Bugzilla ID: 811352
Bugzilla Summary: Additional Root CA for ACCV

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	ACCV
Website URL	http://www.accv.es
Organizational type	ACCV is a CA operated by a government agency of Spain. Initially had a regional character but now operates nationally.
Primark Market / Customer Base	The ACCV CA focuses its activities mainly in Spain but is collaborating in international recognition of certificates. ACCV issues certificates for all citizens for their personal use and for its relations with the public administration and business.
Impact to Mozilla Users	The ACCV CA is operated by the government of the Valencia region of Spain. ACCV issues certificates for persons (with email), web sites and for signing code, in different policies, but with the same root. ACCV is a public certificate service provider and the intended use for this root certificate is to improve the electronic administration between citizens and the administration. ACCV continues to issue certificates to citizens and the administration as the primary mechanism to ensure communication between the two. The set of users who will find our certificates is formed mainly by citizens having to contact or exchange information with the public administration (state and regional). This exchange can be for web, mail or by any other mechanism or service available to citizens. ACCV certificates are also being used by private companies to secure their business.
CA Contact Information	CA Email Alias: accv@accv.es CA Phone Number: 0034961923161, 606943079 Title / Department: Systems and development department

Technical information about each root certificate

Certificate Name	ACCVRAIZ1
Certificate Issuer Field	C = ES O = ACCV OU = PKIACCV CN = ACCVRAIZ1
Certificate Summary	What is the relation of this root to the "Root CA Generalitat Valenciana" root that was included via bug #274100? E.g. will this root eventually replace the other root?
Root Cert URL	http://www.accv.es/fileadmin/Archivos/certificados/ACCVRAIZ1.crt
SHA1 Fingerprint	93:05:7A:88:15:C6:4F:CE:88:2F:FA:91:16:52:28:78:BC:53:64:17
Valid From	2011-05-05
Valid To	2030-12-31
Certificate Version	3

Cert Signature Algorithm	SHA-1
Signing key parameters	4096
Test Website URL (SSL)	https://ulik2.accv.es/
CRL URL	http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl http://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl (NextUpdate: 3 days) http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl (NextUpdate: 3 days) CPS section 4.9.9: ACCV shall publish a new CRL in its repository at maximum intervals of 3 hours, even if there have been no modifications to the CRL (changes to the status of certificates) during the aforementioned period.
OCSP URL	http://ocsp.accv.es
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV
EV Policy OID(s)	Not Applicable. Not requesting EV treatment.

CA Hierarchy information for each root certificate

CA Hierarchy	This root cert has signed two internally-operated subordinate CA certificates, ACCVCA-110 and ACCVCA-120.
Externally Operated SubCAs	None
Cross-Signing	None
Technical Constraints on Third-party Issuers	Not applicable. All CAs are operated by the ACCV.

Verification Policies and Practices

Policy Documentation	Documents are in Spanish. CPS has been translated into English. Document Repository: http://www.accv.es/quienes-somos/practicas-y-politicas-de-certificacion/ CPS (EN): http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-V3.0-EN.pdf All CP Documents listed by certificate usage: http://www.accv.es/quienes-somos/practicas-y-politicas-de-certificacion/politicas-de-certificacion/ SSL CP: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-03V3.0-c.pdf Code Signing CP: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/nuevo_23_07_08/PKIGVA-CP-04V2.0-c.pdf (what's the new version of this?) Qualified Certs CP for Public Employees: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-13V4.0-c.pdf Qualified Certs CP for Citizens: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-07V5.0-c.pdf
Audits	Audit Type: WebTrust CA Auditor: DNB

	Auditor Website: http://www.dnbcons.com/ URL to Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1352 (2012.07.20) ISO27001 http://www.accv.es/fileadmin/Archivos/iso27001/Cert-ISO27001-ACCV.pdf Please update your WebTrust seal at http://www.accv.es/webtrust
Baseline Requirements (SSL)	What is your status in regards to complying with the CAB Forum Baseline Requirements? (https://www.cabforum.org/Baseline_Requirements_V1.pdf) As per the CAB Forum Baseline Requirement # 8.3, where is the "Commitment to Comply" statement that should be in your CP or CPS?
Organization Verification Procedures	Please translate the sections of the SSL CP that describe the steps taken to authenticate the organization, certificate subscriber, and the authority of the subscriber to act on behalf of the organization.
Code Signing Subscriber Verification Procedures	Please translate the sections of the Code Signing CP that describe the steps taken to authenticate the organization, certificate subscriber, and the authority of the subscriber to act on behalf of the organization.
SSL Verification Procedures	SSL CP section 3.2.4 Checking the application domain The ACCV verify that domains and addresses associated with the certificate belong to the applicant by consulting the records assigned by ICANN / IANA. This check will be made with using records WHOIS queries enabled by the organization Red.es http://www.nic.es or equivalent in national domains or those provided by Verisign for generic domains (whois.verisigngrs. com) . Besides WHOIS query connection will be tested by secure protocol (eg HTTPS) with the domain in question if possible and test DNS response. For any irregularity ACCV contact the applicant for the license and the issuance of the certificate will be suspended until its cure. If this is not remedied within the period of one month the application would be denied. In the verification process, the information obtained from the WHOIS or equivalent records was compared with that provided by the applicant, sending personalized emails to technical and administrative contacts obtained from both sources and if necessary to ensure that the data is correct and that domain ownership is confirmed is make phone calls asking for clarification.
Email Address Verification Procedures	The following was copied from my notes from bug #274100. Please update as needed. ** Email: Civil servants certificates are issued from the official lists supplied by the public administration concerned. These official lists are drawn from selective processes with maximum guarantees (determine who is a civil servant) and involve a process in person at the registration point of administration. Public administration provides its employees with email accounts for his work as a civil servant. These email accounts are corporate and internally generated. The ACCV accepts these mail accounts because they are imposed by the administration and not by the user. ** Snippets of Translations from Qualified Certs CP for Public Employees… *** Section 3.2.2: The license application defined in this policy is limited Certification to public authorities or administrations with which agreement has been established certification contract or some other formula that implements the service by the ACCV. *** Section 3.2.3: The determination of the public employee status is the responsibility of the Administration or Public entity applicant, which shall check the condition of public employee, either in its database, if it is updated, or by

	requesting the document by which the subscriber has purchased This condition, if not any indication as to the Administration or Public Entity applicant. … The Autoritat of Certification of the Valencia only guarantee that the email address stated on the certificate was provided by the Administration or public entity that owns the subscriber in the upon finalization of your application and / or shown as linked to subscriber bases personal data of the Government or the Civil Service to which belongs applicant. ** Snippets of Translations from Qualified Certs CP for Citizens: *** Section 3.2.2 : The application for certificates associated to this Certificate Policy is limited to public entities or administrations which have established a certification agreement, contract or some other formula that supports the ACCV service provision. The public entity or administration identification process will be held in the organization enrollment to be signed by an authorized representative of the entity or administration. *** Section 3.2.3: The certificate applicant identity authentication will be made in person while applying or during the certificate delivery. Thus, Registration is delegated to the certificate issuing entity which signed an agreement, contract or some other formula that supports the ACCV service provision. Presence of the civil servant to whom a certificate is issued will not be required when his/her identity and civil servant status are already recorded in the Personnel Registry of the Public or Corporate Entity or Public Administration which the civil servant belongs to and where his/her application is directed to. The applicant public entity or administration has the entire responsibility of determining the civil servant status. The public entity or administration will check the public servant status in its database if it is updated or by requesting a document where the subscriber's status is stated in case that the applicant public entity or administration has not this record. These certificates include the subscriber's email address as a necessary element to support digital signature and email encryption operations. However, the Autoritat de Certificació de la Comunitat Valenciana does not guarantee that this electronic address is linked to the certificate subscriber, thus the confidence that this email is linked to the certificate subscriber relates to the relying party only. The Autoritat de Certificació de la Comunitat Valenciana just guarantees that the email stated in the certificate was provided by the Administration or Public Entity which the subscriber belonged to at the time that the application was made and/or that this email is linked to the subscriber in the Valencia Government or other Public Administration personnel data base that the applicant belongs to. *** Section 4.1: This certificate request is responsibility of the Public Entity or Administration which shall verify the certificate owner's civil servant status by checking their organization personnel registry.
Multi-factor Authentication	All accounts capable of directly causing certificate issuance require user certificates on smart card. Besides access to the certificate issuance system can only be made from selected systems, with specific IP addresses.
Network Security	Please provide the section numbers of the CPS or CP that cover network and system security.

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

Publicly Available CP and CPS	Yes. See above.
CA Hierarchy	Yes. See above.
Audit Criteria	Yes. See above.
Document Handling of IDNs in CP/CPS	?
Revocation of Compromised Certificates	?

Verifying Domain Name Ownership	Yes. See above.
Verifying Email Address Control	Yes. See above.
Verifying Identity of Code Signing Certificate Subscriber	Yes. See above.
DNS names go in SAN	?
Domain owned by a Natural Person	?
OCSP	Yes. Tested in Firefox browser.

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

Long-lived DV certificates	?
Wildcard DV SSL certificates	?
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	**Yes**. The following was copied from my notes from bug #274100. Please update a needed. *** CPS section 1.3.2: Bodies of the Autonomous Government of Valencia as well as other entities can be Registration Authorities provided that the corresponding collaboration agreement has been entered into. These Registration Authorities are referred to as User Registration Points or PRUs in the documentation relating to the Certification Authority of the Community of Valencia, and they are entrusted with confirmation of the requester's identity and delivery of the certificate. *** Obligations of the Registration Authority are defined in CPS section 9.6.2. *** CPS section 5.2.1.7: Auditor… must verify all aspects mentioned in the security policy, copies policies, certification practices, Certification Policies, etc. in the group of ACCV systems and within the ACCV personnel, as well as in the PRUs. * CPS section 9.6.2: The persons that operate in the RAs integrated into the hierarchy of the ACCV – User Registration Point Operators – are obliged to: * Carry out their operations in accordance with this CPS. * Carry out their operations in accordance with the Certification Policy that is applicable for the type of certificate requested on each occasion. * Exhaustively verify the identity of the persons granted the digital certificate processed by the Operators, for which purpose they will require the physical presence of the requester and the presentation of their current National ID Card (not a photocopy), or a Spanish passport. Non-Spanish users must present a Residence Card/Foreigner's ID Card.
Issuing end entity certificates directly from roots	No.
Allowing external entities to operate subordinate CAs	No.
Distributing generated private keys in PKCS#12 files	?
Certificates referencing hostnames or private IP addresses	?

Issuing SSL Certificates for Internal Domains	?
OCSP Responses signed by a certificate under a different root	OCSP responds without error in Firefox browser.
CRL with critical CIDP Extension	CRLs imported without error into Firefox browser.
Generic names for CAs	ACCV included in CN and O of cert
Lack of Communication With End Users	No