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 (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 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	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 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/crlscar CA of AAPP no rec: http://crl.izenpe.com/cgi-bin/crlinterna	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
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 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-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 ○ 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-mail, code signing, OCSP, and TSA. • SSL with EV certificates CA ○ Issues EV SSL certs.

SubCAs 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. CPS in Spanish: http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/DPC%204.3%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): Servidor Seguro con Validación Extendida (SSL EV) Documentación específica http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Documentacin%20especfica%20%20SSL%20EV%20castellano.pdf Section 3.1.2: Verification of Organization Section 3.1.3: Verification of Domain ownership Procedures for Secure Server Certificates (Spanish): "procedimiento certificado servidor seguro" http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Procedimiento_Servidor_castellano_06-01-	

	10.pdf Section 1.2: Procedures for verifying the identity of the applicant/organization Section 1.3: Verification of Domain ownership Procedures for Code Signing Certificates (Spanish): "procedimiento certificado firma codigo" 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: Procedures for verifying the identity of the applicant/organization Procedures for Corporate Certificates (Spanish): http://www.izenpe.com/s15-12020/es/contenidos/informacion/cert_corporativos/es_cert/adjuntos/Documentaci%C3%B3n%20Espec%C3%ADfica%20Corporativo%20reconocido%20castellano.pdf
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 Ownership / Control	Non-EV SSL Certs: http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Procedimiento_Servidor_castellano_06-01-10.pdf Section 1.2: Procedures for verifying the identity of the applicant/organization Section 1.3, Google Translation: Delivered signed the application, the public key and the required documentation IZENPE proceed with the issuance of the certificate. Prior to the issuance of the certificate and only if domain external IZENPE finds that the domain to be included in the certificate is ownership of the applicant.
EV Verification Procedures	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 #62: English Translations of the EV SSL specific documentation provided in attachment https://bugzilla.mozilla.org/attachment.cgi?id=384413 Original text is in the Procedures for EV SSL Secure Server Certificates: Servidor Seguro con Validación Extendida (SSL EV) Documentación específica http://www.izenpe.com/s15-12020/es/contenidos/informacion/solicitar_certificado_digital/es_solicita/adjuntos/Documentacin%20especfica%20%20SSL%20EV%20castellano.pdf Google Translation of section 3.1.3: 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 minutes whois query 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 delegated official registrar for each domain type. Specifically, you can check the whois for the more usual Domains. Com. Net. Org. Info Network Solutions http://www.networksolutions.com/whois/index.jsp Dominos. Is ESNIC 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 registrar the certified report submitted 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.
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 but those certs are not only DV certs. Izenpe also checks the organization or entity name • 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. • 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 ○ 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. Comment #75: The ETSI 101 456 is only for qualified certificates, so that means, that SSL or code signing certificates are excluded, are out of the scope. Last week, we had the re-certification for another 3 years in this one, plus the webtrust for Ev implementation audit which also have been passed. As previously suggested I have sent email to KPMG on 8/31/2009 and then again on 9/2/2009 to ask if their recent audits of Izenpe included the verification procedures for issuance of SSL (not EV) certificates? And, if yes, which audit covered the non-EV SSL certs. I have not yet received a response. Comment #93 1)As mentioned Izenpe has the following certifications: - ISO27001 with the scope related to the CA and all its operations - ETSI TS 101 456 which is related to the qualified certs - Webtrust for EV, related to SSL EV certs We don´t have any specific audit that covers the issuance of SSL and code signing certs, but as metioned, ETSI 101 456 is above ETSI 102 042 which is related to non qualified certs, SSL and code signing. I think Patrick Paling will answer you soon because he told me about your email.

	Besides, we´re a government CA so we have more restrictions to issue certificates, qualified and non-qualified and must follow all the spanish and european legislation, in fact, for issuing EV certs we didn´t need to modify our procedures a lot because we already asked for identification process and keeped all the information. Audit Type: WebTrust EV Readiness Auditor: KPMG Audit Report and Management Assertions: https://bugzilla.mozilla.org/attachment.cgi?id=359717 (2009-01-29) Confirmation of authenticity of the WebTrust EV Readiness audit: > From: Paling, Patrick <Paling.Patrick@kpmg.nl> > Subject: RE: Verifying Authenticity of Audit Report provided by Izenpe > Date: Saturday, June 27, 2009, 10:58 PM > Kathleen, > I hereby confirm that KPMG Advisory NV in the Netherlands performed the > audit activities and issued the report referenced in the URL. > Best regards, > Patrick Paling