Print this page

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 1) Publicly Available CP and CPS: CP: https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20natural/080-PCN-F015-INGLES.pdf CPS: https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/DPC/080-DPC-F014-INGLES.pdf 2) CA Hierarchy: in CPS section 8.9 3) Audit Criteria: in CPS section 17 4) Document Handling of IDNs in CP/CPS: ???? 5) Revocation of Compromised Certificates: in CPS section 12.4 6) Verifying Domain Name Ownership: ???? 7) Verifying Email Address Control: ???? 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates. 9) DNS names go in SAN: ???? 10) Domain owned by a Natural Person: in CPS 12.1.1 11) OCSP: in CP section 16.1 12) Network Security Controls: in CPS section 15.7	**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 1) Long-lived DV certificates: ???? 2) Wildcard DV SSL certificates: ???? 3) Email Address Prefixes for DV Certs: ???? 4) Delegation of Domain / Email validation to third parties: ???? 5) Issuing end entity certificates directly from roots: ???? 6) Allowing external entities to operate subordinate CAs: ???? 7) Distributing generated private keys in PKCS#12 files: in CPS 15.4.2 8) Certificates referencing hostnames or private IP addresses: ???? 9) Issuing SSL Certificates for Internal Domains: ???? 10) OCSP Responses signed by a certificate under a different root: ???? 11) SHA-1 Certificates: ???? 12) Generic names for CAs: in CPS section 12.1.1 13) Lack of Communication With End Users: ???? 14) Backdating the notBefore date: ????	**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
Trust Bits	Email; Websites	Verified?	Verified
SSL Validation Type	DV	Verified?	Verified
EV Policy OID(s)	Not EV	Verified?	Not Applicable
Root Stores Included In	Microsoft	Verified?	Verified
Mozilla Applied Constraints	no	Verified?	Verified

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	no errors.	Verified?	Verified
CA/Browser Forum Lint Test	test website: https://crt.sh/ all errors must be fixed in CA/Browser Forum lint: ERROR: CA certificates must set keyUsage extension as critical in X.509 lint: ERROR: Invalid type in SAN entry ERROR: IP address in dns name	Verified?	Need Response From CA

Test Website Lint Test	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed. Test tool under maintenance.	**Verified?**	Not Verified
EV Tested	Not requesting EV treatment.	**Verified?**	Not Applicable

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	The PSC-FII does not has Sub-CA current.	**Verified?**	Verified
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	in CPS section 11 and 14	**Verified?**	Verified

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	**Verified?**	Verified

	/DPC_PC2015/PC/PC%20operador /Aprobar_080-PCO-F018.pdf		
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://bug667466.bmoattachments.org /attachment.cgi?id=8670835	Verified?	Not Verified
Standard Audit Type	ETSI TS 102 042	Verified?	Verified
Standard Audit Statement Date	6/12/2015	Verified?	Verified
BR Audit	As specified in the CPS (https://publicador-psc.fii.gob.ve /docs/DPC_PC2016/DPC/080-DPC-F014-INGLES.pdf), Section 17.2 Please provide BR statement file link for verification purpose.	Verified?	Need Response From CA
BR Audit Type	ETSI TS 102 042	Verified?	Need Response From CA
BR Audit Statement Date	6/12/2015	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. in CPS section 4, its hard to confirm that PSC-FII committed to comply with BR.	Verified?	Need Response From CA
SSL Verification Procedures	in CPS section 13.	Verified?	Verified
EV SSL Verification Procedures	Not requesting EV treatment	Verified?	Not Applicable
Organization Verification Procedures	in CPS section 12	Verified?	Verified
Email Address Verification Procedures	Validate all Data included in Certificates The domain/email validation is performed by the RA Operator or VA Operator. described in CPS section 13.1.2 and section 8.3	Verified?	Verified

Code Signing Subscriber Verification Pro	in CPS section 13 and 12.	Verified?	Verified
Multi-Factor Authentication	in CPS section 16.1, 14.4, 14.5.5 and 17	Verified?	Verified
Network Security	in CPS section 14 and 15	Verified?	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	The PSC-FII does not has Sub CA	Verified?	Verified