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.

General Information	Data
CA Name	ACCV
Website URL (English version)	http://www.pki.gva.es/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	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. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	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.

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	Our CA issues certificates for persons (with email), web sites and for signing code, in different policies, but with the same root. We are a public certificate service provider and the intended use for this root certificate is to improve the electronic administration between our citizens and the administration.
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
CRL URL	http://www.pki.gva.es/gestcert/rootgva_der.crl What is the nextUpdate set to in the CRL for end-entity certificates?
OCSP (if applicable) OCSP Responder URL Max time until OCSP responders updated to reflect end-entity revocation	http://ocsp.pki.gva.es/
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	Please provide a diagram or description of the CA hierarchy, showing all of the subordinate CAs of this root and the types of end-entity certificates that they issue. For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CP/CPS, and that any audit covers them as well as the root.
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.	Does this root have any subordinate CA's that are operated by external 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
List any other root CAs that have issued cross-signing certificates for this root CA	Has this root been involved in cross-signing with another root?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code (Code Signing)
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: 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? Or 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

Translations into English of sections of CP/CPS documents pertaining to: • Verification of Identity and Organization • 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	Please provide translations into English of sections of CP/CPS documents pertaining to: • Verification of Identity and Organization • Verification of ownership/control of domain name for SSL certs • Verification of ownership/control of email address for email (S/MIME) certs • Section 7 of http://www.mozilla.org/projects/security/certs/policy/ • Potentially Problematic Practices, http://wiki.mozilla.org/CA:Problematic_Practices
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. For SSL certificates this should also include URLs of one or more web servers using the certificate(s).	For testing purposes, please provide a URL to a website whose SSL certificate chains up to this root. Note that this can be a test site.
CP/CPS	All are in Spanish Declaracion de Practicas de Certificacion (CPS) de la ACCV, v1.7 http://www.accv.es/pdf-politicas/ACCV-CPS-V1.7-v.pdf Certification policies and practices for the different types of certificates: http://www.pki.gva.es/legislacion_c.htm Certification Practices • Certification Practices Statement. • Privacy Policy. Certification Policies • Policy Certification certificates of public employee. • Policy Certification certificates in support of software for people. • Policy Certification recognized certificates to secure citizens. • Policy Certification certificates recognized entity. • Servers with SSL support. • VPN servers. • Code signing. • Application. • Time Stamping Policy. • Policy Certification Certificates logon Windows. • Policy Certification Certified Domain Controller

	Certification Practices for Server Certificates with SSL http://www.pki.gva.es/pdf-politicas/PKIGVA-CP-03V2.0-c2007.pdf Certification Practices for Code Signing Certificates http://www.pki.gva.es/pdf-politicas/PKIGVA-CP-04V2.0-c.pdf
AUDIT	Audit Type: WebTrust CA Auditor: Seguridad y Sistemas de Información S.L. Auditor Website: http://www.ssiconsultores.com/ Audit: https://cert.webtrust.org/ViewSeal?id=571. 10 de Abril de 2006 Do you have a more recent audit?

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