Bugzilla ID: 489240
Bugzilla Summary: Add Autoridad de Certificacion Raiz del Estado Venezolano root certificate

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.

General Information	Data
CA Name	SUSCERTE Superintendencia de Servicios de Certificación Electrónica República Bolivariana de Venezuela Ministerio del Poder Popular para las Telecomunicaciones y la Informática
Website URL (English version)	http://www.suscerte.gob.ve/ (Spanish only)
Organizational type	National Government CA
Primary market / customer base	SUSCERTE stands for 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.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	Autoridad de Certificacion Raiz del Estado Venezolano
Cert summary / comments	This root CA is the Root Certification Authority of Venezuela's National Infrastructure of Electronic Certification. The main function of this root is to issue the intermediate CAs to the Certification Service Suppliers (CSS) of the public and private sector, according to the Law on Data Messages and Electronic Signature (LSMDFE). Once a CSS has been accredited by SUSCERTE according to the LSMDFE, the CSS must issue the certificates in accordance with the purpose of the electronic certificates specified in their own Declaration of Practices of Certification (DPC) and Policy of Certificates (PC). SUSCERTE is responsible for elaborating and approving each DPC, as well as its modifications, following the model that SUSCERTE itself provides for the elaboration. Furthermore, SUSCERTE evaluates the DPC of each CSS of the National Infrastructure of Electronic Certification of Venezuela. Consequently, the DPC must have the specifications of the requirements used by the Root CA, for the generation, publication and administration of certificates of electronic signature to the Subordinated CSS, based on RFC 3647.

	All the public and private entities of the Venezuelan State complying with the requisites requested by SUSCERTE can request the accreditation to the confidence chain.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=375214
SHA-1 fingerprint	DD:83:C5:19:D4:34:81:FA:D4:C2:2C:03:D7:02:FE:9F:3B:22:F5:17
Valid from	2007.02.16
Valid to	2027.02.11
Cert Version	3
Modulus length	4096
CRL URL	http://www.suscerte.gob.ve/lcr http://www.suscerte.gob.ve/lcr/CERTIFICADO-RAIZ-SHA1CRLDER.crl This CRL downloads without error into Firefox. NextUpdate for this CRL is 6 months. A CRL for the FII subCA was attached to the bug: https://bugzilla.mozilla.org/attachment.cgi?id=375842 NextUpdate for this CRL is one month. I need to import into Firefox a CRL for end-entity certs chaining up to this root. For these websites https://acraiz.suscerte.gob.ve/certificados/ https://ar.fii.gob.ve https://www.vencert.gob.ve the website cert URL distribution point is https://publicador-psc.fii.gob.ve/crl/cacrl.crl publicador-psc.fii.gob.ve uses an invalid security certificate. The certificate is only valid for the following names: 150.186.246.51 , acraiz.suscerte.gob.ve (Error code: ssl_error_bad_cert_domain)
OCSP Responder URL	http://ocsp.suscerte.gob.ve When I force Firefox to use OCSP and to error-out if the OCSP connection fails, the following two sites fail with error Invalid OCSP signing certificate in OCSP response. https://ar.fii.gob.ve https://www.vencert.gob.ve However, the certificados site works: https://acraiz.suscerte.gob.ve/certificados/

List or description of subordinate CAs operated by the CA organization associated with the root CA.	Certificate hierarchy information is provided in the attachment: https://bug489240.bugzilla.mozilla.org/attachment.cgi?id=373743 The root and its subordinate CAs can be downloaded from https://acraiz.suscerte.gob.ve/certificados/: CERTIFICADO-RAIZ-SHA1= Autoridad de Certificacion Raiz del Estado Venezolano; which is the SUSCERTE Root Certificate in sha1 format. This is the root that is requested for inclusion. • PROVEEDOR-FII-SHA1-11-07-2008 = PSC Publico del MCT para el Estado Venzolano. This is the subordinate CA for the company FII • PROVEEDOR-PROCERT-SHA1-14-07-2008 - this is a other certificate CA subordinate (company PROCERT) issued by the SUSCERTE root CA in sha1 format Not related to this request, but listed on the website: CERTIFICADO-RAIZ-SHA256 - this is the SUSCERTE Root Certificate in sha256 format PROVEEDOR-FII-SHA256-11-07-2008 – SUSCERTE subCA for company FII in sha256 format CERTIFICADO-ACPASS-SHA256 – Self-signed root, for managing the CA for Electronical Passport Venezuelan. CERTIFICADO-PASAPORTE-SHA256 – Subordinate CA of CERTIFICADO-ACPASS-SHA256.
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	The root signs intermediate CAs that are operated by third parties. The intermediate CAs can also sign subordinate CAs. For the externally-operated subordinate CAs, please provide the information listed in the SubordinateCA Checklist: https://wiki.mozilla.org/CA:SubordinateCA_checklist The two current subordinate CAs are FII and PROCERT: • PROVEEDOR-FII-SHA1-11-07-2008 = PSC Publico del MCT para el Estado Venzolano. This is the subordinate CA for the company FII • PROVEEDOR-PROCERT-SHA1-14-07-2008 - this is a other certificate CA subordinate (company PROCERT) issued by the SUSCERTE root CA in sha1 format 1) PSC FII CA Documentation CSP and CP URL https://ar.fii.gob.ve/pub/docs/ (Spanish) Public CA -- Provider Certificated of a Government Institution. The certificates can be issued to individuals and corporations of the sector private and public. Certificates can be issued to Natural Persons, Legal Representatives of Companies, and Servers. There are also certificates for the CA and RA Operators. An example of certificates usable for signing and encrypting email messages you can download in this site http://ar.fii.gob.ve, In the left bar menu you select “Gestión de Certificados-->Búsqueda de Certificados” after you write the following email (cmarino@suscerte.gob.ve or lblanco@suscerte.gob.ve) in the box "Correo Electrónico", press the

	button “Continuar”. In this moment you can download the certificate. 2) Procert CA Documentation CSP and CP URL http://www.procert.net/eng/declaration.asp (Spanish) Private CA -- Private Provider Certificated The certificates can issued to individuals and corporations of the sector private and public The Procert intermediate CA signs electronic signature certificates for Private Company Employees, Legal Representatives of a Public Companies, Legal Representatives of a Private Companies, and individuals. The Procert intermediate CA also signs electronic certificates for VPN, Secure Server, Mobile Device, Software Signature, E-Mail, and Logic Access Control.
List any other root CAs that have issued cross-signing certificates for this root CA	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing Document 032 = http://www.suscerte.gob.ve/images/Norma-032.pdf National Infrasturucture of Electronic Certificate: Structure, Certificate, and CRL
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV.	OV Certification Electronic Services Superintendence (SUSCERTE) verifies the domain name referenced in the certificate and this is regulated in the Document 032. Each Provider Certificated (Public and Private CA) through the registration authority, validates this information before issuing the certificate SUSCERTE in the Document 032 define the value of the Organization attribute for any type of certificate. This should include: O=Sistema Nacional de Certificacion Electronica Is mandatory that each Provider Certificated, through the registration authority, validates this information before issuing the certificate
EV policy OID(s)	Not EV
Translations into English of sections of CP/CPS documents pertaining to: • Verification of Identity and Organization	Please provide the document and section numbers, and translations into English of the parts of the CP/CPS documents pertaining to: • Verification of Identity and Organization for End-Entity Certs • Verification of ownership/control of domain name for End-Entity Certs • Verification of ownership/control of email address for End-Entity Certs

• Verification of ownership/control of domain name • Verification of ownership/control of email address • Section 7 of http://www.mozilla.org/projects/security/certs/policy/ • Potentially Problematic Practices, http://wiki.mozilla.org/CA:Problematic_Practices	• Section 7 of http://www.mozilla.org/projects/security/certs/policy/ • Potentially Problematic Practices, http://wiki.mozilla.org/CA:Problematic_Practices
Website(s) whose SSL cert chains up to this root.	https://acraiz.suscerte.gob.ve/certificados/ https://ar.fii.gob.ve https://www.vencert.gob.ve
CP/CPS	All documents are in Spanish, except for the CPS of the root which is at the level of approving intermediate CAs. 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.

AUDIT	In the following URL is found a list with the information of the accredited auditors: http://www.suscerte.gob.ve/index.php?option=com_content&view=article&id=132&Itemid=49 The last audit was made for Mariclen Villegas (email:mariclen_villegas@cantv.net). The audit report is send you when will request by Mozilla. Please see sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/ We need a publishable statement or letter from an auditor (who meets the policy requirements) that states that they have reviewed the practices as outlined in the CP/CPS for this root, and that the CA does indeed follow these practices and meets the requirements of one of: • ETSI TS 101 456 • ETSI TS 102 042 • WebTrust Principles and Criteria for Certification Authorities

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
- Verify identity info in code signing certs is that of subscriber
- Make sure it's clear which checks are done for which context (cert usage)
- All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
- Wildcard DV SSL certificates
- Delegation of Domain / Email validation to third parties
- Issuing end entity certificates directly from roots
- Allowing external entities to operate unconstrained subordinate CAs
- Distributing generated private keys in PKCS#12 files
- Certificates referencing hostnames or private IP addresses

- OCSP Responses signed by a certificate under a different root
- CRL with critical CIDP Extension
- Generic names for CAs

Verify Audits
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)
- Validate contact info in report, call to verify that they did indeed issue this report.
- For EV CA's, verify current WebTrust EV Audit done.
- Review Audit to flag any issues noted in the report