**Bugzilla ID:** 435736
**Bugzilla Summary:** Add Spanish FNMT root certificate

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 | Fábrica Nacional de Moneda y Timbre, FNMT |
| Website URL | http://www.cert.fnmt.es |
| Organizational type | Government |
| Primark Market / Customer Base | Fábrica Nacional de Moneda y Timbre (FNMT) is a government agency that provides services to Spain as a national CA. |
| Inclusion in other major browsers | IE, Safari |
| CA Primary Point of Contact (POC) | https://wiki.mozilla.org/CA:Information_checklist#CA_Primary_Point_of_Contact_.28POC.29<br>POC direct email: rafael.medina@fnmt.es<br>CA Email Alias: ceres@fnmt.es<br>CA Phone Number: 902 181 696<br>Title / Department: Management Information Systems - Department CERES |

## Technical information about each root certificate

| | |
|---|---|
| Certificate Name | AC RAIZ FNMT-RCM |
| Certificate Issuer Field | OU = AC RAIZ FNMT-RCM<br>O = FNMT-RCM<br>C = ES |
| Certificate Summary | This root signs internally-operated sub-CAs which sign end-entity certs. |
| Root Cert URL | http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt<br>FNMT Certificate Repository: https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt |
| SHA1 Fingerprint | B8:65:13:0B:ED:CA:38:D2:7F:69:92:94:20:77:0B:ED:86:EF:BC:10 |
| Valid From | 2008-10-29 GMT |
| Valid To | 2030-01-01 GMT |
| Certificate Version | 3 |
| Cert Signature Algorithm | PKCS #1 SHA-1 With RSA Encryption |
| Signing key parameters | 4096 |
| Test Website URL | https://www.sede.fnmt.gob.es/certificados |
| CRL URL | ldap://ldapfnmt.cert.fnmt.es |

| | |
|---|---|
| OCSP URL | http://ocspape.cert.fnmt.es/ocspape/OcspResponder (URI in AIA of intermediate cert)<br>http://ocspap.cert.fnmt.es/ocspap/OcspResponder (URI in AIA of end-entity cert) |
| Requested Trust Bits | Websites (SSL/TLS)<br>Code Signing |
| SSL Validation Type | OV |
| EV Policy OID(s) | Not requesting EV treatment |
| Non-sequential serial numbers and entropy in cert | Please describe what entropy is used in cert issuance.<br><br>http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html<br>“9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ...<br>- all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number).”<br><br>The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration.<br>This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn’t an acceptable hash algorithm for certificates in this hierarchy. |

**CA Hierarchy information for each root certificate**

| | |
|---|---|
| CA Hierarchy | Is the following still accurate?<br>There are currently two intermediate CAs, "AC Administración Pública" and APE CA. "AC Administración Pública" is an updated version of the “APE CA” in order to meet new requirements from Spanish Goverment about certificates of Public Administrations. Both have 2048 bit keys. |
| Externally Operated SubCAs | None, and none planned. |
| Cross-Signing | None – There is no plan to have this root cert cross-sign with the "FNMT Clase 2 CA"root cert. |
| Technical Constraints on Third-party Issuers | Comment #56: We have RAs that validate information only for citizen certificates but never for SSL server certificates.<br>Comment #91: There aren't third parties that issue SSL or codesigning certificates directly or indirectly. |
| Potential Constraints on this CA Hierarchy. | Mozilla is adding the capability to apply name constraints to root certificates.<br>https://bugzilla.mozilla.org/show_bug.cgi?id=743700<br>Would it be reasonable to constrain certificate issuance within this CA hierarchy to certain domains, such as *.es? |

**Verification Policies and Practices**

| | |
|---|---|
| Policy Documentation | All documents are in Spanish.<br>Document Repository: http://www.cert.fnmt.es/dpcs/<br>Which CPS documents apply to this CA Hierarchy? |
| Audits | Audit Frequency, as documented in the CPS<br>Audit Type: |

| | |
|---|---|
| | Auditor:<br>Auditor Website:<br>URL to Audit Report and Management's Assertions: |
| Baseline Requirements (SSL) | The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.<br>Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results. |
| Responses to CA Communications | https://wiki.mozilla.org/CA:Communications#February_17.2C_2012<br>Response: https://bugzilla.mozilla.org/show_bug.cgi?id=435736#c100<br>https://wiki.mozilla.org/CA:Communications#January_10.2C_2013<br>Response:<br>https://wiki.mozilla.org/CA:Communications#July_30.2C_2013<br>Response: |
| SSL Verification Procedures | Please provide English translations of the sections of publicly-available documentation (such as the CP/CPS) with the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices<br>See section 11.1.1 of the CA/Browser Forum's Baseline Requirements (https://cabforum.org/documents/) |
| Organization Verification Procedures | |
| Email Address Verification Procedures | Not Applicable. Not requesting email trust bit. |
| Code Signing Subscriber Verification Procedures | If you are requesting to enable the Code Signing Trust Bit, then provide (In English, with reference to publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices |
| Multi-factor Authentication | Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices |
| Network Security | Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices |

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

| | |
|---|---|
| Publicly Available CP and CPS | See above. |
| CA Hierarchy | See above. |
| Audit Criteria | See above. |
| Document Handling of IDNs in CP/CPS | ?? |
| Revocation of Compromised Certificates | ?? |

| | |
|---|---|
| Verifying Domain Name Ownership | See above. |
| Verifying Email Address Control | Not applicable. |
| Verifying Identity of Code Signing Certificate Subscriber | See above. |
| DNS names go in SAN | ?? |
| Domain owned by a Natural Person | ?? |
| OCSP | Tested |

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

| | |
|---|---|
| Long-lived DV certificates | Comment #97: "SSL certificates issued by any SubCA chaining to "AC RAIZ FNMT-RCM" root will be valid for a maximum of 3 years" |
| Wildcard DV SSL certificates | Comment #12: FNMT doesn´t issue wildcard certificates. |
| Email Address Prefixes for DV Certs | SSL certs are IV/OV. See above. |
| Delegation of Domain / Email validation to third parties | Comment #56: We have RAs that validate information only for citizen certificates but never for SSL server certificates.<br>Comment #91: There aren't third parties that issue SSL or codesigning certificates directly or indirectly. |
| Issuing end entity certificates directly from roots | This root does not sign end-entity certs directly. |
| Allowing external entities to operate subordinate CAs | Externally-operated sub-CAs are not allowed. |
| Distributing generated private keys in PKCS#12 files | Not allowed. |
| Certificates referencing hostnames or private IP addresses | FNMT-RCM CA doesn´t issue certificates referencing hostnames or private IP addresses. |
| Issuing SSL Certificates for Internal Domains | FNMT-RCM CA doesn´t issue certificates referencing hostnames or private IP addresses. |
| OCSP Responses signed by a certificate under a different root | FNMT-RCM OCSP responses are signed by a certificate issued by the same CA that issues end entity certificates. |
| CRL with critical CIDP Extension | CRLs are LDAP |
| Generic names for CAs | Root name includes "FNMT" |
| Lack of Communication With End Users | ?? |
| Backdating the notBefore date | ?? |