Bugzilla ID: 667466
Bugzilla Summary: Add PSC-FII AC Certificate as trust anchor

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	Government Organization
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, cperez@fii.gob.ve CA Phone Number: (58-212) 9034690 Title / Department: CIES PSC-FII

Technical information about each trust anchor certificate to be included in NSS

Certificate Name	PSC Público del MCT para el Estado Venezolano
Certificate Summary	This is a sub-CA of the "Autoridad de Certificacion Raiz del Estado Venezolano" root certificate owned by SUSCERTE (Superintendencia de Servicios de Certificación Electrónica), which is part of the Ministry of People's Power for Telecommunications and Informatics in the Bolivarian Republic of Venezuela. SUSCERTE is a national government CA that provides electronic certification services to the Bolivarian Republic of the Government of Venezuela. In Bug #489240 it was determined that SUSCERTE's sub-CAs would apply for inclusion themselves as separate trust anchors. This "PSC Público del MCT para el Estado Venezolano" cert shows up under "Sistema Nacional de Certificacion Electronica", which is the O of the Issuer, the "Autoridad de Certificacion Raiz del Estado Venezolano" root certificate.

Certificate Issuer Field	E = acraiz@suscerte.gob.ve
	OU = Superintendencia de Servicios de Certificacion Electronica
	O = Sistema Nacional de Certificacion Electronica
	ST = Distrito Capital
	L = Caracas
	C = VE
	CN = Autoridad de Certificacion Raiz del Estado Venezolano

Certificate Subject Field	E = admin-pki@fii.org
	CN = PSC Publico del MCT para el Estado Venezolano
	L = Baruta
	ST = Miranda

	OU = Fundacion Instituto de Ingenieria
	O = Sistema Nacional de Certificacion Electronica
	C = VE

Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=542275
SHA1 Fingerprint	B2:60:C7:09:D5:B7:D0:BD:97:42:DE:DA:AF:EF:87:6B:33:6C:A7:39
Valid From	2008-07-11
Valid To	2018-07-09
Certificate Version	3
Certificate Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption
Signing key parameters	4096
Test Website URL	https://ar.fii.gob.ve The SSL cert for this website does not chain up to the Cert listed in this inclusion request. Need a website whose SSL cert chains up to the cert to be included.
CRL URL	https://publicador-psc.fii.gob.ve/crl/cacrl.crl NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS. Test: Results of importing into Firefox browser
OCSP URL	Please see https://wiki.mozilla.org/CA:Recommended_Practices#OCSP
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 (English): https://ar.fii.gob.ve/pub/docs/DPC1.pdf Note: In this document the name of the organization "PSC-FII" gets translated to "CSP-FEI" 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-deauditores SUSCERTE lists FII as an accredited Electronic Certification Services provider: http://www.suscerte.gob.ve/index.php/es/certificacion/proveedores-acreditados
SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Organization Verification Procedures	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. CPS section 4.2.3: The RA is responsible for obtaining confirmation of the membership of the organization and will be responsible for obtaining confirmation of the identity of the signatory who applies for a certificate. The identity verification is carried out either at the time of application for the certificate or prior to that request authentication using the documentation included in the directories and files of the RA. In case of certificates of legal person - public body must be verified in the Official Gazette of the Bolivarian Republic of Venezuela, the creation of the entity or agency, functions of the applicant and the appointment of office. In case of certificates of legal person - a private institution, it must be verified in the document establishing the company's creation of the entity, the functions of the applicant and the appointment of office.

Email Address Verification Procedures	If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes
CA Hierarchy	See above.
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	?
Revocation of Compromised Certificates	?
Verifying Domain Name Ownership	?
Verifying Email Address Control	?
Verifying Identity of Code Signing Certificate Subscriber	?
DNS names go in SAN	?
Domain owned by a Natural Person	?
OCSP	?

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	**This cert currently signs end-entity certs directly. If it is to be included as a trust anchor in NSS, then it will need to have issuing intermediate certificates.**
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	**?**
CRL with critical CIDP Extension	Not applicable

Generic names for CAs	Not applicable