Bugzilla ID: Bug 667466

Bugzilla Summary:

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
   a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
   b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	PSC-FII
Website URL	https://ar.fii.gob.ve
Organizational type	Organización Gubernamental
Primark Market / Customer Base	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.
CA Contact Information	CA Email Alias: karog@fii.gov.ve CA Email Alias: cperez@fii.gob.ve CA Phone Number: (58-212) 9034690 Title / Department: CIES PSC-FII

Technical information about each root certificate

Certificate Name	PSC Público del MCT para el Estado Venezolano
Certificate Subject Field	C=VE O=Sistema Nacional de Certificacion Electronica OU=Fundacion Instituto de Ingenieria ST=Miranda L=Baruta CN=PSC Publico del MCT para el Estado Venezolano/emailAddress=admin-pki@fii.org

Certificate Issuer Field	CN=Autoridad de Certificacion Raiz del Estado Venezolano C=VE L=Caracas ST=Distrito Capital O=Sistema Nacional de Certificacion Electronica OU=Superintendencia de Servicios de Certificacion Electronica/emailAddress=acraiz@suscerte.gob.ve
Certificate Summary	We are a Sub-CA-supervised SUCERTE (Superintendence of Electronic Certification Services) belonging to the Government of the Bolivarian Republic of Venezuela, our nature is public and belongs to the Ministry for Power polular Telecommunications and Informatics.
Root Cert URL	https://ar.fii.gob.ve/pub/cacert/cacert.crt
SHA1 Fingerprint	95:2f:77:39:fa:b5:3b:63:5e:58:51:44:02:36:8c:6e:0e:8e:
Valid From	2009-07-11
Valid To	2018-07-09
Certificate Version	3
Certificate Signature Algorithm	sha1WithRSAEncryption
Signing key parameters	Modulus Length= 4096
Test Website URL (SSL) Example Certificate (non-SSL)	https://ar.fii.gob.ve
CRL URL	https://publicador-psc.fii.gob.ve/crl/cacrl.crl
OCSP URL	
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV
EV Policy OID(s)	Not EV

CA Hierarchy information for each root certificate

CA Hierarchy	PSC-FII is signed by the SUSCERT root. PSC-FII signs end-entity certificates directly. PSC-FII has not signed any intermediate certificates
Externally Operated SubCAs	None
Cross-Signing	None

Verification Policies and Practices

Policy Documentation	CPS (Spanish) https://ar.fii.gob.ve/pub/docs/DPC2009.pdf

	CPS(Inglish) https://ar.fii.gob.ve/pub/docs/DPC1.pdf PC Certified Secure Servers: https://ar.fii.gob.ve/pub/docs/Servidores_2009.pdf PC Certified Legal Person: https://ar.fii.gob.ve/pub/docs/Persona_Juridica_2009.pdf PC Certificates for Natural Persons: https://ar.fii.gob.ve/pub/docs/Persona_Natural_2009.pdf PC Certified Operators AR/AC: https://ar.fii.gob.ve/pub/docs/Operadores_2009.pdf PC Desantendida Signature Certificates: https://ar.fii.gob.ve/pub/docs/PCFirmaDesatendidaPSCIIFirmado.pdf Since this cert chains up to the SUSCERT root, PSC-FII must also comply with the following practices. http://acraiz.suscerte.gob.ve/dpc/DPC_AC_RAIZ_V1.0.pdf (Spanish) http://acraiz.suscerte.gob.ve/dpc/DPC_AC_RAIZ_V1.0_en.pdf (English) Document 054: Certification Practice Statement and Certificate Policies of Root CA of Venezuala. This document is only at the level of authenticating and approving the Certification Service Suppliers (CSS); eg the intermediate CAs that are signed by this root. http://www.suscerte.gob.ve/images/norma-22-2008.pdf (Spanish) Document 022: Model of Certification Practice Statement and Certificate Policies for Certification Service Provider (PSC) http://www.suscerte.gob.ve/images/norma-027.pdf (Spanish) Document 027: Guide for Accreditation of Certification Service Provider (PSC) http://www.suscerte.gob.ve/images/SUSCERTENorma040_E21.pdf (Spanish) Document 040: Guide Technology Standards and Guidelines for Accreditation of Certification Service Provider http://www.suscerte.gob.ve/images/norma-032.pdf (Spanish) Document 032: National Infrastructure of Electronic Certificate: Structure, Certificate, and CRL.
Audits	Audit Type: ETSI 101 456 Auditor: Milthon J. Chavez (CISA) SUSCERTE accredited auditor: http://www.suscerte.gob.ve/index.php/es/certificacion/registro-de-auditores SUSCERTE lists FII as an accredited Electronic Certification Services provider: http://www.suscerte.gob.ve/index.php/es/certificacion/proveedores-acreditados

Organization Identity Verification	CPS (Spanish) https://ar.fii.gob.ve/pub/docs/DPC2009.pdf CPS (Inglish) In Section 4.2 Initial Identity Validation is the Test Methods for possession of the private key, Authentication of Organization Identity, Authentication of individual identity and authentication of subscriber identity.. Applications for Certificates is described in Section 5.1.1.2.1 Care Applications in Electronic Certificates. Sections 4.2 each of the documents Certification Policy describes the methods used to verify the identity of the subscriber.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV and are only valid for one year.
Wildcard DV SSL certificates	SSL certs are OV.
Email Address Prefixes for DV Certs	SSL certs are OV.
Delegation of Domain / Email validation to third parties	Not applicable.
Issuing end entity certificates directly from roots	"PSC-FII" is the anchor of trust that will include the NSS and is signed by the root SUSCERTE.
Allowing external entities to operate subordinate CAs	Not applicable
Distributing generated private keys in PKCS#12 files	Not applicable
Certificates referencing hostnames or private IP addresses	PSC-FII: hostnames or private IP addresses are include in subject alternative name (certificates field)
Issuing SSL Certificates for Internal Domains	Not applicable
OCSP Responses signed by a certificate under a different root	OCSP PSC_FII fits with RFC 2650.
CRL with critical CIDP Extension	Not applicable
Generic names for CAs	Not applicable