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

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	Fábrica Nacional de Moneda y Timbre, FNMT
Website URL	http://www.cert.fnmt.es
Organizational type	government
Primary market / customer base	Fábrica Nacional de Moneda y Timbre (FNMT) is a government agency that provides services to Spain as a national CA.
CA Contact Information	CA Email Alias: ceres@fnmt.es (rafamdn@gmail.com is the primary FNMT contact contributing info in the bug) CA Phone Number: 902 181 696 Title / Department: Management Information Systems - Department CERES

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**	**Data**
Certificate Name	FNMT Clase 2 CA	AC RAIZ FNMT-RCM
Cert summary / comments	This root has no subordinate CAs, and has modulus length of 1024. FNMT will be transitioning end-entity certs from this root to the new root. However, Spanish users still need the "FNMT Clase 2 CA" because there are more than 2,200,000 certificates issued that will be active for several years.	This is the new root, which the certificates from the "FNMT Clase 2 CA" hierarchy will be transitioned to. This root has modulus length of 4096. This new root signs internally-operated sub-CAs which sign end-entity certs. There is currently one intermediate CA, AC APE, which is 2048-bit.
URL of root cert	http://www.cert.fnmt.es/content/pages_std/certificados/FNMTClase2CA.cer	http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt
SHA-1 fingerprint.	43:F9:B1:10:D5:BA:FD:48:22:52:31:B0:DO:08:2B:37:2F:EF:9A:54	B8:65:13:0B:ED:CA:38:D2:7F:69:92:94:20:77:0B:ED:86:EF:BC:10
Valid from	1999-03-18	2008-10-29
Valid to	2019-03-18	2029-12-31
Cert Version	3	3
Modulus length	1024 Comment #56: We plan to stop issuing certificates under this root in December 2010. Certs are valid for 3 years.	4096

Test Website	https://www.cert.fnmt.es https://www.citaprevia.sanidadmadrid.org/	https://www.agenciatributaria.gob.es/ https://sedemeh.gob.es/ https://www.sede.fnmt.gob.es
CRL	ldap://ldap.cert.fnmt.es I don't think LDAP CRLs are supported in Mozilla products	ldap://ldap.cert.fnmt.es
OCSP Responder URL	http://apus.cert.fnmt.es/appsUsuario/ocsp/OcspResponder There is a OCSP Responder but it's not free. Only FNMT-RCM clients can access that service. Neither of the SSL certs for the test websites have the AIA extension set, so the Firefox browser would not use the OCSP responder.	http://ocspape.cert.fnmt.es/ocspape/OcspResponder For the above test urls when I enforce OCSP I get (Error code: sec_error_bad_database) This usually means that the OCSP responder is responding to the OCSP request with an error code.
CA Hierarchy	There are no subordinate CAs issued by this root. This root CA directly issues end entity certificates.	This new root signs internally-operated sub-CAs which sign end-entity certs.
Externally Operated Sub-CAs	None	None
Cross-Signing	None	None
Requested Trust Bits	Websites Code	Websites Code
SSL Validation Type DV, OV, and/or EV	IV/OV	IV/OV
EV policy OID(s)	Not EV	Not EV
CP/CPS	All documents are in Spanish. All CPS documents: http://www.cert.fnmt.es/dpcs/ CPS of a FNMT's subordinated CA, AC APE: https://bugzilla.mozilla.org/attachment.cgi?id=427559 General CPS applicable to all FNMT's CAs: https://bugzilla.mozilla.org/attachment.cgi?id=427562 CPS of FNMT Clase 2 CA (current Spanish users CA): https://bugzilla.mozilla.org/attachment.cgi?id=427570	
AUDIT	Audit Type: ETSI 101 456 Auditor: BSI Management Systems B.V Auditor Website: http://www.bsi-global.com Audit Report: ? Comment #56: We expect to get the preliminary audit report at 10/03/2010	
Organization Identity Verification	Comment #12: "FNMT-RCM Certification Authority doesn´t issue SSL Certificates with an organization attribute for every entity that request certificates but in the general process of checking documentation authenticity we check that entity legal person is correct." In paragraph V.2 of FNMT-RCM's Certification Practices Statement, Life cycle management of the certificates of components (we call Certificate of Components to SSL-enabled certificates, Code signing certificate and certificates issued for applications	

	that needs authentication each other) are shown the necessary steps for obtaining an SSL Server Certificate. The first one is: The entity interested in applying for a SSL Certificate, must maintain a previous contact with the Royal Spanish Mint (FNMT-RCM) in order to be provided with the information necessary for the issuance of the certificate requested, as well as the forms to be filled. The necessary documents are: • Request Form for SSL Certificate fully completed and signed by the person in charge of Certificate. • Authorization Form for SSL Certificate request for information as a person in charge for it. • Photocopy of National Identity Document, or National Identity Card for Foreigners, with the original valid and in force, from the Responsible of the SSL Certificate. • A document proving the ownership of the domain name or IP address or in case of SSL Certificate for intranets services, internal document proving the intranet name. • Writing Constitution or the Official State Gazette publication for proving the entity legal person, whether private or public. • Certificate Request File in PKCS#10 or SPKAC (Signed Public Key And Challenge) format. Upon receipt of this documentation, the Royal Spanish Mint checks the accuracy and authenticity of all data provided and then process the request.
Domain Name Ownership / Control Nombre de Dominio	Comment #24: We verify domain and the organization identity (at National Trade Registry) Described in Section V.2 of the CPS. English translation provided in Comment #12: The subscriber must provide a document proving the ownership of the domain name or IP address or in case of SSL Certificate for intranets services, internal document proving the intranet name. Upon receipt of this documentation, the Royal Spanish Mint checks the accuracy and authenticity of all data provided and then processes the request. Comment #56: > What CPS document for the AC RAIZ FNMT-RCM root describes the procedures that > must be taken for all SSL end-entity certs issued within its hierarchy in > regards to verifying that the subscriber owns/controls the domain name to be > included in the certificate? > I'll suggest to our Legal Department to include this information in next version of CPS. Currently there is only a sub-ca but in the future will be several sub-cas so we'll include general information about verification procedures (will be equivalent in rigor). Then we'll include specific practices by CA in each sub-ca specific CPS. Comment #56: > Found in translations of CPS of FNMT Clase 2 CA (current Spanish users CA): > “Document proving ownership of the domain name or IP address or internal > document attesting to the Intranet.”

	> How is this information verified? Having the subscriber provide documentation > is not sufficient. The information that is provided by the subscriber needs to > be verified by the CA. The CA needs to have documented/audited procedures for > verifying that the subscriber owns/controls the domain name to be included in > the certificate. That information is verified with responsible entity of managing the registry of Internet domain names (i.e. Red.es in Spain). I'll suggest to our Legal Department to include this information in next version of CPS Comment #56: > Google Translations from CPS of a FNMT's subordinated CA, AC APE: > 145. FNMT-RCM will not, in such Certificate, the responsibility of verifying: > • The authority and competence of the Registry to request a Certificate of > based electronic identification on behalf of the body, agency or entity > administration concerned and certificate holder. > • Ownership of the organ or agency of government on the direction > electronic and / or domain to be included in the Certificate > > This seems to say that FNMT-RCM does not verify that the subscriber owns the > domain name to be included in the certificate. Is this a correct translation? Well, the Spanish Mint is not responsible of verify the ownership of electronic direction. This CA is only for public entities and we have legislation that requires that entities to publish their electronic direction (and ownership) previously in Official State Gazette (BOE). FNMT-RCM verifies publication of this information before issuing certificate. This practice is stablished at internal procedures of FNMT-RCM CA and I'll suggest to our Legal Department to include this information in next version of CPS
Email Address Ownership / Control	Not applicable – not requesting Email trust bit at this time. FNMT may file a new bug if FNMT decides to support S/MIME with certs issued under these roots, and the verification procedures in the CP/CPS meet the requirements of section 7 of http://www.mozilla.org/projects/security/certs/policy/.
Identity of Code Signing Subscriber	Described in Section V.2 of the CPS. English translation provided below. Photocopy of National Identity Document or National Identity Card for Foreigners, with the original valid and in force, from the Responsible of the SSL Certificate.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o Comment #24: “We verify domain and the organization identity (at National Trade Registry)”

	○ SSL certificates issued by FNMT-RCM CA has four year of validity period. • Wildcard DV SSL certificates ○ Comment #12: "FNMT-RCM CA CPS claims that FNMT CA doesn´t issue wildcard certificates". • 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. • Issuing end entity certificates directly from roots ○ Comment #12: "**Yes**. In our current deployment the end entity certificates are issued directly by our root CA. In the new deployment the end entity certificates will be issued by a subordinate CA. Root CA which will be offline". • Allowing external entities to operate unconstrained subordinate CAs ○ No. No subordinate CAs, and not allowed as per FNMT-RCM CA CPS. • Distributing generated private keys in PKCS#12 files ○ Not allowed as per FNMT-RCM CA CPS. • Certificates referencing hostnames or private IP addresses ○ 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"
Translations from CPS of FNMT Clase 2 CA (current Spanish users CA)	V.2. LIFE CYCLE MANAGEMENT CERTIFICATES OF COMPONENTS V.2.1 Component Certificate Request The following describes the application procedure by which personal data are taken from a Certificate Applicant component, confirms the identity of domain ownership and where the ability to make the request on behalf of the entity for which issues a certificate of component and formalizing their contract with the FNMT-RCM for the subsequent issuance of a certificate after completing the component relevant validations. These activities are carried out directly by the Registration Area of the FNMT-RCM. To request these products the requester must be part first of the Electronic Community. The DNI-e (Electronic National ID card, which includes an individual secure certificate itself) computing features will be taken into account for the process, as established by legislation. Prior Contact The entity/organization interested in applying for a Component Certificate must hold a prior meeting with FNMT-RCM to be provided with the necessary information and forms to be completed :

	Upon receiving the documentation, FNMT-RCM verifies the correctness of this information, which in any case must include: • Component Request Form fully completed and signed by the representative in charge of the component. This form can be found in the “Form Models” section. • Form authorizing the request of an electronic component as representative in charge of it. This form can be viewed in the "Form Models" section. • Photocopy of the National ID (or Spanish Resident Foreigner ID) valid and non-expired card of the Representative of the Component. • Document proving ownership of the domain name or IP address or internal document attesting to the Intranet. • Legal constitution registration form (and copy of the creation and publication in a government journal, if applicable) of the Entity/Organization interested, whether it is a public or private one. • PKCS # 10 file of the certificate request component • In the case of a component for Code Signing, for Advanced Client Services or a Generic Electronic Component, the PKCS#10 can be generated and inserted in the infrastructure of the FNMT-RCM following the same process that for the pre-request for Individual People Certificates. The Request Code generated during the pre-request proccess must be attached to the rest of documentation. Processing the request and documentation by FNMT-RCM The FNMT-RCM after receiving the application and relevant documentation, will process the request using its internal software applications. It will generate a contract to submit to the Applicant for his signature, and will sign itself the Component specific request, for processing by FNMT-RCM. Depending on the type of component is specified in the request, the procedure will generate: • In the case of a Web server, a download code after having validated the record, which will be printed for later download the PKCS # 7 or certificate. • In the case of a signature or a code component, once validated record a message confirming the submission. To download the Certificate of components is found, the request code provided by the Applicant. V.2.2 Certificate for component The FNMT-RCM, through its electronic signature, authenticate the certificates. Furthermore, and in order to avoid manipulation of the information contained in the certificates, the FNMT-RCM uses cryptographic mechanisms to provide authentication and integrity to the certificates. The FNMT-RCM act to: · Check that the Certificate Applicant uses the private key corresponding to public key. This FNMT-RCM shall verify that the private key and public key. · Making the information contained in the Certificate is based on information provided by the Applicant.

	· Not ignore known facts that may affect the reliability of the Certificate. · Making the distinguished name assigned in the Certificate is unique in the Public Key Infrastructure FNMT-RCM. For the composition of the distinguished name of the components, we make a division based on whether the component will be a Web Server, Code Signing component or a generic component. The FNMT-RCM will not consider names for the certificates of computer components than those shown here, and so will not consider the particular use of "wildcards" in the distinguished names of certificates of component or in any certificate extensions. Certificate Server with SSL support With the component data collected during the Certificate Application process, we proceed to compose the distinctive name under X.500 standard ensuring that the name makes sense and not give rise to ambiguities. The DN for these certificates is composed of the following: ≡ DN CN, OU, OU, OU, O, C The set of attributes OU, OU, OU, O, C is the branch of the directory where is located the entry for the component in question. The CN attribute containing the name of the web server. The name may be dns or ip and must correspond to the way service invocation. Example: CN = www.ceres.fnmt.es CN = 213.170.35.210 Once made up the distinguished name that identifies the component creates a corresponding entry in the directory making sure that the distinguished name is unique in the entire infrastructure of the certifying authority. Certificate Code Signing components, Client Services and Advanced Computer Components. With the component data collected during the Certificate Application process, we proceed to compose the distinctive name under X.500 standard ensuring that the name makes sense and not give rise to ambiguities. The DN for a user is comprised of the following: ≡ DN CN, OU, OU, OU, O, C The set of attributes OU, OU, OU, O, C is the branch of the directory where is located the entry for the user. The CN attribute containing the identification data of the component that will be responsible for signing code and owner of that component. The syntax of this field depends on the type of user for the case of Code Signing components is: DESCRIPTION CN = d - e ENTITY - CIF 12345678B Where: DESCRIPTION, ENTITY, CIF are labels [1] d is the description of the equipment or software. It is appropriate that this description makes sense. [2] and is the entity that owns the equipment or software [2] 12345678B is the CIF of the owning entity [3], [1] The labels are always capitalized and the value are separated by a space. The value> <etiqueta, pairs are separated

	between them with a blank space, a hyphen and a blank space ("-") [2] With all uppercase characters, except tilde over the letter, which should always be in lowercase. Do not include symbols (commas, etc..) Or accented characters. [3] NIF user = 8 digits + 1 capital letter, without any separation between them. In the case of a user NIF would be smaller than 8 digits, zeros are included at the beginning of the number to complete the 8 figures. Once made up the distinguished name that identifies the component creates a corresponding entry in the directory making sure that the distinguished name is unique in the entire infrastructure of the certifying authority. Composition of alternative identity The alternative identity of the component to which the certificate as provided in this certification policy contains information relating to the entity that owns the component and the natural person acting as responsible. SubjectAltName extension is used as defined in X.509 version 3 to deliver this information. Within this extension, directoryName subfield is used to include a set of attributes defined by the Mint, RCM, which incorporate information about the entity to be certificate subscriber, using the following criteria:
Translations from CPS of a FNMT's subordinated CA, AC APE	11.2. CERTIFICATION PRACTICE RELATING TO THE CERTIFICATES ISSUED VENUES FOR ELECTRONIC IDENTIFICATION OF PUBLIC ADMINISTRATION PUBLIC AGENCIES AND ORGANIZATIONS WORKING OR DEPENDENT 135. The FNMT-RCM in his work as Certification Service Provider and to demonstrate the necessary reliability for the provision of such services, has developed a Certification Practice Statement aimed at the public information on the general conditions of provision of certification services by the FNMT RCM in his capacity as Certification Service Provider. 136. In particular account shall be taken interpretive purposes of this Annex paragraph "Definitions" of the main body of the General Declaration of Practices Certification. 137. The present document brings cause and an integral part of the General Declaration Certification Practices FNMT-RCM and defines the set of particular practices adopted by the FNMT-RCM as Certification Service Provider for the management lifecycle of certificates for electronic identification of sites Public Administration, issued under the Certification Policy of Certification for electronic identification of sites of public administration, agencies and entities associated or dependent public identified with the OID 1.3.6.1.4.1.5734.3.12. 11.2.1. Management Services of the Keys of the Users and Holders 138. The FNMT-RCM in any way generate or store the private keys Holders, which are generated under his sole control and responsibility of the Office of Register whose custody is under your responsibility or, where appropriate, under the responsibility of the person designated by the Registration Office. 11.2.2. Life cycle management of Certificates 11.2.2.1. Register of Holders of Certificates of public domain electronic headquarters 139. As a preliminary to the establishment of any institutional relationship with Owners, FNMT-RCM informed through the media and web addresses cited in this Practice

	and, secondarily, in the General Declaration of Certification Practices, about Terms of Service and the obligations, warranties and responsibilities of the parties involved in the issuance and use of certificates issued by it in its work as Certification Service Provider. 140. The FNMT-RCM in its activity as Certification Service Provider through Registration Offices made the identification of applicants and future Holders requesting certificates for electronic identification of sites by those and procedures are available for this. FNMT-RCM deemed competent to effect any request comes by the head of the Office of Registration concerned which shall be considered representative of the Contractor. 141. The FNMT-RCM applicants seek only that information received from the Office Registration, required for the issuance of certificates and for checking of identity, legitimacy and competence of representatives, storing information required by the electronic signature legislation during the period of fifteen (15) years, treating it with due diligence to comply with national legislation force in the protection of personal data. 142. The FNMT, RCM, given that their activity as Certification Service Provider not generates the key pair of you, put all the necessary mechanisms for the Certificates process to enable the head of the Office of Register and / or representative of the holder is in possession of private key associated with the Public Key is certified. 11.2.2.2. Certificate application procedure for the identification of electronic venues 143. The following describes the procedure for application for Certificate laying takes the official name of the Administration, agency or public entity that will be the Holders of the Certificates, the personal data of the representatives of you, is confirms the identity, validity of office or employment and is formalized, between you and the FNMT-RCM document terms of use or emission standard contract for the subsequent issuance of a Certificate for the electronic identification. 144. It is noted that FNMT-RCM, according to the list of headlines provided by the Administration, an agency or public entity shall consider, under the responsibility of the relevant agencies, and / or entities acting through the Office of Register, which these Headlines meet the requirements of this Declaration and, therefore, have the legitimacy and competence necessary to seek and obtain the Certificate-based electronic identification. The presumed FNMT-RCM with powers and sufficient competition to Owners' representatives entrusted with the responsibility of the Registry. 145. FNMT-RCM will not, in such Certificate, the responsibility of verifying:

	• The authority and competence of the Registry to request a Certificate of based electronic identification on behalf of the body, agency or entity administration concerned and certificate holder. • Ownership of the organ or agency of government on the direction electronic and / or domain to be included in the Certificate • The Certificate Applicant has the status of staff to the Public administration Holder with legitimacy and competence sufficient to initiate the application and act as signatory and / or custodian of the Certificate. 146. Therefore, all verification activities are carried out by the Offices of Registry implemented by the agency or instrumentality of the government as a matter which correspond, in each case, with the agency or certificate holder and e-mail address through which you can access your electronic headquarters. 11.2.2.3. Pre-application 147. The representative of the Contractor which usually is responsible for the Office of Corresponding record in the electronic signature system or device-based insurance equivalent, generates public and private keys to be linked to the Certificate, later became creation data and signature verification respectively. 148. The representative and / or responsible for the Registration Office up an application Electronic Certificate, usually in PKCS # 10, and accesses the website Certification Service Provider, the FNMT, RCM, through the leadership https: / / ape.cert.fnmt.es / PrerregistroSolicitudesComponentesAPE / index.html 149. where it shows a form in which the representative must enter the data Head organ in charge of the electronic platform for which the certificate is issued, and data in its own individual status in charge of keeping diligent the signature creation data. Additionally, the manager must also introduce previously generated electronic application. 150. In response to form submission FNMT-RCM and shall assign the responsibility an application code for use in the Registration Office and at the time of the Certificate request 151. First of all the representative and / or responsible for the Office of Registration and Administration, that Holder should consult the General Declaration of Practices Certification and these Certification Policies and Practices Certification Individuals in the direction http://www.cert.fnmt.es/dpcs/ 152. with the use conditions and obligations for the parties and can perform searches as appropriate, on the scope of this Declaration, all of this without prejudice to

	subsequently, the representative of the Consultant responsible for the Office of Registration and FNMT-RCM, must sign the document in terms of use or if applicable the debt agreement. In any case the continuation of pre-application procedure implies the conclusion of the process. 153. In performing this pre-application is sent to the FNMT-RCM Public Key generated, together with such proof of possession of private key for the subsequent issuance of Certificate. 154. The FNMT, RCM, after receiving this information, checked by the Public Key petitioner the validity of the signed pre-application information, checking only the possession and correspondence of the pair of cryptographic keys by the representative and / or responsible for the registration office. 155. This information will not result in the generation of a certificate by the FNMTRCM, while it does not get signed by the head of the Office of the Register Certificate application. 11.2.2.4. Confirmation of the identities and requirements of Parts 156. The head of the Registration Office will be identified through their national identity or identification document alternative to the FNMT-RCM, by application for registration and use of your own certificates. FNMTRCM presumed responsible for the registration office is in the exercise of competence and capacity to complete the formalities for obtaining this certificates. 11.2.2.5. Impartiality of the Applicant to the Registry Offices 157. In cases other than the involvement of the Head of the Registry Office, for the purposes of obtaining the Certificate, Applicant shall be deemed to legitimation and competition enough to the person designated by the certificate holder of an electronic seat. 158. To obtain the Certificate, Applicant, appearing before an Office of Record designated for that purpose by the agency or certificate holder. 11.2.2.6. Hearing and documentation 159. In cases other than the involvement of the Head of the Registry Office, for the purposes of obtaining the certificate, the representative of the Contractor Applicant is people, and show data is required, and demonstrating, to the Registration Office: • personal identity, • your staff provided the service of body, agency or entity Administration certificate holder and holder of the e-mail through which is accessed to the electronic order Certificate • your condition or designated person authorized to manage the address electronically through which you access the electronic Certificate object

	160. FNMT-RCM will and admit, in any case and report to the function that performs the Office Record designated by the Administration. In the case of failure to demonstrate the points above, the Registration Office will not continue processing the request Certificate. 11.2.2.7. Sending Information to the FNMT-RCM 161. After confirming the identity of the Applicant and force conditions legitimacy and competence required of it, including but not limited to the ownership of email address, be signed document operating conditions or, event contract request by the Applicant on behalf of the Contractor and / or responsible for the Registration Office. The above information and documents will be sent, together with the request code contained in the pre-application phase of the FNMT-RCM. Data Personal and treatment shall be subject to specific legislation. 162. This shipment will only occur if the Registry has legitimacy and competence to so act on behalf of the organ or agency of the Public Administration Certificate of the electronic identification and if this administration holds e-mail address through which you access the electronic object Certificate. 163. The transmission of information to the FNMT-RCM was conducted by communications safety required for that purpose between the Registry and the FNMT-RCM.