Bugzilla ID: 925740
Bugzilla Summary: Add "Autoridad Certificadora Raíz Nacional de Uruguay" Root Certificate to NSS

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	Autoridad Certificadora Raíz Nacional de Uruguay
Website URL	http://www.agesic.gub.uy/acrn
Organizational type & Primark Market / Customer Base	The ACRN (Spanish acronym of National Root Certification Authority of Uruguay - Autoridad Certificadora Raiz Nacional de Uruguay) is the root of the chain of trust of the Uruguayan National PKI (PKI Uruguay). According to the provisions of Law 18,600 "Electronic Document and Electronic Signature", the operation of the ACRN is performed by AGESIC which is a national government agency which aims to ensure improved services to citizens, using the possibilities offered by information and communications technology. Through the ACRN, AGESIC enables technologically the operation of the Accredited Certification Service Providers (PSCA for its acronym in Spanish) issuing electronic certificates for their Certifying Authorities (ACPA - Spanish acronym for Certification Authority of the Accredited Provider). Thus, the ACPA become part of the trust chain of PKI Uruguay. The ACRN and all their subordinate CA (ACPA) will be under the control and regulations of the UCE. The UCE (Spanish acronym of Electronic Certification Unit) was created by Article 12 of Law No. 18,600 "Electronic Document and Electronic Signature" as a decentralized body of AGESIC in order to regulate and control the ACRN and subordinate CA.
Impact to Mozilla Users	A "Recognized Electronic Certificate of Natural Person" (CERPF for its acronym in Spanish), in the context of the National Infrastructure of Electronic Certification (INCE - Uruguay PKI) is an electronic certificate issued by a PSCA to a previously identified individual. This certificate allows the individual to perform advanced electronic signatures and authenticate their identity with the legal validity granted by Law No. 18,600. Mozilla users will benefit, as the advanced electronic signature will be used as a legal signature in the message exchange. The PSCA may issue certificates for SSL or code to third parties so that end users will benefit also.
Inclusion in other major browsers	Recently accepted into Microsoft's root program. Have also applied for inclusion in Apple's root program.
CA Contact Information	Name: AGESIC E-mail address: acrn@agesic.gub.uy Telephone number: (+598) 2901 2929

Technical information about each root certificate

Certificate Name	Autoridad Certificadora Raíz Nacional de Uruguay
Certificate Issuer Field	C = UY O = AGESIC CN = Autoridad Certificadora Raíz Nacional de Uruguay

Certificate Summary	This root signs externally-operated intermediate issuing certificates.
Root Cert URL	http://uce.gub.uy/acrn/acrn.cer https://bugzilla.mozilla.org/attachment.cgi?id=815844
SHA1 Fingerprint	7A:1C:DD:E3:D2:19:7E:71:37:43:3D:3F:99:C0:B3:69:F7:06:C7:49
Valid From	2011-11-03
Valid To	2031-10-29
Certificate Version	3
Cert Signature Algorithm	SHA-256
Signing key parameters	4096
Test Website URL (SSL) Example Cert (S/MIME)	If requesting the Websites trust bit, please provide a URL to a website (may be a test website) whose SSL cert chains up to this root. If not requesting the Websites trust bit, please provide an example cert and chain.
CRL URL	http://www.agesic.gub.uy/acrn/acrn.crl
OCSP URL (Required if the Websites trust bit is to be enabled)	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses Baseline Requirement #13.2.2: "The CA SHALL update information provided via an Online Certificate Status Protocol..." BR Appendix B regarding authorityInformationAccess in Subordinate CA Certificate and Subscriber Certificate: "With the exception of stapling .... this extension MUST be present ... and it MUST contain the HTTP URL of the Issuing CA's OCSP responder"
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV and OV
EV Policy OID(s)	Not applicable. Not requesting EV treatment.
Non-sequential serial numbers and entropy in cert	Please see Baseline Requirement #9.6 in https://www.cabforum.org/Baseline_Requirements_V1_1_5.pdf

CA Hierarchy information for each root certificate

CA Hierarchy	This root signs externally-operated intermediate issuing certificates. Currently they are three PSCA: "Interior Ministry (Ministerio del Interior)", "Uruguayan mail (Correo Uruguayo)" and "Abitab".
Externally Operated SubCAs	Please provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	No
Technical Constraints on Third-party Issuers	CA = TRUE Length 0

Verification Policies and Practices

Policy Documentation	All documents are in Spanish. Document repository: http://www.agesic.gub.uy/acrn/ CP: www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf CPS: http://uce.gub.uy/acrn/cps_acrn.pdf
Audits	Audit Type: WebTrust Auditor: Deloitte Auditor Website: http://www.deloitte.com/view/es_UY/uy/index.htm Audit Report: -- need current audit report
Baseline Requirements (SSL)	Please provide the CP/CPS section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3. Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results.
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	The verification procedures are described in CP section 3 “Identification and Authorization”. The process performed to establish the PSC is made by the UCE.
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
Multi-factor Authentication	Baseline Requirement (https://www.cabforum.org/Baseline_Requirements_V1_1_5.pdf) #16.5: “The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.” Please provide the CP/CPS section number(s) where it is specified that multi-factor authentication is required for all accounts capable of directly causing certificate issuance.
Network Security	CP section 6.8

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

Publicly Available CP and CPS	Yes, see above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	???
Revocation of Compromised Certificates	Yes
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate	See above

Subscriber	
DNS names go in SAN	See Baseline Requirement #9.2.1
Domain owned by a Natural Person	Yes
OCSP	See above

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

Long-lived DV certificates	??? See Baseline requirement #11.3
Wildcard DV SSL certificates	??? See Baseline requirement #11.1.3.
Email Address Prefixes for DV Certs	??? See Baseline requirement #11.1.1.
Delegation of Domain / Email validation to third parties	See response to subCA checklist.
Issuing end entity certificates directly from roots	No CP section 1.4 and 7.1
Allowing external entities to operate subordinate CAs	See response to subCA checklist. Once credited the PSCA, this is controlled and regulated by the UCE. PSCA must meet the CP of the root CA (ACRN).
Distributing generated private keys in PKCS#12 files	??? regarding end-entity certs
Certificates referencing hostnames or private IP addresses	??? See Baseline requirement #11.1.4. Also See https://wiki.mozilla.org/CA:Communications#July_30.2C_2013
Issuing SSL Certificates for Internal Domains	
OCSP Responses signed by a certificate under a different root	???
CRL with critical CIDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	No. CP section 2.1.1.1. h Have a service that allows answering queries from subscribers of certificates issued by the PSCA and Third acceptors of such certificates.