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.

General Information	Data
CA Name	izenpe
Website URL	www.izenpe.com The web is only in Spanish and in Basque. The CPS is translated.
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 and accepted and validated by all of the PKIs in Spain, so the geographical area relates to Spain.

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

Info Needed	Data – Old Root	Data – New Root, SHA-256
Certificate Name	Izenpe.com	Izenpe.com
Cert summary / comments	This is the original 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	The number (2) is for the new hierarchy, the Izenpe 2007. 1.- CA of CCEE rec: http://crl.izenpe.com/cgi-bin/crl http://crl.izenpe.com/cgi-bin/crl2 2.- CA of CCEE no rec: http://crl.izenpe.com/cgi-bin/crlscinr http://crl.izenpe.com/cgi-bin/crlscinr2 3.- CA of AAPP rec: http://crl.izenpe.com/cgi-bin/crlscar http://crl.izenpe.com/cgi-bin/crlscar2 4.- CA of AAPP no rec: http://crl.izenpe.com/cgi-bin/crlinterna http://crl.izenpe.com/cgi-bin/crlinterna2 5.- CA of SSL EV: http://crl.izenpe.com/cgi-bin/crlsslev	
nextUpdate in the CRL for end-entity certs	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	http://ocsp.izenpe.com:8094 When I enforce OCSP and go to the test website, I get an error Error code: sec_error_ocsp_invalid_signing_cert Comment #61: The problem with the OCSP is more complex. 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
	  o Issues certs for SSL client and e-mail.
	• Citizen and Entity CA, non qualified certificates
	  o Issues certs for SSL Server, SSL client, E-mail, and code signing.
	• Public Adminstration, qualified certificates CA
	  o Issues certs for SSL client and e-mail.
	• Public Adminstration, non qualified certificates CA
	  o Issues certs for SSL Server, SSL client, E-mail, code signing, OCSP, and TSA.
		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
		  o Issues certs for SSL client and e-mail.
		• Citizen and Entity CA, non qualified certificates
		  o Issues certs for SSL Server, SSL client, E-mail, and code signing.
		• Public Adminstration, qualified certificates CA
		  o Issues certs for SSL client and e-mail.
		• Public Adminstration, non qualified certificates CA
		  o Issues certs for SSL Server, SSL client, E-mail, code signing, OCSP, and TSA.
		• SSL with EV certificates CA
		  o Issues EV SSL certs.

Subordinate CAs operated by third parties.	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
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, 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/informacion_juridica/es_i_juridi/adjuntos/DPC%204.3%20ingles.pdf In the CPS we don't mention specific information of any certificate, that's why we have the specific documentation. Declaration of Practices for each type of certificate (Spanish and Basque) http://www.izenpe.com/s15-12020/es/contenidos/informacion/informacion_juridica/es_i_juridi/informacion_juridica.html (I'm not able to tell from here where to find the specific declaration of practices for each type of cert.)	

Identity / Organization Verification Procedures	English CPS: **3.1.8 Authentication of organization identity** Authentication of the identity of an organization is described in the *Specific documentation for each certificate.* **3.1.9 Authentication of the identity of a natural person** Authentication of the identity of a natural person is described in the *Specific documentation for each certificate.* 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. So taking for example the specific documentation for EV certs (it´s the same in the rest of policies) this is what we do Authentication of the identity of a natural person 3.1.1 Proof of identity / the applicant The requester of the certificate must go to the RA and provide an original or certified true copy of the following documents: a. Identity card or passport, in the case of nationals. b. If a foreign: I. EU Member States or the European Economic Area, an NIE will be required with a valid identity document for verification of their identity. II. In relation to citizens, will be required for a residence card. c. May be appointed to the RA If the firm / the applicant in the application of issuing the certificate has been legitimized in the presence of notary. Or in the cases referred to in Article 13.4 of the LFE (Spanish law), unless the procedure of issuing callable outside of the appointed / the applicant for any purpose other than to identify, for example to ensure a safe delivery of the certificate. For authenticate an organization or entity Will be delivered the following documents on the legal person, Tax Identification Number (TIN) of the Institution. - The agencies and public corporations will make the legal decision (law, decree, ...) delivered by the constituent body to which they are attached. Must state the date and reference of the law. The corporations and other legal persons whose registration is mandatory in the Register, credited the valid constitution by providing original or certified copy of a certificate from the Trade Register on the constitution and legal personality of the same. ¬ Associations, Foundations and Cooperatives credited the valid constitution by providing original or certified true copy of a public register showing the entry on its constitution. The civil societies and other legal persons, provide original or certified true copy of the document attesting to their constitution

	public solid evidence. - The requester of the certificate must provide the following documentation: The administrators / legal representatives or as a legal person subject to registration which must provide original or certified true copy of the certificate of registry on their appointment and term of office. The certificate must be issued during the fifteen days preceding the date of application for the certificate. Others volunteer as, must provide original or certified true copy of the power of attorney specific, clearly identified and explicitly stated to apply for electronic certificates and perform for and on behalf of the legal administrative and technical tasks necessary for using the electronic certificate. It is not necessary to obtain supporting evidence for the existence of the entity and to the powers of representation of acting on their behalf, provided that these events were covered by standard.
Verification of Domain Name and Email address Ownership	Please provide pointers to the sections (and translations into English) in the CP/CPS that demonstrate that reasonable measures are taken to verify the following information for end-entity certificates chaining up to these roots, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/. a)for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; b)for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; c) for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; Comment #53: English Translation of EV SSL validation procedure provided in attachment https://bugzilla.mozilla.org/attachment.cgi?id=376196 “The Internet domain (not applicable to internal domains) Query the whois database, verify that the domain is registered, consulting registrars valid. A copy of the printed record of the whois query validation. There is a list of registrars supported by domain type (http://www.iana.org/domains/root/db/) and are generic (gTLD's) or country (country-code, ccTLDs), indicating Delegate is the official record for each domain. In particular, one can see the whois for the more usual Domains. Com. Net. Org. Http://www.networksolutions.com/whois/index.jsp info Network Solutions Dominos. EsNIC is http://www.nic.es It verifies that the owner (registrant) agrees with the applicant organization. If no match, the applicant must provide documentation to support 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.” Comment #55: >> Translated SSL EV validation procedure Please also provide a link to the original document (and the section or page number) where this text was translated from.

	The translated document for SSL EV validation procedure meets the requirement in regards to verification of domain ownership. However, this only applies to EV SSL certs. I also need the translated text for SSL (non-EV) verification procedures. Comment #65: Please provide the specific urls to the CP/CPS for issuance of email, SSL, EV SSL, and code signing certs. For each document, please clearly indicate the types of certs that it covers.
EV Verification Procedures	English translations of the Verification steps for EV certs, demonstrating compliance with the CAB Forum Guidelines http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Attached in Comment #53: SSL EV validation procedure https://bugzilla.mozilla.org/attachment.cgi?id=376196 Comment #62: English Translations of the EV SSL specific documentation provided in attachment https://bugzilla.mozilla.org/attachment.cgi?id=384413 (Note: still need links to the original documentation from which this is translated)
Potentially Problematic Practices	(http://wiki.mozilla.org/CA:Problematic_Practices) • Long-lived DV certificates o SSL certs are OV o Comment #50: Izenpe issues SSL standard certificates for a period of 3 years but those certs are not only DV certs. Izenpe also checks the organization or entity name • Wildcard DV SSL certificates o Izenpe does not issue Wildcard certificates • Delegation of Domain / Email validation to third parties o It looks like Registration Authorities are external to IZENPE, as per the CPS. o 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. • Issuing end entity certificates directly from roots o The root signs intermediate CAs, which issue the end-entity certs. • Allowing external entities to operate unconstrained subordinate CAs o There are no externally-operated subordinate CAs. • Distributing generated private keys in PKCS#12 files o 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 o No • OCSP Responses signed by a certificate under a different root o No, Izenpe does not do this • CRL with critical CIDP Extension o The CRLs import into Firefox without error. • Generic names for CAs o There´s no generic name for a CA
AUDIT	Audit Type: ETSI 101.456 Auditor: BSI Management Systems B.V. Audit Certificate: http://www.izenpe.com/s15-12020/es/contenidos/informacion/acreditaciones/es_acredita/adjuntos/certificado_etsi.pdf (Valid 2006 to 2009) Comment #52: The ETSI certificate is not old, it has a validity of 3 years, and every year we have had audit surveillances from KPMG. This year, 2009, we have re-certification for another 3 years if we meet all the requirements and it´s scheduled for July. In the URL you mention, the ETSI document you can see the expiry date for August 1st 2009, so our ETSI audit is still valid. Audit Type: WebTrust EV Readiness Auditor: KPMG Audit Report and Management Assertions: https://bugzilla.mozilla.org/attachment.cgi?id=359717 (2009-01-29) **Verify Audits** (Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/) • Validate contact info in report, call to verify that they did indeed issue this report. o 6/26: Sent email to auditor to confirm the authenticity of the audit report as per Mozilla policy. • For EV CA's, verify current WebTrust EV Audit done. o Current WebTrust EV audit provided • Review Audit to flag any issues noted in the report o No issues noted in the report