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 An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. 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	
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/ When OCSP is enforced, and I try to access https://www.accv.es/ I get Error code: sec_error_ocsp_unauthorized_response Please read section 4.2.2.2 "Authorized Responders" on pages 10-11 of RFC 2560. NSS strictly enforces the 3 rules at the bottom of page 10, and gives this error code when the response does not conform to those rules. Enforce OCSP in Firefox: Tools->Options…->Advanced->Encryption->Validation Select the box for "When an OCSP server connection failes, treat the certificate as invalid"
CA Hierarchy	This root has the following subordinate CAs: · CA GVA -- issues end-entity certificates for ACCV subscribers · ACCV-CA1 -- issues certificates for legal entities · ACCV-CA2 -- issues certificates for ACCV subscribers · ACCV-CA3 -- issues certificates for the identification of Windows domain users Please explain the types of certs that can be issued from each sub-CA. Are all of these sub-CAs internally operated?
Externally Operated sub-CAs	Does this root have any subordinate CA's that are operated by external third parties? Can it, in the future, have sub-CAs operated by third parties? For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. See https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List any other root CAs that have issued cross-signing certificates for this root CA
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code (Code Signing)
SSL Validation Type DV, OV, and/or EV	DV, IV Comment #11: We issue a mixture. Mainly identity/organisationally-validated certificates for everyone, but also we issue SSL certificates and domain-validated for public organizations Do you perform identity/organization verification for all SSL certificates? Is it ever the case for SSL certs that the domain name is verified, but the identity/organization of the subscriber is not verified?

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/nuevo_23_07_08/PKIGVA-CP-03V2.0-c2007.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) The audit document is locked, so I cannot copy-and-paste the text into a translator. Would you please translate the document into English and attach the translated version to this bug?
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 (Google translation, please correct) The right to request certificates defined in this Policy is Certification 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 Guide to People and services related to that person. In case of not belonging to the Generalitat Valenciana, the applicant must attach the publication of Appointment (Gazette) or document inauguration of the post held or certificate issued by a body of personnel management 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. (What does this mean? Does it mean that they must have a Qualified certificate before they can apply for an SSL certificate?)
Domain Name Ownership / Control	SSL CP: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/nuevo_23_07_08/PKIGVA-CP-03V2.0-c2007.pdf SSL CP section 4.1. Certificate Request (Google translation, please correct) The applicant received a certificate to this Policy shall complete Certification an application for certification through the application of non-personal management of certificates (NPSC) located at https: / / npsc.accv.es: 8450/npsc, where you can embed the file PKCS # 10 generated by the applicant. The completed application is sent, signed with a digital certificate recognized admitted Autoritat of Certification by the Comunitat Valenciana. It is the responsibility of the Registration Authority to determine the suitability of a type certificate to Characteristics of the applicant, according to the provisions of the applicable Certificate Policy, and thereby deny access or manage the application for certification thereof. In the case of refusal of the application for certification by the Authority Operator Register, the applicant will receive an email at the address noted in its application, informing him of the reasons for rejecting it.

	SSL CP section 4.2. Issuing Certificates (Google translation, please correct) The issuance of the certificate will take place once the registration authority for this Certification Policy has conducted necessary investigations to validate the certification request. The mechanism for determining the nature and how to perform these checks is the Certification Policy. Upon issuance of the certificate, the Registration Authority shall notify the subscriber of the same through sending a signed e-mail to the address shown on the application. The user must Sign in implementing non-personal management of certificates (NPSC) located in https: / / npsc.accv.es: 8450/npsc to collect the certificate, signing the contract beforehand Certification in this application with your personal certificate recognized. The Certification Agreement is a document to be signed electronically by the applicant, whose purpose is to link it with the action of the application, with the knowledge and usage rules with the accuracy of the data presented. section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate or has been authorized by the domain registrant to act on the registrant's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text. 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.
Email Address Ownership / Control	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 (Google translation, please correct) 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: (Please provide translations for sections 3.2, 4.1, 4.2, 4.3, 4.4) http://www.accv.es/fileadmin/Archivos/politicas_certificacion/ACCV-CP-07V4.0-c.pdf Section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on the account holder's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text. 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.
Identity of Code Signing Subscriber	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 (Google translation, please correct) The right to request certificates defined in this Policy is Certification 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 Guide to People and services related to that person. In case of not belonging to the Generalitat Valenciana, the applicant must attach the publication of Appointment (Gazette) or document inauguration of the post held or certificate issued by a body of personnel management in his organization, which clearly indicates his position and responsibility. Code Signing CP section 3.1.9 Authentication of the identity of an individual (Google translation, please correct) 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. Section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate or has been authorized by the entity referenced in the certificate to act on that entity's behalf;

Potentially Problematic Practices	Please review the list of Potentially Problematic Practices at http://wiki.mozilla.org/CA:Problematic_Practices. Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information and translations into English of the CP/CPS where relevant. • Long-lived DV certificates o Are SSL certs DV or OV? o SSL CP section 6.3.2: Certificates issued under this policy are valid for three (3) years. • Wildcard DV SSL certificates o • 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 • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • Issuing SSL Certificates for Internal Domains o • OCSP Responses signed by a certificate under a different root o Get Error code: sec_error_ocsp_unauthorized_response when OCSP is enforced. • CRL with critical CIDP Extension o CRLS import into Firefox browser without error. • Generic names for CAs o Root name is not generic