Policy identifier	Policy OID	eIDAS identification level	Signature type eIDAS
Non-qualified professional	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.11.4.2	n/a (not qualified)	Advanced

APPLICATION			
BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
Application	Izenpe software container	NCP	1.3.6.1.4.1.14777.12.1.2

IOT DEVICE			
BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
Device	Software	NCP	1.3.6.1.4.1.14777.12.2.2

INTERNAL SECURE SERVER (SSL/TLS)			
BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.14.1.2

1.1.4 Hierarchy CA root 2024 (CN=ROOT CA SSL IZENPE)

SAFE SERVER 2024			
BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.50.1.2
SSL 0V	Software	0VCP	1.3.6.1.4.1.14777.50.2.2
Qualified SSL	Software	QCP-w	1.3.6.1.4.1.14777.50.3.2

1.2 Document name and identification

This document is called "Izenpe's Certification Practice Statement" and internally, it shall be called by its acronym, "CPS."

This document does not bear on the individual aspects of the different certification practices and policies, the signature service on the server or the time stamp that Izenpe implements to provide trust services. These particularities are discussed in their pertinent documents, with this CPS acting as the general framework for application.

The different Particular Certification Policies shall prevail regarding the particular nature and referring to the types of certificates and/or services they address over what is set forth in the main body of this CPS.

Izenpe's Security Committee regularly reviews the risks to which the Organisation is exposed and approves necessary handling plans to guarantee security of the services defined in each one of the Certification Policies.

Conditions for use, limitations, liabilities, properties and all other information considered specific to each type of certificate are set forth in the Particular Certification Statements dependent upon this CPS.

These procedures are mainly based on regulations from the European Telecommunications Standards Institute (ETSI).

In order to be able to individually identify each type of certificate issued by IZENPE according to this Certification Practice Statement, an object identifier (OID) is assigned to each kind. These may be viewed in the profile document available at www.izenpe.com. Furthermore, according to the ETSI EN 319 412-5 definition, the following identifiers are included:

- QcCompliance: qualified certificate according to eIDAS
- QcSSCD: certificate issued on a qualified signature creation device
- QcRetentiodPeriod: documentation retention period
- QcPDS: path to conditions for use
- Qctype: indicates the signature type according to eIDAS (stamp, signature, web)

1.3 Participants in the Public Key Infrastructure (PKI)

The roles for administration and operation of the Certification Entity are listed below:

- Certification Authorities.
- Registration Authorities.
- Certificate Subscribers or Owners
- Relying Parties
- Other participants

1.3.1 Certification Authorities

IZENPE has the following certification authorities:

- CN = Izenpe.com
  - CA Citizens /Qualified Entities
  - CA Citizens /NON-Qualified Entities
  - CA AAPP NON-Qualified
  - CA AAPP Qualified
  - CA SSL EV
  - CA SSL EV 2018
- CN = ROOT CA QC IZENPE
  - CN= SUBCA QC IZENPE – TSA
  - CN= SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-PUBLIC ADMINISTRATION
  - CN= SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CITIZEN AND COMPANY
- CN= ROOT CA NQC IZENPE
  - CN= CA NQC IZENPE - PERTSONA FISIKOA-NATURAL PERSON
  - CN= CA NQC IZENPE - GAILUA-DEVICE
  - CN= CA NQC IZENPE - TEKNIKOA-TECHNICAL
  - CN= CA NQC IZENPE - SSL EZ PUBLIKOA-NON-PUBLIC SSL
- CN = ROOT CA SSL IZENPE 2024
  - CN= SUBCA SSL 2024

The profiles of each certificate are published at the following url https://www.izenpe.eus/contenidos/informacion/doc_juridica/es_def/adjuntos/Perfiles_de_Certificados.pdf.

1.3.2 Registration Entities

This Certification Practice Statement applies to the Registration Authorities used by IZENPE in procedures when issuing and managing certificates.

Registration Entities perform the tasks of identifying applicants, subscribers and owners of certificate keys, verifying the documentation accrediting the circumstances on the certificates, as well as validating and approving requests to issue, revoke and renew certificates.

IZENPE or the user entities with which IZENPE signs the corresponding legal instrument are the registration authorities.

1.3.3 Certificate Subscribers

A Certificate Subscriber may be an entity other than the Signatory when there is a relationship of representation or belonging to an Organisation, such that the latter is considered the Subscribing Entity, or when Electronic Stamp or Web Authentication Certificates are in question. Notwithstanding, each Particular Certification Policy Statement shall determine this possible separation between the roles of Signatory and Subscriber.

The Signatories are the individuals who retain sole use of the signature creation data associated with the Certificates of which they are Holders.

1.3.4 Trusting third parties

For the purposes of this Certification Practice Statement, the natural or legal persons who receive certificates and timestamps issued by IZENPE are third parties who trust in certificates and timestamps issued by IZENPE and, as such, are governed by the stipulations contained in this Certification Practice Statement when they decide to effectively trust the certificates or timestamps.

Third parties are understood to trust the certificates and timestamps in accordance with the use they make thereof in their relationships with subscribers.

When this use has been made, special consideration shall be given to the fact that the party has made no declarations expressing lack of reliance on the certificates or digital signatures attached to the messages, and therefore establishing that the party did effectively rely on the certificates and digital signatures, provided that the certificates were valid, signatures were created during the validity period of the certificates and all other requirements determining the trustworthiness of a certificate have been met.

Third parties shall exercise due diligence in using each type of certificate and timestamp and shall keep to the principle of good faith and loyalty, abstaining from any fraudulent or neglectful conduct meant to repudiate messages issued within the level of trust attached to the category of certificate or timestamp.

1.3.5 Other participants

Izenpe is the Time Stamp Authority when it provides the Trust Service of electronic time stamp creation under the pertinent Particular Practice Statement.

1.4 Certificate uses

The permitted and prohibited usages of the certificates issued by IZENPE are described below.

1.4.1 Appropriate certificate uses

Qualified certificates

Qualified electronic signature certificates guarantee the identity of the subscriber and the private key holder.

Electronic signature qualified certificates can also be used, if so defined in the corresponding certificate type, to sign authentication messages, in particular SSL or TLS client challenges, encrypted without key recovery or others. This digital signature guarantees the identity of the signature certificate subscriber.

Additionally, said certificates can provide support for different kinds of authentication and advanced electronic signatures, used along with IT applications that reliably protect the private signature key.

The electronic stamp certificate links validation data from a stamp with the legal person and confirms the name of that person. They generate electronic stamps, which act as proof that an electronic document was issued by a legal person, providing certainty as to the origin and integrity of the document.
The electronic seal certificates issued by Izenpe meet requirements from Annex III in eIDAS1, elDAS2 in order to be considered as qualified.

Website authentication certificates authenticate a website and link the website to the natural or legal person to whom the certificate was issued. The web certificates issued by Izenpe meet requirements from Annex IV in eIDAS1 and elDAS2 in order to be considered as qualified.

Electronic stamp certificates are issued to public administrations for the identification of the body and the electronic sealing of documents, as provided for in Royal Decree 203/2021, of 30 March, which approves the Regulations for the action and operation of the public sector by electronic means

Izenpe's qualified certificates heed to technical standard ETSI EN 319 411-2.

Non-qualified certificate

Non-qualified certificates do not reliably guarantee the identity of the subscriber and, when appropriate, the private key holder; in any event, if used to sign,

they should also be used in conjunction with a reasonably secure signature generation mechanism. In this case, it shall not be equal to the signatory's handwritten signature.

Unqualified certificates can also be used, if so defined in the corresponding certificate type, to sign authentication messages, in particular SSL or TLS client challenges, encrypted without key recovery or others.

Izenpe's qualified certificates comply with technical standard ETSI EN 319 411-1.

Scope of use of certificates

There are two scenarios that illustrate certificate usage:

- Certificates issued by IZENPE to the general public are used by subscribers or, where applicable, key owners to conduct electronic transactions with Public Entity Users and public or private institutions that have accepted the use of the certificate system.

  Details on the scope of usage for each certificate are provided in the *Specific documentation for each certificate*.

- Certificates issued by IZENPE and those requested by User Entities will be used within the scope of their characteristics as a natural or legal person, according to eIDAS specifications. However, key owners may also employ these certificates for other uses provided that they respect the usage limitations set forth in the paragraph above.

  Details on the scope of usage for each certificate are provided in the *Specific documentation for each certificate*.

Test certificate

For reasons of security in legal traffic, test certificates will be issued, by default, with the following identification data:

National Identity Document Number (DNI): 0000000T

Foreigner Identity Number (NIE): X0000000T, Y0000000R, Z0000000W

Name: Name

Surname One: ApellidoUno

Second Surname: ApellidoDos

If necessary, test certificates may be generated with other data, in which case the competent supervisory body will be informed in advance.

Certificates issued with this data will only be used for the purpose of testing applications in the Basque public sector.

1.4.2 Prohibited certificate uses

The certificates must be used for their own function and established purpose, and may not be used in other functions and for other purposes.

Furthermore, the certificates must only be used according to governing laws.

The certificates are not designed, cannot be used and are not authorised for use or resale as equipment for monitoring hazardous situations or for uses requiring fail-safe performance, such as the operation of nuclear facilities, airborne navigation or communications systems, or weapons control systems, where failure could directly lead to death, personal injury or severe environmental damage.

1.5 Policy administration

1.5.1 Entity responsible for managing documentation

IZENPE, with corporate headquarters at Beato Tomás de Zumárraga 71, 1rst, with Tax ID Number A-01337260, is the Certification Authority that issues the certificates to which this Certification Practice Statement is applicable.

1.5.2 Contact details

Provider name	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.
Address	c/ Beato Tomás de Zumárraga, no. 71, 1rst floor. 01008 Vitoria-Gasteiz
Email	izenpe@izenpe.eus
Telephone number	900 840 123

To report security issues, such as suspicion of compromised keys, improper use of certificates, fraud or other issues, email seguridad@izenpe.eus

See channel “4.9.3 Processing revocation requests” to discover channels for revocation.

1.5.3 In charge of adapting the Certificate Practice Statement

The IZENPE Security Committee is the body in charge of approving this Certificate Practice Statement and any possible changes to it.

1.5.4 Procedure to approve the Certificate Practice Statement

The final changes made to this document are approved by the IZENPE Security Committee once it is determined that they meet the set requirements.

1.6 Definitions and acronyms

1.6.1 Definitions

- **Data Protection Agency (DPA)**: a body under public law, with its own legal personality and unlimited public and private legal capacity, which acts fully independently of the public administrations in the performance of its tasks and whose main purpose is to ensure compliance with the legislation on data protection and ensure its application.
- **Certification Authority (CA):** the Certification Authority is the entity that automatically issues the necessary certificates requested by the Registration Authority following confirmation from the Local Registration Authority.
- **Registration Authority (RA):** the responsibility of the registration authority is to identify applicants, subscribers and holders of certificate keys, verify the documentation accrediting the circumstances appearing in the certificates, and validate and approve requests to issue, revoke and renew certificates. The user must contact the registration authority to request a certificate with the guarantee of the certification authority associated with the registration authority.
- **Timestamping Authority (TSA)**: authority that issues timestamp tokens
- **Certificate**: an electronic document signed electronically by a Certification Service Provider who links signature verification data to a signatory and confirms his or her identity.
- **Root Certificate:** a certificate whose subscriber is a Certification Authority belonging to the IZENPE hierarchy, and which contains the CA's Signature Verification Data signed with the CA's Signature Creation Data as Certification Service Provider. The IZENPE issuing entities form a hierarchy by which there is one common root entity for any type of certificate and several subordinate entities for the different types of certificates.
- **Qualified certificate:** electronic certificates issued by a Certification Service Provider that complies with the requirements set forth in eIDAS1 and elDAS2 with regard to verification of the identity and other details of applicants and to the reliability and guarantees of the certification services rendered.
- **Non-certified certificates:** these are ordinary certificates, without the legal status of qualified certificates.
- **Key:** sequence of symbols used for encrypting and decrypting operations.
- **Confidentiality:** confidentiality is the capacity to keep an electronic document inaccessible to all users except to a specific list of individuals.

By doing so, communications are not disclosed to others and documents can only be read by the indicated recipient.

- **Cryptography**: cryptography is a branch of mathematics based on the transformation of legible data into data that cannot be read directly, e.g., information that must be decoded in order to be read.
- **Signature creation data (Private Key):** a private key is one single secret number that is held by only one person in such a way that the person can be identified by his or her private key. This key is asymmetric to the person's public key. One key can verify and decrypt what the other has signed or encrypted.
- **Signature verification data (Private Key):** a public key is one single number held by only one person, but as opposed to a private key, it is published. It is linked with a private key through mathematical methods and is used to encrypt and verify digital signatures.
- **Certification Practice Statement (CPD):** statement which IZENPE makes easily available through electronic means at no cost. A security document which details, within the framework and provisions of eIDAS, the obligations that Certification Service Providers pledge to undertake with regard to the management of signature creation and verification of data and of electronic certificates; conditions applicable to the application, issuance, use and validity of certificates; technical and organisational security measures; profiles and information mechanisms on certificate validity; and, where applicable, the procedures for coordinating with the corresponding public registers to allow the immediate exchange of information concerning the validity of the powers indicated in the certificates and which must necessarily be included in the registers.
- **Certificate Directory:** repository of information that conforms to standard X.500 of the ITU-T. Izenpe keeps an updated directory of certificates which includes all of the certificates issued.
- **Qualified signature creation device:** device to create electronic signatures that meets the requirements listed in Annex II from eIDAS.
- **Electronic signature:** the data in electronic format annexed to other electronic data or logically associated with them, used by the signatory to sign.
- **Advanced electronic signature:** electronic signature that meets requirements stipulated by article 26 of eIDAS1 and eIDAS2.
- **Qualified electronic signature:** advanced electronic signature created with a qualified electronic signature creation device based on a qualified electronic signature certificate.
- **Signatory**: the person who holds a signature creation device and who acts on his or her own behalf or on behalf of an individual or legal entity.
- **Hash or digital fingerprint:** a fixed-length output obtained by applying a hash function to a message, and which is associated only with the initial data.

- **HSM (hardware security module):** hardware-based security device that generates and protects cryptographic keys.
- **Public Key Infrastructure (PKI, Public Key Infrastructure):** a PKI determines which entities form part of a certification system, the roles they play, the norms and protocols that must be followed in order to operate within the system, the way in which digital information is encoded and transmitted, and the information contained in the objects and documents managed by the infrastructure. All of this is based on Public Key technology (two keys).
- **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons regarding personal data processing and the free circulation of these data, repealing Directive 95/46/EC (GDPR).** A European Regulation whose purpose is, in respect of personal data processing, to guarantee and protect the public freedoms and fundamental rights of natural persons, and especially their honour and personal and family privacy.
- **Certificate Revocation Lists (CRLs):** the CRL is a list of the revoked or suspended certificates which IZENPE issues immediately when a certificate is revoked. A permanent Web service is also available to consult incremental updates of certificates revoked by IZENPE. As for publication of Certificate Revocation Lists, certificate users and subscribers are ensured secure and fast access.
- **Certificate serial number:** a whole unique number unmistakably associated with a certificate issued by any certification service provider.
- **OCSP (Online Certificate Status Protocol):** a computer protocol used to determine the status of a digital certificate.
- **OID (Object Identifier):** a unique sequence of non-negative integers separated by dots, which can be assigned to registered objects and that are unique from the rest of OIDs.
- **PIN (Personal Identification Number):** A sequence of characters known only to the subject who has access to a resource protected by this mechanism.
- **Certification Policy:** an annex to the Certification Practice Statement which covers the scope of application, the technical characteristics of the different types of certificates, the rules indicating the procedures to be followed in rendering certification services, and the terms of use.
- **Key holders:** the natural persons who own or are responsible for safeguarding the digital signature and decryption keys.
- **Qualified trust service provider (TSP):** trust service provider that provides one of several qualified trust services according to eIDAS and to whom the supervision authority has granted qualification

- **Advanced Verification Service:** a service that enables the User Entity to benefit from the use of certificates issued by IZENPE by verifying the status of certificates based on the OCSP (Online Certificate Status Protocol).
- **Publication Service:** the service that publishes all the documents associated with the certification system that should be made available to certificate users.
- **Time-Stamping Service:** this service provides user entities with proof of the existence of a certain piece of information at a particular time.
- **Secure Server:** a secure server is a Web server that uses encryption to safely transmit data from end to end. In order to perform this operation, the server must hold a valid certificate.
- **Certificate applicant:** the individual who requests the issuance of a certificate in his or her own name or on behalf of an organisation.
- **SSL (Secure Socket Layer):** a protocol that allows encrypted data to be transmitted between an Internet browser and a server.
- **Certificate Subscriber:** the individual whose personal identity is linked to the electronically signed data by means of a Public Key certified by the Certification Service Provider.
- **Cryptographic card:** a card considered to be a Secure Signature Creation Device used by the Subscriber to: store private digital signature and encryption keys, generate electronic signatures and decrypt data messages.
- **Relying parties:** the natural or legal persons who are issued certificates by IZENPE. Upon making the decision to effectively rely on the certificates, relying parties are thus governed by the stipulations contained in this Certification Practice Statement.
- **Certificate users:** entities that are certificate end users are individuals and organisations that receive digital certificate issuance, management and user services.
- **Stamp creator:** legal person who creates an electronic stamp
- **Electronic stamp:** data in electronic format attached to other data in electronic format, or logically associated with them, to guarantee their origin and integrity.
- **Advanced electronic stamp**: electronic stamp that meets requirements stipulated by article 36 of eIDAS.
- **Qualified electronic signature:** advanced signature created with a qualified electronic signature creation device based on a qualified electronic signature certificate.
- **Electronic stamp creation data:** unique data that the electronic stamp creator uses to create it.

- **Electronic stamp certificate:** electronic statement that links validation data from a stamp with the legal person and confirms the name of that person.
- **Qualified electronic stamp certificate:** electronic stamp certificate issued by a qualified trust service provider that meets the requirements established in Annex III of eIDAS.
- **Electronic stamp creation device**: IT equipment or programme configured to be used to create an electronic stamp.
- **Qualified electronic stamp creation device:** device to create electronic stamps that meet mutatis mutandis the requirements listed in Annex II from eIDAS.
- **Electronic time stamp:** electronic-format data linking other electronic format data to a specific moment in time, providing proof that these last data existed at that time.
- **Qualified electronic time stamp:** electronic time stamp that meets requirements established in article 42 of eIDAS.

1.6.2 Acronyms

ARL: Authority Revocation List

CA: Certification Authorities

CN: Common Name

CRL: Certificate Revocation List

DN: Distinguished Name

DPC: Certification Practices Statement

QSCD: Qualified Signature Creation Device

ETSI: European Telecommunications Standards Institute

GN: Given name of a certificate holder

HSM: Hardware Security Module

LRA: Local Registration Authority

OCSP: Online Certificate Status Protocol (repository of revoked certificates based on a specific time and date)

OID: Object Identifier

PIN: Personal Identification Number

PKCS: Public Key Cryptography Standards (PKI standards developed by RSA Laboratories)

PKI: Public Key Infrastructure PSC:

PSC: Trust Services Provider

RA: Local Registration Authority

SSL Secure Socket Layer

TSA: Time Stamp Authority Server

eIDAS1 European Parliament and Council Regulation (EU) Num. 910/2014 dated 23 July 2014, on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC.

eIDAS2: Regulation 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation 910/2014 as regards the establishment of the European digital identity framework

2 Publication and supervisors of information repository

2.1 Information repository

IZENPE has a public information repository at **www.izenpe.com** available 24 hours a day, 7 days a week.

2.2 Publication of certification information

IZENPE guarantees the availability of the CPS, specific certificate policies and terms and conditions for use of certificates at www.izenpe.eus.

IZENPE guarantees secure, fast and free access to information on the certificate status to users and subscribers. This access bears two forms:

- Online consultation (OCSP): Izenpe facilitates the use of a fast and secure service to consult the status of the issued certificates, available to third parties who trust the certificates.
- Offline consultation (CRL): by publication of the Revoked Certificate Lists (RCLs).

Izenpe maintains test websites for software vendors to test their products with SSL/TLS certificates in production environment. Izenpe holds different websites with at least one final living, expired and revoked certificate. See the route of each one of them in the Specific Policy.

2.2.1 Publication and notification policy

IZENPE shall notify users of changes in specifications or in the terms and conditions of services via www.izenpe.com. IZENPE may establish additional communication channels for specific situations.

The CPS and Terms and Conditions for Use shall be kept at www.izenpe.com indefinitely, both the current versions and all previous versions.

2.2.2 Items not published in the Certification Practice Statement

The list of components, subcomponents and elements that exist but due to their confidential nature are not disclosed to the public are included in section “9.3.2 Information beyond the scope” of the present Certification Practice Statement.

2.3 Frequency of publication

The Certificate Practice Statement is published as soon as it is approved if no changes have been made in the annual review. Changes to the Certification Practice Statement are governed by the provisions of this document.

Information on the status of the certificates is published as established in sections “4.9.7 below” and “4.9.10 Online revocation checking requisites” in this document.

2.4 Controlling access to the repository

IZENPE allows access to reading the information published in its repository and controls are put in place to keep unauthorised individuals from adding, changing or deleting the registers provided by this service to protect the integrity and authenticity of the documents.

IZENPE uses reliable systems to access the information repository, so that:

- Only authorised persons can make annotations and modifications.
- The authenticity of the information can be verified.
- The certificates are available for consultation.
- Any technical changes affecting security requirements can be detected.

3 Names

3.1.1 Types of names

All end-entity user certificates contain a given name in the Subject Name field.

The attributes specified in the differentiated name in the subject field are contained in the section corresponding to the certificate profile.

The authenticated value in the *Common Name* field is the name of the subscriber, and if applicable, the key owner.

Additionally, the s*ubjectAltName* field is also used on occasion to place a name that can be used to identify the subject, but different from the name that appears in the Subject Name field.

Issuer

This field contains the identification of IZENPE, the Certification Authority that signed and issued the certificate.

The field cannot be left blank and must contain a differentiated number (DN) composed of a set of attributes, consistent in number or tags and an associated value.

The issuer field of the subordinate CAs coincides with the subject field of the CA that has issued the certificates.

Subject

This field contains the identification of the subscriber or owner of the certificate issued by IZENPE (the CA identified in the Issuer field).

The field may not be left blank and must contain a distinguished name (DN). A distinguished name is a set of attributes consisting of a name or label and an associated value.

The *Specific documentation for each certificate* establishes the detailed profile for each certificate.

3.1.2 Meaning of names

All distinguished names (DNs) in the Subject Name field are meaningful. The description of the attributes associated with the Certificate Subscriber is legible to humans (see section 7.1.4 Format of names in this document).

3.1.3 Pseudonyms

Each Particular Certification Policy Statement will determine this aspect for Certificates issued under said policies.

3.1.4 Rules for interpreting name formats

The subject and name of the issuer of a certificate identifies the person (natural or legal) or device and must have meaning in the sense that the RA holds proof of the association between these names or pseudonyms and the entities to which they are assigned. The names must be truthful. This does not exclude pseudonym certificates defined in section “3.1.5 Uniqueness of names”.

3.1.5 Uniqueness of names

Subscriber names and, where applicable, key owner names are unique for each type of certificate. In the common name (CN) all uniqueness and space requirements in the name spaces must be met. Izenpe may issue pseudonym certificates, but they cannot be CA or subordinate CA certificates. Details on the profile of each certificate type may be viewed at www.izenpe.eus.

3.1.6 Resolving conflicts relating to names and processing trademarks

Certificate applicants must not include names in applications for issuance that may involve infringement of third-party rights by the future subscriber.

IZENPE does not verify whether a certificate applicant has any rights over the name appearing in a certificate application. Izenpe does not act as an arbitrator or mediator, nor does it otherwise resolve any dispute concerning the ownership of names of persons or organisations or domain names.

IZENPE reserves the right to reject any certificate application because of a name claim dispute.

3.2 Validation of identity

3.2.1 Methods for proving possession of the private key

When a pair of keys is generated,

- By a Registration Authority and the keys are stored on a cryptographic card, proof of possession of the private key is by virtue of the trusted procedure of delivery and acceptance of the cryptographic card and of the corresponding certificate and key pair stored within.
- By a Registration Authority and the keys are stored in a HSM, the key owner, possession of the private key is demonstrated by virtue of the reliable custody of the HSM and the trusted procedure for exclusive access to keys by the subscriber.
- By the certificate key owner, possession of the private key is demonstrated by the proper use of the certificate.
- For the browser's key container, possession of the private key is shown by the reliable procedure of generating the key pair and issuing the certificate.
- For the mobile device key container, possession of the private key is shown by the reliable procedure of generating the key pair and issuing the certificate.

3.2.2 Authentication of the Organisation Identity

Izenpe is based on specifications from Commission Regulation on Execution (EU) 2015/1502 dated 8 September, 2015, on setting specifications and minimum technical procedures for security levels for electronic identification methods as stipulated in article 8, section 3, of the European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market. See corresponding Policy.

3.2.3 Authentication of the identity of the natural person applicant

Izenpe is based on specifications from Commission Regulation on Execution (EU) 2015/1502 dated 8 September, 2015, on setting specifications and minimum technical procedures for security levels for electronic identification methods as stipulated in article 8, section 3, of the European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market. See corresponding Policy.

3.2.4 Unverified subscriber information

Each Particular Certification Policy Statement will determine this aspect for Certificates issued under said policies.

3.2.5 Authority validation

Each Particular Certification Policy Statement will determine this aspect for Certificates issued under said policies.

3.2.6 Interoperability criteria

There are no interactivity relations with Certification Authorities outside FNMT-RCM.

3.3 Identification and authentication for requests to reissue keys

Conditions for identification and authentication of a re-issue application are indicated in the corresponding policy.

3.3.1 Routine renewal

Each Particular Certification Policy Statement will determine this aspect for Certificates issued under said policies.

3.3.2 Renewal after revocation

The Certificate renewal process after revocation of the certificate is the same as the process followed for the initial issue of said certificate.

3.4 Identification and authentication for revocation requests

Conditions for identification and authentication of a revocation application are indicated in the corresponding policy.

4 Operative requisites for the certificates' life cycle

This Certificate Practice Statement regulates the common operative requisites for the issued certificates. In the event that Izenpe performs cross certification with an external CA, said CA shall be required to comply with all requirements defined in this Certification Practice Statement and related certificate policies.

The specific regulation for each type of certificate may be consulted in the corresponding policy.

4.1 Certificate application

A new *Issue Application* will not be necessary for issues made as a result of a revocation due to a technical failure in the issuance and/or distribution of a certificate or associated documentation.

They are collected exactly, (within the technical limits established in the certificate content) in regard to the identifying information for each type of certificate. See *Specific policy for each certificate*.

4.1.1 Verification of application

Prior to issuing the certificate, IZENPE will check the data in the application according to the corresponding Certificate policy.

4.1.2 Signing up process and responsibilities.

Identification and accreditation tasks for the information on the certificate, as well as validation and approval of applications for issue, revocation and renewal of certificates shall be performed by own Registration Authorities or user entities with whom Izenpe enters into the corresponding legal instrument. The latter shall undertake the following obligations:

- To verify the identity and other personal circumstances of the applicant, subscriber or key holder on the certificates, or that are relevant for the purpose of the certificates, as per these procedures.
- Save all information and documentation regarding certificates for which it manages the issue, renewal, revocation or reactivation.
- To notify IZENPE of certificate revocation requests with due diligence and in a swift and reliable manner.
- To allow IZENPE access to its procedure's archives and audit logs in order to perform its functions and maintain the necessary information.

- To inform IZENPE of all issuance, renewal, reactivation requests and any other aspects related to the certificates issued by IZENPE.
- Verify, with due diligence, the reasons for revocation that may affect the validity of the certificates.
- To comply with the procedures established by IZENPE and with the current legislation in this area, in its management operations related to the issuance, renewal and revocation of certificates.
- In the event that the certificate type requires doing so, take on the role of making electronic signature technical creation and verification procedures available to the subscriber and/or key owner.

4.2 Processing applications

4.2.1 Carrying out identification and authentication functions

It is IZENPE's responsibility to identify the subscriber properly. This process must be carried out prior to issuing the certificate and no more than one month may elapse between the two processes.

In any event, users should refer to the Specific documentation in the *specific Policy for each certificate* for details regarding each one.

4.2.2 Approve or deny applications

Once the certificate has been requested, the RA should verify the information provided by the applicant, including validation of the subscriber identity.

If the information is not correct, the RA will deny the request and contact the applicant to explain why. If it is correct, the certificate will be issued.

When the application is for a certificate that includes a domain name to authenticate a server, Izenpe shall examine the authorised CA register, CAA, according to RFC 6844, and if the CAAs are present but do not allow Izenpe to issue the certificates because the server is not registered, Izenpe will not issue the certificate but will allow applicants to make another request after Izenpe has resolved the incident.

In any event, users should refer to the Specific documentation in the *specific Policy for each certificate* for details regarding each one.

4.2.3 Application processing time

Each Particular Certification Policy Statement will determine this aspect for Certificates issued under said policies.

4.3 Certificate issuance

All applications must be fully approved before certificates can be issued. IZENPE shall issue the certificate and deliver it according to terms in its Certificate Policy

corresponding Furthermore, Izenpe shall deliver the unblock codes to the owner when Izenpe generates the keys.

If the applicant has not received the certificate within 1 month of applying for issue, they should contact IZENPE.

4.3.1 CA actions during issuance

See details for each type of certificate in the *Specific policy for each certificate.*

4.3.2 Notification to the issuance subscriber

IZENPE notifies the subscriber about the certificate emission.

4.4 Certificate acceptance

The acceptance of a certificate constitutes the subscriber's acceptance of the terms and conditions of the contract which determines the rights and obligations of IZENPE and the subscriber's understanding of the provisions of this Certification Practice Statement, which governs the technical and operational aspects of the digital certification services provided by IZENPE.

The subscriber/key owner has 15 days from when the certificate has been delivered to ensure that it functions properly and, if necessary, return it to Izenpe.

If the return is due to functional defects for technical reasons (including: improper certificate format operation, programme compatibility problems, technical error in the certificate, etc.) or due to errors in the data contained in the certificate, IZENPE shall revoke the issued certificate and shall issue a new certificate.

4.4.1 Certificate acceptance process

In signing the certificate application document, one also accepts the terms and conditions for use, available at www.izenpe.com.

4.4.2 Publication of the certificate by the CA

Once the certificate has been accepted by the subscriber and generated, the certificate will be published in Izenpe's internal certificate repositories. Anyone may access information on the certificate's status by consulting the VA or the CRL.

4.4.3 Notification of certificate issuance by the CA and other entities

Secure Server certificates (SSL) are published in the Certificate Transparency Log Server (CT), based on Google's policy. The rest of certificates are not notified to any other entity.

4.5 Pair of keys and uses of the certificate

4.5.1 Subscriber's private key and use of the certificate

The subscriber who has custody of the keys,

- Will guarantee the proper usage and maintenance of certificate media storage.
- Will make proper use of the certificate and in particular, comply with the usage limitations thereto.
- Will diligently safeguard the private key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of the Certification Practice Statement.
- Will notify IZENPE and any other person the subscriber thinks might rely on the certificate without any reasonable delay if any of the following occur:
    - Loss, theft or potential compromise of the private key.
    - Loss of control over the private key, due to compromise of activation data (for example, the cryptographic device PIN) or for any other reason.
    - Inaccuracies or changes to the certificate of which the subscriber is aware or may be aware, urging that the certificate be revoked when said modification is a reason for it to be revoked.
- Will cease using the private key at the end of the certificate validity period.
- Will transfer specific obligations to key owners.
- Will refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from the Certification Authority.
- Will refrain from intentionally compromising the security of certification services.
- Will refrain from using the private keys corresponding to the public keys included in the certificates for the purpose of signing a certificate as if performing the function of a Certification Authority.
- Subscribers of qualified certificates who generate digital signatures using the private key corresponding to the public key listed in the certificate must acknowledge in the appropriate legal instrument that such electronic signatures are equivalent to handwritten signatures, provided that a cryptographic device is used, pursuant to indications from eIDAS.

The subscriber whose keys are hosted on Izenpe,

- Will make proper use of the certificate and in particular, comply with the usage limitations thereto.

- Will diligently safeguard the private key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of the Certification Practice Statement.
- Will notify IZENPE and any other person the subscriber thinks might rely on the certificate without any reasonable delay if any of the following occur:
    - Control over the subscriber's private key has been lost due to compromise of activation data or for any other reason.
    - Inaccuracies or changes to the certificate of which the subscriber is aware or may be aware, urging that the certificate be revoked when said modification is a reason for it to be revoked.
- Will cease using the private key at the end of the certificate validity period.
- Shall accept the obligations stipulated in this Certification Practice Statement.
- Will refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from the Certification Authority.
- Will refrain from intentionally compromising the security of certification services.
- Subscribers of qualified certificates who generate digital signatures using the private key corresponding to the public key listed in the certificate must acknowledge in the appropriate legal instrument that such electronic signatures are equivalent to handwritten signatures, provided that a qualified signature creation device is used, pursuant to eIDAS.

4.5.2 Use of the public key and the certificate by relying parties

The certificate verification user undertakes to:

- Independently ensure that the certificate is appropriate for its intended use.
- Be aware of the conditions for using the certificates in compliance with what is set forth in the Certificate Practice Statement.
- Verify the validity or revocation of issued certificates, to which end the user shall use information on the status of the certificates.
- Verify all certificates in the certificate hierarchy, before trusting the digital signature or any of the certificates in the hierarchy.
- Bear in mind any limitation in the use of the certificate, regardless of whether this is found in the very certificate itself or in the verifying contract.
- Bear in mind any precaution stipulated in a contract or other instrument, regardless of its legal nature.

- Notify any anomalous circumstance or situation regarding the certificate that may be deemed as a cause to revoke it.
- Refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from IZENPE.
- Refrain from intentionally compromising the security of certification services.
- Recognise that said electronic signatures are equivalent to handwritten signatures pursuant to eIDAS1 and elDAS2.

4.6 Certificate revocation

Certificate renewal consists of issuing a new certificate to the subscriber without changing any subscriber (or other participant) information, or any other information appearing on the certificate. Depending on the certificate type, the validity period may be different. Issuance costs are stipulated at www.izenpe.com. Keys may be maintained in the cases stipulated according to the Specific certificate policy.

4.6.1 Circumstances for certificate renewal

Izenpe makes reasonable efforts to notify subscribers as to the certificate's next expiration. Notification normally takes place during the 60 days prior to certificate expiration.

4.6.2 Who may apply for renewal

Any subscriber can ask for their certificate to be renewed if they meet the circumstances described in the Specific certificate policy. Izenpe does not automatically renew any certificate.

4.6.3 Processing certificate renewal requests

The subscriber can contact IZENPE and request its renewal. IZENPE will inform you how to formalise your application. Guidelines from the corresponding Certificate policy will be used.

4.6.4 Notification to the subscriber

The same notification process as for new certificate applications should be used.

4.6.5 Renewed certificate acceptance procedure

The same notification process as for new certificate applications should be used.

4.6.6 Publishing the certificate

Once the certificate has been renewed, the new certificate shall be published in the same internal repository as the new certificates.

4.6.7 Notifying other entities

As indicated in point 4.4.3.

4.7 Renewal with certificate key regeneration

The "re-key" process consists of creating a new certificate with a different public key (and serial number) while the subject content from the old certificate is kept. The new certificate will contain validity information and a new key pair but will keep the same subject.

The keys will be renewed during the certificate renewal pursuant to the Specific certificate policy.

4.7.1 Circumstances to regenerate certificate keys

Certificate key regeneration shall take place as part of certificate renewal, pursuant to section 3.2 of the CPS. Certificate keys may also be regenerated when compromised.

4.7.2 Who can apply

Izenpe may regenerate CA certificate keys, pursuant to the CA or subCA generation ceremony document. Izenpe may regenerate VA and TSA service certificate keys pursuant to internal procedure.

Any subscriber can ask for their certificate to be renewed if they meet the circumstances described in the Specific certificate policy.

4.7.3 Processing renewal applications with key regeneration

The subscriber can contact IZENPE and request its renewal. IZENPE will inform you how to formalise your application. Guidelines from the corresponding Certificate policy will be used.

4.7.4 Notification to the subscriber

The same notification process as for new certificate applications should be used.

4.7.5 Renewed certificate acceptance procedure

The same notification process as for new certificate applications should be used.

4.7.6 Publishing the certificate

Once the certificate has been renewed, the new certificate can be published in the certificate repositories considered necessary.

4.7.7 Notifying other entities

As indicated in point 4.4.3.

4.8 Modification of the certificate

When necessary to modify any information on the certificate, IZENPE will revoke the certificate and issue a new one.

4.8.1 Circumstances for certificate modification

Modification is not stipulated.

4.8.2 Who may apply for certificate modification?

Modification is not stipulated.

4.8.3 Processing of certificate modification applications

Modification is not stipulated.

4.8.4 Notification of certificate modification

Modification is not stipulated.

4.8.5 Conduct constituting acceptance of the certificate modification

Modification is not stipulated.

4.8.6 Publication of the modified certificate

Modification is not stipulated.

4.8.7 Notification of certificate modification to other entities

Modification is not stipulated.

4.9 Revocation

4.9.1 Circumstances for revocation

IZENPE will revoke certificates if any of the following events occur:

- A revocation request is made by the signatory, the natural or legal person represented by the signatory, an authorised third party, or a natural person who applied for a digital certificate for a legal person.

- The signature creation data of the signatory or the certification service provider has been compromised or if the signatory or a third party has misused the data.
- When a legal or administrative order has been issued to this effect.
- The death or termination of the signatory's legal personhood, death or termination of the legal personhood represented by the signatory, total or partial unforeseeable incapacity of the signatory or person represented by the signatory, termination of the representation, dissolution of the legal personhood represented, change in the circumstances of the safekeeping or use of the signature creation data included in the certificates issued to a legal person.
- IZENPE terminates its activity, except in cases where the signatory has given his or her consent for electronic certificate management processes to be transferred to another certification service provider.
- Change in the data supplied in order to obtain the certificate or modification in the circumstances verified for certificate issuance.
- The certificate is lost, stolen or rendered useless due to damage to the certificate media, or when the support has been changed to another support not envisaged in the certification policy.
- One of the parties breaches its obligations.
- An error is detected in the certificate issuance procedure, either because one of the prerequisites has not been satisfied or due to technical problems during the certificate issuance process.
- There is a potential threat to the security of the systems and the reliability of certificates issued by IZENPE for reasons other than the compromise of signature creation data.
- Technical failure in the issuance and/or distribution of certificates or associated documentation.
- Three months have elapsed from the time the certification was requested to the time it is collected.
- If IZENPE receives an application for issuance of a certificate, and a valid certificate of the same class and uniqueness already exists, the valid certificate will be revoked upon revocation request from the applicant.

4.9.2 Who can request revocation

The revocation of the certificate may be requested by the following,

- The subscriber.
- Legal Representative of the subscribing entity or authorised third party.
- Staff Manager or authorised third party.
- The applicant.

- Izenpe, in the cases for technical reasons set forth in this document.

4.9.3 Processing revocation requests

The revocation applicant shall process the *Revocation Application* before IZENPE. If revocation is requested by someone other than the applicant, subscriber or key owner, either before or concurrent with revocation, IZENPE shall inform the certificate key owner and subscriber of the revocation of its certificate and specify the reason for revocation.

The applicant may revoke the certificate through the following channels,

- In person before,
  - At Izenpe, requesting a prior appointment at www.izenpe.com
  - Or to the subscribing organisation with which Izenpe has signed the relevant legal instrument.
- Online, at the website www.izenpe.com
- By email, sending the revocation request form to izenpe@izenpe.eus signed with a qualified certificate

The authenticated revocation request, as well as the information justifying the revocation, is registered and archived.

4.9.4 Grace period for the revocation request

There is no grace period associated with this process, as revocation takes place immediately upon verified receipt of the revocation request.

4.9.5 CA deadline to process the revocation

Once instructions from section "4.9.3 Processing revocation requests", have been carried out and the revocation has been duly processed by the RA (or by Izenpe in the cases indicated in section "4.9.1 Circumstances for revocation"), the revocation will be made immediately effective.

4.9.6 Obligation to verify revocations by relying parties

The verification of the state of the certificates is compulsory for each certificate use, either by consulting the certificate revocation list (CRL) or the OCSP service.

IZENPE supplies information to verifiers on how and where to find the corresponding CRL and/or OCSP.

4.9.7 Frequency of CRL generation

IZENPE immediately issues a Certificate Revocation List (hereinafter CRL) the moment a certificate is revoked.

The scheduled time for issuing a new CRL is indicated in the CRL, although a CRL may be issued before the deadline indicated in the previous CRL. If no revocations occur, the Certificate Revocation List is regenerated daily.

The CRL for end-entity certificates is issued at least every 24 hours, or when a revocation occurs, with a validity of 10 days.

The CRL of CA certificates (ARLs) is issued every 12 months or when a revocation occurs.

Revoked certificates that expire are removed from the CRL. They are then retained in IZENPE's internal register for a period of 15 years.

4.9.8 Time passing between generation and publication of the CRLs

The maximum latency time is set at 30 seconds from the generation of the CRL.

The publication time is immediate but the server that displays them may cache them for a period of 1 hour.

4.9.9 Availability of the online verification system for the status of certificates

IZENPE provides its User Entities with a real-time certificate checking service based on OCSP (Online Certificate Status Protocol), so that user applications verify the certificate status.

This service is available 24 hours a day, 7 days a week.

4.9.10 Online revocation checking requisites

The use of the CRLs service, which is freely accessible, shall require,

- To check in any case the last CRL issued, which can be downloaded from the URL address contained in the certificate itself in the extension 'CRL Distribution Point'.
- For the user to additionally check the relevant CRL(s) of the hierarchy's certification chain.
- For the user to ensure that the revocation list is signed by the authority that has issued the certificate to be validated.

Revoked certificates that expire will be removed from the CRL, however, information on the status of the certificate will still be provided via the online check, regardless of whether it is expired.

The use of the freely available OCSP service will require:

- Checking the URL address contained in the certificate itself in the 'Authority Info Access' extension.
- The user must ensure that the response is signed by the CA that issued the certificate to be validated.

4.9.11 Other revocation notifications available

Izenpe sends an informative email to the certificate subscriber when a certificate is revoked.

4.9.12 Special committed key requisites

If the private key associated with the certificate is compromised, the subscriber/key owner shall notify IZENPE to request certificate revocation and cease using the certificate.

The communication to Izenpe about the commitment of a private key through the email account seguridad@izenpe.eus indicated in section 1.5.2, must in any case include proof of such commitment and indicate in the subject line of the email: "Key commitment". To prove it, the parties may use the following methods:

- Sending the compromised private key or a challenge response signed by the private key and verifiable by the public key, as well as the public key itself.
- Providing references to vulnerabilities and/or sources of security incidents from which the key compromise is verifiable.

Izenpe may accept other types of evidence that adequately demonstrate key compromise.

If the IZENPE CA private key is compromised, the procedure shall be in accordance with section 5.7.3 of the present document.

4.9.13 Circumstances for suspension

Izenpe does not allow suspension of any of its certificates.

4.9.14 Who can request suspension?

Izenpe does not allow suspension of any of its certificates.

4.9.15 Procedure for requesting suspension

Izenpe does not allow suspension of any of its certificates.

4.9.16 Limits on the period of suspension

Izenpe does not allow suspension of any of its certificates.

4.10 Certificate status services

4.10.1 Operational characteristics

IZENPE offers a free service to publish the Certificate Revocation Lists (CRL) without restricting access. Additionally, it offers certificate validation services by means of the OCSP protocol (Online Certificate Status Protocol).

4.10.2 Service availability

IZENPE provides the user entities with a 24x7 revocation service (24 hours a day, 7 days a week)

4.10.3 Optional characteristics

Not stipulated.

4.11 Termination of subscription

The certificate is no longer valid for use after the end of the validity period or when it has been revoked.

The expiry of each certificate is indicated in the specific Policy.

4.12 Custody and recovery of keys

4.12.1 Key custody and recovery practices and policies

Izenpe will not retrieve private keys from Certificate Holders.

4.12.2 Session key protection and recovery practices and policies

Not stipulated.

5 Physical, procedural and personnel security controls

5.1 Physical security controls

IZENPE has physical security controls at all sites where IZENPE provides services.

5.1.1 Site location and construction

The facilities where information is processed fulfils the following requirements:

- The building with the information processing facilities is physically solid, the exterior walls are solidly built, the site is continuously monitored by video cameras and only duly authorized personnel are allowed access to the site.
- All of the doors and windows are locked and protected to prevent unauthorized access.

5.1.2 Physical access

Data Processing Centre

The IZENPE facility has a complete physical access control system consisting of:

- Perimeter security which extends from true floor to ceiling to prevent unauthorized access.
- Control over physical access to the facility,
    - Only authorized personnel are allowed access.
    - The rights to access the security area are reviewed and updated periodically.
    - All personnel are required to wear or carry some type of visible identification, and employees are encouraged to question anyone who does not comply with this requirement.
    - Personnel not on the IZENPE access list who may be working on the site are properly supervised.

A secure site access log is kept.

Access mechanisms on the building's perimeter doors at the IZENPE site.

A system of closed-circuit television which monitors the components IZENPE uses in providing its certification services.

Registration Authorities (RAs)

RAs meet necessary security criteria, defined both in Izenpe's Security Policy and its Provider Security Policy.

5.1.3 Power and air conditioning

The data processing centre is provided with power and air conditioning sufficient to create a reliable operating environment.

The IZENPE facilities are also provided with an uninterrupted power supply (UPS and electro-power unit) which keeps the equipment running for the time needed to shut down the systems in an orderly fashion in the event of a power failure or if the air-conditioning system causes a shutdown.

5.1.4 Exposure to water

IZENPE has taken the necessary precautions to minimize the impact of water exposure.

5.1.5 Fire prevention and protection

The IZENPE data processing centre has physical barriers which extend from the true floor to the true ceiling, as well as automatic fire detection systems for the purposes of:

- Notifying surveillance and IZENPE personnel of the onset of a fire.
- Disconnecting the ventilation system, closing the fireproof gates, turning off the power supply and triggering the automatic fire extinction facility.

5.1.6 Media storage

Media containing backup information is stored in a safe and secure manner.

5.1.7 Waste processing

A policy is in place to regulate the procedures governing the destruction of information media.

Storage media that contains confidential information is destroyed to ensure that data is no longer readable or recoverable after disposal.

5.1.8 Off-site backup

IZENPE keeps backup copies of storage media in a safe and secure environment protected against accidents and at a sufficient distance to prevent damage in the event of a disaster at the primary site.

5.2 Procedural controls

5.2.1 Trusted roles

A "trusted role" is defined as a person assigned responsibilities than can lead to security problems if not performed satisfactorily, whether accidentally or maliciously.

To ensure that trusted persons perform their corresponding duties properly, the following considerations are addressed:

- The first is that the technology is designed and configured so as to prevent errors and improper conduct.
- The second is that duties are distributed among several individuals so that any improper conduct would require the complicity of a number of them.

IZENPE has full definitions of all of the roles carried out in the organisation. The roles and responsibilities are defined for each one of them.

5.2.2 Number of people per task

To reinforce system security, more than one person is assigned to each role, with the exception of the role of operator, which can be fulfilled by the administrator.

Several individuals may also be assigned to the same role.

5.2.3 Identification and authentication for each role

Trusted roles require verification of identity by secure means; all trusted roles are performed by individuals.

IZENPE has specific documentation giving further details of each role.

5.2.4 Separating tasks into different roles

IZENPE follows the security policy CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures) and it is defined in the security model.

5.3 Personnel controls

5.3.1 Background, qualifications, experience, and clearance requirements

IZENPE employs personnel with the experience and qualifications needed to perform their job responsibilities.

All personnel with trusted roles are free from any interests that may affect their impartiality regarding IZENPE operations.

5.3.2 Background check procedures

With its Human Resource procedures, Izenpe carries out pertinent research before hiring anyone. Due to legal limitations, a criminal background check is not included.

5.3.3 Training requirements

IZENPE provides its personnel with the training needed to perform their job responsibilities competently and satisfactorily. Training is carried out at least once per year, which includes at least the following points:

- A copy of the Certification Practice Statement.
- Awareness-raising on security.
- Software and hardware operation for each specific role.
- Security procedures for each specific role.
- Management and operation procedures for each specific role.
- Disaster recovery procedure.
- Incident management procedures.

Specific awareness-raising and training shall be given to RA operators at least when beginning, and then with the frequency defined by Izenpe.

5.3.4 Retraining frequency and requirements

Any significant change in IZENPE's operation will call for a training plan and implementation of the plan will be documented. "Trusted Role" staff must receive training at least once per year to maintain their skill levels. This training must always include a review of content.

5.3.5 Sequence and frequency of job rotation

Employees are rotated according to the needs of the role itself, or at the behest of the employee.

5.3.6 Sanctions for unauthorised actions

Information security incidents

IZENPE has a security incident management plan.

Punitive process

There is an internal disciplinary regime which defines sanctions against personnel.

5.3.7 Recruitment requirements

All personnel subcontracted by Izenpe to carry out roles related to operating Izenpe services is subject to the same requirements from Izenpe's Provider Security Policy.

5.3.8 Provision of documentation to staff

All personnel with trusted roles receive:

- A copy of the Certification Practice Statement.
- Documentation which defines the obligations and procedures associated with each role.
- Personnel also have access to the operations manuals on the various components of the system.

5.4 Audit

Audit logs are used to reconstruct significant events recorded in the IZENPE or Registration Authority software, and the user or event that gave rise to the log. Logs will also be used in arbitration to resolve any possible disputes by checking the validity of a signature at a given time.

5.4.1 Type of events recorded

The following logs are stored:

- New certificate applications
- Rejected certificate applications
- Account access violation
- Certificate signature
- Revoking the certificate
- Account logon
- CRLs signature
- CA modifications
- Certificate expiry

This list is not inclusive and is limited to events that are directly related to managing certificates or administrative roles. Particularly, technical events registered at other sites are not included.

The time and date are recorded for each event using a reliable time basis.

5.4.2 Frequency of log processing

The logs are continuously processed and audited on a quarterly basis by the technical area. The audit report includes the following aspects:

- List of unauthorised access attempts
- Errors generated in each CA

5.4.3 Period for audit log retention

The information generated in the log file is retained online until it is archived. After they are archived, log files are retained for 7 years.

5.4.4 Protecting the audit log

Access to log information is assigned to all personnel who require access as part of their role. The Auditor role may access it. The log is stored in the database, and access is protected at different levels.

Unauthorised deletion and modification of log records is blocked. There are contingency methods to prevent log data from being lost.

5.4.5 Audit log backup procedure

The logs are hosted in the database, so they are included in the daily database backup, according to the security copy policy.

5.4.6 Compiling logs

CA and RA log files are stored in IZENPE's internal systems.

5.4.7 Notifying the action causing the logs

There is no provision for notification regarding the subject giving rise to the log.

5.4.8 Vulnerability analysis

Both external and internal vulnerabilities in IZENPE's internal systems are assessed on a quarterly basis. A penetration test is also performed annually.

5.5 Archiving of records

5.5.1 Type of records archived

The following data or files, in addition to others, are recorded:

- Data related to the certificate registration and application procedure:
- The audit logs described in the previous section;
- Key record.

5.5.2 File retention period

All of the information and documentation related to qualified certificates is retained for 15 years (from date of issuance); documents related to other types of certificates are retained for 7 years (from certificate end date).

5.5.3 File protection

The Archive Management Procedure indicates the protective measures taken so that both paper registers and electronic registers cannot be handled or have their content destroyed.

5.5.4 Archive backup procedures

There is a security copy policy and contingency plan that define the criteria and strategies for action should an incident occur. The design of the strategy for action in the case of incidents is based on the corresponding assets inventory and risk analysis.

5.5.5 Requisites for time stamping the records

The information systems used by IZENPE ensure that a record is kept of the exact time each logged event occurs. The exact time used by the systems comes from a reliable time source for the date and time. All of the systems synchronise their time based on this source.

5.5.6 Filing system

The archive collection system is located on-site at IZENPE and at the facilities of the entities taking part in rendering of services.

5.5.7 Procedures to obtain and verify the archive information

Access to this information is limited to authorized personnel and is therefore protected against physical and logical access in accordance with sections 5 and 6 of this Certification Practice Statement.

5.6 CA key change

To minimise the risk of compromising a CA private key, the key must be changed according to the security level of the algorithms used. Once changed, the new key should only be used for signature purposes. The old key, although still valid, should be available to verify old signatures until all of the certificates signed with it have expired. The private key should only be kept if used to sign CRLs that have certificates signed with this key and shall be protected with the same protection level as the new one. The procedure to generate a new CA key is defined in the Generation Ceremony Document for new CAs and migration from old CAs. Section 6.1.5 defines key sizes and algorithms used.

5.7 Incident Management and Contingency Plan

5.7.1 Incident management procedures

There is a Contingency Plan that describes all of the actions carried out and the resources and personnel used should an incident, whether intentional or accidental, damage or render unusable the certification resources or services provided by IZENPE.

The main objectives of the Contingency Plan are:

- To maximise the effectiveness of recovery operations by establishing three phases:

- Notification/Evaluation/Activation phase to detect and assess the damage and set the plan in motion.
- Recovery phase aimed at temporarily and partially re-establishing services until the damage to the original system has been repaired.
- Reconstitution phase to restore regular operations and processes.

- Identify the activities, resources and procedures needed to provide partial certification services in an alternate CPD during prolonged interruptions to regular operations.
- Assign responsibilities to personnel designated by IZENPE and provide a guide for the recovery of regular operations during long periods of interruption.
- Ensure coordination among all stakeholders (departments of the entity, external points of contact and salespeople) taking part in the planned contingency strategy.

The IZENPE Contingency Plan applies to all of the functions, operations and resources needed to restore the provision of certification services. The plan applies to IZENPE personnel associated with the provision of certification services.

The Contingency Plan establishes the participation of certain groups in the recovery of IZENPE operations.

Assessments of damages and the action plan are described in the Contingency Plan.

Should the algorithm, combination of key sizes used, or any other technical circumstance significantly reduce the technical security of the system, the Contingency Plan shall be applied. An economic impact analysis will be conducted. The analysis will address the critical nature of the security problem, its scope and the recovery strategy to manage the incident. The following points must be defined in the impact analysis report:

- Detailed description of the contingency, timeframe, etc.
- Critical nature, field
- Proposed solution or solutions
- Deployment plan for the chosen solution, which shall include at least the following aspects:
  - Notification of users by whatever means are considered most effective. Certificate applicants, subscribers and verifiers (trusted third parties) shall be included.
  - The contingency will be posted on the website
  - Revocation of affected certificates
  - Renewal strategy

5.7.2 Action plan to deal with corrupt data and software

The strategy for dealing with problems of this type is provided in the IZENPE Contingency Plan.

5.7.3 Procedure in case of compromise of the CA's private key

After addressing the factors that led to revocation, the Root CA can:

- Generate a new certificate for the issuing CA.
- Make sure that all of the new certificates and the CRL issued by the CA are signed using the new key.

The Root CA will publish the revoked certificate in the ARL (Certification Authority Revocation List).

This contingency will be included in Izenpe's Business Continuity Plan, and shall determine, amongst others, the following actions to take:

1) Cease providing the affected service.
2) Revoke certificates that may be affected.
3) Notify subscribers, users and third parties. In the same fashion, a notification to TSPs shall be included with trust agreements, browser manufacturers and in general, any entity with which Izenpe holds any contractual use-of-service relationship.
4) Study the need to execute the TSP Activity Termination Plan according to the CPS and laws in force.

5.7.4 Business continuity after a disaster

The operation of the CA will be suspended until the disaster recovery procedure has been finalised and secure operations are re-established at the primary site location or an alternative facility.

The IZENPE Business Contingency and Continuity Plan will put into action.

5.8 CA or RA termination

5.8.1 Certification Authority

IZENPE has a Termination Plan which specifies the procedure to be carried out should such an event occur.

In the event of activity termination, IZENPE must notify subscribers at least two months prior to the termination of operations, by any means that will ensure the proper communication and reception of its intent to cease its activity as a certification service provider. This notification shall indicate that all certificates in force will be revoked within a 2-month period.

In the event that a CA finalises due to expiry or revocation, consultations on the status of the certificate shall still be responded to through the OCSP service. Once the CA is finalised, OCSP responses on certificates issued by that CA shall be signed by another one of Izenpe's CAs in force of Izenpe.

Izenpe's CRLs do not include expired certificates, as indicated in section 4.9.7 Frequency of CRLs under this CPS.

In the event that Izenpe ceases activity, information on certificate revocation shall be provided through a last CRL, with a nextUpdate of "99991231235959Z" according to specifications in section 6.3.9 of ETSI EN 319 411-1.
ETSI EN 319 411-1:

TSPs, browser manufacturers and any entity with which IZENPE has entered into a contractual relationship for the use of its certificates shall also be notified.

For as long as necessary according to specifications in this CPS, Izenpe shall keep all information on registration, status of revocation and log archives. If transferred to another entity, measures shall be taken so that said transfer is conducted with all guarantees necessary.

The party responsible for this notification is the IZENPE Directorate General or individual(s) appointed by the Board of Administrators, who shall decide on the most appropriate mechanism.

Izenpe shall inform the Supervising Entity of termination of its activity, including information on Certificates whose validity will expire. This communication will be made through the notification-sending platform of the electronic headquarters of the Ministry responsible for the provision of trust services, with a minimum of 3 months' notice prior to cessation of its activity.

Any authorisation with a thirty party with whom Izenpe holds a service provision contract (identification, issue, hosting, etc.) shall be deemed as terminated.

Izenpe or the entity with whom Izenpe agrees to transfer the service shall offer validity information on all its qualified certificates, even when the certificate has expired (until the expiry date for the subordinate CA that issued the certificate).

5.8.2 Registration Authority

After the Registration Authority ceases to perform its operations, it shall transfer to IZENPE any records it is required to retain; any other information will be cancelled and destroyed.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The root and subordinate CA cryptographic keys must be generated in a cryptographic hardware module (HSM) that meets with FIPS 140-2 level 3 (or later) and Common Criteria EAL 4+ for the corresponding protection profile.

The VA cryptographic keys must be generated in a cryptographic hardware module (HSM) that complies with FIPS 140-2 level 3 (or later).

The TSA cryptographic keys must be generated in a cryptographic hardware module (HSM) that complies with FIPS 140-2 level 3 or FIPS 140-3 level 3 (or later).

All cryptographic keys must be generated pursuant to minimum algorithm and key length recommendations stipulated in ETSI TS 119 312. In the case of qualified certificates for which Izenpe generates the keys, they shall be generated as cards, cryptographic tokens or cryptographic hardware.

When an end user of these qualified certificates generates the keys, they may be generated on the following devices:

- Client key container (e.g.: web server)
- Izenpe's secure container
- Izenpe's application container for mobile phones

6.1.2 Private key delivery to subscriber

Delivery method of the private key depends on the certificate and device type. See the corresponding Certificate policy.

6.1.3 Public key delivery to certificate issuer

The Public Key, generated together with the Private Key on the key generation and custody device, is delivered to the Certification Authority by sending a certification request.

The method used by the different entities that comprise or collaborate with IZENPE for delivering the public key to the corresponding certificate issuer is as follows:

- Keys generated by Izenpe (card, token, HSM): hosted on the cryptographic device or secure container.
- Keys generated in mobile phones: stored in the Izenpe application container

6.1.4 Secure server certificate keys (SSL): Izenpe Certification Authority public key delivery to certificate users

IZENPE CA public keys are delivered by different means, including via the IZENPE website. Section 1.3.1.1 and 1.3.1.2 of this Certification Practice Statement also contains the root CA and issuing CA prints.

6.1.5 Key sizes

Key size, depending on each case, is:

- No fewer than 2048 bits for keys for natural or legal persons or for device keys, OCSP Servers and technical certificates.
- No less than 4096 bits for CAs issued after 2007

The TSU server key size is issued with 4096

6.1.6 Public Key Generation and Quality Assurance Parameters

The Algorithm Identifier (AlgorithmIdentifier) used by IZENPE to sign the certificates is SHA2 (hash algorithm) with RSA (signing algorithm) which corresponds to the identifier for "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc. The padding scheme used is emsa-pkcs1-v2.1 (according to RFC 3447 section 9.2)".

End user certificates are signed with RSA with SHA-256. IZENPE recommends that end users employ RSA with SHA-256 or higher when signing a certificate.

IZENPE uses an algorithm qualified by the industry and appropriate for the qualified signature proposal. To this end, the certificate expiry date will be taken into account, in addition to following the recommendations indicated by the CA/B Forum and by the different ETSI standards.

Should the algorithm, combination of key sizes used, or any other technical circumstance significantly reduce the technical security of the system, the Contingency Plan shall be applied. An economic impact analysis will be conducted. The analysis will address the critical nature of the security problem, its scope and the recovery strategy to manage the incident. The following points must be defined in the impact analysis report:

- Detailed description of the contingency, timeframe, etc.
- Critical nature, field
- Proposed solution or solutions
- Deployment plan for the chosen solution, which shall include at least the following aspects:
    - Notification of users by whatever means are considered most effective. Certificate applicants, subscribers and verifiers (trusted third parties) shall be included.
    - The contingency will be posted on the website
    - Revocation of affected certificates

- Renewal strategy

6.1.7 Supported Key Usages (KeyUsage field X.509v3)

All certificates include the Key Usage and Extended Key Usage extension, indicating the enabled key uses.

The Root CA keys are used to sign the certificates of the Sub CAs and the ARLs. Sub CA or issuing CA keys are only used to sign end-user certificates, CRLs, TSU certificates and OCSP certificates.

The supported key uses for end certificates are defined in the certificate profiles document available at www.izenpe.eus.

6.2 Private key protection

6.2.1 Standards for cryptographic modules

A hardware security module (HSM) is a security device that generates and protects cryptographic keys. It is required that the HSM meet FIPS 140-2 Level 3 criteria at minimum, or Common Criteria EAL 4+ for the corresponding protection profile.

IZENPE holds protocols to check that an HSM has not been manipulated during transport and storage.

Cryptographic devices with qualified electronic signature certificates, suitable as qualified signature creation devices (DSCF), meet the requirements of security level CC EAL4+, although certifications complying with a minimum of ITSEC E3 or FIPS 140-2 Level 2 security criteria or equivalent are also acceptable.

In the event that these devices lose the secure device certification and this entails the loss of the condition of qualified signature, Izenpe will proceed to revoke the certificate; always as determined by the supervisory body and/or current regulations.

The European reference standard for subscriber devices used is Commission Implementing Decision (EU) 2016/650 dated 25 April 2016.

IZENPE, in any case, maintains control over the preparation, storage and distribution of the subscriber devices where IZENPE generates keys.

6.2.2 Private key (n out of m) multi-person control

The use of CA private keys requires the approval of at least two persons.

6.2.3 Private key custody

The root CA private key is held by a cryptographic hardware device certified with the FIPS 140-2 level 3 and/or CC EAL4+ standard, guaranteeing that the private key is never outside the cryptographic device. The activation and use of the private key requires multi-person control as explained above.

The Subordinate CA private keys are held in secure cryptographic devices certified with the FIPS 140-2 level 3 standard.

In cases where subscribers keep the private key, it will be their responsibility to keep it under their exclusive control.

6.2.4 Private key backup

There is a procedure for the recovery of cryptographic module keys of the CA (root or subordinate) which can be applied in the event of contingency.

There is a procedure for recovering subscriber cryptographic module keys under Izenpe's custody which can be applied in the cases defined in the respective.

In both cases, the same controls are applied as those indicated in point 6.2.2.

6.2.5 Private key archiving

Izenpe may make a backup copy of the Private Keys, ensuring that the security of the duplicated data is of the same level as that of the original data and that the amount of duplicated data does not exceed the minimum necessary to guarantee the continuity of the service. Signature creation data is not duplicated for any other purpose.

6.2.6 Transfer of the private key to or from the cryptographic module

The root CA private key, subordinate CAs, VA and TSA are generated in an HSM pursuant to point 6.2.1 and exportation is not possible. As a contingency measure, it is possible to recover private keys as indicated in section 6.2.4.

For the following devices used to issue end user certificates, keys are generated in the cryptographic module, and it is not possible to export the private key:

- ✓ Card/cryptographic token

When the subscriber generates the keys, the subscriber shall also be responsible for their custody.

6.2.7 Storage of the private key in the cryptographic module

There is a CA root and subordinate CA key ceremony document describing the processes for generating the private key and the use of cryptographic hardware.

In generating CA keys, Izenpe follows the recommendations of ETSI EN 319 411-1, and CABForum Baseline Requirement Guidelines.

To generate subscriber keys in the cryptographic card, Izenpe follows European Commission recommendations (eIDAS) and EN 319 411-1.

In cases where private keys are stored outside the cryptographic modules, they will be protected so as to ensure the same level of protection as if they were physically inside the cryptographic modules.

6.2.8 Private key activation method

Private Keys of Certification Authorities are generated and held in custody by a cryptographic device that meets the security requirements of FIPS 140-2 Level 3.

Activation and use mechanisms of Private Keys of End Entity Certificates are described in the Specific Policy for each certificate.

6.2.9 Private key deactivation method

A person with the administrator role may deactivate the Certification Authorities key by stopping the system. To reactivate it, action must be taken as described in section "6.2.8 Private key activation method".

Regarding deactivation of Private Keys of End Entity Certificates, this is described in the Specific Policy for each certificate.

6.2.10 Private key destruction method

There is a procedure for the destruction of CA keys.

In the event of withdrawing the HSM that houses the CA keys, the established procedure shall be followed.

This procedure is not applied to user signature or authentication keys issued on a cryptographic card or secure container, except in the case of key changeovers using the same cryptographic device.

6.2.11 Qualifying the cryptographic module

As indicated in section 6.2.1 of this document

6.3 Other aspects of key pair management

6.3.1 Public key archiving

The certificates generated by the CA, and therefore the public keys, are stored by the CA for the period of time stipulated under current law.

6.3.2 Certificate operation periods and key pair use periods

Periods of use for the certificates issued by Izenpe are:

- ✓ The root CA certificate 2007 is valid for 30 years.
- ✓ The root CA certificate 2020 is valid for 25 years.
- ✓ The root CA certificate 2024 is valid for 25 years.
- ✓ The subordinate CA certificate issued by EVs is valid for 10 years. The rest of subordinate CAs are valid until the root CA's expiry.
- ✓ Changing the CA certificate (root and subordinate) keys is upon request, according to the standards determined by the industry.

- ✓ End user certificates have a different duration in each case, see Specific policy. For all natural and legal person certificates, renewal means that keys are regenerated.

6.4 Activation data

6.4.1 Generation and installation of activation data

Activation data, both for root CA keys and for subordinate CA keys issued by End Entity Certificates, are generated during the creation key ceremony of said Certification Authorities.

Regarding activation data of Keys of End Entity Certificates, they are described, if necessary, in the Specific Policy for each certificate.

6.4.2 Activation data protection

The root CA key activation data are distributed between several different physical cards, and at least two people are needed to perform any operation. The card keys are kept in custody in different safes.

The subordinate CA key activation data are distributed between several different physical cards, and at least two people are needed to perform any operation. The card keys are kept in custody in different safes.

The TSA and VA keys are generated and managed in the same HSM as the subordinate CA keys. The same rules apply.

Subscribers are compelled to keep their activation data secret.

6.4.3 Other aspects of the activation data

See specific policy for each certificate type.

6.5 Computer security controls

6.5.1 Specific technical requirements for computer security

A series of controls are in place in the different components making up the IZENPE certification service system (CAs, IZENPE databases, IZENPE Internet Services, CA Operation and Network Management):

- Operational controls.
  - All of the operations procedures are duly documented in the corresponding operations manuals.

    There is a Contingency Plan.
  - Tools have been implemented to protect against viruses and malicious codes.
  - The equipment is maintained on an ongoing basis to ensure uninterrupted availability and integrity.

- A procedure exists for saving, deleting and safely eliminating storage media, removable media and obsolete equipment.

- Data exchange. The following data exchanges are encrypted to ensure confidentiality.
  - Transmission of registration data between RAs and the registration database.
  - Transmission of pre-registration data.
  - Communication between RAs and CAs.
- The revocation publication service possesses the functions necessary to be available on a 24x7 basis.
- Access control.
  - Unique user IDs are used in such a way that users are associated with, and can be held responsible for, their actions.
  - Rights are assigned according to the principal of providing users with the least amount of system privileges they need to do their jobs.
  - Access rights are immediately cancelled whenever users change jobs or leave the organisation.
  - The access level assigned to users is revised every three months.
  - System privileges are assigned on a case-by-case basis and terminated once the reason for their assignation is no longer valid.
  - There are quality guidelines for passwords
  - All operator accounts with capacity to issue certificates have double factor-based access control.

Izenpe has a security policy and specific procedures to guarantee security at different levels.

6.5.2 Assessment of the level of IT security

The products used for the provision of certification services have the international certificate based on standard ISO/IEC 15408.

6.6 Life cycle engineering controls

6.6.1 System development controls

Implementation of the software for the production systems is controlled.

To prevent possible problems with these systems, the following controls should be considered:

- Izenpe's policy includes rules to securely develop applications and systems
- There is a formal procedure to track changes. Changes are limited to those necessary, and undergo thorough control

- When operational systems are changed, the business applications deemed critical according to the Business Continuity Plan are reviewed
- Secure system engineering principles are established
- The development setting is duly protected
- Outsourced development is supervised and controlled by Izenpe
- Operational security tests are performed during development
- Acceptance testing programmes are established for new information systems, updates and versions
- Test data are selected, protected and controlled

6.6.2 Security management controls

Izenpe constantly monitors to ensure that systems and communications operate according to Izenpe's Security Policy. All processes are logged and audited according to valid legislation and regulations.

6.6.3 Life cycle security controls

In order to conduct test, a large volume of data as similar as possible to production data is required. The use of production databases containing personal information is avoided.

6.7 Network security controls

The network's security is based on the concept of multi-level zoning with multiple redundant firewalls. The confidential information transferred by insecure networks is encrypted by using SSL/TLS protocols. There are IPS systems for internal and external traffic.

6.8 Time source

IZENPE obtains the time from their systems by means of a connection with the Royal Navy Observatory by following the NTP protocol. . A description of the NTP protocol may be found in the IETF RFC 5905 standard.

Based on this internal service, Izenpe offers a time stamp service (TSA) that can be used to create time stamps on arbitrary documents, according to IETF RFC 3161 and ETSI EN 319 421. More information in Izenpe's Timestamp Practice Statement.

7 Revoked Certificate and CRL profiles

7.1 Certificate profile

The certificates issued by IZENPE conform to the following standards:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) May 2008
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) December 2005
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) August 2006
- ITU-T Recommendation X.509 (2005): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.
- ETSI EN 319 412
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile.

7.1.1 Version number

Certificates issued under this Certification Practice Statement use the X.509 standard, version 3 (populate version field with integer "2").

7.1.2 Certificate extensions

These may be viewed in the profile document available at www.izenpe.com .

7.1.3 Algorithm object identifiers

The algorithm identifier used by IZENPE to sign the certificate SHA-256/RSA which corresponds to the identifier 1.2.840.113549.1.1.11

7.1.4 Name Formats

The formats are indicated in the profiles document, available at www.izenpe.com. The profiles of the CAs are given in section 1.3.1 of this document.

7.1.5 Name restrictions

The "name constraints" extension is not included in the Izenpe Subordinate Authority certificate profile, therefore this type of constraint is not given.

7.1.6 Certificate Policy Object Identifier

As specified in section 1.2 of this Certification Practice Statement.

7.1.7 Use of extension policy restrictions

No policy restrictions are used.

7.1.8 Syntax and semantics of policy qualifiers

The Certificate Policies extension contains the following policy qualifiers:

- **CPS Pointer**: contains a pointer to the IZENPE Certification Practice Statement, http://www.Izenpe.com/cps
- **User notice:** Text note that is displayed on the screen, at the request of an application or user, when a third party verifies the certificate.
- **Policy Identifier**: Indicates the OID of the certificate User

Notice common to all certificates (except SSL certificates):

USER NOTICE	Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consult www.izenpe.com for terms and conditions before using or relying on the certificate.

7.1.9 Semantic treatment for the "Certificate policy" extension.

The Certificate Policy extension allows to identify the policy that IZENPE associates to the certificate and where these policies can be found.

7.2 Certificate revocation list profile

The certificates issued by IZENPE conform to the following standards:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) May 2008
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) December 2005
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) August 2006.

As described in RFC 6962, a pre-certificate shall not be considered a certificate with the characteristics defined in RFC 5280.

7.2.1 Version number

Version 2 (populate version field with integer '1').

7.2.2 List of certificate revocation and extensions of elements from the list

The extensions used are as follows:

Field	Mandatory	Critical
X.509v2 Extensions		
1. Authority key Identifier	Yes	No
2. CRL Number	Yes	No
3. Issuing Distribution Point	Yes	No
4. Invalidity Date	Yes	No

7.3 OCSP profile

Izenpe OCSP responses are compliant with RFC 6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP), and are signed by the OCSP Responder whose certificate has been signed by the same CA with which the certificate being queried was issued.

7.3.1 Version number

Version 3.

7.3.2 OCSP Extensions

Field	Mandatory	Critical
1. Issuer Alternative Name	No	No
2. Authority/Subject key Identifier	No	No
3. CRL Distribution Point	No	No
4. Key usage	Yes	Yes
5. Enhanced Key usage	Yes	Yes

7.3.3 Other OCSP aspects

- The OCSP service supports the GET method
- The information on this certificate status is constantly updated
- OCSP responses expire at 48 hours
- In status requests for certificates that were not issued by Izenpe, the response is REVOKED
- In status requests for certificates issued by Izenpe, if REVOKED, the extension id-pkix-ocsp-extended-revoke is included in the OCSP response
- For certificates that are not Izenpe's, the response obtained from @Firma is returned
- Izenpe does not support OCSP Stapling.

8 Compliance audits

Verification of compliance with security requirements, also known as security audit or security review, is an activity carried out to ensure compliance and adequacy with the security plan of the IZENPE certification delivery system and is defined in an Audit Plan.

On-site verification is conducted to determine whether IZENPE personnel follow the specified procedures and safeguards.

8.1 Audit frequency

Verification of conformity with security requirements is performed regularly and planned and integrated into other activities.

8.2 Auditor qualifications

Auditors are qualified and have demonstrated proficiency in auditing secure systems of production, especially digital certification systems. The auditor must be accredited as per ETSI EN 319 403.

8.3 Relationship of the auditor with the audited company

Both internal and external auditors are used, but in all cases they are independent of the production service being audited.

8.4 Elements to be audited

The compliance audit will cover the following topics:

- PKI processes
- Information systems.
- Protection of the data processing centre.
- Documents.

Details on how each of these topics is audited are provided in the IZENPE Auditing Plan.

8.5 Decision-making as the result of deficiencies

Izenpe implements a permanent improvement model, and the results from a compliance audit are handled according to this model. Depending on severity and urgency, all observations, improvements and non-compliance issues are entered into a tracking system and are handled as incidents or problems. With a support tool, Izenpe ensures that all problems are handled by their deadline.

8.6 Communication of results

Audit results reports will be delivered to the Security Committee for study.

9 Other legal and activity matters

9.1 Fees

IZENPE will receive the corresponding economic remuneration in accordance with the fees approved by its Board of Directors.

9.1.1 Fees for the issue or renewal of certificates

The fees that users must pay for issuance or renewal of certificates appear in section 10.1.

9.1.2 Fees for access to certificates

Not stipulated.

9.1.3 Certificate status information access fees

IZENPE offers certificate status information services through CRLs or the OCSP free of charge.

9.1.4 Fees for other services

The fees applicable for other services will be agreed on between IZENPE and the customers of these services.

9.1.5 Refund policy

IZENPE does not have a refund policy.

9.2 Financial responsibility

IZENPE, the Registration Authorities and the User Entities shall have sufficient financial resources to maintain their operations and perform their duties.

9.2.1 Liability insurance

IZENPE maintains a liability insurance policy for any errors and omissions resulting from the generation of certificates, which exclusively covers the activities performed by IZENPE. The relationship between IZENPE and the Registration Authorities, when intervening, and certificate subscribers and users is neither mandatory nor fiduciary. Certificate subscribers and users cannot compel IZENPE or the Registration Authorities to provide any services whatsoever, either by contract or any other means.

9.2.2 Other assets

Not stipulated.

9.2.3 Insurance and guarantees for end entities

Not stipulated.

9.3 Information confidentiality

9.3.1 Scope of confidential information

In order to provide services, IZENPE and the Registration Authorities need to collect and store certain types of data including personal information. This information is gathered directly from the affected parties with their express consent, or without consent from the affected parties in cases where the law on personal data protection provides for the collection of this type of information.

IZENPE and the Registration Authorities only collect data needed for the issuance and management of certificates and for providing other electronic signature services; data may not be used for any other purpose without the express written consent of the signatory.

IZENPE's privacy policy has been developed in accordance with the current law on personal data protection.

IZENPE and the Registration Authorities shall not disclose or share personal information except those situations described in the sections of this Certification Practice Statement and in the section on the termination of services provided by IZENPE and the Registration Authorities.

The following information is kept confidential by IZENPE and the Registration Authorities:

- Certificate applications, whether approved or disapproved, and all other personal information obtained from the issuance and maintenance of certificates, except for the information indicated in the corresponding section.
- Private keys generated and/or stored by IZENPE.
- Transactional records, including full records and the audit trail of transactions.
- Internal and external audit trail records created and/or retained by IZENPE or the Registration Authorities and their respective auditors.
- Business continuity and disaster recovery plans.
- Security policy and plans.
- Records on operations and other operational plans, such as archival, monitoring and other analogous plans.

9.3.2 Information beyond the scope

The following information is not considered confidential and is thus acknowledged by the affected parties in the legal instrument signed with IZENPE:

- Certificates that have been or are in the process of being issued.
- Information linking the natural person subscriber to a certificate issued by IZENPE.
- The name and surname of the certificate subscriber, in the case of certificates in which the subscriber and signer is a natural person, or of the signers, in the case of

certificates in which the subscriber is a legal person or administrative body, as well as any other circumstance or personal data of the holder, in the event that it is significant based on the purpose of the certificate.

- If included, the email address of the certificate subscriber in the case of certificates whose subscriber and signatory are a natural person, or the e-mail address of the key owner in the case of certificates whose subscriber is a legal person or government agency, or the e-mail address assigned by the subscriber for device certificates.
- The usages and financial limitations included in the certificates.
- The validity period, the date of issuance and the expiry date of the certificate.
- The certificate serial number.
- The different situations or status dates of the certificate and the commencement date for each, specifically: pending generation and/or issuance, valid, revoked, suspended or expired, and the reason for the change in status.
- Certificate Revocation Lists (CRLs), and other information regarding revocation status.
- The information contained in the IZENPE Repository.
- Any other information that is not indicated in the section on confidential information in this Certification Practice Statement.

9.3.3 Responsibility to protect confidential information

IZENPE or the Registration Authorities shall be entitled to disclose confidential information to the extent required by law.

Specifically, records that certify the trustworthiness of the information included on the certificate will be disclosed if required as evidence of certification in judicial proceedings, even without consent from the certificate subscriber.

The certificates shall be published in accordance with the provisions of the eIDAS1 and eIDAS2 Regulation and Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.

9.4 Personal data protection

Izenpe publishes its Processing Activity Recording and other information on personal data so that interested parties may view it at the following website: www.izenpe.eus/datos

9.4.1 Privacy Plan

Izenpe's personal data processing is aligned with provisions in EU Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of individuals with

regard to the processing of personal data and their free circulation and which repeals Directive 95/46/EC (General Data Protection Regulation, hereinafter, GDPR), as well as requirements applicable due to specific national regulations in this regard.

9.4.2 Information treated as private

Izenpe considers personal information on all individuals using the Trusted Services that must not be incorporated into certificates and the mechanisms using the Information and Certificate Validity Status Consultation Service as private.

In any event, all personal information collected during request, renewal and revocation processes for electronic certificates (with the exception set forth in the section below), the Private Keys in the possession of the Trusted Service Provider and all information clearly identified as private, are considered private.

Izenpe applies suitable safeguards to protect private information.

9.4.3 Information not considered private

Information incorporated into electronic certificates, information on the validity status of certificates, the start date of said status (active, revoked, expired, etc.), as well as the reason behind the change in status is not considered private information. Therefore, electronic certificates, lists of revoked certificates and all of their content is not deemed private information.

9.4.4 Responsibility to protect private information

Izenpe adopts the security measures required by the GDPR regarding access and processing for Certificate applicant and subscribers' personal data.

The technical and organisational measures shall be established considering the cost of the technique, costs of application, as well as the nature, scope, context and purposes of processing and the risks to rights and liberties.

9.4.4.1 Data Protection Officer

Izenpe's DPO's contact data are published on www.izenp.eus/datos. Said contact data include the email address to which interested parties may address queries regarding their personal data processing and to exercise their rights, pursuant to article 38.4 of the GDPR.

9.4.4.2 Processing activity record

Izenpe has a record of the processing activity it conducts under its own responsibility, including the "Identification Means Management" on the activity that this Entity conducts as a

Trusted Service Provider. For each processing identified, this record includes the following information:

a) Purpose
b) Responsible entity
c) Personal data categories
d) Who provides the data
e) Who is the party affected by the personal data
f) Who are data processors
g) Data sharing
h) International Data Transfers
i) Deletion period
j) Security measures

The Processing Activity Record document may be viewed at www.izenpe.eus/datos.

9.4.4.3 Rights of interested parties

Interested parties may exercise their rights to access, correct, delete, limit processing, oppose and transfer data pursuant to provisions in articles 15 through 22 of the GDPR by:

- Post: accompanying the request with a copy of the National ID Document.
- Electronically, signing the request with the qualified natural person certificate.

9.4.4.4 Cooperation with the authorities

Izenpe shall cooperate with the Spanish Data Protection Agency when required to do so.

9.4.4.5 Security violation notifications

Izenpe shall notify the Spanish Data Protection Agency (AEPD) of any security violation to personal data without delay and, in any event, within 72 hours after the responsible party becomes aware of the circumstances, provided that this violation may prove a risk to the rights and liberties of the natural persons affected.
In cases where it is likely that the security violation may entail a high risk to the rights and liberties of the interested parties, the notification to the AEPD shall be complemented by a notification addressed to said parties so that they may take measures to protect themselves from the consequences.

9.4.5 Notice and consent to use private information

Obtaining private information from natural persons during processes related to the life cycle of the Certificates (request, identity accreditation, renewal, revocation, etc.) shall always be subject to unequivocal consent from said individuals, meaning a statement from the

interested party or by means of a clear affirmative action.

9.4.6 Disclosure pursuant to judicial or administrative process

Izenpe shall not share personal data, barring a request from administrative or legal authorities.

9.4.7 Other disclosure circumstances

Not stipulated.

9.5 Intellectual property rights

9.5.1 Property rights in certificates

IZENPE is the only entity that retains the intellectual property rights to the certificates it issues.

Intellectual and industrial property rights derived from software used in the digital certification system and owned by third parties are excluded.

The same rules apply to the certificate revocation data system.

9.5.2 Property rights in certification practice

IZENPE retains all property rights to this Certification Practice Statement.

9.5.3 Property rights in names

The subscriber, and where applicable the key owner, retains all rights (if any), to any trademark, product or trade name contained in the certificate.

The subscriber, and where applicable the key owner, is the owner of the distinguished name of the certificate, consisting of the information specified in section 3 of the Certification Practice Statement.

9.5.4 Property rights in keys and key material

Key pairs are the property of certificate subscribers.

9.6 Obligations and guarantees

As the Certification Authority responsible for issuing the certificates in accordance with this Certification Practice Statement, IZENPE undertakes the following obligations:

9.6.1 Obligations of the CA

9.6.1.1 Obligation of providing service

IZENPE provides its certification services in accordance with this Certification Practices Statement, which details its functions, operating procedures and security measures, and in

particular, is responsible for compliance with all obligations that correspond to it except those expressly carried out by the Registration Entity, provided that it does not act as such. These Certification Entity obligations are the following:

- Not copying signature creation data of the person to whom its services were provided.
- Keeping a system to indicate the issued certificates and if they are valid or if their validity has been suspended or expired.
- Keeping a record by any secure means of all information and documentation regarding the qualified certificates and certification practice statements that are valid at all times, for at least 15 years as of the date of their issue, so that the signatures made with the certificate and in relation to the rest of certificates can be validated for 7 years.
- Ensuring that the signatory possesses the signature creation data for the verification data on the certificate.
- Guaranteeing that the creation and signature verification data are complementary, as long as they are both generated by the certification service supplier.
- It will meet the security standards and rules (General Register of Data Protection, ISO, ETSI and Izenpe Security Policy).
- It will require that hosting suppliers meet the security standards and rules (GDPR, ISO, ETSI, CABForum and Izenpe Provider Security Policy).

9.6.1.2 Reliable operation obligations

IZENPE guarantees the following:

- That the identity contained in the certificate unambiguously matches the public key contained therein.
- Rapidity and security in providing the service. In particular, it provides a fast and secure service aimed at checking certificate validity and ensures secure and immediate notification of the termination of effectiveness of the certificates in accordance with this Certification Practice Statement. The service is available 24 hours X 7 days a week.
- Compliance with technical and staff requirements stipulated by governing legislation on electronic signatures:

    1. Demonstrating the reliability necessary to provide certification services.
    2. Guaranteeing that the date and time when a certificate was issued or expired can be precisely determined.
    3. Employing staff with the qualification, knowledge and experience necessary to provide the certification services offered and the security and management procedures as required within the scope of electronic signatures.
    4. Using reliable systems and products that are protected against all alteration, and that guarantee technical security, and if applicable, cryptographic security of the certification processes that they support, as per the Security Policy.

5. Taking measures against the forgery of certificates and guaranteeing confidentiality during the generation process in conformity with section 6 and ensure secure delivery of the certificate to the signatory.

6. Using reliable systems to store qualified certificates that verify their authentication and prevent unauthorised individuals from altering the data, restricting their accessibility in the cases, or to the individuals, that the signatory has indicated, and that detect any modification that would affect these security conditions.

- Proper security management, thanks to implementing an Information Security Management System as per the principles stipulated by ISO/IEC 27001, which includes, but is not limited to, the following measures:

1. Periodically performing regular security checks to verify compliance with established standards.

2. Comprehensively managing security events, in order to guarantee detection, resolution and optimisation.

3. Maintaining appropriate contact and relationships with special interest groups in security, such as specialists, security forums and professional associations related to information security.

4. Appropriately planning system maintenance and evolution, in order to guarantee appropriate performance at all times, as well as service that is guaranteed to comply with user and client expectations.

9.6.1.3 Identification obligations

For qualified certificates, IZENPE identifies the certificate subscriber, as per the assurance levels defined in Commission Implementing Regulation (EU) 2015/1502 dated 8 September 2015, and this Certification Practice Statement.

9.6.1.4 User information obligations

- Before issuing and delivering the certificate to the subscriber, IZENPE informs them by referencing the document "Terms and Conditions for Use and Dissemination Agreement for the Public Key Infrastructure (PKI - PDS)", available at www.izenpe.com, of the terms and conditions for use of the certificate, of its price (when established), its limitations of use and the binding legal instruments to which 2.1.1.6 of this Certification Practice Statement makes reference.

- IZENPE will inform the key holder about the expiry of their certificate prior to or at the same time as the electronic certificate expires, specifying the reasons and date and time that the certificate will no longer be effective.

- IZENPE shall communicate cessation of its activity in providing certification services to signatories two months beforehand, and if applicable, shall inform as to the

characteristics of the provider to whom it is proposed to transfer certificate management. Notification to signatories will be conducted in accordance with the stipulations of this document.

- IZENPE has a termination of service plan which specifies the conditions under which such an event would take place.

9.6.1.5 Obligations regarding verification programmes

IZENPE provides the public with verification mechanisms to check the validity of certificates through systems described in this Certification Practice Statement.

9.6.1.6 Obligations regarding legal regulation of the certification service

IZENPE assumes all of the obligations directly incorporated in the certificate or incorporated by reference. Incorporation by reference is the inclusion of an object identifier in the certificate, or another way to link to a document.

The legal instrument that binds IZENPE and the applicant, subscriber or key holder and the relying party is in writing and in readily understandable language, and contains, at least, the following content:

- Provisions set forth to comply with sections 2.1.4, 2.1.5, 2.1.6, 2.2, 2.3 and 2.4 of this Certification Practice Statement.
- Indication of the applicable Certification Practice Statement, indicating, if applicable, that the certificates are issued to the public and the need to use a secure signature creation of message decryption device.
- Clauses on the issue, revocation, renewal, and if applicable, recovery of private keys.
- Statement that the information contained in the certificate is correct, excepting a notification otherwise by the subscriber.
- Consent for storing the information used for the subscriber log file, for supplying a cryptographic device and for the disclosure of such information to third parties should IZENPE terminate its services without revocation of valid certificates.
- Usage limitations, including those set forth in section 1.3.2.
- Information on how to validate a certificate, including the requirement of verifying the certificate's status, and the conditions under which one can reasonably trust the certificate.
- Applicable limitations of liability, including the usages for which IZENPE accepts or excludes liability.
- Archive period for information from certification application.
- Archive period for audit records.

- Applicable procedures to dispute resolution.
- Applicable law and competent jurisdiction.
- Whether IZENPE has been declared in conformity with the certification policies of other public entities and, if so, with which system.
- The way in which IZENPE guarantees liability for damages.

9.6.2 Registration Authority obligations

Before Izenpe authorises delegation of the Registration Authority functions with a third party, said party must formally undertake the following obligations by means of the pertinent legal instrument:

- To verify the identity and other personal circumstances of the applicant, subscriber or key holder on the certificates, or that are relevant for the purpose of the certificates, as per these procedures.
- Save all information and documentation regarding certificates for which it manages the issue, renewal, revocation or reactivation.
- To notify IZENPE of certificate revocation requests with due diligence and in a swift and reliable manner.
- To allow IZENPE access to its procedures archives and audit logs in order to perform its functions and maintain the necessary information.
- To inform IZENPE of all issuance, renewal, reactivation requests and any other aspects related to the certificates issued by IZENPE.
- Verify, with due diligence, the reasons for revocation that may affect the validity of the certificates.
- To comply with the procedures established by IZENPE and with the current legislation in this area, in its management operations connected with the issuance, renewal, revocation and reactivation of certificates.
- To comply with Izenpe's Provider Security Policy.

9.6.3 Holder obligations

The certificate applicant undertakes to:

- Guarantee that the information provided on the certificate request, and that should be included therein, is truthful, complete and up-to-date.
- Comply with the application procedure defined in the specific documentation.
- Within a maximum period of three months, pay the amount due for the type of certificate, under the conditions set forth by Izenpe.

The subscriber undertakes to:

- Provide IZENPE with complete and appropriate information in accordance with the requirements described in the Certification Practice Statement, particularly with regard to the registration procedure.
- Guarantee that the information that should be included therein, is truthful, complete and up-to-date.
- Be aware of, and accept conditions for certificate use, as well as modifications made to said conditions.
- State their consent prior to issuing and delivering a certificate.
- Guarantee the proper usage and maintenance of certificate media storage.
- Make proper use of the certificate and in particular, comply with the usage limitations thereto.
- Diligently safeguard the private key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of the Certification Practice Statement.
- Notify IZENPE and any other person the subscriber thinks might rely on the certificate without any reasonable delay if any of the following occur:
    - Loss, theft or potential compromise of the private key.
    - Loss of control over the private key, due to compromise of activation data (for example, the cryptographic device PIN) or for any other reason.
    - Inaccuracies or changes to the certificate of which the subscriber is aware or may be aware, urging that the certificate be revoked when said modification is a reason for it to be revoked.
- Cease using the private key at the end of the certificate validity period.
- Transfer specific obligations to key owners.
- Refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from the Certification Authority.
- Refrain from intentionally compromising the security of certification services.
- Refrain from using the private keys corresponding to the public keys included in the certificates for the purpose of signing a certificate as if performing the function of a Certification Authority.

9.6.4 Obligations of the relying parties

The certificate verification user undertakes to:

- Independently ensure that the certificate is appropriate for its intended use.
- Understand the terms and conditions of use of the certificates in accordance with the Certification Practice Statement and the certification service contract signed by the certificate verifier and IZENPE.

- Verify the validity or revocation of issued certificates, to which end the user shall use information on the status of the certificates.
- Verify all certificates in the certificate hierarchy, before trusting the digital signature or any of the certificates in the hierarchy.
- Bear in mind any limitation in the use of the certificate, regardless of whether this is found in the very certificate itself or in the verifying contract.
- Bear in mind any precaution stipulated in a contract or other instrument, regardless of its legal nature.
- Notify any anomalous circumstance or situation regarding the certificate that may be deemed as a cause to revoke it.
- Refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from IZENPE.
- Refrain from intentionally compromising the security of certification services.

9.6.5 Obligations of other participants

In providing its service as a Time Stamp Authority, Izenpe takes responsibility for variation in the time reference, regarding the reference provided by the Time Section of the Royal Institute and Observatory of the Armada, which inserts it into the electronic time stamps at the moment of request, but not for the veracity nor the content represented by the electronic data sent by service user entities that are the object of the electronic time stamp issued.

9.7 Waiver of guarantees

Not stipulated.

9.8 Liability limitation

9.8.1 Certification Authority liabilities

IZENPE is liable for negligence or a lack of due diligence exercised in providing the certification services described in this Certification Practice Statement, and for a failure to meet any of the legal obligations set forth in electronic signature legislation, except in the following cases:

- In no event shall IZENPE be held liable for damages caused by the information contained in the certificates provided that the content thereof substantially complies with the Certification Practice Statement.
- In no event shall IZENPE be held liable for damages caused by certificate expiration, provided that it substantially complies with the publication obligations set forth in this Certification Practice Statement.
- IZENPE shall not be liable for any direct, indirect, special, incidental, consequential damages, lost profits, loss of data, punitive damages, whether foreseeable or not, arising in connection with the use, delivery, licencing, operation or

non-operation of the Certificates, digital signatures, or any other transaction or service offered or contemplated in the Certification Practices Statement in case of misuse.

- In no event shall IZENPE be held liable for damages to subscribers or bona fide third parties due to inaccuracies in the information contained in the certificate when such information has been certified by an official, notarized or otherwise authorized document, except in the case of documents supplied by the Registration Authority.
- IZENPE shall not be held liable for damages to subscribers or bona fide third parties for failure to comply with the duties attached to subscribers or relying parties.

IZENPE shall be held liable for harm and damage caused to any individual, due to a lack of or delay in inclusion in the consulting service for the validity of certificates or expiry of certificate validity.

Furthermore, it shall be held liable to third parties for actions of individuals to whom it has delegated the roles necessary to provide certification services. In this regard, a civil liability insurance policy has been taken out to cover the risk of liability for harm and damage that may arise in using the certificates.

9.8.2 Registration authority liabilities

Any organisation other than IZENPE that acts in the role of Registration Authority shall be liable to IZENPE for damages incurred in the performance of the duties it assumes, under the terms established in the corresponding legal agreement.

When the identification functions are carried out by the Public Administrations that subscribe to the certificates, the patrimonial responsibility of the Public Administrations will apply, as established by the Law on the Legal Regime of Public Administrations and the Common Administrative Procedure.

9.8.3 Subscriber liabilities

The Subscriber shall be held liable for all of the authenticated electronic transactions using a digital signature generated with the Subscriber's private key when the certificate has been validated through the verification services provided by IZENPE.

If no notification of loss or theft of the certificate is received, as laid down in this Certificate Practice Statement, any liability resulting from the unauthorized use and/or misuse of the certificates shall, in all cases, be the responsibility of the Subscriber.

By accepting the certificates, the Subscriber undertakes to protect and, where applicable, indemnify IZENPE, the Registration Authorities and the User Entities for any act or omission that may result in damages, loss, debts, legal fees or any other type of expense, including payment for professional services, incurred by IZENPE, the Registration Authorities and the User Entities, caused by the use or publication of certificates, and which result from:

- the failure to comply with the terms and conditions laid down in the legal instrument that binds it to the Certification Authority,
- the use of digital certificates in electronic transactions with unauthorized persons,
- a falsehood or misrepresentation of fact by the Subscriber,
- failure by the Subscriber to disclose a material fact in the certificates, if the misrepresentation or omission was made negligently or with intent to deceive IZENPE, the Public Entity Users or parties relying on the Subscriber's certificate, and
- the failure to protect the private key or to otherwise take reasonable precautions to prevent the loss, disclosure, modification or unauthorized use of the private keys.

In this sense, IZENPE shall not be held liable for damages to subscribers or bona fide third parties for failure to comply with the following duties attached to the subscriber:

- Provide IZENPE or the Registration Authority with full, complete and precise information on their certificate applications and the any other information needed for the issuance or revocation thereof, when inaccuracies in the information have not been detected by the service provider.
- Promptly notify IZENPE or the Registration Authority of any changes in the information submitted for the certificate.
- Diligently save signature creation data in order to ensure confidentiality and protect the data from any access or revelation.
- Apply for certificate revocation if there is any doubt regarding maintaining the confidentiality of signature creation data.
- Abstain from using the signature creation data from the time the certificate's validity period expires, or the service provider notifies that it is no longer valid.
- Follow the limits on the certificate regarding its possible uses, and using it as per the established conditions communicated to the certification services signatory.

9.8.4 Relying third party liability

A relying party who vests trust in a certificate that has not been verified assumes all of the risks associated therewith and under no circumstances shall hold IZENPE, the Registration Authorities, User Entities or Subscribers liable for any circumstance resulting from their trust in such certificates and signatures.

In this sense, IZENPE shall not be held liable for damages to subscribers or bona fide third parties if the recipient of the electronically signed documents fails to comply with any of the following due diligence obligations:

- Verifying and bearing in mind the restrictions on the certificate regarding its possible uses and the itemised amount of transactions that can be made with it.
- Ensuring the validity of the certificate.
- Check the digital identifier of the qualified certificate in the Trusted Service List (TSL).

9.9 Compensation

Should IZENPE fail to meet its obligations or breach the requirements of the law, indemnification clauses are included in the legal instruments which link IZENPE to the subscriber and verifier.

9.10 Validity period

9.10.1 Term

The CPS comes into force as soon as it is published.

9.10.2 Termination

The current CPS will be revoked as soon as a new version of the document is published. The new version will fully substitute the previous document.

9.10.3 Effects of termination

For the valid certificates issued under a previous CPS, the new version will prevail over the former in everything not opposed to it.

9.11 Individual notifications and communication with participants

IZENPE establishes the media and deadlines for notifications in the binding legal instrument.

In general, the IZENPE website www.izenpe.eus will be used to make any type of notification and communication.

9.12 Amendments to this document

9.12.1 Procedure for changes

Modifications to this document shall be approved by IZENPE's Security Committee. Amendments will be set forth in a document entitled Certification Practice Statement Update, the maintenance of which is guaranteed by IZENPE.

The updated versions of the Certification Practice Statement, along with the list of amendments made, can be consulted online at www.izenpe.com.

IZENPE may unilaterally amend the Certification Practice Statement provided that the following procedure is observed:

- Any amendment must be justified from a technical, legal or commercial perspective, and must be attested by IZENPE management.
- All of the technical and legal implications should be considered part of the new version of specifications.
- An amendment control procedure shall be established to ensure that the resulting specifications meet the requirements they set out to fulfil and which brought about the change.
- The implications of the change in specifications to the user must be established and the user must be notified of such changes.

9.12.2 Notification period and mechanism

The IZENPE Security Committee will annually review the CPS and, in any case, when it must be modified. This review will be performed jointly among responsible areas and participants in drawing it up and maintaining it.

IZENPE may make modifications to this document without having to previously inform users, for example:

- Typographical corrections made in the document
- Changes in contact details.

Modifications that could require informing users, such as:

- Changes in the specifications or service conditions.
- Changes in URLs

9.12.3 Circumstances under which an OID must be changed

The OID will be changed when one of the procedures described in this document is changed.

9.13 Complaints and dispute resolution

IZENPE is subject to the commercial arbitration system pursuant to the provisions of applicable law as a means of addressing and resolving disputes or claims lodged by applicants or subscribers of citizen certificates; all decisions are deemed to be final and binding by both parties.

To this effect it is understood that the applicant or subscriber conforms to the system from the time the claim for arbitration is submitted to the corresponding commercial arbitration board.

Any other contentious matters brought forward by applicants or subscribers with regard to citizen certificates not regulated by the commercial arbitration system shall be subject to the competent jurisdiction.

9.14 Applicable regulations

The implementation, preparation, interpretation and validity of this Certification Practice Statement are governed in accordance with Spanish law on electronic signatures.

The applicable regulations to this document and the operations deriving from them are as follows:

- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.
- Regulation 910/2014 on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC
- Regulation 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation 910/2014 as regards the establishment of the European digital identity framework

- Public Administration Common Administrative Procedural Law 39/2015
- Public Sector Legal Scheme Law 40-2015
- Organic Law 3/2018 of 5 December on Personal Data Protection and guarantee of digital rights.
- (EU) Regulation 2016/679 on the protection of natural persons regarding personal data processing and the free circulation of these data, repealing Directive 95/46/EC (GDPR)

Additionally, the practice for trust services intended by Izenpe follow these standards:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- General Statement of Trust Service and Electronic Certification Practices Version 5.7
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- CABForum Baseline Requirements
- CABForum EV Certificate Guidelines

9.15 Compliance with applicable legislation

The parties shall submit to the competent jurisdiction governed by Spanish procedural law.

In any case, IZENPE demonstrates meeting the standards given in section 9.14.

9.16 Various stipulations

9.16.1 Full agreement

Each clause contained in this Certification Practice Statement is valid in itself and does not impair the remainder of the clauses. The invalid or incomplete clause can be substituted for another equivalent clause.

None of the terms and provisions of this Certification Practice Statement which directly affect the rights and obligations of IZENPE and do not affect the remaining parties may be amended, waived, supplemented, modified or eliminated without authorized written consent from IZENPE; in no case does such a change effect a novation but rather a modification which does not affect the remainder of the rights and obligations of the other parties.

9.16.2 Allocation

Izenpe shall not be held liable for lack of service of anomalies therein, nor for damages and harm that may be directly or indirectly caused when the failure or disaster is caused by force majeure, terrorist attack, sabotage or wildcat strikes; all this notwithstanding conducting the actions necessary to remedy and/or re-initiate the service as quickly as possible.

9.16.3 Severability

Not stipulated.

9.16.4 Compliance

Not stipulated.

9.16.5 Force Majeure

Not stipulated.

9.16.6 Other stipulations

As Trust Service Provider, Izenpe shall provide services to all interested parties who request them under the conditions set forth in this CPS and the Policies, Practices and Laws for Issue applicable to the subject of the request.

When used and combined appropriately, Izenpe's trust services shall allow Users, Subscribers, Holders and more to exchange information on the security measures necessary for the identification, authentication, non-repudiation and confidentiality of the parties.

Izenpe manages its certification services and issues SSL certificates pursuant to the latest version of "Base Requirements for Issue and Management of Trust Certificates," requirements established by the CA/BrowserForum entity (which may be viewed at https://cabforum.org/baseline-requirements-documents/) and pursuant to the latest version of requirements defined by the entity CA/Browser Forum in its "guide for issue and management of Extended Validation Certificates" (which may be viewed at https://cabforum.org/extended- validation/).

Izenpe shall review its certification policies and practices to keep them in line with the aforementioned requirements. If there is any discrepancy between this document and the “Guide for issue and management of Extended Validation Certificates”, the guidelines that appear in said guide shall prevail over this document.

Izenpe allows third parties to verify and test all kinds of certificates that it issues. To this end, it has a set of test certificates available at www.izenpe.eus.