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.

General Information	Data
CA Name	CATCert
Website URL (English version)	www.catcert.net
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 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. (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?)	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	To Do, based on CA hierarchy information.
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
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

List or description of subordinate CAs operated by the CA organization associated with the root CA.	Is this the full list of subordinate CA chaining up to this EC-ACC root?
	Which of these sub-CAs are operated internally, and which of these are operated by external third parties?
	
	The subordinate CAs are:
	• EC-GENCAT: Generalitat de Catalunya
	  ○ http://www.catcert.net/descarrega/gencat.crt
	  ○ 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-idCat: Entitat publica de certificacio de ciutadans
	  ○ http://www.catcert.net/descarrega/ec-idcat.cer
	  ○ EC- idCAT's certificates are issued to catalan citizens.
	• EC-AL: Administracions Locals de Catalunya
	  ○ http://www.catcert.net/descarrega/al_csrs.crt
	  ○ 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-SAFP: Secretaria d'Administració i Funció Pública
	  ○ http://www.catcert.net/descarrega/safs_csrs.crt
	  ○ 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-Parlament: Parlament de Catalunya
	  ○ http://www.catcert.net/descarrega/parlament_csrs.crt
	  ○ EC-PARLAMENT's certificates are not issued to general public, but only to the civil servants and computers or devices of the Catalan Parliament.
	• EC-UR: Universitats i Recerca
	  ○ http://www.catcert.net/descarrega/ur_csrs.crt
	  ○ 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
	  ○ http://www.catcert.net/descarrega/urv_csrs.crt
	  ○ 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).

Subordinate CAs operated by third parties	Does this root have any subordinate CAs 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. Also, see https://wiki.mozilla.org/CA:SubordinateCA_checklist English CPS section 1.1.2: Class 1 Digital Certification Service allows the Administration using this service to obtain corporative digital certificates for its staff working in the mentioned user Administration. In this type of service the user Administration acts as subject of the certificates and gives properly checked register information, with the errand of a **CATCert** register entity, but with this function limited to the environment of the same user Administration. Class 2 Digital Certification Service allows the Administration using this service to supply digital certificates for outside entities and for their staff, to use them in their professional and administrative relationships with any user Administration adherent to the Certificates Verification Service. In this type of service the user Administration acts as register entity collaborating with **CATCert**. Class 2 service is one offered in free competition with the rest of certificate services providers, especially private sector providers. The acceptance of the certificates issued by these providers is done through their classification made by **CATCert**.

	English CPS section 1.1.3: First, certificates are issued to entities linked to the hierarchy. These certificates are termed **Infrastructure Certificates (CIC)** and are released only to certification entities, so that they can issue certificates to other end-users. CIC are classified into two types: level 1, which are certificates released to other certification entities so that, in their turn, they can issue certificates to other certification entities of an inferior level within the hierarchy and to target entities; level 2, which are certificates released to other certification entities so that they can issue certificates to target entities. The rest of certificates are released to target entities, which can be organizations, natural persons, and computer devices, by bound certification entities owned by **CATCert**.
List any other root CAs that have issued cross-signing certificates for this root CA	Has this root been involved in cross-signing with any other roots?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • DV – only the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. • OV – in addition to verifying the domain name, the value of the Organization attribute is verified to be that associated with the certificate subscriber. • EV -- Extended Validation Certificate	OV
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	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 Please either provide pointers to the text/sections in the English CPS, or provide translations into English

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	of the sections of the appropriate CP/CPS documents pertaining to: • 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
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).	https://www.e-ajrubi.net/ -- works when OCSP is enforced Authority Information Access: Not Critical OCSP: URI: http://ocsp.catcert.net https://actes.urv.cat – gives error when OCSP is enforced. Authority Information Access: Not Critical OCSP: URI: http://ocsp.catcert.net https://www.idcat.net/ -- gives error when OCSP is enforced. Does redirect when OCSP not enforced.
CP/CPS	English version of CPS https://bugzilla.mozilla.org/attachment.cgi?id=184501 CPS in Catalan https://bugzilla.mozilla.org/attachment.cgi?id=184504 CP in Catalan https://bugzilla.mozilla.org/attachment.cgi?id=184505 The CPS/CP for each sub-CA in Catalan http://www.catcert.net/registre EC-AL http://www.catcert.net/descarrega/doc_legal/EC-AL_dpc.pdf http://www.catcert.net/descarrega/doc_legal/EC-AL_pdc_general.pdf

	EC-idCAT http://www.catcert.net/descarrega/doc_legal/idCAT_dpc.pdf http://www.catcert.cat/descarrega/doc_legal/idCAT_pdc_general.pdf http://www.catcert.net/descarrega/doc_legal/idCAT_pedc.pdf EC-UR http://www.catcert.net/descarrega/doc_legal/EC-UR_dpc.pdf http://www.catcert.cat/descarrega/doc_legal/EC-UR_pdc_general.pdf http://www.catcert.net/descarrega/doc_legal/EC-UR_pedc.pdf EC-URV http://www.catcert.net/descarrega/doc_legal/EC-URV_dpc.pdf EC-SAFP http://www.catcert.net/descarrega/doc_legal/EC-SAFP_dpc.pdf http://www.catcert.net/descarrega/doc_legal/EC-SAFP_pdc_general.pdf http://www.catcert.cat/descarrega/doc_legal/EC-SAFP_cge.pdf EC-PARLAMENT http://www.catcert.net/descarrega/doc_legal/EC-AL_pdc_general.pdf
AUDIT	Audit Type (WebTrust, ETSI etc.): Web Trust CA Auditor: Ernst &Young Auditor Website: www.ey.com/es Audit Report and Management Assertions: https://cert.webtrust.org/SealFile?seal=466&file=pdf The WebTrust audit is from 2005. 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
    - English CPS section 1.1.2:
        - Class 2 Digital Certification Service allows the Administration using this service to supply digital certificates for outside entities and for their staff, to use them in their professional and administrative relationships with any user Administration adherent to the Certificates Verification Service. In this type of service the user Administration acts as register entity collaborating with **CATCert**. Class 2 service is one offered in free competition with the rest of certificate services providers, especially private sector providers. The acceptance of the certificates issued by these providers is done through their classification made by **CATCert**.
        - The Register Service Delegated to **CATCert** and to other register entities collaborating with **CATCert** allows the user Administration to delegate to **CATCert** the accomplishment of the functions of a local register entity, taking on the correspondent responsibility. In any case, the Administration is responsible for the document verification of data included in the certificate, as a virtual register entity.
- 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
    - The CRLs import into Firefox without error.
- 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