Bugzilla ID: 274100
Bugzilla Summary: Add ACCV CA certificate (Spain)

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.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	ACCV (Autoritat de Certificacio de la Comunidat Valenciana)
Website URL	http://www.pki.gva.es/
Organizational type	Regional Government CA of Spain A discussion in mozilla.dev.security.policy called "Accepting root CA certificates for regional government CAs", indicates that we can proceed with processing the Spain regional government CAs.
Primary market / customer base	ACCV (Autoritat de Certificacio de la Comunitat Valenciana) is a CA operated by the government of the Valencia region of Spain. The Valencia region has five million inhabitants and five hundred twenty-four cities.
Impact to Mozilla Users	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.
CA Contact Information	CA Email Alias: accv@accv.es CA Phone Number: 34·961 923150 Title / Department: Autoritat de Certificació de la Comunitat Valenciana

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

Info Needed	Data
Certificate Name	Root CA Generalitat Valenciana
Cert summary / comments	This root has four internally-operated subordinate CAs which sign end-entity certificates for individuals and organizations.
The root CA certificate URL	http://www.pki.gva.es/gestcert/rootca.crt
SHA-1 fingerprint.	A0:73:E5:C5:BD:43:61:0D:86:4C:21:13:0A:85:58:57:CC:9C:EA:46
Valid from	2001-07-06
Valid to	2021-07-01
Cert Version	3
Modulus length	2048
Test Website	https://www.accv.es/ (SSL cert is signed by ACCV-CA2, which is signed by this root)

CRL URL	http://www.pki.gva.es/gestcert/rootgva_der.crl http://www.accv.es/gestcert/accv_ca2.crl (NextUpdate is 2 days) ACCV CPS section 4.9.9. Frequency of issue of CRLs: 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 Responder URL	http://ocsp.pki.gva.es/
CA Hierarchy	This root has the following internally-operated sub-CAs: • CAGVA - Issues end entity certificates; personal certificates, code signing certificates and SSL certificates. ACCV checks the data from end entities exhaustively (vital statistics and data domain). This CA no longer issues certificates (CRL signing only). • ACCV-CA1 - Issues end entity certificates. Mainly company certificates. • ACCV-CA2 - Replaces CAGVA. Issues end entity certificates; personal certificates, code signing certificates and SSL certificates. ACCV checks the data from end entities exhaustively (vital statistics and data domain). • ACCV-CA3 - Issues Windows logon certificates and DC certificates for internal domains.
Externally Operated sub-CAs	ACCV does not have externally operated sub-CAs, and does not plan to have them in the future.
Cross-Signing	ACCV does not have cross-signing certificates with other CA.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code (Code Signing)
SSL Validation Type DV, OV, and/or EV	OV Comment #22: ACCV verify the identity/organization of the subscriber in all certificates issued. The only way to request a SSL certificate or a code signing certificate is to have a personal certificate from the ACCV.
EV policy OID(s)	Not EV
CP/CPS	English translation of the ACCV CPS: https://bugzilla.mozilla.org/attachment.cgi?id=426960 All of the following documents are in Spanish. All CPS and CP documents are available here: http://www.accv.es/quienes-somos/practicas-y-politicas-de-certificacion/ ACCV Certification Practice Statement (CPS): http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-V1.7-c.pdf All Certification Policy (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/PKIGVA-CP-03V2.0-c2010.pdf Code Signing CP: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/nuevo_23_07_08/PKIGVA-CP-04V2.0-c.pdf Qualified Certs CP for Public Employees:

	http://www.accv.es/fileadmin/Archivos/Politicas_de_certificacion/ACCV-CP-13V2.0-c.pdf Qualified Certs CP for Citizens: http://www.accv.es/fileadmin/Archivos/politicas_certificacion/ACCV-CP-07V4.0-c.pdf
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young, www.ey.com/es Audit: https://cert.webtrust.org/SealFile?seal=943&file=pdf (2009.06.30) Translation of audit: https://bugzilla.mozilla.org/attachment.cgi?id=440459
Organization Identity Verification	ACCV CPS section 3.2.2. Authentication of the identity of an organisation. In the event that a Certification Policy deems it necessary for an organisation's identity to be authenticated, this policy shall determine the necessary methods for verifying the aforementioned identity.This CPS explicitly prohibits the use of remote methods of identification of organizations. ACCV CPS section 3.2.3. Authentication of the identity of an individual. The process of individual identification is defined by the Certification Policy applicable for each type of certificate. The process shall not be regarded as having to be less strict than other systems of authentication used by the Autonomous Government of Valencia. As a general rule, remote methods of identification shall not be used that are different from the digital signature produced with certificates issued by the ACCV itself or by any other recognised Certification Services Provider. ACCV CPS section 9.6.2. Obligations of the Registration Authority 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. SSL CP section 3.1.8, Authentication of the identity of an organization The right to request certificates defined in this Certification Policy is limited to natural persons. We will not accept applications for certification made on behalf of people legal persons, entities or organizations. Therefore not considered necessary to identify any organization. For applicants belonging to the scope of the Generalitat Valenciana your order will be validated with information from the official directory. In case of not belonging to the Generalitat Valenciana, the applicant must attach the publication of the official appointment or document the job occupation or certificate issued by human resources department in his organization,

	which clearly indicates his position and responsibility. SSL CP section 3.1.9, Authentication of the identity of an individual The authentication of the identity of applicants for a certificate will be made through the use of their personal digital certificate to sign the certificate request. Comment #22: You must have a qualified personal certificate before applying for an SSL certificate or similar.
Domain Name Ownership / Control	SSL CP: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/PKIGVA-CP-03V2.0-c2010.pdf SSL CP section 3.1.10. Checking the Request Domain The ACCV will check that domains and addresses associated to the certificate actually belong to the applicant by looking up the records assigned by ICANN/IANA. This checking will be made by using WHOIS queries in the records authorized by the Red.es agency at http://www.nic.es or its equivalent for national domains or those provided by VeriSign for the generic domains (whois.verisign-grs.com). Besides WHOIS query, DNS response and connection tests using secure protocol (e.g. HTTPS) with the domain under consideration will be made when possible. In the light of any irregularity, the ACCV will contact the certificate applicant and leave the certificate issuance pending until correction. If this correction is not fixed within a month the request will be denied. SSL CP section 4.1. Certificate Request The applicant of a certificate issued under this Certification Policy must fulfill an online certificate request using the non-personal certificate management application (NPSC) available at https://npsc.accv.es:8450/npsc where the PKCS#10 file that was previously generated by the applicant will be embed. Once the application form is fulfilled, it will be sent by signing the request with one of the qualified certificates admitted by the Autoritat de Certificació de la Comunitat Valenciana. The Registration Authority has the responsibility to determine the suitability of the certificate type to the applicant characteristics depending on the provisions of the applicable Certification Policy and thus manage or deny the applicant certification request. Should the Registration Authority Operator refuse the request, an email informing of reasons for rejection will be sent to the address stated in the application. SSL CP section 4.2. Issuing Certificates The certificate issuing procedure will start once the Registration Authority associated to this Certification Policy has checked all necessary requirements for validating the certification request. This Certification Policy will be the mechanism for determining the nature and how to perform this checking. Upon issuance of the certificate, the Registration Authority shall notify the subscriber by sending a signed e-mail to the address included in the request. The user must sign in to the non-personal certificate management application (NPSC)

	available at https://npsc.accv.es:8450/npsc to pick up the certificate by previously signing the Certificate Agreement in this application with a personal qualified certificate. The Certificate Agreement is a document that must be digitally signed by the applicant in order to bind him/her to the request action, the knowledge of certificate use rules and the accuracy of provided data. Comment #22: By the time a request arrives, ACCV verifies the identity of the applicant and the information provided (the company in which the user works and the domain requested by the user). All requests are digitally signed with qualified personal certificates. These qualified certificates require that the user is physically present in a registration point and proves his identity.
Email Address Ownership / Control	Comment #22: 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. Qualified Certs CP for Public Employees: http://www.accv.es/fileadmin/Archivos/Politicas_de_certificacion/ACCV-CP-13V2.0-c.pdf 3.2. Initial validation of identity 3.2.2 Authentication of the identity of an organization. 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. The identification of the Administration or Organization shall be effected in the registration process of the Entity to be signed by a person capable of representing the Administration or Entity. 3.2.3 Authentication of the identity of an individual. The authentication of the identity of applicants for a certificate shall be made by his Impartiality in the application or delivery of the certificate. The Registry is the entity to delegate The certificates are issued, and which has implemented the provision of services by part of the ACCV by contract, agreement or other formula. Impartiality is not necessary for the public employee that will generate the certificate if their identity and status of public employee were highlighted in the Register of Staff Public Administration or Public Authority or Corporate to which they belong and to which we direct your application. 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. In this type of license includes the email address of the subscriber as a operations needed to support electronic signatures and email encryption, but the Autoritat of Certification of the Valencia does not guarantee that this email is

	linked to the certificate subscriber, so the confidence that this address is that of Subscriber certificate relates only to the relying party. 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. 4.1 Certificate Request The application of such certificates is the responsibility of public administration entities public character, which must verify the status of public employee holders certified by consultation with the personnel records of the organization within its competence. The process begins by discharging the Administration, agency or entity, from a registration form of entity, as set out in Annex III of the Certification Policy. In this form should indicate the persons authorized to manage certificates public employee personnel belonging to the entity in question. To carry out the license application form must be used to refer to Annex IV the Autoritat of Certification of the Valencia signed by a person qualified to perform certificate management. 4.2 Application for License After receiving the request for certificates by persons authorized to do so and once accepted, if any, the economic proposal if any, will proceed to the generation of certificates and the preparation of documentation associated with them. Once completed, was sent to administration or public entity applicant, through the persons authorized to manage. The persons authorized to manage the certificates will be responsible for the delivery of certificates to its subscribers and to forward the contracts to Autoritat certification of Certificació de la Comunitat Valenciana. 4.3 Issuing certificates ACCV is not responsible for the monitoring, investigation or confirmation of the accuracy of the information contained in the certificate after its issuance. In the case of receiving information about the inaccuracy or no current applicability of the information contained in the certificate, it can be revoked. The issuance of the certificate will take place once the ACCV has carried out checks necessary to validate the certification request. The mechanism that determines the nature and how to perform these checks is the Certification Policy. When the ACCV CA issues a certificate in accordance with a valid certification application, send a copy to the Registration Authority which submitted the application and another repository ACCV It is up to the Registration Authority to notify the subscriber of a certificate issuance thereof and provide a copy, or alternatively, inform you of how you can get it. Qualified Certs CP for Citizens: http://www.accv.es/fileadmin/Archivos/politicas_certificacion/ACCV-CP-07V4.0-c.pdf 3.2 Initial Identity Validation 3.2.1. Test methods of the possession of the private key

	As specified in the ACCV Certification Practices Statement (CPS). 3.2.2 Identity authentication of an organization 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. 3.2.3. Identity authentication of an individual. 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.** 4.1. Certificate Request 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. The process starts with the Administration, organization or entity enrollment using an entity sign up form as shown in the Annex III of this Certificate Policy. The persons who will be authorized for the civil servant certificate management of the related entity staff members must be stated in this form. In order to make a certificates request, the form shown in Annex IV shall be used, signed by one of the certificate management authorized persons and sent to the Autoritat de Certificació de la Comunitat Valenciana. 4.2. Certificate application processing After receiving the certificates request from the corresponding authorized persons and once, as appropriate, the economic proposal –if any- is accepted, the certificates will be issued and the associated documents prepared. Upon finishing, all will be sent to the applicant Administration or public Entity though the authorized persons.

	These certificate management authorized persons will be responsible of the certificate delivery to the subscribers and of sending the certificate agreements back to the Autoritat de Certificació de la Comunitat Valenciana. 4.3. Certificate Issuing ACCV is not responsible of the monitoring, investigation or confirmation of the certificate information accuracy after issuing. Should any information about the inaccuracy or non applicability of data contained in the certificate be received, the certificate can be revoked. The certificate issuing procedure will start once the ACCV checks all necessary requirements for validating the certification request. This Certification Policy will be the mechanism for determining the nature and how to perform this checking. When the ACCV CA issues a certificate associated to a valid certification request, it will send a copy to the Registry Authority that submitted the application and to the ACCV repository. It is up to the Registry Authority to notify the subscriber of the issuance of the certificate and provide a copy, or failing that, inform them of how to get it. 4.4 Certificate Acceptance Subscribers accept certificates by signing the certificate agreement associated to each Certificate Policy. The acceptance of agreement implies the Certificate Policy knowledge and acceptance by the subscriber. The certificate agreement has to be signed by both the subscriber and the person attached to the User Registry Point. Thus, the individual associated to a certificate is linked to the request, the knowledge of use rules and to the accuracy of provided data. The Certificate Agreement form is included in Annex I of this Certificate Policy.
Identity of Code Signing Subscriber	Comment #22: As stated in the policy the code-signing certificates can only be ordered with personal qualified certificates. The ACCV requires the applicant to provide documentation or references to ensure their identity in the organization. Code Signing CP: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/nuevo_23_07_08/PKIGVA-CP-04V2.0-c.pdf Code Signing CP section 3.1.8. Authentication of the identity of an organization 3.1.8. Identity Authentication of an Organization The right to apply for certificates defined in this Certificate Policy is limited to individuals. No certificate applications made by legal persons, entities or organizations will be admitted. Thus, no organization identification is required. When the applicant belongs to the Valencia Government staff, his/her application will be validated with the information contained in the People and Services' Guide. If they are not Valencia Government staff members, the applicant must submit the appointment publication (Government Gazette) or the civil servants' inauguration certificate or a certificate from his/her organization personnel department specifying occupation and responsibilities. 3.1.9. Identity Authentication of an Individual The identity authentication of a certificate applicant shall be made by his/her personal digital certificate that is used to sign the certificate application.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  o SSL certs are OV
	  o SSL CP section 6.3.2: Certificates issued under this policy are valid for three (3) years.
	• Wildcard DV SSL certificates
	  o SSL certs are OV
	• Delegation of Domain / Email validation to third parties
	  o ACCV 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.
	  o ACCV CPS section 9.6.2. Obligations of the Registration Authority
	  o ACCV 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.
	• Issuing end entity certificates directly from roots
	  o No. Root only signs intermediate CAs.
	• Allowing external entities to operate unconstrained subordinate CAs
	  o All sub-CAs are internally operated.
	• Distributing generated private keys in PKCS#12 files
	  o Not found.
	• Certificates referencing hostnames or private IP addresses
	  o Not found.
	• Issuing SSL Certificates for Internal Domains
	  o The subCA ACCV-CA3 issues Windows logon certificates and DC certificates for internal domains.
	• OCSP Responses signed by a certificate under a different root
	  o OCSP responses are signed by a certificate signed by the root CA, which also signed the subordinate CA.
	• CRL with critical CIDP Extension
	  o CRLS import into Firefox browser without error.
	• Generic names for CAs
	  o Root name is not generic