Bugzilla ID: 361957
Bugzilla Summary: Add Izenpe CA EV root certificate (Spain)

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	Izenpe
Website URL	www.izenpe.com (in Spanish and in Basque)
Organizational type	Regional Government CA in Spain -- Basque A discussion in mozilla.dev.security.policy called "Accepting root CA certificates for regional government CAs", indicates that we can proceed with processing the Spain regional government CAs.
Primary market / customer base	Izenpe is a public company belonging to the Basque Country Government so the general nature is government. The primary geographical area is the Basque Country but all of their certificates are recognized, accepted, and validated by all of the PKIs in Spain, so the geographical area relates to Spain.
CA Contact Information	CA Email Alias: info@izenpe.com CA Phone Number: 945 017 940 Title / Department: Empresa de Certificación y Servicios

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data – SHA1 Root	Data – SHA256 Root
Certificate Name	Izenpe.com	Izenpe.com
Cert summary / comments	This is the original SHA1 root, which is still needed. This root has four internally-operated subordinate CAs. There are two sub-CAs for Qualified certificates, one for Public Administration, and one for Citizens and Entities. There are also two sub-CAs for non-Qualified certificates, one for Public Administration and one for Citizens and Entities, which issue SSL Server, Email, and Code Signing certs.	This is the new root, signed with SHA-256. This root has five internally-operated subordinate CAs. One sub-CA issues EV SSL certs. Two of the sub-CAs are for Qualified certificates, one for Public Administration, and one for Citizens and Entities. There are also two sub-CAs for non-Qualified certificates, one for Public Administration and one for Citizens and Entities, which issue SSL Server, Email, and Code Signing certs.
Root URL	https://bugzilla.mozilla.org/attachment.cgi?id=385225	https://bugzilla.mozilla.org/attachment.cgi?id=385230
SHA-1 fingerprint	4a:3f:8d:6b:dc:0e:1e:cf:cd:72:e3:77:de:f2:d7:ff:92:c1:9b:c7	2F:78:3D:25:52:18:A7:4A:65:39:71:B5:2C:A2:9C:45:15:6F:E9:19
Valid from	2003-01-30	2007-12-13
Valid to	2018-01-30	2037-12-13
Cert Version	3	3
Modulus length	2048	4096

Test Websites	https://servicios.izenpe.com/jsp/descarga_ca/s27descarga_ca_c.jsp	https://www.ermua.es/
CRL URL	CA of CCEE rec: http://crl.izenpe.com/cgi-bin/crl CA of CCEE no rec: http://crl.izenpe.com/cgi-bin/crlscinr CA of AAPP rec: http://crl.izenpe.com/cgi-bin/crlscar CA of AAPP no rec: http://crl.izenpe.com/cgi-bin/crlinterna	CA of CCEE rec: http://crl.izenpe.com/cgi-bin/crl2 CA of CCEE no rec: http://crl.izenpe.com/cgi-bin/crlscinr2 CA of AAPP rec: http://crl.izenpe.com/cgi-bin/crlscar2 CA of AAPP no rec: http://crl.izenpe.com/cgi-bin/crlinterna2 CA of SSL EV: http://crl.izenpe.com/cgi-bin/crlsslev
CRL Issuance Frequency	Comment #61: Our CRLs have a validity [nextUpdate] of 10 days now and are refreshed every 1 day, so, if there aren't revocations, everyday we have a new CRL and if there's one revocation, immediately we issue a new CRL.	
OCSP Responder URL	http://ocsp.izenpe.com:8094 When I enforced OCSP and go to the website (https://servicios.izenpe.com/jsp/descarga_ca/s27descarga_ca_c.jsp) I get Error code: sec_error_ocsp_invalid_signing_cert	http://ocsp.izenpe.com:8094 When I enforce OCSP and go to the test website for the new root, I get Error code: sec_error_ocsp_invalid_signing_cert Comment #61: We have a Technical CA that signs the VA and TSA, but this is for the old hierarchy, we can't migrate to the new 4k hierarchy until all the applications of our partners and clients are migrated because if we do, we can have inconsistencies and issues.
OCSP max time (EV)	http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf , Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days." Comment #52: The OCSP response time is immediately (when you revoke a certificate the VA knows instantly) and it's updated permanently because it's asking the CA and gets all the information so no need to synchronize. The nextupdate is an optional field and our VA only uses that field if we use the CRL. Right now there's no response in the nextupdate because we don't need to update it because it's always update at any time.	
CA Hierarchy	The CA hierarchy diagram is shown at https://servicios.izenpe.com/jsp/descarga_ca/s27descarga_ca_c.jsp	

List or description of subordinate CAs operated by the CA organization	The sub-CAs of the old root are:
	• Citizen and Entity CA, qualified certificates
	  ○ Issues certs for SSL client and e-mail.
	• Citizen and Entity CA, non qualified certificates
	  ○ Issues certs for SSL Server, SSL client, E-mail, and code signing.
	• Public Adminstration, qualified certificates CA
	  ○ Issues certs for SSL client and e-mail.
	• Public Adminstration, non qualified certificates CA
	  ○ Issues certs for SSL Server, SSL client, E-
		All of the old sub CAs are under the new root, so this has all the same sub CAs as the old root, plus the new subCA for EV.
		• Citizen and Entity CA, qualified certificates
		  ○ Issues certs for SSL client and e-mail.
		• Citizen and Entity CA, non qualified certificates
		  ○ Issues certs for SSL Server, SSL client, E-mail, and code signing.
		• Public Adminstration, qualified certificates CA
		  ○ Issues certs for SSL client and e-mail.
		• Public Adminstration, non qualified certificates CA

	mail, code signing, OCSP, and TSA.	○ Issues certs for SSL Server, SSL client, E-mail, code signing, OCSP, and TSA. • SSL with EV certificates CA ○ Issues EV SSL certs.
Externally Operated sub-CAs	None Comment #50: No. We are the only one who manage the root and the sub CAs.	
Cross-signing	None	
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Verification type; DV, OV, and/or EV	OV	OV, EV
EV policy OID(s)	Not EV	EV OID: 1.3.6.1.4.1.14777.6.1.1
CP/CPS	CPS (Spanish, Basque and English): http://www.izenpe.com/cps CPS in English, direct access: http://www.izenpe.com/s15-12020/es/contenidos/informacion/descarga_certificados/es_url/adjuntos/DPC%20V4%206-EN.pdf In the CPS we don't mention specific information of any certificate, that's why we have the specific documentation. CPS in Spanish: http://www.izenpe.com/s15-12020/es/contenidos/informacion/descarga_certificados/es_url/adjuntos/DPC%20V4.6%20castellano.pdf Certificate Specific Documentation: http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/solicitar_certificado_digital.html Procedures for EV SSL Secure Server Certificates (Spanish): "Documentación Específica de Certificado de Servidor Seguro con EV" http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Documentaci%C3%B3n%20espec%C3%ADfica%20%20SSL%20EV%20castellano_nov09.pdf Procedures for Secure Server Certificates (Spanish): "Documentación Específica de Certificado de Servidor Seguro" http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Documentaci%C3%B3n%20espec%C3%ADfica%20SSL%20castellano_nov09.pdf	

	Procedures for Code Signing Certificates (Spanish): "Procedimiento certificado de firma de código" http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Procedimiento_Firma_C%C3%B3digo_castellano_06-03-24.pdf Procedures for Corporate Certificates (Spanish): "Documentación Específica Certificado Corporativo reconocido público" http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Documentaci%C3%B3n%20Espec%C3%ADfica%20Corporativo%20reconocido%20castellano_nov09.pdf
AUDIT	Audit Type: ETSI 101.456 Auditor: BSI Management Systems B.V. Auditor Website: http://www.bsi-global.com/ClientDirectory Audit Certificate: https://bugzilla.mozilla.org/attachment.cgi?id=401406 (2009.07.30) The ETSI audits are done every 3 years. The ETSI certificate can be verified by going to the BSI website listed above, and entering Izenpe for the search. Audit Type: WebTrust EV Readiness Auditor: KPMG Audit Report and Management Assertions: https://cert.webtrust.org/SealFile?seal=1017&file=pdf (2010-01-15)
Identity / Organization Verification Procedures	Comment #50: Izenpe, as all the Spanish CSP must follow the Spanish law 59/2003 which regulates the authentication of the natural person and the entities. So all the CSP have the same protocol and procedure because it's defined in the law. The identity/organization verification procedures are described in the specific documentation for each type of certificate. See below for the translations from the SSL and EV SSL documentation.
Verification of Domain Name Ownership / Control Non-EV	Non-EV SSL Certs: Procedures for Secure Server Certificates (Spanish) "Documentación Específica de Certificado de Servidor Seguro" http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Documentaci%C3%B3n%20espec%C3%ADfica%20SSL%20castellano_nov09.pdf Google Translation: 3.2 Accreditation 3.2.1 The identity of the applicant The requester of the certificate must appear before the registrar and submit original or certified copy of the following documents:

	a. ID card or passport, in case of national citizen. b. If a foreign national: I. Member of the European Union or of States party to the EEA European, an NIE will be payable together with an identity in force for the purpose of verification of their identity. II. In relation to non-EU citizens, the card will be required residence. c. Impartiality may be omitted before the registrar: If the signature of / the applicant in the application of the certificate has been standing in the presence of attorney. Or in the cases referred to in Article 13.4 of the LFE, except where the procedure of issuing callable outside the Impartiality of the applicant to purposes other than identification, eg to ensure safe delivery the certificate. The registrar shall keep minutes of verification of the identity of the applicant. 3.2.2 In the organization It will provide the following documentation on the applicant, Taxpayer Identification Number (TIN) of the entity. agencies and public corporations will provide the legal resolution (law, decree, ...) delivered by the constituent body, to which they are assigned. Should state the date and reference to the law. corporations and other legal persons whose registration is mandatory the Commercial Register, credited the valid constitution by providing original or a certified true copy of the Commercial Register on data from constitution and legal personality of the same. Associations, Foundations and Cooperatives credited the valid constitution through providing original or certified copy of a public registry where consisting registered on its constitution. civil societies and other legal persons, provide original or certified copy of public document proving irrefutably its constitution. The requester of the certificate must provide the following documentation, - Original or certified copy of the deed or official document derive the representation accompanied by a demonstration of the applicant responsible confirming its powers and the applicability thereof. - The applicant must provide the documentation required by this section solely on the first application of the certificate is sufficient, in successive applications a statement that have not changed the circumstances of the applicant or the person entity from whom it represents. - It is not necessary to obtain supporting evidence for the existence of the entity or powers of representation of the one acting on its behalf, provided that these events were covered by standard. The registrar shall keep minutes of checking documents 3.3 Validation IZENPE validate the documentation provided by the requester is not process starts issuance of certificates until the required documentation has been delivered and validated. General Counsel of IZENPE, check the documentation regarding the user entity, In general, be accepted as valid and will not require pre - documents that have been certified by a notary. official national or regional public bodies to which owned agencies and public enterprises. public records which must be legally registered entities. With respect to domains and Internet addresses, only consult IZENPE registrars appointed by ICANN / IANA for domain names

	and addresses associated with the certificate. It verifies that the domain does not appear in the listings as at risk (see Chapter 3.8). Constitution, date, name, NIF that we will make the constitution of the body applicant, verified by consulting the register or gazette where required establish its existence and commonality with the documentation provided by the applicant. Address: will check if registration data are consistent with the documentation provided. In the event that both directions are not coincident IZENPE verify that the address on the application refers to a location in which the entity applicant operates stably. This checking may be undertaken through signed statement or proof of payment of taxes. Phone. IZENPE must verify that the phone (must be a landline, not cell) belongs to the applicant entity (consulting the yellow pages and registration subsequent verification by call). Evidence of activity of organization: Certificate issued by an entity bank certifying the existence of an account on behalf of the applicant, proof of payment of local taxes. On the Internet domain (not applicable to internal domains): Search the whois database, verify that the domain is registered, consulting valid records. Be attached copy of the whois query the minutes of validation. There is a list of registrars supported by domain type (http://www.iana.org/domains/root/db/) that are either generic (gTLD's) or country (country-code, ccTLDs) that indicates which is the official registrar for each delegate type of domain. Specifically, you can check the whois for the more usual Dominios .com .net .org .info -- http://www.networksolutions.com/whois/index.jsp Dominos .es -- http://www.nic.es How the owner (registrant) agrees with the applicant organization. In case of a mismatch, the applicant must provide documentation to establish the right of use by the owner. IZENPE contact the owner listed in the whois to verify that the applicant has the right to use the domain or subdomain. The technical application is reviewed and validated by the Technical Area IZENPE. IZENPE General Counsel of the certified report submitted by the applicant. Be recorded in the minutes as well, the public register used to validate the information.
EV Verification Procedures	Procedures for EV SSL Secure Server Certificates "Documentación Específica de Certificado de Servidor Seguro con EV" http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Documentaci%C3%B3n%20espec%C3%ADfica%20%20SSL%20EV%20castellano_nov09.pdf Google Translation: 3.1 Application for Certificate Entities made applications for licenses for servers they deem appropriate. The applicant, owner or representative of the competent organ of the Authority shall complete the certificate application form and provide the documentation indicated. The processing of the application form before IZENPE be held through 2 pathways:

	- Via telematics: in http://www.izenpe.com the web address / concerned as / as have the application form, which may be completed and submitted IZENPE telematics storing it as a pre-registration. - Or face: The requester can go to any of the Entities Record identified in the published list and perform http://www.izenpe.com license application. These requests will be managed by IZENPE or, where appropriate, by the registrar that determine IZENPE (hereinafter references to IZENPE be construed or held to IZENPE Registration Authority). Previously, the subscriber will have generated a key pair on the server itself IZENPE handing the public key together with the application form. The Consultant subscriber to be the applicant organization and the key holder is the server itself performs the operation automatically under the responsibility of the subscriber of certificate. 3.1.1 Proof of identity of the applicant The requester of the certificate must appear before the registrar and submit original or certified copy of the following documents: a. ID card or passport, in case of national citizen. b. If a foreign national: I. Member of the European Union or of States party to the EEA European, an NIE will be payable together with an identity in force for the purpose of verification of their identity. II. In relation to non-EU citizens, the card will be required residence. c. Impartiality may be omitted before the registrar: □ If the signature of / the applicant in the application of the certificate has been standing in the presence of attorney. □ Or in the cases referred to in Article 13.4 of the LFE, except where the procedure of issuing callable outside the Impartiality of the applicant to purposes other than identification, eg to ensure safe delivery the certificate. The registrar shall keep minutes of verification of the identity of the applicant. 3.1.2 Proof of identity of the organization It will provide the following documentation on the legal person, □ Taxpayer Identification Number (TIN) of the entity. □ agencies and public corporations will provide the legal resolution (law, decree, ...) delivered by the constituent body, to which they are assigned. Should state the date and reference to the law. □ corporations and other legal persons whose inclusion is mandatory in the commercial register, the valid constitution credited by providing original or certified copy of a certificate from the Trade Register on data from constitution and legal personality of the same. □ Associations, Foundations and Cooperatives credited the valid constitution by providing original or certified copy of a certificate of registration attesting to registered public on its constitution. □ civil societies and other legal persons, provide original or certified copy public document proving irrefutably its constitution. - The / The license applicants must bring the following documents: □ administrators / legal representatives as a legal person subject to registration which must provide original or certified true copy of the Register concerning their appointment and term of office. Saidcertificate shall have been issued during the fifteen days

	preceding the date of application for the license. Other representatives, they must provide original or certified copy of specific power of attorney, and enunciated clearly determined specifically for electronic certificate request and perform for and on behalf of the person legal administrative and technical tasks necessary for the use of the certificate mail. not required to obtain supporting evidence for the existence of the entity or powers of representation of the one acting on its behalf, provided that these events were covered by standard. 3.1.3 Validation IZENPE validate the documentation provided by the requester is not process starts issuance of certificates until the required documentation has been delivered and validated. The validation was conducted by the Legal and Technical Area. The documentation relating to the user organization will be verified by the Advisory Legal IZENPE. The Technical Department will review and validate all information subsequently provided by the Legal Area and finally determined by signature that the documentation is correct The technical application is reviewed and validated by the Technical Area IZENPE. The Legal and Technical Department analyze the documentation regarding the registration of each entity in the appropriate register, the register may contact via other means. In general, be accepted as valid and will not require pre - documents that have been certified by a notary. Newsletters official national or regional public bodies to which owned agencies and public enterprises. public records which must be legally registered entities. With respect to domains and Internet addresses, only consult IZENPEregistrars appointed by ICANN / IANA for domain names and addressesassociated with the certificate. The Legal and Technical Area Contact verify the documentation provided by the firm: It verifies that domain does not appear in the listings as at risk (see Chapter 3.8). Address: will check if registration data are consistent with the documentation provided. In the event that both directions are not coincident IZENPE verify that the address on the application refers to a location in which the entity applicant operates stably. This checking may be undertaken through signed statement or proof of payment of taxes. Phone. IZENPE must verify that the phone (must be a landline, not cell) belongs to the applicant entity (consulting the yellow pages and registration subsequent verification by call). Evidence of activity of organization: Certificate issued by an entity bank certifying the existence of an account on behalf of the entity applicant, proof of payment of local taxes. Requirement does not apply in the case of Public Administration. On the Internet domain (not applicable to internal domains): Search the whois database, verify that the domain is registered, consulting valid records. Be attached copy of the whois query the minutes of validation.

	□ There is a list of registrars supported by domain type(http://www.iana.org/domains/root/db/) that are either generic (gTLD's) or country (country-code, ccTLDs) that indicates which is the official registrar for each delegate type of domain. Specifically, you can check the whois for the most common in Dominios .com .net .org .info -- http://www.networksolutions.com/whois/index.jsp Dominos .es -- http://www.nic.es □ How the owner (registrant) agrees with the applicant organization. In case of a mismatch, the applicant must provide documentation supporting the right of use by the owner. IZENPE contact the owner listed whois in verifying that the applicant has the right to use the domain or subdomain. The Legal and Technical Area Testing minuted by the applicant. The minutes shall record in the public register also used to validate the information.
Verification of Email Address Ownership / Control	Comment #93: the verification of the email as is an optional field is not done by Izenpe but the requestor company. Comment #91: <For Email certificates> you have to check the corporate certificates, these are qualified certificates and are intended to the employees of the Administration, so these are for the public servants because by law it´s a need. In any case this field is optional and sometimes is not filled up. The identification process is the same that for all qualified certificates, but in this case we use to sign a contract with the correspondent department or public society in order to themselves to identify their own employees and they give us all the information needed and they are in charge of those information, and this is according to the spanish legislation. Here are 2 links in the web site in which you can find some info. In the second one, just go to the "declaracion de practicas de certificacion (DPC)especifia" which is a specific CPS for this certificate, and once inside the doc you can check points 2 and 3 for the identification process. http://www.izenpe.com/s15-12020/es/contenidos/informacion/certificado_corporativo_recono/es_c_recono/certificado_corporativo_recono.html <This webpage describes the procedures for verifying the identity of the person or corporation.> http://www.izenpe.com/s15-12020/es/contenidos/informacion/cert_corporativos/es_cert/certificado_corporativo.html -- Recognized corporate public certs: http://www.izenpe.com/s15-12020/es/contenidos/informacion/cert_corporativos/es_cert/adjuntos/Documentaci%C3%B3n%20Espec%C3%ADfica%20Corporativo%20reconocido%20castellano.pdf Google Translations: 2.1 Identification Obligations IZENPE checks on registers, by itself or through the With user organizations signing the corresponding agreement, the identity and

	any other personal circumstances of applicants, subscribers and key holders of the certificates relevant to their own end. Also, verify that the key holder is duly authorized by the subscriber. 2.1.1 Subscriber Liability Certificate Regarding the obligations relating to subscriber status, both the subscriber as the possessor of keys have the burden of requesting revocation of the certificate in the terms stipulated in the Certification Practice Statement. 3 Identification and Authentication Initial 3.1 Registration 3.1.1 Types of names The distinguished name of the Subject field of certificates Corporate Name is recognized the legal name of the organization or unit of the organization. 3.1.1.1 Subject (requirement of Article 11.2 letter e) of Law 59/2003 of December 19, 2003) The attributes that make up the Distinguished Name of the certificate subject field Corporate recognized are those contained in the section on profile certificate. 3.1.1.2 Meaning of names You can not use pseudonyms. The key holder's name on the certificates recognized corporate whose Subscriber is a legal entity, consists of the name of holder along with its number of Passport or NIE 3.1.1.3 Resolution of disputes concerning names Certificates recognized corporate name conflicts holders keys that appear on the certificates identified under his real name is overcome by the inclusion in the Distinguished Name of the certificate, the NIF or other identifier assigned by the subscriber, in accordance with the provisions of preceding paragraph. 3.1.2 Authentication of organization identity For the issuance of certificates of type Corporate recognized Registration Authority recorded: - Documentation proving the formation of the entity on the license. The identity of the person seeking the certificate in accordance with section follows (paragraph 3.1.9 Specific Documentation Corporate Certificate recognized) - And when needed, your enrollment in the public register appropriate. Specifically, the registrar checks the supporting documentation provided by the applicant on the following: a) Full legal name of the organization b) State the organization's legal c) Tax Identification Number d) particulars of registration, if applicable. To perform the verification of data relating to the constitution and personality legal consultations will be relevant in the Public Registry if they are compulsory registration. The registrar will record the verification. 3.1.3 Authentication of the identity of an individual

	3.1.3.1 Identification Subjects IZENPE identify the applicant for the certificate. 3.1.3.2 Identification Required Elements To prove the identity of applicants, will require the following documentation: a) ID card or passport, in case of national citizen. b) If a foreign national: I. European Union Member States or part of Space European Economic an NIE will be required accompanied by a valid identity document for verification of their identity. II. In relation to non-EU citizens, the card will be required residence. 3.1.3.3 Accreditation of identification elements The registrar shall perform such audit of the documentation indicated in the previous section by noting that documentary was made. In particular for verification of data on the extent and validity of the powers of compulsory registration mentioned in the previous section will be appropriate consultation in the Public Registry. 3.1.3.4 The need for personal presence The identification and accreditation of the applicant require the Entity to the Impartiality of Registration, which shall be recorded. Impartiality may be omitted that, if the signature of the application for the certificate: - Has been legitimized in the presence of attorney - Or in the circumstances envisaged in Article 13.4 of the LFE, except where the procedure of issuing callable outside the Impartiality of the applicant for other than identification, eg to ensure safe delivery of certificate. 4.1 Application for Certificate The Public Entity applicant must complete the license application form, for individuals in positions or positions in your organization that deem appropriate, and deal with IZENPE (or user with the Public Entity that IZENPE sign the relevant agreement) through two channels: - Via telematics: in the web address stakeholders http://www.izenpe.com have the application form, which may be completed and sent Entity telematic registry which stores it as a pre-registration. (*) Within one month of completion of pre-registration, if the applicant fails appearing personally in any of the offices of the registrar to perform the effective application of the certificate, are eliminated in their data pre-registration. - Or face: The applicant could go to any of the Registration Entities identified in the list published in http://www.izenpe.com and make the license application. The subscriber of the certificate is the public entity applicant who does not exercise powers administrative and key holder is the individual who plays a office or position at the Institution, whose name and title or position entered into the certificate in the case that voluntarily want this information recorded in the certificate. 4.1.1 Proof of identity of applicant Identification Elements The license applicants must appear before the registrar and submit original or certified copy of the following documents: a) ID card or passport, in case of national citizen. b) If a foreign national: I. European Union Member States or part of Space European Economic an NIE will be required accompanied by a valid identity document for verification of their identity.

	II. In relation to non-EU citizens, the card will be required c) Furthermore the applicant through the application of the certificate evidence to the registrar, of each nuclear future Key: • Identity • Approval by the public entity applicant. • Justification of office or post held, if applicable. The registrar shall keep minutes of verification of the identity of the applicant. 4.1.2 Proof of identity of the organization A document stating the valid constitution of the legal person and power enough of the applicant The following documentation will be submitted for the purpose of verification by the Entity Registration: 1) Proof of valid constitution of the legal person □ Taxpayer Identification Number (TIN) of the entity. □ corporations and other legal persons whose inclusion is mandatory in the commercial register or any other public register credited the valid constitution by providing original or copy authenticity of the certificate of registry data on the constitution and legal personality of the same. Another case □ provide original or certified true copy of public document proving irrefutably constitution 2) Proof of the applicant sufficient power A document stating the power sufficient for the purpose of seeking electronic certificate. To this end, - In addition to administrators and legal representatives, - Is considered to have sufficient power of volunteer representatives provide proof enough power to carry out acts of administration or concluding contracts on behalf of the entity. The license applicants must bring the following documents: If □ administrator or legal representative of a legal person subject to registration, must provide original or certified true copy of registry concerning their appointment and term of office. This certificate shall have been issued during the fifteen working days preceding the date of application for the license. □ If the applicant is voluntary representative must provide the same original or certified copy of the deed or official document representation to derive the expression of their authority and their term. It will be necessary to obtain supporting evidence for the existence of the entity and to the powers of representation of the one acting on its behalf, provided that the actions were governed by rule. Registration Authority will credit the checking of documentation submitted by the applicant attorney. 4.2 Proof of identity of holders of key The key holder attesting to their identity to the registrar and shall, for this purpose, it required documents to the applicant (see section 4.1.1). Also submitted to the registrar a request signed by the applicant and the registrar in the records of your data and copy signed the initial request for the certificate. 4.3 Issue of Certificate Credited the applicant's identity before the registrar, he shall sign the application of the certificate, thus accepting the contract

	subscriber. 4.4 Delivery of certificate The registrar shall deliver the certificate to the key holder, who may opt in the following ways: 1. Delivery at the time of issuing the certificate, the PIN code Unblocking the PIN (PUK) and a sheet containing the password Identification telephone and was informed of the conditions of use certificate. Likewise, the key holder should sign the sheet Delivery and Acceptance. 2. Personal delivery of the certificate to the applicant's mailing address given delivery in the application for certificate issuance and delivery by post of the PIN and PIN unlock code (PUK) and as a sheet containing the telephone identification and password be informed of the conditions of use of the certificate. Likewise, the key holder must sign the sheet of Delivery and Acceptance. -- Comment #93: 2) As said, everything is under a contract between the requestor company and Izenpe. As government CA we have to be very careful with the identification process on the qualified certificates because according to the spanish law, the signature with those certificates is the same than the hand written signature, so identification is crucial. Having said this, the verification of the email as is an optional field is not done by Izenpe but the requestor company. We have customers that they have 5 employees and I can go and identify all of them, one by one with all the information needed, but most of them are companies with more than 100 employees, we have ones with 8000 employees, and all the funcionaries, which can be more than 10000, in which is impossible to identify them all, so we sign a contract with them. This contract is usually signed by the general manager/ministry of the company/dept and we identify that person but all the information provided by them is their responsability by contract and we can´t check that. This have been talked with several lawyers about data protection law, electronic siganture law and so on and this was the solution. Even more, the procedure has been marked as a best practice by the government and auditors for improvement of the speeding of the processing and developing the electronic signature in the public administration. About the PIN, the procedure is different depending on the issuance process, if this is online, the card with the PIN/PUK envelope is giving inmediatly to the requestor because he´s on the RA requesting the certificate and if this is in batch mode, the card is delivered to the identification place in which took place by courier and the PIN/PUK is sent by post to the address filled in the request form. Sometimes is necessary to change this one, and then the card and the PIN/PUK are sent to the address but with 1 day difference and one by courier and the other by post.
Code Signing	Procedures for Code Signing Certificates (Spanish): “Procedimiento certificado de firma de código” http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Procedimiento_Firma_C%C3%B3digo_castellano_06-03-24.pdf

	Section 1.2, Accreditation of Identity of Applicant (Google Translation) The applicant must prove his identity, and where applicable, the constitution of the entity he represents, providing the necessary documentation. Documents needed The applicant must provide an original or certified true copy of the following documentation: A) Identification Elements 1) ID card or passport, in case of national citizen 2) In case a foreign national: - Member of the European Union or of States party to the EEA European, an NIE will be payable together with an identity in force for the purpose of verification of their identity. - With regard to non-EU citizens, the card will be required residence. B) Elements of proving the constitution of the Public Entity and the license □ Articles of Incorporation of the entity, registered in the official concerned. □ Record in showing the powers of the applicant. Accompanied by a statement confirming the applicant's responsibility the valid constitution of the entity and the authority and validity of the same. It will be necessary to obtain supporting evidence for the existence of the entity and to the powers of representation of the one acting on its behalf, provided that the actions were governed by rule.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL certs are OV
	  ○ Comment #50: Izenpe issues SSL standard certificates for a period of 3 years... Izenpe also checks the organization or entity name
	  ○ EV SSL CP: IZENPE issues Secure Server Certificates EV SSL with a maximum period of 12 months.
	• Wildcard DV SSL certificates
	  ○ Izenpe does not issue Wildcard certificates
	• Delegation of Domain / Email validation to third parties
	  ○ It looks like Registration Authorities are external to IZENPE, as per the CPS.
	  ○ Comment #50: They´re not external, unless you mean for not Izenpe employees, but they´re under contract and with rigorous clauses as all the auditors have checked.
	  ○ **The Corporation requesting that the email address be included in certs for their employees is responsible for verifying the ownership/control of the email address.**
	• Issuing end entity certificates directly from roots
	  ○ The root signs intermediate CAs, which issue the end-entity certs.

	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ There are no externally-operated subordinate CAs.
	• Distributing generated private keys in PKCS#12 files
	  ○ Comment #50: Izenpe does not generate the private keys. Izenpe provide a software to do that, but the keys are generated by the customer and then send to Izenpe to generate the certificate and then send back to the customer
	• Certificates referencing hostnames or private IP addresses
	  ○ No
	• OCSP Responses signed by a certificate under a different root
	  ○ No, Izenpe does not do this
	• CRL with critical CIDP Extension
	  ○ The CRLs import into Firefox without error.
	• Generic names for CAs
	  ○ The company name is included in the CN.