Bugzilla ID: 720326
Bugzilla Summary: Add SHA-256 EC-ACC root certificate and Enable EV

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	CATCert
Website URL	www.catcert.net
Organizational type	Public Company. Regional Government CA in Spain. The Region of the Autonomic Community of Catalunya.
Primark 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.
CA Contact Information	Primary contact: Manuel Rella Ruiz, mrella@catcert.cat CA Email alias: usos@catcert.cat CA Phone Number: +34 93.272.26.00 Title/Department: Àrea de Certificació i Qualitat

Technical information about each root certificate

Cert Name	EC-ACC
Certificate Issuer Field	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
Certificate Summary	This is the SHA-256 version of the EC-ACC root certificate that was included in NSS per bug #295474.
Root Cert URL	http://www.catcert.cat/descarrega/acc_sha2.crt
SHA1 Fingerprint	A1:DA:3F:18:BF:40:AF:2A:A7:48:07:9C:1F:0F:14:DC:39:D4:3C:7A
Valid From	2012-04-17
Valid To	2031-01-07
Cert Version	3
Cert Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	2048
Test Website URL (SSL)	https://test_ev_cds.catcert.cat https://test_ev_seu_mig.catcert.cat

	https://test_ev_seu_alt.catcert.cat The certificate is not trusted because **no issuer chain was provided.** (Error code: sec_error_unknown_issuer)
CRL URL	
End-entity CRL NextUpdate	CP section 4.9.7.2: The Certification Body shall issue a Linked CRL at least every 24 hours.
OCSP URL	http://ocsp.catcert.net
OCSP Max expiration time	Section 14 of https://wiki.mozilla.org/CA:Information_checklist#Technical_information_about_each_root_certificate The sections of your CP/CPS specifying availability and update requirements for the OCSP service. CA/Browser Forum's EV Guidelines Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days." Test results of: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	OV and EV
EV Policy OID	

CA Hierarchy information for each root certificate

CA Hierarchy	This root will have internally-operated subordinate CAs. The subCAs are used to distinguish who the certificates are issued to. ** The EC-idCAT subCA issues certificates to Catalan citizens. It does not issue SSL certificates to other administrations (except itself SSL certificate for the www.idcat.cat domain). ** The EC-SAFP (sub-CA of EC-GENCAT), EC-AL (Administracions Locals de Catalunya), and EC-Parlament (Parlament de Catalunya) subCAs only issue certificates to the civil servants and computers or devices of the Regional Catalan government, the Catalan Government, and the Catalan Parliament. Including city and town councils, regional councils, county councils, as well as autonomous agencies and public funded companies. ** The EC-UR (Universitats i Recerca) and EC-URV (Universitat Rovira i Virgili) subCAs only issue certificates 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). There are now two valid and equivalent hierarchies, the one with SHA-1 and the new with SHA-256. These are the SHA-256 certificates: http://www.catcert.cat/descarrega/acc_sha2.crt http://www.catcert.cat/descarrega/gencat_sha2.crt http://www.catcert.cat/descarrega/safp_sha2.crt http://www.catcert.cat/descarrega/al_sha2.crt http://www.catcert.cat/descarrega/idcat_sha2.crt http://www.catcert.cat/descarrega/parlament_sha2.crt http://www.catcert.cat/descarrega/ur_sha2.crt http://www.catcert.cat/descarrega/urv_sha2.crt

	Will there be separate subCAs for EV? Or will some of these existing subCAs support both EV and non-EV? Will they have separate subCAs for EV versus non-EV?
Externally Operated SubCAs	This root does not have externally Operated SubCAs, and none planned.
Cross-Signing	This root is not involved in cross-signing with any other CAs.

Verification Policies and Practices

Policy Documentation	Document Repository (Spanish): http://www.catcert.cat/registro CP (Spanish): http://www.catcert.cat/web/cas/5_1_politica_general.jsp DPC (Declaración de Prácticas de Certificación) for each sub-CA (Spanish): http://www.catcert.cat/web/cas/5_2_declaracio.jsp Document Repository (Catalan): http://www.catcert.cat/registre CP (Catalan): http://www.catcert.cat/web/cat/5_1_politica_general.jsp DPC (Declaración de Prácticas de Certificación) 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 This can be found at the public procedure, applied by all the ER-TCAT (Registration Entities) at the URL: http://www.catcert.cat/web/cas/1_0_2_er_tcat.jsp. The link is called "Procediments". Inside the ZIP file there is the operative procedure for the registration entities: D1132-PO-00-procediment_operatiu_ER _T-CAT_20110808.pdf
Audits	Audit Type (WebTrust, ETSI etc.): WebTrust CA Auditor: Ernst &Young 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 This audit includes the root and its sub-CAs. Audit Type (WebTrust, ETSI etc.): WebTrust EV Auditor: Ernst &Young Audit Report and Management Assertions: https://cert.webtrust.org/ViewSeal?id=1189 (2011.07.01) This audit includes the root and its sub-CAs.
Organization Verification Procedures	Translations of sections 3.2.2 and 3.2.3 of the CP were provided as an attachment to bug #295474. https://bugzilla.mozilla.org/attachment.cgi?id=479370 Class 1 are certificates issued only to public administrations or to people that have a direct work contract with them (these are public employees). And Class 2 are certificates issued to citizens. In the specific case of server certificates we only issue class 1 certificates. CP section 3.2.2.3.1, "Requirements for class 1 certificates", refers to the case that the Registry entity organization requests certificates to itself. In this case, the organization doesn't have to apply controls to

	authenticate to itself because this identity is already well known. For example, when the registry entity of the Barcelona Council has to request certificates to itself it doesn't have to verify the existence of the Barcelona Council as an organization. CP section 3.2.2.3.2, "Requirements for class 2 certificates", is there in case some day the commercial strategy of CATCert changes in order to issue certificates to private corporations, then they would apply. Currently no class 2 SSL certificates are issued, and there is no plan to do so. This section is in the CP just in case that ever changes.
SSL Verification Procedures	SSL certificates are only issued to the limited well-known public governments and administrations of Catalonia. The subCAs that can issue SSL certs are EC-SAFP, EC-AL, EC-UR, EC-URV, and EC-Parlamant. Their DPC documents have the following in section 3.2.2: For device certificates secure server and domain controller, in addition to checking has been carried out by the organization responsible for the secure server is checked: ** The existence of the server. ** Ownership of the domain name from the registry. **Authorization for the organization of the issuance of the certificate on the server. Verification of SSL certificate subscribers requires a manual step of identity/organization verification. Additionally,CATCert has automatic blocks in place for high-profile domain names.
EV Organization Verification Procedures	Section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices "If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations. Please provide translations into English of the relevant sections.
EV SSL Domain Name Verification Procedures	
Email Address Verification Procedures	N/A. Not requesting the email trust bit at this time.
Code Signing Subscriber Verification Procedures	N/A. Not requesting the code signing trust bit at this time.
Multi-factor Authentication	Registry entities access the certificate request/approval/issuance interface by using certificates stored in secure cryptographic smartcards.
Network Security	CATCert has performed the network security checks as listed here: https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices In addition CATCert is undergoing further penetration testing, and is working to add further automation in regards to monitoring their network. CP sections 5.4, 5.7, and 6.5.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes

CA Hierarchy	Yes
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	???
Revocation of Compromised Certificates	???
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	N/A
Verifying Identity of Code Signing Certificate Subscriber	N/A
DNS names go in SAN	???
Domain owned by a Natural Person	???
OCSP	Yes

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV or EV.
Wildcard DV SSL certificates	SSL certs are OV or EV.
Email Address Prefixes for DV Certs	SSL certs are OV or EV.
Delegation of Domain / Email validation to third parties	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 subordinate CAs	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	No
CRL with critical CIDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	No