Mozilla - CA Program

Case Information

Case Number	00000036	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	PSC-FII	**Request Status**	Need Information from CA

Additional Case Information

Subject	New Owner/Root inclusion requested	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=667466

General information about CA's associated organization

CA Email Alias 1	dmin-pki@fii.gob.ve		
CA Email Alias 2			
Company Website	https://ar.fii.gob.ve/	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)	The CA is operated by a government agency of Venezuela (Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico) and The type national.	**Verified?**	Verified
Geographic Focus	Venezuela	**Verified?**	Verified
Primary Market / Customer Base	Customers are the public and private sector of Venezuela. Market Segment: E-government secure.	**Verified?**	Verified
Impact to Mozilla Users	PSC-FII is a public entity belonging to the Government of the Bolivarian Republic of Venezuela accredited as a Provider of Electronic Certification Services (PSC) by the Superintendence of Electronic Certification Services (Spanish acronym, SUSCERTE) under the Law on Data Messages and Signatures Electronic. PSC-FII's primary market are public and private users in Venezuela.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Recommended Practices	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Verified?**	Need Response From CA

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	PSC Publico del MppCTII para el Estado Venezolano	**Root Case No**	R00000044
Request Status	Need Information from CA	**Case Number**	00000036

Additional Root Case Information

Subject	Include PSC Publico del MppCTII para el Estado Venezolano root cert

Technical Information about Root Certificate

O From Issuer Field	Sistema Nacional de Certificacion Electronica	**Verified?**	Verified
OU From Issuer Field	Superintendencia de Servicios de Certificacion Electronica	**Verified?**	Verified
Certificate Summary	This is a sub-CA of the “Autoridad de Certificacion Raiz del Estado Venezolano” root certificate owned by SUSCERTE. In Bug #489240 it was determined that SUSCERTE’s sub-CAs would apply for inclusion themselves as separate trust anchors.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8670003	**Verified?**	Verified
Valid From	2011 Jan 25	**Verified?**	Verified
Valid To	2021 Jan 22	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://publicador-psc.fii.gob.ve	**Verified?**	Verified

CRL URL(s)	http://www.suscerte.gob.ve /lcr/CERTIFICADO-RAIZ-SHA384CRLDER.crl https://publicador-psc.fii.gob.ve/crlsha256 /cacrl.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.acraiz.suscerte.gob.ve http://publicador-psc.fii.gob.ve:2560/ocsp	**Verified?**	Verified
Revocation Tested	NEED to resolve all errors returned by https://certificate.revocationcheck.com /publicador-psc.fii.gob.ve	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not requesting EV treatment.	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs.	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	3E:B1:8B:67:37:B3:30:2F:03:55:16:34:58:1C:FB:BF:38:EA:92:96	**Verified?**	Verified
SHA-256 Fingerprint	24:A9:C8:E1:15:0D:89:0D:42:D8:2B:1D:57:BF:3A:BB:F2:AD:AE:84:6B:3A:DD:EC:7A:79:28:5C:9D:4C:C7:7C	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The PSC Publico del MppCTII para el Estado Venezolano (PSC-FII) is the first public provider credited by the Venezuelan state to offer electronic signature certificates. Is a subCA under the venezuelan root of certification ("Sistema Nacional de Certificacion Electronica"). This root signs end-entity certificates directly.	**Verified?**	Verified
Externally Operated SubCAs	NEED: Can this certificate sign externally-operated subCA certificates?	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Foruom's Baseline Requirements - https://www.mozilla.org/en-US/about/governance /policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org /CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	Email CP: https://ar.fii.gob.ve/pub/docs/DPC_PC2015/PC/pc%20servidor/pc_serv_email-F017/Aprobar_080-PCS-F017.pdf SSL CP: https://ar.fii.gob.ve/pub/docs/DPC_PC2015/PC/pc%20servidor/pc_serv_ssl-F073/Aprobar_080-PCS-F073.pdf Code Signing CP: https://ar.fii.gob.ve/pub/docs/DPC_PC2015/PC/pc%20firma%20codigo/Aprobar_080-PCS-F075.pdf Operadores AR/AC CP: https://ar.fii.gob.ve/pub/docs/DPC_PC2015/PC/PC%20operador/Aprobar_080-PCO-F018.pdf	**Verified?**	Verified
CA Document Repository	https://ar.fii.gob.ve/	**Verified?**	Verified
CP Doc Language	Spanish		
CP	https://ar.fii.gob.ve/pub/docs/DPC_PC2015/PC/pc%20servidor/pc_serv_ssl-F073/Aprobar_080-PCS-F073.pdf	**Verified?**	Verified
CP Doc Language	Spanish		
CPS	https://ar.fii.gob.ve/pub/docs/DPC_PC2015/DPC/080-DPC-F014.pdf	**Verified?**	Verified
Other Relevant Documents	Accredited provider: http://www.suscerte.gob.ve/acreditacion/	**Verified?**	Verified
Auditor Name	Milthon J. Chavez	**Verified?**	Verified
Auditor Website		**Verified?**	Not Applicable
Auditor Qualifications	http://www.suscerte.gob.ve/registro/	**Verified?**	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8665614	**Verified?**	Not Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	6/12/2015	**Verified?**	Verified
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference section 11 of the CA/Browser Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the	**Verified?**	Need Response From CA

	certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership		
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	NEED: - URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the certificate subscriber's identity and authority, and the organization's identity and existence. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber	**Verified?**	Need Response From CA
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA