Bugzilla ID: 295474
Bugzilla Summary: Add CATCert root 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	CATCert
Website URL	www.catcert.net
Organizational type	Public Company. Regional Government CA in Spain. The Region of the Autonomic Community of Catalunya. 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	CATCert is the Catalan Agency of Certification (Agència Catalana de Certificació). CATCert's aim is to provide digital certification services and promote the usage of digital signature in order to make safer the communications within the Catalan government and the communications (within and for) the Catalan government. CATCert is issuing email encryption and signing certificates free of charge to Catalan citizens that request them, and these certificates are accepted by various national agencies.

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

Info Needed	Data
Certificate Name	Common Name: EC-ACC Full Name: Entitat de Certificació de l'Agència Catalana de Certificació
Cert summary / comments	This root has seven internally-operated subordinate CAs. The subordinate CAs are used to distinguish who the certificates are issued to. The EC-IDCAT certificates are issued to Catalan citizens. The EC-SAFP (a sub-CA of EG-GENCAT), EC-AL, and EC-PARLAMENT certificates are not issued to the general public, but only to the civil servants and computers or devices of the Regional Catalan government, the Catalan Government, and the Catalan Parliament. The EC-UR and EC-URV certificates are not issued to the general public, but to employees, students and computers or devices of Catalan universities and research centers connected to the "Anella Científica" group, and the Universitat Rovira i Virgili (URV).
The root CA certificate URL	http://www.catcert.net/descarrega/acc.crt
SHA-1 fingerprint.	28:90:3A:63:5B:52:80:FA:E6:77:4C:0B:6D:A7:D6:BA:A6:4A:F2:E8
Valid from	2003-01-07
Valid to	2031-01-07

Cert Version	3
Modulus length	2048
Test Website(s)	https://www.e-ajrubi.net/ https://actes.urv.cat
CRL URL	http://epscd.catcert.net/crl/ec-acc.crl http://epscd.catcert.net/crl/ec-al.crl http://epscd.catcert.net/crl/ec-gencat.crl http://epscd.catcert.net/crl/ec-safp.crl http://epscd.catcert.net/crl/ec-ur.crl http://epscd.catcert.net/crl/ec-urv.crl http://epscd.catcert.net/crl/ec-parlament.crl http://epscd.catcert.net/crl/ec-idcat.crl English CPS section 4.4.9: In personal and device certificates the Certification Entity issues a CRL at the very least every 24 hours. In the CRL is indicated the intended time for the next CRL issuance, but a CRL can be issued before the time indicated, in the previous CRL.
OCSP Responder URL	http://ocsp.catcert.net I still get errors trying to browse to the test websites (https://www.e-ajrubi.net/ and https://actes.urv.cat) in my Firefox browser, with OCSP enforced. Please see https://wiki.mozilla.org/CA:Recommended_Practices#OCSP. Before including a root in NSS, the websites with SSL certs chaining to this root must work, even when OCSP is enforced.

CA Hierarchy	Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=379561
	The subordinate CAs are:
	• EC-GENCAT: Generalitat de Catalunya
	  ○ EC-GENCAT is providing digital certification services and promoting the usage of digital signature in order to make safer the communications within and for the Regional Catalan government.
	• EC-SAFP: Secretaria d'Administració i Funció Pública
	  ○ This is a sub-CA of EC-GENCAT
	  ○ EC-SAFP's certificates are not issued to general public, but only to the civil servants and computers or devices of agencies and departments of the Catalan Regional Government and public funded companies of the Catalan Regional Government (depending on the Secretaria d'Administració i Funció Pública).
	• EC-idCat: Entitat publica de certificacio de ciutadans
	  ○ EC- idCAT's certificates are issued to catalan citizens.
	• EC-AL: Administracions Locals de Catalunya
	  ○ EC-AL's certificates are not issued to general public, but only to the civil servants and computers or devices of the Catalan government: this is city and town councils, regional councils, county councils,

	as well as autonomous agencies and public funded companies.
	• EC-UR: Universitats i Recerca
	  ○ EC-UR's certificates are not issued to general public, but to employees, students and computers or devices of Catalan universities and research centres connected to the "Anella Científica" group.
	• EC-URV: Universitat Rovira i Virgili
	  ○ This is a sub-CA of EC-UR
	  ○ EC-URV's certificates are not issued to general public, but to employees,students and computers or devices of the Universitat Rovira i Virgili (URV).
	• EC-Parlament: Parlament de Catalunya
	  ○ EC-PARLAMENT's certificates are not issued to general public, but only to the civil servants and computers or devices of the Catalan Parliament.

Externally operated subCAs	Comment #27: There are not Sub-CA's operated by third parties. Just the Registration Authorities.
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	OV
EV policy OID(s)	Not EV
CP/CPS	Here is my current list of the main documents of interest pertaining to this root inclusion request: Document Repository: http://www.catcert.cat/web/cat/5_0_regulacio.jsp General Certification Policy (Catalan): http://www.catcert.cat/web/cat/5_1_politica_general.jsp Certification Practice Statement for each sub-CA (Catalan): http://www.catcert.cat/web/cat/5_2_declaracio.jsp Operative Procedure (Catalan): http://www.catcert.cat/descarrega/ER_T_CAT/Procediments.zip Comment #2 "English version of CATCert's CPS": https://bugzilla.mozilla.org/attachment.cgi?id=184501 Please tell me which document this "English version of CATCert's CPS" corresponds to in the web pages listed above.
AUDIT	Audit Type (WebTrust, ETSI etc.): WebTrust CA Auditor: Ernst &Young Auditor Website: www.ey.com/es Audit Report and Management Assertions: https://cert.webtrust.org/ViewSeal?id=1063 (2010.07.01) English Translation of audit report: https://bugzilla.mozilla.org/attachment.cgi?id=459806 The audit includes this root and its sub-CAs.
Organization Identity Verification	The CPS has been translated into English: https://bugzilla.mozilla.org/attachment.cgi?id=184501 Section 3.1.8, Authentication of the identity of an Organization Section 3.1.9, Authentication of the identity of a natural person
Domain Name Ownership / Control	Comment #46: 1.- Only authorized personal from Catalan Administration can request a certificate (Domain Server Certificate). 2.- (Items 1.3.2.1 – 1.3.2.5) It's checked the applicant is an authorized person.

	3.- (Item 1.3.2.7) It is checked using www.whois.net the existence of the server and the ownership. For full English translations of items 1.3.2.1-1.3.2.7 of the Operative Procedure document, see https://bugzilla.mozilla.org/show_bug.cgi?id=295474#c46 The CPS has been translated into English: https://bugzilla.mozilla.org/attachment.cgi?id=184501 Section 3.1.8.3: …the following items are verified: 1) The existence of the server. 2) The dominion name ownership, verified in the correlative register. 3) The authorization to organize the issuance of the certificate to the server. Comment #46: Item 1.3.2.7 of the Operative Procedure, explains how the ownership/control of the domain name is verified. 1.3.2.7 Checking of the certificate data (Domain Server Certificates) In case of Domain Server Certificates requests, the person in charge of the Registration Entity will verify the existence and ownership of the server URL and the registration data using the WHO IS (www.whois.net). This way he/she verifies the existence of the server. The result will be converted to pdf format and it will be signed digitally by de person in charge of the Registration Entity. A digital copy will be stored and another will be printed and attached to the request, stored into the Registration Entity archive. Comment #36: This merely verifies the existence of the domain name. It does not verify that the person, company, or organization requesting a site certificate actually owns and controls that domain and is authorized to request a certificate for the domain. Comment #38: I did not find anything about how the output of WHOIS is used or compared to the data of the applicant in order to verify that the applicant owns/controls that domain. I think that what's missing is how is the information from whois used to confirm that the applicant owns/controls the domain name? eg. Do you use the whois information to contact the domain owner (using the contact information provided in whois) to confirm the authority of the applicant? Or do you send an email to a particular email address, which uses that domain name (eg a challenge-response mechanism)? Or, do you have the applicant place something on the server that you can confirm is there (eg from the English translation it said the "existence of the server" is verified)?
Email Address Ownership / Control	Not requesting the email trust bit at this time.
Identity of Code	Not requesting the code signing trust bit at this time.

Signing Subscriber	

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL certs are OV
	• Wildcard DV SSL certificates
	  ○ SSL certs are OV
	• Email Address Prefixes for DV SSL Certs
	  ○ SSL certs are OV
	• Delegation of Domain / Email validation to third parties
	  ○ Is the validation of domain ownernship/control delegated to third parties? If yes, Please see
	  ▪ https://wiki.mozilla.org/CA:Problematic_Practices#Delegation_of_Domain_.2F_Email_validation_to_third_parties
	  ▪ "The CA must demonstrate clear and efficient controls attesting the performance of its RAs."
	  ▪ This information should be in the CP/CPS.
	• Issuing end entity certificates directly from roots
	  ○ No. The root signs intermediate certificates, which sign end-entity certs.
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ Comment #27: There are not Sub-CA's operated by third parties. Just the Registration Authorities.
	• Distributing generated private keys in PKCS#12 files
	  ○ Not for SSL certs.
	• Certificates referencing hostnames or private IP addresses
	  ○ ?
	• Issuing SSL Certificates for Internal Domains
	  ○ ?
	• OCSP Responses signed by a certificate under a different root
	  ○ I cannot browse to the test websites with OCSP enorced.
	• CRL with critical CIDP Extension
	  ○ CRLs imported successfully into Firefox browser.
	• Generic names for CAs
	  ○ Root CN is EC-ACC, which stands for Entitat de Certificació de l'Agència Catalana de Certificació