Global Trust Practices Statement

Digitally signed by
ZIURTAPEN ETA ZERBITZU
ENPRESA-EMPRESA DE
CERTIFICACION Y SERVIC
Date: 2025.09.03 13:54:57
+02'00'

© Izenpe 2025

Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.eus
izenpe@izenpe.eus

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 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, 1.1.1 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
8.0	19/06/2025	Adaptation of the Certification Practice Statement to the amendment of Regulation (EU) No 910/2014.

Table of contents

Content

1 Introduction. 15

1.1 Presentation. 15

1.2 Document name and identification. 16

1.2.1 Identification. 16

1.2.2 Certificates identifier. 17

1.3 Participants in the Public Key Infrastructure (PKI). 19

1.3.1 Certification Authorities. 20

1.3.2 Registration Authorities. 23

1.3.3 Certificate Subscribers. 24

1.3.4 Trusting Third Parties. 24

1.3.5 Other participants. 24

1.4 Certificate uses. 24

1.4.1 Appropriate certificate uses. 24

1.4.2 Prohibited certificate uses. 33

1.5 Policy Administration. 33

1.5.1 Entity responsible for managing documentation. 33

1.5.2 Contact details. 34

1.5.3 Responsible Parties for the Adaptation of the GTPS 34

1.5.4 GTPS Approval Procedure 34

1.6 Definitions and acronyms. 34

1.6.1 Definitions. 34

1.6.2 Acronyms 37

2 Publication and supervisors of information repository. 40

2.1 Information repository. 40

2.2 Publication of certification information. 40

2.2.1 Publication and Notification Policy. 40

2.2.2 Items not published in the Global Certification Practice Statement 40

2.3 Frequency of publication. 40

2.4 Controlling access to the repository. 40

3 Identification and Authentication. 42

3.1 Names. 42

3.1.1 Types of names. 42

3.1.2 Meaning of names. 42

3.1.3 Pseudonyms. 42

3.1.4 Rules for interpreting name formats. 42

3.1.5 Uniqueness of names. 42

3.1.6 Resolving conflicts relating to names and processing trademarks. 42

3.1.7 Issuer. 43

3.1.8 Subject. 43

3.2 Validation of identity. 43

3.2.1 Methods for proving possession of the private key. 43

3.2.2 Authentication of the Organisation Identity. 43

3.2.3 Authentication of the identity of the natural person applicant. 44

3.2.4 Unverified subscriber information. 44

3.2.5 Authority validation. 44

3.2.6 Interoperability criteria. 44

3.3 Identification and authentication for requests to reissue keys. 44

3.3.1 Routine renewal. 44

3.3.2 Renewal after revocation. 44

3.4 Identification and authentication for revocation requests. 45

4 Operative requisites for the certificates' life cycle 46

4.1 Certificate application. 46

4.1.1 Verification of application. 46

4.1.2 Signing up process and responsibilities. 46

4.2 Request Management. 47

4.2.1 Carrying out identification and authentication functions. 47

4.2.2 Application processing time. 47

4.3 Certificate issuance. 47

4.3.1 CA actions during issuance. 47

4.3.2 Izenpe will proceed with the issuance of the certificate as determined in the relevant CPS or PDS. Notification of certificate issuance. 47

4.3.3 Verification of the certificate. 47

4.4 Certificate acceptance. 48

4.4.1 Certificate acceptance process. 48

4.4.2 Publication of the certificate by the CA. 48

4.4.3 Notification of certificate issuance by the CA and other entities. 48

4.5 Pair of keys and uses of the certificate. 48

4.5.1 Subscriber's private key and use of the certificate. 48

4.5.2 Use of the public key and the certificate by relying parties 49

4.6 Certificate revocation. 50

4.6.1 Circumstances for certificate renewal. 50

4.6.2 Who may apply for renewal. 50

4.6.3 Processing certificate renewal requests. 50

4.6.4 Notification to the subscriber. 50

4.6.5 Renewed certificate acceptance procedure. 50

4.6.6 Publishing the certificate. 50

4.6.7 Notifying other entities. 51

4.7 Renewal with certificate key regeneration. 51

4.7.1 Circumstances to regenerate certificate keys. 51

4.7.2 Who can apply. 51

4.7.3 Processing renewal applications with key regeneration. 51

4.7.4 Renewed certificate acceptance procedure. 51

4.7.5 Publishing the certificate. 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. 52

4.8.4 Notification of certificate modification. 52

4.8.5 Publication of the modified certificate. 52

4.8.6 Notification of certificate modification to other entities. 52

4.9 Revocation. 52

4.9.1 Circumstances for revocation. 52

4.9.2 Who can request revocation. 53

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. 54

4.9.6 Obligation to verify revocations by relying parties. 54

4.9.7 Frequency of CRL generation. 54

4.9.8 Time passing between generation and publication of the CRLs. 54
4.9.9 Online revocation checking requisites. 54
4.9.10 Other revocation notifications available. 55
4.9.11 Special committed key requisites. 55
4.9.12 Circumstances for suspension. 55
4.9.13 Who can request suspension. 55
4.9.14 Procedure for requesting suspension. 55
4.9.15 Limits on the period of suspension. 55
4.10 Certificate status services. 56
4.10.1 Operational characteristics. 56
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. 57
5.1.4 Exposure to water. 57
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. 58

5.2.1 Trusted roles. 58

5.2.2 Number of people per task. 58

5.2.3 Identification and authentication for each role. 58

5.2.4 Separating tasks into different roles. 59

5.3 Personnel controls. 59

5.3.1 Background, qualifications, experience, and clearance requirements. 59

5.3.2 Background check procedures. 59

5.3.3 Training requirements. 59

5.3.4 Retraining frequency and requirements. 59

5.3.5 Sequence and frequency of job rotation. 59

5.3.6 Sanctions for unauthorised actions. 59

5.3.7 Recruitment requirements. 60

5.3.8 Provision of documentation to staff. 60

5.4 Audit. 60

5.4.1 Type of events recorded. 60

5.4.2 Frequency of log processing. 60

5.4.3 Period for audit log retention. 61

5.4.4 Protecting the audit log. 61

5.4.5 Audit log backup procedure. 61

5.4.6 Compiling logs. 61

5.4.7 Vulnerability analysis. 61

5.5 Archiving of records. 61

5.5.1 Type of records archived. 61

5.5.2 File retention period. 61
5.5.3 File protection. 62
5.5.4 Archive backup procedures. 62
5.5.5 Requisites for time stamping the records. 62
5.5.6 Filing system. 62
5.5.7 Procedures to obtain and verify the archive information. 62
5.6 CA key change. 62
5.7 Incident Management and Contingency Plan. 62
5.7.1 Incident management procedures. 62
5.7.2 Action plan to deal with corrupt data and software. 63
5.7.3 Procedure in case of compromise of the CA's private key. 63
5.7.4 Business continuity after a disaster. 64
5.8 CA or RA termination. 64
5.8.1 Certification Authority. 64
5.8.2 Registration Authority. 65
6 Technical security controls 66
6.1 Key pair generation and installation. 66
6.1.1 Key pair generation. 66
6.1.2 Private key delivery to subscriber. 66
6.1.3 Public key delivery to certificate issuer. 66
6.1.4 Certification Authority public key delivery to certificate users 67. 66
6.1.5 Key sizes. 66
6.1.6 Public Key Generation and Quality Assurance Parameters. 67
6.1.7 Supported Key Usages (KeyUsage field X.509 v3). 67
6.2 Private key protection. 68

6.2.1 Standards for cryptographic modules. 68
6.2.2 Private key (n out of m) multi-person control. 68
6.2.3 Private key custody. 68
6.2.4 Private key backup. 68
6.2.5 Private key archiving. 69
6.2.6 Transfer of the private key to or from the cryptographic module. 69
6.2.7 Storage of the private key in the cryptographic module. 69
6.2.8 Private key activation method. 69
6.2.9 Private key deactivation method. 69
6.2.10 Private key destruction method. 69
6.2.11 Qualifying the cryptographic module. 70
6.3 Other aspects of key pair management. 70
6.3.1 Public key archiving. 70
6.3.2 Certificate operation periods and key pair use periods. 70
6.4 Activation data. 70
6.4.1 Generation and installation of activation data. 70
6.4.2 Activation data protection. 70
6.4.3 Other aspects of the activation data. 71
6.5 Computer security controls. 71
6.5.1 Specific technical requirements for computer security. 71
6.5.2 Assessment of the level of IT security. 72
6.6 Life cycle engineering controls. 72
6.6.1 System development controls. 72
6.6.2 Security management controls. 72
6.6.3 Life cycle security controls 72

6.7 Network security controls. 72

6.8 Time source. 73

7 Revoked Certificate and CRL profiles. 74

7.1 Certificate profile. 74

7.1.1 Version number 74

7.1.2 Certificate extensions. 74

7.1.3 Algorithm object identifiers. 74

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. 75

7.1.8 Syntax and semantics of policy qualifiers. 75

7.1.9 Semantic treatment for the “Certificate policy” extension. 75

7.2 Certificate revocation list profile. 75

7.2.1 Version number. 76

7.2.2 List of certificate revocation and extensions of elements from the list. 76

7.3 OCSP profile. 76

7.3.1 Version number. 76

7.3.2 OCSP Extensions. 76

7.3.3 Other OCSP aspects. 76

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

9 Other legal and activity matters. 79

9.1 Fees. 79

9.1.1 Fees for the issue or renewal of certificates. 79

9.1.2 Fees for access to certificates. 79

9.1.3 Certificate status information access fees. 79

9.1.4 Fees for other services. 79

9.1.5 Refund policy. 79

9.2 Financial responsibility. 79

9.2.1 Liability insurance. 79

9.2.2 Other assets. 79

9.2.3 Insurance and guarantees for end entities. 79

9.2.4 Scope of confidential information. 80

9.2.5 Information beyond the scope. 80

9.2.6 Responsibility to protect confidential information. 81

9.3 Personal data protection. 81

9.3.1 Privacy Plan. 81

9.3.2 Information treated as private. 81

9.3.3 Information not considered private. 81

9.3.4 Responsibility to protect private information. 81

9.3.5 Notice and consent to use private information. 82

9.3.6 Disclosure pursuant to judicial or administrative process. 82

9.3.7 Other disclosure circumstances. 82

9.4 Intellectual property rights 82

9.4.1 Property rights in certificates. 82

9.4.2 Ownership of the GTPS. 83
9.4.3 Property rights in names. 83
9.4.4 Property rights in keys and key material. 83
9.5 Obligations and guarantees. 83
9.5.1 Obligations of the CA. 83
9.5.2 Registration Authority obligations. 86
9.5.3 Holder obligations. 86
9.5.4 Obligations of the relying parties. 87
9.5.5 Obligations of other participants. 88
9.6 Waiver of guarantees. 88
9.7 Liability limitation. 88
9.7.1 Certification Authority liabilities 88
9.7.2 Registration authority liabilities 89
9.7.3 Subscriber liabilities 89
9.7.4 Relying third party liability 90
9.8 Compensations. 90
9.9 Validity period. 90
9.9.1 Entry into Force. 90
9.9.2 Termination. 90
9.9.3 Effects of termination. 91
9.10 Individual notifications and communication with participants. 91
9.11 Amendments to this document. 91
9.11.1 Procedure for changes. 91
9.11.2 Notification period and mechanism. 91
9.11.3 Circumstances under which an OID must be changed. 92

9.12 Complaints and dispute resolution. 92

9.13 Applicable regulations. 92

9.14 Compliance with applicable legislation. 93

9.15 Various stipulations. 93

9.15.1 Full agreement. 93

9.15.2 Allocation. 93

9.15.3 Severability. 93

9.15.4 Compliance 93

9.15.5 Force Majeure 93

9.15.6 Other stipulations. 93

1 Introduction.

1. 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.
2. Based on these principles, the Basque Government and the Provincial Councils, through their respective IT companies, decided to develop, within a collaborative framework, a proprietary and common certification and electronic signature system that ensures interoperability, so that the certificates issued would be valid across applications and procedures of the different administrations.
3. This collaborative intention was first expressed with the establishment, in June 2002, of the commercial company "Ziurtapen eta Zerbitzu Enpresa - Certification and Services Company, IZENPE, S.A." (hereinafter, Izenpe). The objective of this collaboration is the development of trust services, as suitable means to advance the simplification of interactions between citizens and the administration.

1.1 Presentation.

4. The eIDAS Regulation contemplates the possibility of becoming a Qualified Trust Service Provider.
5. 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.
6. 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.
7. 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.
8. Izenpe, in providing trust services, follows the guidelines of the ETSI (European Telecommunications Standards Institute) standards. In the case of secure server certificates (SSLs), the guidelines approved by the CA/Browser Forum, available at www.cabforum.org, are also followed.
9. The technical specifications (ETSI TS) defined in these standards set out the basic requirements concerning the management and practices of trust service providers issuing qualified and unqualified certificates, as well as time stamps, within the legal framework of

the eIDAS Regulation incorporated into the legal regime of "Law 6/2020, of 11 November, regulating certain aspects of electronic trust services." These have recently been appropriately updated in new European standards: EN 319 411-1 for certificate issuance, EN 319 411-2 for the issuance of qualified certificates under the eIDAS Regulation, and EN 319 421 for the issuance of time stamps as established in the eIDAS Regulation.

10. 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.
11. Izenpe incorporates remote video identification for the issuance of certificates in accordance with "Order ETD/465/2021, of 6 May, regulating remote video identification methods for the issuance of qualified electronic certificates," and with Order ETD/743/2022, of 26 July, which amends Order ETD/465/2021, of 6 May.
12. 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.
13. In addition to qualified trust services, Izenpe offers other unqualified trust services, including the following:
    - Issue of unqualified electronic signature certificates.
    - Issue of unqualified website authentication electronic certificates.
    - Validation of not qualified signatures.

1.2 Document name and identification.

1.2.1 Identification.

14. This document is entitled the "Izenpe Global Trust Practices Statement" and will be referred to internally by its acronym GTPS. This document is structured according to RFC 3647.
15. Izenpe's Security Committee regularly reviews the risks to which the organisation is exposed and approves the necessary treatment plans to ensure the security of the services defined both in this GTPS and in the disclosure texts (PDS).
16. The terms of use, limitations, responsibilities, properties, and any other information deemed specific to each type of certificate will be reflected in the PDS derived from this GTPS, and, where applicable, in the particular CPS documents.
17. These procedures are mainly based on regulations from the European Telecommunications Standards Institute (ETSI).
18. In order to be able to individually identify each type of certificate issued by IZENPE according to this GTPS, an object identifier (OID) is assigned to each kind. These may be viewed in the profile document available at www.izenpe.eus. 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 the disclosure statements (PDS).
- Qctype: indicates the signature type according to eIDAS (stamp, signature, web).

1.2.2 Certificates identifier.

19. Izenpe operates an Infrastructure with a view to providing the following qualified services:
    - Issue of qualified electronic signature certificates.
    - Issue of qualified electronic stamp certificates.
    - Issue of qualified website authentication electronic certificates.
    - Issue of qualified electronic time stamp service.

20. Within the scope of this GTPS and the PDSs, Izenpe issues the following types of certificates:

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

1.2.2.1.1 Qualified eIDAS certificates.

Description	Policy	OID
Citizen Certificate		
Citizen (chip)	QCP-n	1.3.6.1.4.1.14777.2.18.1
BaKQ (HSM)	QCP-n	1.3.6.1.4.1.14777.2.18.3
Entity Representative Certificates		
Representative (software)	QCP-n	1.3.6.1.4.1.14777.2.12
Representative (chip)	QCP-n	1.3.6.1.4.1.14777.2.16
Entity Representative Certificates SPJ		
SPJ Entity Representative (HSM)	QCP-n	1.3.6.1.4.1.14777.2.15
SPJ Entity Representative (chip).	QCP-n	1.3.6.1.4.1.14777.2.13
SPJ Entity Representative (software)	QCP-n	1.3.6.1.4.1.14777.2.17
Public Employee Certificates (PEP)		
Public Employee (chip)	QCP-n	1.3.6.1.4.1.14777.4.14.1
Public Employee (software)	QCP-n	1.3.6.1.4.1.14777.4.14.2
Public Employee (HSM)	QCP-n	1.3.6.1.4.1.14777.4.14.3
Public Employee Personnel Certificates (PEP) with pseudonym		
Public Entity Personnel with pseudonym (chip) SIGNATURE	QCP-n	1.3.6.1.4.1.14777.4.13.1.1

Public Entity Staff with pseudonym (software)	QCP-n	1.3.6.1.4.1.14777.4.13.2
Professional Certificates		
Qualified Corporate (chip)	QCP-n	1.3.6.1.4.1.14777.2.19.1
Qualified Corporate (software)	QCP-n	1.3.6.1.4.1.14777.2.19.2
Qualified Corporate (HSM)	QCP-n	1.3.6.1.4.1.14777.2.19.3
Entity Electronic Seal Certificates		
Entity Seal (container)	QCP-l	1.3.6.1.4.1.14777.2.11
Entity seal (HSM)	QCP-l	1.3.6.1.4.1.14777.2.20
Administration Electronic Seal Certificates		
Administration stamp (software)	QCP-l	1.3.6.1.4.1.14777.4.11.2
Administration seal (HSM)	QCP-l	1.3.6.1.4.1.14777.4.11.3
Web Authentication Certificates		
Qualified SSL	QEVCP-w	1.3.6.1.4.1.14777.50.3.2
Qualified SSL	QEVCP-w	1.3.6.1.4.1.14777.6.1.3

1.2.2.1.2 Unqualified certificates

Description	Policy	OID
Unqualified self-employed certificates		
BaK	NCP	1.3.6.1.4.1.14777.5.2.5
Izenpe Mobile (APP)	NCP	1.3.6.1.4.1.14777.5.2.5.4
Self-employed (software)	NCP	1.3.6.1.4.1.14777.5.2.7.2
Unqualified Professional Certificates		
Public employee personnel with pseudonym (chip) for Authentication	NCP+	1.3.6.1.4.1.14777.4.13.1.2
Public employee personnel with pseudonym (chip) for Encryption	N/A	1.3.6.1.4.1.14777.4.13.1.3
No Qualified Corporate (chip) Not recognised public corporate (chip)	NCP+	1.3.6.1.4.1.14777.1.1.1
Unrecognised private corporate (chip)	NCP+	1.3.6.1.4.1.14777.5.2.2
Unqualified Web Authentication Certificates		
SSL DV	DVCP	1.3.6.1.4.1.14777.1.2.4
SSL OV	OVCP	1.3.6.1.4.1.14777.1.2.1
Unqualified Application Certificates		
Application (software)	NCP	1.3.6.1.4.1.14777.1.2.2

Unqualified IOT Device Certificates		
Device (software)	NCP	1.3.6.1.4.1.14777.1.3.2

1.2.2.2 Hierarchy CA root 2020.

1.2.2.2.1 SSL Certificates.

Description	Policy	OID
Web Authentication Certificates		
SSL DV	DVCP	1.3.6.1.4.1.14777.14.1.2

1.2.2.2.2 Time stamp Certificate.

Description	Policy	OID
Time stamp Certificate		
TSA		1.3.6.1.4.1.14777.10.1

1.2.2.3 Hierarchy CA root 2024.

1.2.2.3.1 Qualified Eidas certificates.

Description	Policy	OID
Web Authentication Certificates		
Qualified SSL	QEVCP-w	1.3.6.1.4.1.14777.50.3.2

1.2.2.3.2 Unqualified certificates

Description	Policy	OID
Unqualified Web Authentication Certificates		
SSL DV	DVCP	1.3.6.1.4.1.14777.50.1.2
SSL OV	OVCP	1.3.6.1.4.1.14777.50.2.2

1.3 Participants in the Public Key Infrastructure (PKI).

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

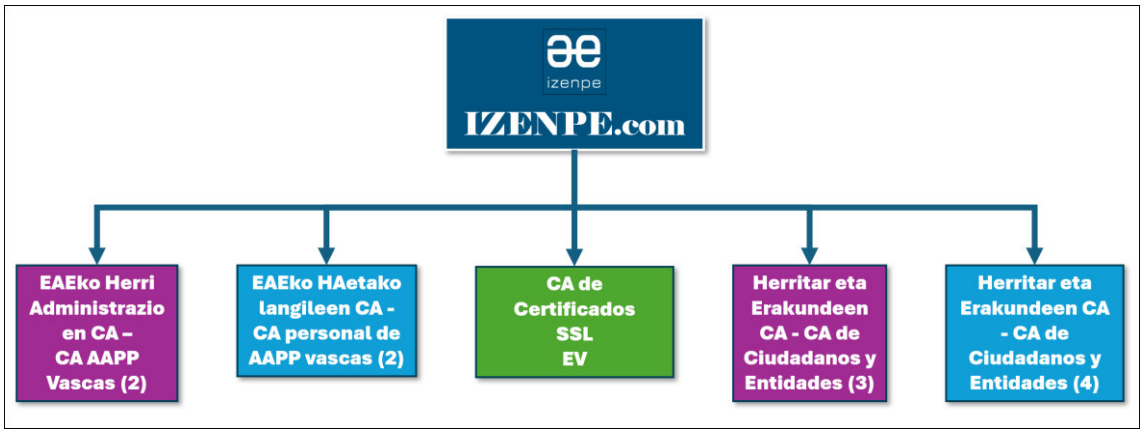
- Certification Authorities.
- Registration Authorities.

- Subscribers and signatories of the certificates.
- Relying Parties.
- Other participants.

1.3.1 Certification Authorities.

22. Izenpe has the following certification authorities:

1.3.1.1 Izenpe.com hierarchy created in 2007.



Root CA Certificate.

CN	Izenpe.com
VALIDITY	13/12/2007 until 13/12/2037
HASH SHA256	25:30:CC:8E:98:32:15:02:BA:D9:6F:9B:1F:BA:1B:09:9E:2D:29:9E:0F:45:48:BB:91:4F:36:3B:C0:D4:53:1F
KEY TYPE	RSA 4096 bits / SHA-256 with RSA

Subordinate CA Certificate.

CN	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)
VALIDITY	20/10/2010 until 13/12/2037
HASH SHA256	CD:6E:B9:37:EE:17:A9:FC:FF:60:A7:90:F8:BD:E0:CA:9A:BC:A0:7B:3E:F4:60:74:DD:19:78:F0:BC:A4:D4:49
KEY TYPE	RSA 4096 bits / SHA-256 with RSA

Subordinate CA Certificate.

CN	Basque PA personnel CA (2)
VALIDITY	20/10/2010 until 13/12/2037
HASH SHA256	25:30:3C:FD:0B:F1:BA:A1:EF:24:8C:29:F0:73:FF:FC:2E:7C:81:58:2E:E2:3B:45:C7:F1:C3:B3:2E:34:1A:D8
KEY TYPE	RSA 4096 bits / SHA-256 with RSA

Subordinate CA Certificate.

CN	Certificate CA EV SSL
VALIDITY	06/07/2018 until 06/07/2028
HASH SHA256	DB:47:63:39:CC:BF:CC:9E:4B:D1:D6:CB:60:6C:A2:7F:00:67:9E:1E:F8:A5:81:E7:23:63:09:B9:D6:3F:FE:37
KEY TYPE	RSA 4096 bits / SHA-256 with RSA

Subordinate CA Certificate.

CN	CA = Citizen and Entity CA (3)
VALIDITY	20/10/2010 until 13/12/2037
HASH SHA256	5A:49:B1:5A:E6:0F:F6:27:DA:27:2A:87:43:D6:71:62:BA:CA:10:96:16:82:03:21:3A:CF:82:27:AF:4C:49:42
KEY TYPE	RSA 4096 bits / SHA-256 with RSA

Subordinate CA Certificate.

CN	CA = Citizen and Entity CA (4)
VALIDITY	20/10/2010 until 13/12/2037
HASH SHA256	7E:D1:93:61:AD:73:4D:70:3F:BA:DF:02:9F:52:EC:3B:66:48:D8:DD:56:BA:BA:08:84:ED:4F:85:9B:5B:93:75
KEY TYPE	RSA 4096 bits / SHA-256 with RSA

1.3.1.2 Hierarchy created in 2020.

Certificate CA ROOT 2020

CN		ROOT CA QC IZENPE
VALIDITY		23/09/2045
HASH SHA256		[d4a81325ebf2e5c19c779192c63db76404c8dafd] (CRT)
KEY TYPE		SHA2

Subordinate CA Certificate

CN	SUBCA QC IZENPE - TSA
VALIDITY	23/09/2045
HASH SHA256	[fa6cf62e148806df05f536bc71dfe34b364023e8] (CRT)
KEY TYPE	SHA2

1.3.1.3 Hierarchy created in 2024

Certificate CA ROOT 2024.

CN	ROOT CA SSL IZENPE 2024
VALIDITY	24/09/2049
HASH SHA256	68E93296DEEB4254C18C49C4E80F5D8FA3D38A93
KEY TYPE	ECC(384 Bits)

Subordinate CA Certificate.

CN	SUBCA SSL 2024
VALIDITY	23/09/2045
HASH SHA256	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18
KEY TYPE	ECC(384 Bits)

1.3.2 Registration Authorities.

23. This GTPS applies to the Registration Authorities used by Izenpe in procedures when issuing and managing certificates.
24. Registration Entities perform the tasks of identifying applicants, subscribers and signatories, verifying the documentation accrediting the circumstances on the certificates, as well as validating and approving requests to issue, revoke and renew certificates.
25. Izenpe or the user entities with which Izenpe signs the corresponding legal instrument are the registration authorities.

1.3.3 Certificate Subscribers.

26. The subscriber shall be the person who requests a certificate.

27. The signatories are the individuals who retain sole use of the signature creation data associated with the certificates of which they are holders.

28. Occasionally, the roles of subscriber and signatory do not coincide: legal entities may request certificates for their employees, partners, or workers, where the natural persons are considered "signatories" and the legal entity is considered the "subscriber."

29. Seal creators are legal entities that create electronic seals which include the identity of the legal entity (commercial company, foundation, public administration, etc.).

1.3.4 Trusting Third Parties.

30. Within the scope of this GTPS, natural or legal persons receiving services provided by Izenpe are third parties who rely on these trust services and, as such, are subject to the provisions established in this GTPS.

31. Before relying on the certificates and the signatures and seals they create, third parties must verify them, as established in this GTPS: They must check that a valid certificate has been used, that signatures or seals were created during the certificate's validity period, and that the instructions and guidelines of this GTPS have been followed.

32. 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, among other things, repudiate messages issued within the level of trust attached to the category of certificate or timestamp.

1.3.5 Other participants.

33. Izenpe is the Time Stamp Authority when it provides the Trust Service of electronic time stamp creation under the pertinent GTPS.

1.4 Certificate uses.

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

1.4.1 Appropriate certificate uses.

1.4.1.1 Qualified certificates

35. Qualified electronic signature certificates guarantee the identity of the subscriber and the signatory. When used with secure signature creation devices, they are suitable to support qualified electronic signatures; that is, advanced electronic signatures based on a qualified certificate and generated using a qualified device, which, according to the eIDAS Regulation, are legally equivalent to handwritten signatures without the need to fulfil any additional requirements.

36. Qualified electronic signature certificates are qualified in accordance with Article 28 and Annex I of the eIDAS Regulation.

37. 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 electronic signature guarantees the identity of the signature certificate subscriber.

38. 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.

39. Electronic stamp certificate: it is an electronic statement that 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.

40. Qualified electronic stamp certificates are qualified in accordance with Article 38 and Annex I of the eIDAS Regulation.

41. 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 comply with the requirements of Annex IV of the eIDAS Regulation to be considered qualified.

42. Electronic seal certificates for bodies are issued to public administrations for the identification of the body and electronic sealing of documents, as established in "Law 40/2015, of 1 October, on the Legal Regime of the Public Sector."

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

1.4.1.2 Unqualifiedcertificate.

44. Non-qualified certificates do not reliably guarantee the identity of the subscriber and, when appropriate, the signatory; 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.

45. 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.

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

1.4.1.3 Scope of use of certificates.

47. There are two scenarios that illustrate certificate usage:

    – Certificates issued by Izenpe to the general public are used by subscribers or, where applicable, signatories to conduct electronic transactions with public entity users and public or private institutions that have accepted the use of the certificate system.

48. Consult the specific details regarding the scope of use of each certificate in the PDS and, where applicable, the particular CPS documents.

    – 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, signatories may also employ these certificates for other uses provided that they respect the usage limitations set forth in the paragraph above.

1.4.1.4 Individual Citizen Certificate.

1.4.1.4.1 Qualified certificates.

- Description: individual certificate.
- Validity: up to 4 years.
- Support: issued on card or HSM (remote signature).

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
Citizen Certificate	Card	QCP-n	eIDAS Profile 1.3.6.1.4.1.14777.2.18.1	Advanced
Citizen BakQ Certificate	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	Advanced

1.4.1.4.2 Unqualified certificates

49. BakQ Certificate

- Description: allows the identification and signing of natural persons.

  It consists of a reference number matching the user's DNI/NIE/passport and a password.

  It is an unqualified certificate issued in a centralised repository that will be used for signing acts. The ETSI LCP policy incorporated by Bak implies that its issuance does not require in-person identification.
- Validity: up to 4 years.
- Support: issued HSM (remote signature).

50. Izenpe Mobile Certificate.

- Description: a means that allows individuals to be identified and authorises the use of a qualified certificate stored in a secure centralised Izenpe repository associated with the person. It consists of:
  - An app installed on a mobile device, linked to a non-qualified certificate that enables secure communication processes.
  - A password or a biometric factor that provides access to the app.
- Validity: up to 4 years.
- Support: issued in software.

51. Self-employed Certificate.

- Description: individual certificate issued for interactions of the individual in their capacity as self-employed with the Basque Provincial Tax Authorities.
- Validity: up to 4 years.
- Support: issued in software.

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
BaK	HSM	LCP	1.3.6.1.4.1.14777.5.2.5	Basic
Izenpe Mobile	APP container	NCP	1.3.6.1.4.1.14777.5.2.5.4	N/A (for signing, the BaKQ or professional certificate is used)
Self-employed	Software	LCP	1.3.6.1.4.1.14777.5.2.7.2	Basic

1.4.1.5 Individual Certificate for Entity Representative.

1.4.1.5.1 Qualified certificates.

- Description: certificate issued to a natural person authorised to act on behalf of and represent a legal entity.
- Validity: up to 4 years.
- Support: issued on card, in software container, or remotely on HSM.

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
Entity representative	Cryptographic chip	QCP-n	1.3.6.1.4.1.14777.2.12	Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.16	Advanced

1.4.1.6 Individual Certificate for Entity Representative without legal personality.

- Description: certificate issued to a natural person authorised to act on behalf of and represent an entity without legal personality.
- Validity: up to 4 years.
- Support: issued on card, in software container, or remotely on HSM.

1.4.1.6.1 Qualified certificates.

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
SPJ Entity Representative	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	Advanced
	Cryptographic chip	QCP-n	1.3.6.1.4.1.14777.2.13	Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.17	Advanced

1.4.1.7 Public Employee Certificate.

1.4.1.7.1 Qualified certificates.

- Description: certificate issued to personnel serving public administrations. Issued under the scope of "Law 40/2015, of 1 October, on the Legal Regime of the Public Sector."
- Validity: up to 4 years.
- Support: issued on card, in software container, or remotely on HSM.

Description	Media	Policy identifier	Policy OID	Signature type eIDAS
Public employee	Cryptographic card	QCP-n	1.3.6.1.4.1.14777.4.14.1	Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.4.14.2	Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Advanced

1.4.1.8 Pseudonymous Public Employee Certificate.

1.4.1.8.1 Qualified certificates.

- Description: certificate issued to personnel serving public administrations, characterised by not including personal data of the certificate holder but being issued to a pseudonym in accordance with the document "Electronic Certificate Profiles of the Ministry of Finance and Public Administrations," under the scope of "Law 40/2015, of 1 October, on the Legal Regime of the Public Sector."
- Validity: up to 4 years.
- Support: issued on card or in software container.

Brief description	Media	Policy identifier	Policy OID	Signature type

				eIDAS
Public employee with pseudonym (signature)	Cryptographic card	QCP-n	1.3.6.1.4.1.14777.4.13.1.1	Advanced
Public employee with pseudonym	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.4.13.2	Advanced

1.4.1.8.2 Unqualified certificates

- Description: certificate for authentication and encryption functions issued alongside the qualified signature certificate.
- Validity: up to 4 years.
- Support: issued on card.

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
Public employee with pseudonym	card	NCP+	Authentication 1.3.6.1.4.1.14777.4.13.1.2	n/a
		n/a	Encryption 1.3.6.1.4.1.14777.4.13.1.3	n/a

1.4.1.9 Individual Professional Certificate.

1.4.1.9.1 Qualified certificates

- Description: certificate issued to personnel of an organisation.
- Validity: up to 4 years.
- Support: issued on card, in software container, or remotely on HSM.

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
Qualified corporate	Card	QCP-n	1.3.6.1.4.1.14777.2.19.1	Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.19.2	Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Advanced

1.4.1.9.2 Unqualified certificates

52. Unqualified Professional-Corporate,

- Description: certificate that identifies, with a medium level of assurance, the acting entity as the subscriber of the certificate, as well as the person holding a position or role within it as the signatory.
- Validity: up to 4 years.
- Support: issued on card.

53. Unqualified Private Professional-Corporate
    - Description: crtificate that identifies, with a medium level of assurance, the acting private entity as the subscriber of the certificate, as well as the person holding a position or role within it as the signatory.
    - Validity: up to 4 years.
    - Support: issued on card.

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
Unqualified corporate	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.1.1.1	Basic
Unrecognised private corporate	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.5.2.2	Basic

1.4.1.10 Entity Electronic Seal Certificate (legal persons and unincorporated entities)

- Description: certificate that enables the identification of the entity, as well as, where applicable, the applicant.

  It serves to prove that an electronic document has been issued by the entity, providing certainty about the origin and integrity of the document.

  It is issued to legal persons and entities without legal personality.

  The subscriber shall be the entity. The applicant shall be the natural person authorised to act on behalf of the entity who requests the certificate.

  Information about the natural person may be included in the certificate if expressly determined.
- Validity: up to 3 years.
- Support: issued in software, or remotely on HSM.

1.4.1.10.1 Qualified certificates.

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
Entity seal	Izenpe software container	QCP-l	1.3.6.1.4.1.14777.2.11	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.2.20	Advanced

1.4.1.11 Administrative Electronic Seal Certificate (organ seal).

- Description: certificate that enables the identification of the administration, organ, public body, or public law entity, as well as, where applicable, the identity of the person holding the organ.

  Issued under the scope of "Law 40/2015, of 1 October, on the Legal Regime of the Public Sector."

  The subscriber shall be the administration, organ, public body, or public law entity

  The certificates are of medium level.
- The certificate will be used by the subscriber in those services defined by their organisation as automated action procedures and in those offered by third parties that accept its use under the conditions and limitations defined in this GTPS.
- Validity: up to 3 years.
- Support: issued in software, or remotely on HSM.

1.4.1.11.1 Qualified certificates.

Brief description	Media	Policy identifier	Policy OID	Signature type eIDAS
Administration stamp	Izenpe software container	QCP-l	1.3.6.1.4.1.14777.4.11.2	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.4.11.3	Advanced

1.4.1.12 Website Authentication Certificate (Secure Server).

1.4.1.12.1 Qualified certificates.

- Description: website authentication certificate.

- Validity: up to 395 days[1].
- Support: issued in software.

Brief description	Media	Policy identifier	Policy OID
Qualified SSL	Software	QEVCP-w	1.3.6.1.4.1.14777.6.1.3
Qualified SSL	Software	QEVCP-w	1.3.6.1.4.1.14777.50.3.2

1.4.1.12.2 Unqualified certificates

Brief description	Media	Policy identifier	OIDpolicy
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
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.50.1.2
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.50.2.2
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.14.1.2

1.4.1.13 Application certificates.

1.4.1.13.1 Unqualified certificate.

- Description: certificate used by a software application to ensure the authenticity and integrity of the electronic data associated with the digital signature.
- Validity: up to 3 years.
- Support: issued in software.

Brief description	Media	Policy identifier	Policy OID
Application	Izenpe software container	NCP	1.3.6.1.4.1.14777.1.2.2

1.4.1.14 IOT device certificates.

1.4.1.14.1 Unqualified certificate.

[1]Validity in accordance with the Cabforum.org regulations.

- Description: certificate that creates an identity for objects within an IoT ecosystem, ensuring the integrity and origin of signed documents.
- Validity: up to 10 years.
- Support: issued in software.

Brief description	Media	Policy identifier	Policy OID
Device	Software	NCP	1.3.6.1.4.1.14777.1.3.2

1.4.1.15 Certificate for TSA/TSU Timestamping.

1.4.1.15.1 Timestamp Certificate.

- Description: electronic seal certificate for a legal person with the activation for use in electronic timestamping.
- Validity: up to 5 years.
- Support: issued in software.

BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
TSU Certificate	Software	NA	1.3.6.1.4.1.14777.10.1

1.4.2 Prohibited certificate uses.

54. The certificates must be used for their own function and established purpose, and may not be used in other functions and for other purposes.
55. Furthermore, the certificates must only be used according to governing laws.
56. 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.
57. End-user certificates may not be used to sign any type of public key certificates, nor to sign certificate revocation lists, nor to sign requests for issuance, renewal, suspension, or revocation of certificates.

1.5 Policy Administration.

1.5.1 Entity responsible for managing documentation.

58. Izenpe, with registered office at Calle Beato Tomás de Zumárraga, No. 71, 1st floor, Postal Code 01008, Vitoria-Gasteiz, and Tax ID A-01337260, is the certification authority issuing the certificates to which this GTPS applies.

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

59. To report security issues, such as suspicion of compromised keys, improper use of certificates, fraud or other issues, email incidencias@izenpe.eus
60. Consult the section “4.9.3Processing revocation requests” to learn about the revocation channels.

1.5.3 Responsible Parties for the Adaptation of the GTPS

61. The Izenpe Security Committee is the body responsible for approving this GTPS, as well as its amendments and the particular CPS and PDS documents when they exist.

1.5.4 GTPS Approval Procedure

62. Final modifications to this document, the CPS, and the PDS are approved by the Izenpe Security Committee, after verifying compliance with the established requirements.

1.6 Definitions and acronyms.

1.6.1 Definitions.

- Certification Authority (CA): entity that issues certificates at the request of the Registration Authority, in an automated manner and after prior confirmation by the Registration Authority.
- Registration Authority (RA): entity responsible for performing identification tasks of applicants, subscribers, and key holders of certificates; it verifies the supporting documentation of the information included in the certificates, as well as the validation and approval of issuance, revocation, and renewal requests for 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. It is the first and main certificate of a PKI hierarchy. It is self-signed and serves to sign the certificates of intermediate or subordinate CAs, which issue the end certificates.

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 with regard to verification of the identity and other details of applicants and to the reliability and guarantees of the certification services rendered.
- Unqualified 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 electronic signatures.
- Certification Practice Statement (GTPS): statement which Izenpe makes easily available through electronic means at no cost. 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 will be detailed within the framework and provisions of eIDAS; 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.
- Certificates 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 the requirements stipulated by article 26 of eIDAS.
- 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 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. There is also a web service available on a permanent basis that allows telematic incremental updates to be consulted for certificates revoked by Izenpe. Regarding the publication of Certificate Revocation Lists, secure and fast access for users and certificate subscribers is guaranteed.
- 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.
- Key holders: the natural persons who own or are responsible for safeguarding the electronic 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 GTPS.
- Certificate users: entities that are certificate end users are individuals and organisations that receive electronic 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:.

- CA: Certification Authorities.
- CN: Common Name.
- CRL: Certificate Revocation List.
- DN: Distinguished Name.
- GTPS: Global Trust 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.
- Certification policies as defined in the ETSI EN 319411-1 standard (*General requirements*):
    - NCP: Normalised Certification Policy that complies with best practices recognised by providers issuing certificates used for any transaction.
    - NCP+: Extended Normalised Certification Policy that complies with the NCP policy practices but certificates require a secure cryptographic device for their use.
    - OVCP: Extended Normalised Certification Policy that complies with the NCP policy practices but certificates require a secure cryptographic device for their use.
    - DVCP: Domain Validated Certification Policy for web authentication certificates, complying with CABForum requirements for domain validation.
- Qualified Certification Policies, as defined in ETSI EN 319411-2 (*Requirements for trust service providers issuing EU qualified certificates*):
    - QCP-n: Qualified Certification Policy referring to advanced electronic signatures based on qualified certificates under Articles 26 and 28 of the eIDAS Regulation, for natural persons.
    - QCP-l: Qualified Certification Policy referring to advanced electronic seals based on qualified certificates under Articles 36 and 38 of the eIDAS Regulation, for legal persons.

- QCP-n-qscd: Qualified Certification Policy referring to qualified electronic signatures defined in Article 3.12 of the eIDAS Regulation, for natural persons.
- QCP-l-qscd: Qualified Certification Policy referring to qualified electronic seals defined in Article 3.27 of the eIDAS Regulation, for legal persons.
- QEVCP-w: Qualified Certification Policy referring to qualified web authentication certificates defined in Articles 3.38 and 3.45 of the eIDAS Regulation, and described in section 4.2.2.5 of ETSI EN 319 411-2.

– RA: Registration Authority.

– SSL Secure Socket Layer.

– TSA: Time Stamp Authority Server.

2 Publication and supervisors of information repository.

2.1 Information repository.

63. Izenpe has a public information repository atwww.izenpe.eus available 24 hours a day, 7 days a week.

2.2 Publication of certification information.

64. Izenpe guarantees the availability of the GTPS, the CPS, the PDS, and the terms and conditions of use for the trust services at www.izenpe.eus.

65. 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).

66. 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. Consult the particular CPS for web authentication certificates.

2.2.1 Publication and Notification Policy.

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

68. In the case of the GTPS and Terms and Conditions of Use, Izenpe will maintain a public version history on www.izenpe.eus.

2.2.2 Items not published in the Global Certification Practice Statement

69. The list of components, subcomponents, and elements that exist but are not publicly available due to their confidential nature are referred to in section “9.2.5 Information beyond the scope” of this GTPS.

2.3 Frequency of publication.

70. The GTPS is published as soon as it is approved if no changes have been made in the annual review. Changes are governed by the provisions of this document.

71. Information on the status of certificates is published in accordance with sections “4.9.7 Frequency of CRL generation” and “4.9.9 Online revocation checking requisites” of this document.

2.4 Controlling access to the repository.

72. 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.

73. 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 Identification and Authentication.

3.1 Names.

3.1.1 Types of names.

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

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

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

77. The Subject Alternative Name extension usually includes alternative identities of the same person who appears as the certificate subscriber.

3.1.2 Meaning of names.

78. 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 Name Formats. of names in this document).

3.1.3 Pseudonyms.

79. Certificates do not allow the use of pseudonyms for the signatory, except for pseudonymous public employee certificates.

3.1.4 Rules for interpreting name formats.

80. The subject of a certificate identifies the person (natural or legal) or device and Izenpe 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”.

81. In website authentication certificates, the requirements of the CABForum (Baseline Requirements and EV Guidelines) must be taken into account.

3.1.5 Uniqueness of names.

82. Subscriber names and, where applicable, signatories 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.

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

84. 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.

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

3.1.7 Issuer.

86. This field contains the identification of Izenpe, the certification authority that signed and issued the certificate.

87. 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.

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

3.1.8 Subject.

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

90. 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.

3.2 Validation of identity.

3.2.1 Methods for proving possession of the private key.

91. 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 or, where applicable, of the signatory.
    - By the certificate signatory, possession of the private key is demonstrated by the proper use of 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.

92. Izenpe is based on the specification of 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.

93. The documentation that each entity must provide according to its legal structure is published at www.izenpe.eus.

94. The identity of the organisation shall be verified through the documentation required according to the type of entity.

95. More information: in the PDS.

3.2.2.1 Domain Validation.

96. The validation of the web domain in website authentication certificates is described in the corresponding PDS.

3.2.3 Authentication of the identity of the natural person applicant.

97. Izenpe is based on the specification of 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.

98. More information can be found in the Identity Verification Service Practice Statement and in the PDS.

99. Izenpe will verify the identity of the applicant:

    - In person.
    - Legitimisation of the Certificate Issuance Request signature by a notary.
    - By means of a valid qualified certificate.
    - Through remote video identification.

3.2.4 Unverified subscriber information.

100. In general, certificate information is verified prior to issuance by cross-checking with information sources. Where PDSs exist, their provisions will be followed.

3.2.5 Authority validation.

101. The corresponding legal instrument will be signed, specifying the conditions of the registration delegation and the responsibilities of the operators.

102. Registration Authorities must:

    - Certify the operators.
    - Provide them with a qualified certificate issued by Izenpe.
    - Ensure they have received sufficient training.
    - Ensure the submission of documentation to Izenpe.

3.2.6 Interoperability criteria.

103. There are no interactivity relations with certification authorities outside Izenpe.

3.3 Identification and authentication for requests to reissue keys.

3.3.1 Routine renewal.

3.3.2 Renewal after revocation.

104. 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.

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

4 Operative requisites for the certificates' life cycle

This GTPS regulates the common operational requirements for the issued certificates. In the event that Izenpe performs cross-certification with an external CA, it will require said

CA to comply with all the requirements defined in the GTPS, the PDS, and the Identity Verification Service Practice Statement.

4.1 Certificate application.

106. 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.

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

4.1.1 Verification of application.

108. Prior to certificate issuance, Izenpe will verify the data contained in the request as specified in the GTPS, CPS, and PDS.

4.1.2 Signing up process and responsibilities.

109. 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 signatories 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 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 signatory.

4.2 Request Management.

4.2.1 Carrying out identification and authentication functions.

110. It is Izenpe's responsibility to properly identify the subscriber in accordance with the Identity Verification Service Practice Statement (DPSV). Approve or deny applications.

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

112. 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.

113. 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 the incident has been resolved.

4.2.2 Application processing time.

114. No more than one month may elapse between the approval of the request and the issuance of the certificate. In any case, each CPS or PDS will specify this aspect.

4.3 Certificate issuance.

115. All applications must be fully approved before certificates can be issued. Izenpe will issue the certificate as determined in this GTPS, the CPS where applicable, and the PDS. Additionally, Izenpe will deliver to the subscriber (or to the signatory in professional certificates) the certificates and/or unlock codes in cases where Izenpe generates the keys.

116. If the applicant is not aware of the certificate issuance, they should contact Izenpe.

4.3.1 CA actions during issuance.

117. It shall comply with the provisions for the issuance of each certificate type as established in the GTPS, CPS, and the Identity Verification Service Practice Statement (DPSV).

4.3.2 Izenpe will proceed with the issuance of the certificate as determined in the relevant CPS or PDS. Notification of certificate issuance.

118. Izenpe notifies the subscriber and/or signatory of the certificate issuance.

4.3.3 Verification of the certificate.

119. The signatory must verify the correct functioning and, if necessary, report any malfunctions to Izenpe.

120. If the malfunctions are due to technical causes (including but not limited to: malfunction of the certificate support, technical error in the certificate, etc.) or errors in the data contained in the certificate attributable to Izenpe, Izenpe will revoke the certificate and proceed to issue a new one, assuming the resulting costs.

4.4 Certificate acceptance.

121. 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 GTPS, which governs the technical and operational aspects of the digital certification services provided by Izenpe.

4.4.1 Certificate acceptance process.

122. 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.

123. Once the certificate has been accepted by the subscriber and generated, the certificate will be published in Izenpe's internal certificate repositories.

124. 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.

125. 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.

126. 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.
- Diligently safeguard the private key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of the GTPS.
- Shall 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 the signatories.
- 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 electronic 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.

127. The subscriber whose keys are hosted on Izenpe,

- Will make proper use of the certificate and in particular, comply with the usage limitations thereto.
- Diligently safeguard the activation key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of the GTPS.
- Shall 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 GTPS.
- 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 electronic 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

128. 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 GTPS.
- 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 electronic 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.
- 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 eIDAS Regulation.

4.6 Certificate revocation.

129. Certificate renewal consists of issuing a new certificate to the subscriber without changing any information appearing on the certificate. Depending on the certificate type, the validity period may be different. Issuance costs are stipulated at www.izenpe.com.

130. Within 60 days prior to the certificate's expiry, renewal may be initiated.

131. Izenpe will process the renewal according to the issuance and delivery procedure applicable in each case.

4.6.1 Circumstances for certificate renewal.

132. 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.

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

4.6.3 Processing certificate renewal requests.

134. The subscriber can contact Izenpe and request its renewal. Izenpe will inform you how to formalise your application.

4.6.4 Notification to the subscriber.

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

4.6.5 Renewed certificate acceptance procedure.

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

4.6.6 Publishing the certificate.

137. 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.

138. As indicated in point 4.4.3.

4.7 Renewal with certificate key regeneration.

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

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

4.7.1 Circumstances to regenerate certificate keys.

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

4.7.2 Who can apply.

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

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

4.7.3 Processing renewal applications with key regeneration.

144. The subscriber can contact Izenpe and request its renewal. Izenpe will inform you how to formalise your application. Notification to the subscriber.

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

4.7.4 Renewed certificate acceptance procedure.

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

4.7.5 Publishing the certificate.

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

148. Notifying other entities.

149. As indicated in point 4.4.3.

4.8 Modification of the certificate.

150. 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.

151. Modification is not stipulated.

4.8.2 Who may apply for certificate modification.

152. Modification is not stipulated.

4.8.3 Processing of certificate modification applications.

153. Modification is not stipulated.

4.8.4 Notification of certificate modification.

154. Modification is not stipulated.

155. Conduct constituting acceptance of the certificate modification.

156. Modification is not stipulated.

4.8.5 Publication of the modified certificate.

157. Modification is not stipulated.

4.8.6 Notification of certificate modification to other entities.

158. Modification is not stipulated.

4.9 Revocation.

4.9.1 Circumstances for revocation.

159. 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 stamp certificate for a legal person or a SSL certificate.
- 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.

160. 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.

161. The revocation applicant shall process the Revocation Application before Izenpe.

162. 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 signatory and subscriber of the revocation of its certificate and specify the reason for revocation.

163. The applicant may revoke the certificate through the following channels,

- In person before,
  - At Izenpe, requesting a prior appointment at www.izenpe.eus..
  - Or to the subscribing organisation with which Izenpe has signed the relevant legal instrument.
- Online: Online revocation application access available at https://servicios.izenpe.com/gestionCertificados/
- By email: Sending the signed revocation request form, signed with a qualified certificate issued by a CA included in the EU Trusted Service List (TSL), to the address izenpe@izenpe.eus.

164. The authenticated revocation request, as well as the information justifying the revocation, shall be registered and archived.

4.9.4 Grace period for the revocation request.

165. 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.

166. Izenpe will revoke the certificate within 24 hours following receipt of the request on a business day and will notify by email the applicant and the subscriber of the certificate status change.

167. Once instructions from section "4.9.3 Processing revocation requests 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.

168. 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.

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

4.9.7 Frequency of CRL generation.

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

171. 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 CRL is regenerated daily.

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

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

174. 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.

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

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

177. Availability of the online verification system for the status of certificates

178. 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.

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

4.9.9 Online revocation checking requisites.

180. 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.

181. 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.

182. 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.

4.9.10 Other revocation notifications available.

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

4.9.11 Special committed key requisites.

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

185. The communication to Izenpe about the commitment of a private key through the email account incidencias@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.

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

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

4.9.12 Circumstances for suspension.

188. Izenpe does not allow suspension of any of its certificates.

4.9.13 Who can request suspension.

189. Izenpe does not allow suspension of any of its certificates.

4.9.14 Procedure for requesting suspension.

190. Izenpe does not allow suspension of its certificates.

4.9.15 Limits on the period of suspension.

191. Izenpe does not allow suspension of its certificates.

4.10 Certificate status services.

4.10.1 Operational characteristics.

192. 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.

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

4.10.3 Optional characteristics.

194. Not stipulated.

4.11 Termination of subscription.

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

196. Qualified certificates may have a maximum validity of 5 years in accordance with Law[2] 6/2020, of 11 November, regulating certain aspects of electronic trust services.

197. Web authentication certificates have a validity period in accordance with the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates[3].

4.12 Custody and recovery of keys.

4.12.1 Key custody and recovery practices and policies.

198. Izenpe will not retrieve private keys from certificate holders.

4.12.2 Session key protection and recovery practices and policies.

199. Not stipulated.

[2]Article 4.2 of Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.

[3]Available at https://cabforum.org

5 Physical, procedural and personnel security controls.

5.1 Physical security controls.

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

5.1.1 Site location and construction.

201. 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.

5.1.2.1 Data Processing Centre.

202. 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 authorised 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.

203. 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.

5.1.2.2 Registration Authorities (RAs).

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

5.1.3 Power and air conditioning.

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

206. 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.

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

5.1.5 Fire prevention and protection.

208. 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.

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

5.1.7 Waste processing.

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

211. 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.

212. 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.

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

214. 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.

215. 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.

216. 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.

217. Several individuals may also be assigned to the same role.

5.2.3 Identification and authentication for each role.

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

219. Izenpe has specific documentation giving further details of each role.

5.2.4 Separating tasks into different roles.

220. 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.

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

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

5.3.2 Background check procedures.

223. 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.

224. 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:

- Delivery of a copy of the GTPS.
- 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.
- Awareness of privacy and data protection.

225. 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.

226. 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.

227. 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.

5.3.6.1 Information security incidents.

228. Izenpe has a security incident management plan.

5.3.6.2 Punitive process.

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

5.3.7 Recruitment requirements.

230. 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.

231. All personnel with trusted roles receive:

- A copy of the GTPS.
- 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.

232. 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.

233. The following logs are stored:

- New certificate applications.
- Rejected certificate applications.
- Account access violation.
- Certificate signature.
- Revoking the certificate.
- Account logon.
- CRLs signature.

234. CA modifications.

- Certificate expiry.

235. 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.

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

5.4.2 Frequency of log processing.

237. Logs are continuously processed and audited quarterly by the Security Officer. The audit report includes the following aspects:

- List of unauthorised access attempts.
- Errors generated in each CA.
- List of administrator users.
- List of software installed on Windows machines.

5.4.3 Period for audit log retention.

238. The information generated in the log file is retained online until it is archived. After they are archived, log files are retained for 15 years.

5.4.4 Protecting the audit log.

239. 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.

240. 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.

241. 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.

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

243. Notifying the action causing the logs.

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

5.4.7 Vulnerability analysis.

245. 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.

246. 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.

247. 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.

248. 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.

249. 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.

250. 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 (seeTime source.).

5.5.6 Filing system.

251. 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.

252. 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 GTPS.

5.6 CA key change.

253. 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.

254. 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.

255. 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.

256. Izenpe's Contingency Plan applies to all functions, operations, and resources necessary to restore the provision of trust services. This plan applies to Izenpe personnel involved in delivering the trust services.

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

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

259. 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.

260. 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.

261. 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.

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

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

- Cease providing the affected service.
- Revoke certificates that may be affected.
- 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.
- Assess the need to execute the "TSP Activity Cessation Plan" in accordance with the GTPS and current legislation.

5.7.4 Business continuity after a disaster.

264. 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.

265. The Izenpe Business Contingency and Continuity Plan will put into action.

5.8 CA or RA termination.

5.8.1 Certification Authority.

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

267. 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.

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

269. 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.

270. 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.

271. Izenpe's CRLs do not include expired certificates, as indicated in section 4.9.7, CRL Generation Frequency, of this GTPS. If transferred to another entity, measures shall be taken so that said transfer is conducted with all guarantees necessary.

272. 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.

273. 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.

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

275. 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.

276. 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.

277. 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.

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

279. 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).

280. 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 or cryptographic hardware.

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

282. Client key container (e.g.: web server).

283. Izenpe's secure container.

- Izenpe's application container for mobile phones.

6.1.2 Private key delivery to subscriber.

284. Delivery method of the private key depends on the certificate and device type. Consult the PDS and/or CPS.

6.1.3 Public key delivery to certificate issuer.

285. 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.

286. 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 the browser: stored in the browser's certificate container.
- Keys generated in mobile phones: stored in the Izenpe application container.
- Secure server certificate keys (SSL): Izenpe.

6.1.4 Certification Authority public key delivery to certificate users 67.

287. 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 GTPS also contains the root CA and issuing CA prints.

6.1.5 Key sizes.

288. Key size, depending on each case, is:

289. 2007, 2020 hierarchy.

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

290. The TSU server key size is issued with 4096 bits.

291. 2024 hierarchy.

292. ECC 256 or 384 bits

293.

6.1.6 Public Key Generation and Quality Assurance Parameters.

294. The Algorithm Identifier used by Izenpe to sign the certificates in 2007 and 2020 hierarchy 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)". In the 2024 hierarchy, ECC256 or ECC384 is used.

295. 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.

296. 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.

297. In the event that the algorithm, the combination of key sizes used, or any other technical circumstance significantly compromises the technical security of the system, Izenpe's "Contingency and Business Continuity Plan" will be applied, and an 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 (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.509 v3).

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

299. 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.

300. 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.

301. 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.

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

303. 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.

304. 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.

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

306. 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.

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

6.2.3 Private key custody.

308. 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.

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

310. 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.

311. 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.

312. 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.

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

6.2.5 Private key archiving.

314. 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.

315. The root CA private key, subordinate CAs, VA and TSA are generated in an HSM pursuant to point 5.2.1 and exportation is not possible. As a contingency measure, it is possible to recover private keys as indicated in section 5.2.4.

316. For the following device 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.

317. 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.

318. 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.

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

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

321. 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.

322. 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.

323. The mechanisms for activation and use of private keys of end-entity certificates are described in the PDS and/or CPS, as applicable.

6.2.9 Private key deactivation method.

324. 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".

325. 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.

326. There is a procedure for the destruction of CA keys.

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

328. 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.

329. As indicated in section 5.2.1 of this document.

6.3 Other aspects of key pair management.

6.3.1 Public key archiving.

330. 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.

331. 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. Qualified certificates for natural persons or electronic seals have a maximum validity of five (5) years. Web authentication certificates have a maximum validity of 365 days. For all natural person certificates and legal person seal certificates, renewal involves key regeneration.

6.4 Activation data.

6.4.1 Generation and installation of activation data.

332. 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.

333. Regarding the activation data for the keys of end-entity certificates, these are described, where applicable, in the Identity Verification Service Practice Statement (DPS) or in the Certification Practice Statement (CPS).

6.4.2 Activation data protection.

334. 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.

335. 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.

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

337. Subscribers are compelled to keep their activation data secret.

6.4.3 Other aspects of the activation data.

338. See the existing ones as well as the disclosure statements (PDS).

6.5 Computer security controls.

6.5.1 Specific technical requirements for computer security.

339. 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):

340. 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.

341. 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.

342. The revocation publication service possesses the functions necessary to be available on a 24x7 basis.

343. 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.

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

6.5.2 Assessment of the level of IT security.

345. 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.

346. 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.

347. 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

348. 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.

349. 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.

350. 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.

351. 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.

352. 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

353. Certificates issued under this GTPS use the X.509 version 3 standard (populate version field with integer "2").

7.1.2 Certificate extensions.

354. These indicated in the profile documents, available at www.izenpe.eus.

7.1.3 Algorithm object identifiers.

355. RSA.

356. Izenpe must indicate that it uses an RSA key through the rsaEncryption algorithm identifier (OID: 1.2.840.113549.1.1.1). The parameters must be present and explicitly NULL.

357. Izenpe must not use a different algorithm, such as the id-RSASSA-PSS algorithm identifier (OID: 1.2.840.113549.1.1.10), to indicate the presence of an RSA key.

358. Once encoded, the algorithm identifier for RSA keys MUST be byte-for-byte identical to the following hex-encoded bytes: 300d06092a864886f70d0101010500 ECDSA.

359. The CA must indicate that it uses an ECDSA key through the id-ecPublicKey algorithm identifier (OID: 1.2.840.10045.2.1). The parameters MUST use namedCurve encoding.

- For P-256 keys, namedCurve MUST be secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, namedCurve MUST be secp384r1 (OID: 1.3.132.0.34).
- For P-521 keys, namedCurve MUST be secp521r1 (OID: 1.3.132.0.35). Once encoded, the algorithm identifier for ECDSA keys MUST be byte-for-byte identical to the following hex bytes.
- For P-256 keys: 301306072a8648ce3d020106082a8648ce3d030107.
- For P-384 keys: 301006072a8648ce3d020106052b81040022.
- For P-521 keys: 301006072a8648ce3d020106052b81040023.

7.1.4 Name Formats.

360. 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.

361. 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

362. As specified in section 1.2 of this GTPS.

7.1.7 Use of extension policy restrictions.

363. No policy restrictions are used.

7.1.8 Syntax and semantics of policy qualifiers.

364. The Certificate Policies extension contains the following policy qualifiers:

- CPS Pointer: contains a pointer to Izenpe's GTPS at www.izenpe.eus.

- 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.

365. Notice common to all certificates (except SSL certificates[4]):

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

7.1.9 Semantic treatment for the "Certificate policy" extension.

366. 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.

367. The certificates issued by Izenpe conform to the following standards:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) May 2008.

[4]The UserNotice field has been prohibited in SSL certificates since version 2.0.0 of the CAB Forum Baseline Requirements.

- 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.

368. 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.

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

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

370. 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.

371. 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.

372. 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.

373. Izenpe annually defines a security and information privacy management plan that facilitates the verification of compliance with established security requirements. ,

8.1 Audit frequency.

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

8.2 Auditor qualifications.

375. The auditor must have proven qualifications and experience in conducting audits of Trust Service Providers. They must be accredited according to ETSI EN 319 403.

8.3 Relationship of the auditor with the audited company.

376. 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.

377. The compliance audit will cover the following topics:

- Trust Services.
- Information Systems.
- Protection of the data processing centre.
- Related Documentation.

8.5 Decision-making as the result of deficiencies.

378. Izenpe implements a permanent improvement model, and the results from a compliance audit are handled according to this model. Depending on the severity and urgency, all observations, improvements, and non-conformities are entered into a tracking system and addressed within a timeframe using a support tool. Communication of results.

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

9 Other legal and activity matters.

9.1 Fees.

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

381. Payment options offered:

- Electronically signed issuance request: online payment via payment gateway.
- Payment letter to be presented at the bank.
- In-person payment at the Izenpe Registration Authority using a bank card.

382. For entities belonging to the Basque Public Sector, the criteria defined in the corresponding regulatory framework shall apply.

9.1.1 Fees for the issue or renewal of certificates.

383. The fees that users must pay for issuance or renewal of certificates appear on https://www.izenpe.eus.

9.1.2 Fees for access to certificates.

384. Not stipulated.

9.1.3 Certificate status information access fees.

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

9.1.4 Fees for other services.

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

9.1.5 Refund policy.

387. Izenpe does not have a refund policy.

9.2 Financial responsibility.

388. 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.

389. Izenpe holds a civil liability insurance policy covering risks of error and/or omission arising from its activities, with a compensation limit of €5,000,000 per claim and insurance period.

9.2.2 Other assets.

390. Not stipulated.

9.2.3 Insurance and guarantees for end entities.

391. Not stipulated.

392. Information confidentiality.

9.2.4 Scope of confidential information.

393. For the provision of the service, Izenpe needs to collect and store certain information, including personal data. 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.

394. Izenpe collects only the data strictly necessary for the issuance and maintenance of certificates and the provision of other certification services, and such data cannot be processed for other purposes without the express consent of the signatory.

395. Izenpe carries out its activities in accordance with the GDPR and its implementing regulations.

396. Izenpe does not disclose or transfer personal data, except in cases provided for in this GTPS.

397. 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.
- 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 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.

9.2.5 Information beyond the scope.

398. 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.
- 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.
- All other information not indicated in the confidential information section of this GTPS.

9.2.6 Responsibility to protect confidential information.

399. Izenpe shall be entitled to disclose confidential information to the extent required by law.

400. 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.

401. Certificates will be published in accordance with the provisions of the eIDAS Regulation and the LSEC.

9.3 Personal data protection.

402. Izenpe publishes information regarding privacy and data protection on the website: www.izenpe.eus/datos.

9.3.1 Privacy Plan.

403. The processing of personal data carried out by Izenpe is aligned with the provisions of the GDPR and the LOPDGDD, as well as with the implementing regulations.

9.3.2 Information treated as private.

404. Izenpe considers all personal information about natural persons using trust services as private.

9.3.3 Information not considered private.

405. 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.

9.3.4 Responsibility to protect private information.

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

407. 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.

9.3.4.1 Data Protection Officer.

408. 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.

9.3.4.2 Processing activity record.

409. 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:

- Purpose
- Responsible entity
- Personal data categories

- Who provides the data
- Who is the party affected by the personal data
- Who are data processors
- Data sharing
- International Data Transfers
- Deletion period
- Security measures

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

9.3.4.3 Rights of interested parties.

411. 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.

9.3.4.4 Cooperation with the authorities.

412. Izenpe shall cooperate with the data protection authorities when required to do so.

9.3.4.5 Security violation notifications.

413. Izenpe shall notify the Basque Data Protection Authority (hereinafter, AVPD) 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.

414. 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 AVPD shall be complemented by a notification addressed to said parties so that they may take measures to protect themselves from the consequences.

9.3.5 Notice and consent to use private information.

415. The collection of private information from natural persons during certificate lifecycle processes (application, identity verification, renewal, revocation, etc.) will be carried out through a statement by the data subject or via a clear affirmative action.

9.3.6 Disclosure pursuant to judicial or administrative process.

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

9.3.7 Other disclosure circumstances.

417. Not stipulated.

9.4 Intellectual property rights

9.4.1 Property rights in certificates.

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

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

420. The same rules apply to the certificate revocation data system.

9.4.2 Ownership of the GTPS.

421. Izenpe is the owner of this GTPS.

9.4.3 Property rights in names.

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

423. The subscriber and, where applicable, the signatory, is the owner of the certificate's distinguished name, composed of the information specified in section 3 of the GTPS.

9.4.4 Property rights in keys and key material.

424. Key pairs are the property of certificate subscribers.

9.5 Obligations and guarantees.

425. Izenpe, as the certification authority issuing certificates in accordance with this GTPS, assumes the following obligations:

9.5.1 Obligations of the CA.

9.5.1.1 Obligations of providing service.

426. Izenpe renders certification services in accordance with this GTPS, in which its roles, operations procedures and security measures are defined; in particular, Izenpe undertakes to fulfil all of its obligations as described in this CPS except those performed expressly by the registration authority when not acting in the capacity thereof.

427. These obligations are as follows:

- 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).

9.5.1.2 Reliable operation obligations.

428. 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 GTPS. The service is available 24 hours X 7 days a week.
- Compliance with technical and staff requirements stipulated by governing legislation on electronic signatures:
  - Demonstrating the reliability necessary to provide certification services.
  - Guaranteeing that the date and time when a certificate was issued or expired can be precisely determined.
  - 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.
  - 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.
  - 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.
  - 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:
  - Periodically performing regular security checks to verify compliance with established standards.
  - Comprehensively managing security events, in order to guarantee detection, resolution and optimisation.
  - Maintaining appropriate contact and relationships with special interest groups in security, such as specialists, security forums and professional associations related to information security.
  - 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.

9.5.1.3 Identification obligations.

429. 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 GTPS.

9.5.1.4 User information obligations.

430. Before issuing and delivering the certificate to the subscriber, Izenpe informs them by referencing the document 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 of this GTPS.

431. Izenpe will inform the signatory 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.

432. 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.

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

9.5.1.5 Obligations regarding verification programmes.

434. IZENPE provides the public with verification mechanisms to check the validity of certificates through systems described in this GTPS.

9.5.1.6 Obligations regarding legal regulation of the certification service.

435. 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.

436. The legal instrument that binds Izenpe and the applicant, subscriber or signatory and the relying party is in writing and in readily understandable language, and contains, at least, the following content:

- Prescriptions to comply with the provisions set out in the sections of section 2 of this GTPS.
- Indication of the applicable GTPS, 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 communication to third parties should Izenpe terminate its services without revocation of valid certificates.
- Usage limitations, including those set forth in section 1.4.

- 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 legislation and competent jurisdiction.
- The way in which Izenpe guarantees liability for damages.

9.5.2 Registration Authority obligations.

437. 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 signatories on the certificates, or that are relevant for the purpose of the certificates.
- 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.

9.5.3 Holder obligations.

438. 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 corresponding PDS

439. The subscriber undertakes to:

- Provide Izenpe with complete and appropriate information in accordance with the requirements described in the GTPS, 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 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 GTPS.
- 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.
- Will transfer specific obligations to the signatories.
- 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.
- 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.

440. Subscribers of qualified certificates who generate electronic signatures using the private key corresponding to 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, as established in the eIDAS.

9.5.4 Obligations of the relying parties.

441. 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 GTPS 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 electronic 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.

9.5.5 Obligations of other participants.

442. 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.

9.6 Waiver of guarantees.

443. Not stipulated.

9.7 Liability limitation.

9.7.1 Certification Authority liabilities

444. Izenpe is liable for negligence or a lack of due diligence exercised in providing the certification services described in this GTPS, 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 GTPS.
    - 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 GTPS.
    - It shall be held liable for any direct, indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or punitive damages arising from, or in connection with, the use, delivery, license, performance or non-performance of certificates, electronic signatures or any other transactions or services offered or contemplated by this GTPS arising from 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, notarised 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.

445. 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.

446. 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.

9.7.2 Registration authority liabilities

447. 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.

448. 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.

9.7.3 Subscriber liabilities

449. The subscriber shall be responsible for all electronic communications authenticated using a digital signature generated with his/her private key, when the certificate has been validly confirmed through the verification services provided by Izenpe.

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

451. By accepting the certificates, the subscriber undertakes to hold harmless and, where applicable, indemnify Izenpe, the registration authorities, and the User Entities from any act or omission causing damages, losses, debts, legal expenses or any other costs, including professional fees, incurred by them, arising from the use or publication of the certificates, and resulting 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 unauthorised 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.

452. 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.

9.7.4 Relying third party liability

453. A third 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.

454. 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).

9.8 Compensations.

455. 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.

9.9 Validity period.

9.9.1 Entry into Force.

456. The GTPS comes into force as soon as it is published.

9.9.2 Termination.

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

9.9.3 Effects of termination.

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

9.10 Individual notifications and communication with participants.

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

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

9.11 Amendments to this document.

9.11.1 Procedure for changes.

461. Modifications to this document will be approved by the Izenpe Security Committee. These modifications will be recorded in a GTPS update document whose maintenance is guaranteed by Izenpe.

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

463. IZENPE may unilaterally amend the GTPS 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 Security Committee.
- 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.

9.11.2 Notification period and mechanism.

464. The Izenpe Security Committee will annually review the GTPS 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.

465. 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.

466. Modifications that could require informing users, such as:

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

9.11.3 Circumstances under which an OID must be changed.

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

9.12 Complaints and dispute resolution.

468. 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.

469. 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.

470. 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.

471. The parties agree to settle any issues that may arise between them by means of a Collaborative Legal procedure, and may take recourse to the Courts of the city of Vitoria-Gasteiz, in the event that they do not reach an agreement.

9.13 Applicable regulations.

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

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

- European Parliament and Council Regulation (EU) Number 910/2014 dated 23 July 2014 on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC
- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.
- (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.
- Organic Law 3/2018 of 5 December on Personal Data Protection and guarantee of digital rights.

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

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- 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.

9.14 Compliance with applicable legislation.

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

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

9.15 Various stipulations.

9.15.1 Full agreement.

477. Each clause contained in this GTPS 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.

9.15.2 Allocation.

478. 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.

9.15.3 Severability.

479. Not stipulated.

9.15.4 Compliance

480. Not stipulated.

9.15.5 Force Majeure

481. Not stipulated.

9.15.6 Other stipulations.

482. As trust service provider, Izenpe shall provide services to all interested parties who request them under the conditions set forth in this GTPS, Particular CPS, and the Practices and Laws for Issue applicable to the subject of the request.

483. 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.

484. 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/Browser Forum 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/).

485. 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.

486. 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.