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.
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

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
	O = Agencia Catalana de Certificacio (NIF Q-0801176-I)
	OU = Jerarquia Entitats de Certificacio Catalanes
	OU = Vegeu https://www.catcert.net/verarrel (c)03
	OU = Serveis Publics de Certificacio
	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).
Root 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 CP section 4.9.7.2: The Certification Body shall issue a Linked CRL at least every 24 hours.
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. ○ This subCA does not issue SSL server certificates to other administrations (except itself SSL certificate for the www.idcat.cat domain). • 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 requesting EV treatment at this time.
CP/CPS	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
AUDIT	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 Identity Verification	Translations of sections 3.2.2 and 3.2.3 of the CP were provided as an attachment to the bug: https://bugzilla.mozilla.org/attachment.cgi?id=479370 Comment #71: 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. In the 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.

	In the 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.
Domain Name Verification in SubCA DPC Documents	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. From CATCert: "We have added to the list of forbidden domain certificates the next ones: - the Alexa 1000 domains - the published hacked Diginotar and Comodo domains So its generation is only possible with the direct approbation at CATCert central office." DPC (Declaración de Prácticas de Certificación) for each sub-CA (Catalan): http://www.catcert.cat/web/cat/5_2_declaracio.jsp The following subCAs can issue SSL certificates: EC-SAFP DPC section 3.2.2.3.3: 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. EC-AL DPC section 3.2.2.1.1.3: 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. EC-UR DPC section 3.2.2.2.3: For device certificates secure server and domain controller, in addition to checking has been carried out by the organization responsible for the secure server checks: The existence of the server. The ownership of the domain name from the registry. The authorization for the organization of the issuance of the certificate on the server. EC-URV DPC section 3.2.2.2.3: 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. EC-PARLAMENT DPC section 3.2.2.2.3: 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.

Domain Name Ownership / Control Operative Procedure	All the registry entities are only allowed to issue certificates to domains explicitly owned by their associated public administrations (that are restricted to catalonian public administration). There are approximately 1800 well known different public administrations in Catalonia that can have certificates from CATCert, all of them have an identification number called CIF, its name is registered in an official and public way by law, and have an associated registry entity for issuing its certificates. All the registry entities have access to a database, managed directly by CATCert, with all the up to date information of these publics administrations, including the different roles and persons authorized for managing certificates lifecycle. In the process of issuing certificates: - The first control of any registry entity is to verify that the request is done by the correct roles and persons of a recognized public administration, this is done by looking to the clients database. In fact only the registered and authorized ones can do electronic requests through the web using his electronic signature in a smartcard. - The second control is to verify that the request is correct, in case of SSL certificates some attributes of the DN are fixed, for example the "O" is fixed to be exactly the name of the requestor public administration. The "CN" can contain any string because the domain name of the webs owned by a public administration is in principle free. Here it is automatically verified that the name is not inside the antiphishing nor the high value domains list of alexa 1000. Here also the registry entity must verify the domain is registered in the whois database and owned by the requestor public administration. - If all OK the certificate is generated and the requestor administration can download the public part of it. For this download it is needed an authorized personal certificate in cryptographic smartcard owned by the requestor organization (this is another point of security control). - The last control is a daily review by CATCert of the issued SSL certificates: we have implemented a daily report of all SSL issued certificates by date, and we now do a second whois control for all the certificates generated by the registry entities, to verify the domain is in fact owned by the requestor public administration. Operative Procedure: 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" points to http://www.catcert.cat/descarrega/ER_T_CAT/Procediments.zip. Inside the ZIP file there is the operative procedure for the registration entities: D1132-PO-00-procediment_operatiu_ER _T-CAT_20110808.pdf CATCert only generates website certificates for Catalan Public Administrations. As per sections 1.3.2.1to 1.3.2.7 of the Operative Procedure, 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. 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 and https://bugzilla.mozilla.org/show_bug.cgi?id=295474#c73 Here's some of the sections: 1.3.2.4 Validation of the identity and authority of the applicant The person in charge of the Registration Entity has to check out that who makes the request for obtaining a digital certificate is authorized, it means that he/she is who was specified in the subscriber card. The valid methods for receiving the information required of a request for obtaining a certificate are detailed next:

1) By electronic mail: The person in charge of the subscriber entity sends an electronic mail to the person in charge of the Registration Entity digitally signed, and he/she attaches the electronic documents, also digitally signed, by the people indicated in the subscriber card. It means, the person in charge of the Registration Entity has to check out that the applicant indicated in the card has signed the request.
In case that the Registration Entity does not have telematic registry, the documentation will be printed after being verified the signature and will be sealed with the indication “It is exact copy of an electronic document, which I have verified that the electronic signature is correct". Also it will be necessary that the person in charge of the Registration Entity signs at the foot of the seal.

2) By postal mail: The person in charge of the subscriber entity makes to arrive at the person in charge of the Registration Entity the documentation in paper signed by the people indicated in the subscriber card. In case the authentication and authorization of the applicant is not correct, the person in charge of the Registration Entity will reject the request and will send a signed electronic mail to the person in charge of the entity subscriber. Otherwise, the process continues.

1.3.2.5 Validation of the identity and authority of the certifier
The person in charge has to check out that who delivers the documental justification really is authorized, it means this person is the Certifier that it was specified in the subscriber card. The valid methods for receiving the information required of a request for obtaining a certificate are detailed next:
1) The person in charge of the subscriber entity sends an electronic mail to the person in charge of the Registration Entity signed digitally, and the electronic documents are attached, also digitally signed by the people indicated in the subscriber card. It means, the person in charge of the Registration Entity has to check out that the certifier indicated in the card is who has signed the certificate.
In case that the Registration Entity does not have telematic registry, the documentation will be printed after being verified the signature and will be sealed with the indication “It is exact copy of an electronic document, which I have verified that the electronic signature is correct". Also it will be necessary that the person in charge of the Registration Entity signs at the foot of the seal.
2) By postal mail:
The person in charge of the subscriber entity makes to arrive at the person in charge of the Registration Entity the documentation in paper signed by the people indicated in the subscriber card.
In case the authentication and authorization of the applicant is not correct, the person in charge of the Registration Entity will reject the request and will send a signed electronic mail to the person in charge of the entity subscriber. Otherwise, the process continues.

1.3.2.6 Verification of the data of server certificates containing public URLs
When receiving requests for server certificates that include a public URL, the person in charge of the ER T-CAT will verify the server URL and the data using the WHO IS service (http://www.whois.net and http://www.internic.net/whois.html for domains .cat). The result will be converted to PDF format and digitally signed. A copy in digital format will be saved and another one will be printed and attached to the request file.
The person in charge will validate that the domain belongs to the same organization that requests the certificate. If it does not, the process must be stopped and the owner of the domain indicated by WHOIS and the responsible for the certificate requesting organization must be contacted in order to validate the correctness of the domain before generating the certificate.

	Otherwise the application also performs automatic controls on the quality of the URL domain, such as: - the automatic validation that the domain is a Fully Qualified Domain Name (FQDN) as the syntax: <subdomain>. <domain>. <tld> , for example: "www.catcert.cat" - it is automatically validated that the URL of the domain is: • not included in the AntiPhishing list www.phishtank.com • not included in any previous certificate issued by CATCert and revoked by phishing reason This anti-phishing control is done in each step of the flow, from the initial request to the final generation, because a domain can enter the anti-phishing lists at any time.
Email Address Verification	Not requesting the email trust bit at this time.
Identity of Code Signing Subscriber	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.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV • Wildcard DV SSL certificates o SSL certs are OV • Email Address Prefixes for DV SSL Certs o SSL certs are OV • Delegation of Domain / Email validation to third parties o 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. o 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 o No. The root signs intermediate certificates, which sign end-entity certs. • Allowing external entities to operate unconstrained subordinate CAs o Comment #27: There are not Sub-CA's operated by third parties. Just the Registration Authorities. • Distributing generated private keys in PKCS#12 files o Not for SSL certs.

	• Certificates referencing hostnames or private IP addresses o Not allowed. • Issuing SSL Certificates for Internal Domains o Not allowed. • OCSP Responses signed by a certificate under a different root o 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 o CRLs imported successfully into Firefox browser. • Generic names for CAs o Root CN is EC-ACC, which stands for Entitat de Certificació de l'Agència Catalana de Certificació