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 EC-ACC stands for: Entitat de Certificació de l'Agència Catalana de Certificació

Issuer	CN = EC-ACC
	OU = Jerarquia Entitats de Certificacio Catalanes
	OU = Vegeu https://www.catcert.net/verarrel (c)03
	OU = Serveis Publics de Certificacio
	O = Agencia Catalana de Certificacio (NIF Q-0801176-I)
	C = ES

Cert summary / comments	This root has internally-operated subordinate CAs. The subCAs 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 only issued 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 only issued 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)	EC-SAFP: https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/notice.pscp?reqCode=searchCn&idCap=203732 EC-AL: https://seu.badalona.cat/portalWeb/badalona.portal?_nfpb=true&_pageLabel=seu_electronica EC-UR: https://seuelectronica.upc.edu/ EC-URV: https://portal.urv.cat/portal/dt
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
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.
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	OV
EV policy OID(s)	Not EV
CP/CPS	Document Repository (Spanish): http://www.catcert.cat/registro General Certification Policy (Spanish): http://www.catcert.cat/web/cas/5_1_politica_general.jsp Certification Practice Statement for each sub-CA (Spanish): http://www.catcert.cat/web/cas/5_2_declaracio.jsp Document Repository (Catalan): http://www.catcert.cat/registre 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
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	See https://bugzilla.mozilla.org/attachment.cgi?id=479370 for English translations of Section 3.2.2 (Authentication of the identity of an Organization) and Section 3.2.3 (Authentication of the identity of a natural person) of Política

	General de Certificación Agència Catalana de Certificació. (http://www.catcert.cat/web/cas/5_1_politica_general.jsp)
Domain Name Ownership / Control	Comment #48: CATCert only generates website certificates for Catalan Public Administrations. As mentioned before (1.3.2.1-1.3.2.7 of the Operative Procedure document) only authorized people can apply for certificates, and it is checked. Registration Entity contacts the owner listed in the whois (http://www.whois.net/ and http://www.internic.net/whois.html for domains .cat) to verify that the applicant has the right to use the domain or subdomain. In order to verify it, the person in charge of the Registration Entity extracts the admin data and sends an e-mail asking if the applicant owns/controls the subdomain. Once the confirmation is received, the certificate is generated. Operative Procedure (Catalan): http://www.catcert.cat/descarrega/ER_T_CAT/Procediments.zip D1132-PO-00-procediment_operatiu_20070920.pdf 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 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. 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.
Email Address Ownership / Control	Not requesting the email trust bit at this time.
Identity of Code Signing Subscriber	Not requesting the code signing trust bit at this time.
Potentially Problematic	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates

Practices	○ 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 ○ Comment #48: 4.1. RAs are external to CATCert but they belong to the Catalan Public Administration. It means they have in common the application of the controls specified at the Spanish Law 30/92 about procedures of the Public Administration. These RAs sign a contract with CATCert, and their way of working is periodically audited using the clauses of the contract. ○ https://bugzilla.mozilla.org/attachment.cgi?id=479369 ▪ This is an English translation of relevant sections of http://www.catcert.cat/descarrega/oficina_politiques/D1111_N-PGDC_v3r3_cat.pdf ▪ It explains the agreements and controls pertaining to RAs. • 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 ○ Not allowed. • Issuing SSL Certificates for Internal Domains ○ Not allowed. • OCSP Responses signed by a certificate under a different root ○ I can browse to the test websites with OCSP enforced, and I have verified that the SSL certs have the OCSP URI in the AIA. • 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