Bugzilla ID: 529286
Bugzilla Summary: Add ipsCA Global and ipsCA Main root certificates
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	ipsCA
Website URL	http://www.ipsca.com/
Organizational type	private corporation
Primary market / customer base	ipsCA, primarily located in Spain, is a worldwide CA which has issued with more than 12,000 SSL certificates to Universities and educational entities (mainly in USA).
CA Contact Information	**CA Email Alias:** general@ipsca.com An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. **CA Phone Number**: 34-916-308-568 A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. **Title / Department**: IPS Certification Authority If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?

Info Needed	Data	Data
Certificate Name	ipsCA Main CA Root	ipsCA Global Root
Cert summary / comments	This root certificate is intended to replace the "IPS SERVIDORES" root that is currently included in NSS.	What is the relation of this global root to "ipsCA Main CA Root" and to the other roots currently in Mozilla/NSS?
URL of root cert	http://certs.ipsca.com/store/ipsCAMain.der	http://certs.ipsca.com/store/ipsCAGlobal.der
SHA-1 fingerprint	cf:e4:31:3d:ba:05:b8:a7:c3:00:63:99:5a:9e:b7:c2:47:ad:8f:d5	3c:71:d7:0e:35:a5:da:a8:b2:e3:81:2d:c3:67:74:17:f5:99:0d:f3
Valid from	2009-09-07	2009-09-07
Valid to	2029-12-25	2029-12-25
Cert Version	3	3
Modulus length	2048	2048
Test Website	Thank you for providing the test cert within the bug. Would you please provide a URL to a test website with this SSL cert?	Thank you for providing the test cert within the bug. Would you please provide a URL to a test website with this SSL cert?
CRL URL	ARL: http://crlmain01.ipsca.com/crl/crlmain01.crl (website note found) CRL for end-entity certs:	ARL: http://crlglobal01.ipsca.com/crl/crlglobal01.crl NextUpdate: 1 month CRL for end-entity certs:
OCSP Responder URL	http://ocspmain01.ipsca.com/	http://ocspglobal01.ipsca.com/

CA Hierarchy	Please provide a description and/or diagram of the planned CA Hierarchy for this root (both short-term and long-term).	Please provide a description and/or diagram of the planned CA Hierarchy for this root (both short-term and long-term).
CAs operated by third parties	Will this root have any subordinate CAs that will be operated by external third parties?	Will this root have any subordinate CAs that will be operated by external third parties?
Cross-Signing	List any other root CAs that have (or will) issued cross-signing certificates for this root CA	List any other root CAs that have (or will) issued cross-signing certificates for this root CA
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites	Websites
SSL Validation Type DV, OV, and/or EV	OV	OV
	From ipsCA: ipsCA will perform verification of certificate information as follows: - Limited check of the applicant's domain name against a public domain name registry; - Confirmation of applicant's Company name, name, address and phone number against information contained in an independent third party business database. - Faxed documentation will be required when applicant's company name cannot be validated using available information.	
EV policy OID(s)	Not EV	Not EV
CP/CPS	CPS: http://www.ipsca.com/es/Certificates/CPSIPSCAv31.pdf	
AUDIT	Audit Type: WebTrust CA Auditor: KPMG Audit: https://cert.webtrust.org/ViewSeal?id=933 (2009.07.08) This audit was performed before the new roots were created.	
Organization Identity Verification	Google Translations of CPS – Please correct. 1.6. May issue certificates CAs Second Level: This paragraph does not apply to IPS Certification Authority. Stated in this CPS as being mandatory for the CA's Second Tier. 1.6.1. B1. E-Certificate valid monthly / yearly. It connects the name you enter in our questionnaire with a valid email account. Allows mail signing and encryption. It has commercial as there is no verification of the identity of the subject. All information contained in the certificate is provided by the entity that acts as Registration Authority under its sole responsibility, or by the user himself as subscriber information is not verified, in accordance with the provisions of this CPS. This paragraph does not apply to IPS Certification Authority. Stated in this CPS as being mandatory for the CA's Second Tier. 1.6.2. B2. Personal Certificate with documentary verification It is necessary to check the identity of the subject through a valid ID. Should send a photocopy of the document. All information contained in the certificate is provided by the entity that acts as Registration Authority under its sole responsibility, or by the user himself as subscriber information is not verified, in accordance with the provisions of this CPS.	

This paragraph does not apply to IPS Certification Authority. Stated in this CPS as being mandatory for the CA's Second Tier.

1.6.3. B3. Certified Personal Face.

The verification of the person will face and documentary. The individual must be lodged with the Registrar with a valid ID. The registrar can be a professional, a department of a company or any other type of Registration Authority duly approved by the CA

Category B3 certificates are used by subscribers to third parties to ensure their identity, authenticity and integrity of their messages, intranet or Internet, including through the use of secure email applications S / MIME to encrypt and sign messages with a higher authentication level to Category 1, is suitable for use in the field of administration in general.

All data contained in the certificate are logged in accordance with applicable official practice according to the specific Registration Authority and should be available on registration practices related, enjoying the certificates of the legal nature of an official document. The signed documents are in any case, private papers.

This paragraph does not apply to IPS Certification Authority. Stated in this CPS as being mandatory for the CA's Second Tier.

1.6.4. B4. Certified Personal Face notary public

The verification of the person and documentary will face before a notary public. The individual must be lodged with the registrar (notary public) with a valid ID.

B4 certificates are used by subscribers to third parties to ensure their identity, authenticity and integrity of their messages, intranet or Internet, including through the use of secure email applications S / MIME to encrypt and sign messages when the law requiring the intervention of a notary public in the transaction. They assume the highest possible level prior authentication of the certificate subscriber.

1.6.5. A1. Certificate Server

Server Certificates enable incorporate the SSL (Secure Socket Layer) on a Web server. Thanks to this protocol all communication between the client and the server remains secure by encrypting the information sent to both points protecting personal data, credit card data, account numbers, passwords, etc. Is particularly important within the area of electronic commerce, where data security is a major scourge for developing this system.

The issuance of a server certificate involves the recognition of the identity of the applicant, have registered the Internet domain under which the server is called and comply with the procedure in section 3.3.5 is detailed.

This paragraph does not apply to IPS Certification Authority. Stated in this CPS as being mandatory for the CA's Second Tier.

3 IDENTIFICATION AND AUTHENTICATION. GENERATION OF CERTIFICATES:

The identification and authentication of the applicant and / or subscriber is determined based on the certificates requested. Only subscribers may be CA certificates Second Tier legal persons. In any case, applicants and / or certificate subscribers shall present to the RA the following documents in order to proceed to their identification and authentication:

-- Notary certified copy of the Book of the claimant company registered or subscribing. Failing that should provide both the original of the Deed of the applicant company or subscriber, such as a copy of it for comparison with IPS Certification Authority.

-- In the case that acting for or on behalf of the applicant, certified notarized copy of power by the authorizing act for or on behalf of the applicant. Failing that should provide both the original power by the authorizing act for or on behalf of the applicant, as the copy for collation by IPS Certification Authority.

3.1.Certificados for CA of Second Level:
This section applies only to IPS Certification Authority. The term CA refers to IPS Certification Authority.
The generation of certificates, including identification and authentication procedure for Second Tier CA is that which then proceeds to detail:
-- Subscriber and / or applicant for such certificate shall generate certificate request for Signature (PCF). In any case, this request must contain the following fields:
Common-name: The name of the applicant organization and / or subscriber. Along with its CIF.
Organization Unit: This field will be at the applicant or subscriber.
Location: City where the applicant organization and / or subscriber.
State: State where the organization and / or subscriber.
Country: Country where the applicant organization and / or subscriber.
-- The procedure for the generation of the PCF and the public and private keys vary depending on the type of dedicated server to issue Certificates of Second Tier CA. This key generation procedure is done in person before a charge specifically authorized by IPS Certification Authority.
-- After completing the PCF, the subscriber and / or deliver it to the applicant specifically authorized by Responsible IPS Certification Authority noted in the previous step.
-- Subscriber and / or applicant must complete the purchase form for CA Certificates of Second Level. In any case the form will contain the following fields:
Name of subscriber.
Address: It must reflect the address, town, province and postal code of the subscriber.
CIF of the subscriber.
Signature of representative with sufficient powers for which he is authorized to act for or on behalf of the applicant and / or subscriber.
Contact Person: Name of the person signing the certificate purchase form.
Phone: Phone Subscriber Certificate.
FAX: FAX number of the applicant.
Name Server: Name Server responsible for issuing Certificates of Second Level.
Email: email address of the contact person.
Postal Mail Postage Certificate: The applicant and / or subscriber must send, by certified mail or hand-deliver the following documents to the address of the CA:
Copy of the PCF, which contains the public key, generated by the server that is responsible for issuing Certificates of Second Level CA.
Certificate Purchase Form for Second Tier CA with all its fields filled in correctly.
Copy of bank transfer voucher or voucher on behalf of IPS Certification Authority, depending on the method of payment. The amount of the bank transfer or heel particular depend on the agreement reached between the subscriber and IPS Certification Authority. This agreement will be reflected in a License Agreement for digital certification for Second Tier CA.

	Notary certified copy of the Articles of Incorporation duly registered subscriber. Failing that should provide both the original of the Deed of the applicant company or subscriber, such as a copy of it for comparison with IPS Certification Authority. Notary certified copy of power by the authorizing act for or on behalf of the applicant and / or subscriber. Failing that should provide both the original power by the authorizing act for or on behalf of the applicant, as the copy for collation by IPS Certification Authority. -- The CA shall make its finding that the data in the subscriber's Articles of Incorporation duly registered and in power by the authorizing act for or on behalf of the applicant and / or subscriber, correspond to the data in the application of PCF sent by the applicant and / or subscriber. -- The CA shall issue the Certificate for Second Tier CA after signing the contract Second Level AC by the representative of the applicant and / or subscriber and verified bank transfer, or once entered the heel on behalf of IPS Certification Authority in your checking account. The signing of the Second Tier CA notary public may be made at the discretion of IPS Certification Authority or the applicant and / or subscriber. Immediately after the issuance of the Certificate IPS Certification Authority shall notify the subscriber / applicant of the fact that broadcast via email. -- Once the certificate issued by the CA, shall verify the contents of the certificate for errors or omissions and will be delivered by hand to the applicant / subscriber by authorized personnel IPS Certification Authority. The extent of the areas of IPS Certification Authority certificates are contained in paragraph 10.1 of this CPS. With regard to the re-issuance of certificates, requests receive the same treatment and carried out the same checks that if it were a new certificate.
Domain Name Ownership / Control	Google Translations of CPS – Please correct. 3.2.5. A1. Server Certificates: This section applies ONLY to the Second Tier CA's holding IPS Certification Authority certificates and CA shall mean the term to refer to a Second Tier CA. The issuance of a server certificate involves the recognition of the identity of the applicant, have registered the Internet domain under which the server is called and comply with the procedure outlined below: -- Subscriber and / or applicant for such certificate shall generate certificate request for Signature (PCF). In any case, this request must contain the following fields: Common-name: The name on the Internet of the organization or individual applicant and / or subscriber. Organization Unit: This field will be at the applicant or subscriber. Location: City where the organization or individual applicant and / or subscriber. State: State where the organization or individual applicant and / or subscriber. Country: Country where the organization or individual applicant and / or subscriber. -- The procedure for the generation of the PCF and the public and private keys vary depending on the type of server on which you install the Certificate Server. -- After completing the PCF, the subscriber and / or applicant must send, along the public key is generated, an email address of RA. -- Subscriber and / or applicant must complete the purchase form of server certificates. In any case the form will contain the following fields:

	Name of subscriber. Address: It must reflect the address, town, province and postal code of the subscriber. NIF / CIF subscriber. Signature of applicant and / or subscriber or, where applicable, signature of its representative with sufficient powers for which he is authorized to act for or on behalf of the applicant and / or subscriber. Contact Person: Name of the person signing the certificate purchase form. Phone: Phone Subscriber Certificate. FAX: FAX number of the applicant. Name Server: Name Server where you install the Certificate Server. Email: email address of the contact person. -- Postal Mail Postage Certificate: The applicant and / or subscriber must send, by certified mail the following documents to the address of RA: Copy of the PCF, which contains the public key, generated by the server where the server certificate installed. section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • 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; It's not clear to me what the procedures are for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber. This needs to be in a CP/CPS or other public and audited document.
Email Address Ownership / Control	Not applicable – Not requesting Email trust bit.
Identity of Code Signing Subscriber	Not applicable – Not requesting Code Signing trust bit.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. . For the ones that are applicable, please provide further information and translations into English of the CP/CPS where relevant. • Long-lived DV certificates o • Wildcard DV SSL certificates o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots

	o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs o Name includes ipsCA