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 get errors trying to browse to the test websites in my Firefox browser, with OCSP enforced. Please see https://wiki.mozilla.org/CA:Recommended_Practices#OCSP.
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) Email (S/MIME) ? Code Signing ?
SSL Validation Type	OV
EV policy OID(s)	Not EV
CP/CPS	CPS in English: https://bugzilla.mozilla.org/attachment.cgi?id=184501 (Needs to be updated?) CPS in Catalan: https://bugzilla.mozilla.org/attachment.cgi?id=184504 (New doc and url?) Operative Procedure in Catalan: https://bug295474.bugzilla.mozilla.org/attachment.cgi?id=387876 (current?) CP in Catalan: http://www.catcert.cat/descarrega/oficina_politiques/D1111_N-PGDC_v3r3_cat.pdf Declaration of Practices for each sub-CA in Catalan: http://www.catcert.cat/web/cat/5_2_declaracio.jsp
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) 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	CPS 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.

	Operative Procedure in Catalan: https://bug295474.bugzilla.mozilla.org/attachment.cgi?id=387876 Google Translation: 1.3.2.7 Verification of the certificate data and CDS CDSDC At the request of a CDS, the Head of SCD verify the URL and the server data using the WHO IS (www.whois.net). This verifies the existence of server. Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership We rely on publicly available documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met. 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; There needs to be information in the CP/CPS that describes 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.
Email Address Ownership / Control	Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control We rely on publicly available documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met. 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; In order to enable the email trust-bit, there needs to be information in the CP/CPS that describes how CATCert verifies that the certificate subscriber owns/controls the email address to be included in the certificate.
Identity of Code Signing Subscriber	If the code-signing trust bit is to be enabled, please provide translations into English of the sections of the CP/CPS documents that describe the identity verification procedures for code signing certs. Please also list the corresponding document(s) and section or page numbers containing the original text.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices: 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
    -
- Wildcard DV SSL certificates
    -
- Email Address Prefixes for DV SSL Certs
    -
- 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.
    - 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
    -
- Allowing external entities to operate unconstrained subordinate CAs
    -
- Distributing generated private keys in PKCS#12 files
    -
- Certificates referencing hostnames or private IP addresses

	○ • Issuing SSL Certificates for Internal Domains ○ • OCSP Responses signed by a certificate under a different root ○ • CRL with critical CIDP Extension ○ • Generic names for CAs ○