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	ldap://ldap.cert.fnmt.es
OCSP Responder URL	http://apus.cert.fnmt.es/appsUsuario/ocsp/OcspResponder	http://ocspape.cert.fnmt.es/ocspape/OcspResponder
	Old (Clase 2) root only: There is an 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.	
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	IV/OV	IV/OV
EV policy OID(s)	Not EV	Not EV
CP/CPS	All documents are in Spanish. Document Repository: http://www.cert.fnmt.es/dpcs/ CPS particular to Component Certificates: http://www.cert.fnmt.es/dpc/dpcc2.pdf CPS of FNMT Clase 2 CA (current Spanish users CA): http://www.cert.fnmt.es/dpc/dpc.pdf General CPS applicable to all FNMT's CAs: http://www.cert.fnmt.es/dpc/dgpc.pdf CPS of a FNMT's subordinated CA, AC APE: http://www.cert.fnmt.es/dpc/ape/dpc.pdf Copy-and-paste enabled, and attached to the bug CPS particular to Component Certificates: https://bugzilla.mozilla.org/attachment.cgi?id=483443 CPS of FNMT Clase 2 CA (current Spanish users CA): https://bugzilla.mozilla.org/attachment.cgi?id=427570 General CPS applicable to all FNMT's CAs: https://bugzilla.mozilla.org/attachment.cgi?id=427562 CPS of a FNMT's subordinated CA, AC APE: https://bugzilla.mozilla.org/attachment.cgi?id=427559	
AUDIT	Audit Type: ETSI 101 456 Auditor: ASIMELEC (Asociación Multisectorial de Empresas de Tecnologías de la Información, Comunicaciones y Electrónica) Auditor Website: http://asimelec.es/ ASIMELEC seal of approval: http://www.asimelec.es/Items/ItemDetail.aspx?ID=3216 (2010.08.27) ASIMELEC scheme is registered in the list of European schemes: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/notification/spain/index_en.htm Audit Statement: https://bugzilla.mozilla.org/attachment.cgi?id=477940 (2010.07.29)	

	-------- Original Message -------- Subject: Re: RV: Confirming Authenticity of Audit Report provided by FNMT Date: Tue, 25 Jan 2011 09:50:52 +0100 From: Julián Inza <julian.inza@interactiva.com.es> To: kwilson@mozilla.com CC: Susana Asensio <susana.asensio@asimelec.es>, 'Francisco Lara' <franlara@asimelec.es> Dear Kathleen, I am Julián Inza, the Chairman (President) of the ASIMELEC CSP Certification Scheme and signer of the statement referred in https://bugzilla.mozilla.org/attachment.cgi?id=477940 I have reviewed completly the audit report issued by auditor company S21Sec, under the rules of the scheme. I have reviewed also all CPS under the scope of the audit and that cover all certification services carried out by FNMT. FNMT-RCM stands out for Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, and is the Spanish Royan Mint, which issues and manages certificates for Government related activities. The summary is as follows: * FNMT Clase 2 CA: is the root CA with which FNMT has been issuing personal certificates for several years. These certificates are managed according to european Directive 1999/93/CE, so this root CA is issuing "qualified certificates" mainly for citizens, and public servants. * AC RAIZ FNMT-RCM: is the new root CA under which the "CA APE" is running. So, APE (which stands for Administración Pública Española - Spanish Government related certificates) is a subordinate CA for AC RAIZ FNMT-RCM. Under APE hierarchy some certificates are designed to fit "sede electrónica" requirements. This means "electronic headquarter" which, in brief, are SSL certificates with additional extensions. Other uses are as qualified certificates for public servants and seal certificates for government agencies. This activity has been specially covered by the audit, so, this root should be included in the Browser Trusted List. * CA FEM: Means "Firma Electrónica Móvil" (Mobile Electronic Signature) and is a special CA for GSM mobile phones certificates, also issued under "qualified certificate" requirements. ASIMELEC audit Scheme for Certification Service Providers (european designation for CAs, Certification Authorities) equals or exceed requirements such as "WebTrust for CAs" and is specially designed to have into account european legislation (Directive 1999/93/CE), and technical requirements such as ETSI TS 101 456, ETSI TS 101 862, ETSI TS 102 280, CWA 14172 (-1, -2 and -3) or CWA 14167-1.

	ASIMELEC is one of the two main Spanish IT Associations, and is the sponsor of the Scheme. It has recently merged with AETIC, the other big association. Together they are now AMETIC, so future compliance statements will be issued by AMETIC which retain all activities of both organitations. ASIMELEC CSP Audit Scheme Web page is available at http://www.asimelec.es/Items/ItemDetail.aspx?ID=993 At this time, information is available in spanish, but we are working in an updated version with the new name of the association that will be available in english. I hope all this information clarifies all what you need. Don´t hesitate to contact me should you need additional information. Best regards, Julian Inza Aldaz Presidente Grupo Interactiva. Blog www.ateneainteractiva.com · Blog www.albalia.com · Blog www.eadtrust.net Blog: blog.inza.com E-Mail: julian.inza@interactiva.com.es Phone: +34 91 7160 555 Phone: +34 902 365 612
Organization Identity Verification	Google Translations from CPS particular to Component Certificates: http://www.cert.fnmt.es/dpc/dpcc2.pdf Copy-and-paste enabled: https://bugzilla.mozilla.org/attachment.cgi?id=483443 Section 5.4.2, Obligations of the Certificate Service Provider: 43. Without prejudice to the legislation on electronic signatures, and its implementing regulations, as well as their specific rules, the Certification Service Provider undertakes to: 44. Prior to the issuance of the Certificate: □ Identify and verify the identity and personal circumstances of the Applicant's Certificate under the provisions of the Certification Practice Statement. In any case certificates issued to minors unless they possess the quality of emancipated. In any case, it will be established in specific legislation regarding the functions envisaged in relation to the effects of DNIe aforementioned □ **In the application process, check the data on the constitution and legal status of the entity and the extent and validity of its powers of representation of the applicant and require the accreditation of the circumstances in which assumptions are based representation.** All these checks will be conducted in accordance with the Certification Practice expressed in this document. In the process of checking the above mentioned points before the FNMT-RCM can perform these checks through the intervention of third parties that hold power notaries, with costs, if these interventions on behalf of stakeholders. □ Verify that all information contained in the certificate request matches that provided by the Applicant.

	□ Check that the Component Responsibility Certificate in possession of the private key will be, once issued the certificate, the signature creation data corresponding to those of Signature Verification Data to be identified in the certificate, and check their complementarity. □ Ensure that the procedures ensure that private keys which are the signature creation data are generated without copies being made or produce the storage by the FNMT-RCM. □ Make disclosure to the person concerned Applicant so as to achieve privacy. □ Make available to the applicant and responsible parties (http://www.ceres.fnmt.es) the Certification Practice Statement and any information that is relevant to the development of procedures related to the lifecycle of this object Certificates Policy in accordance with applicable law. Section 6.1.1, Certificate application process Component: 63. The following describes the application procedure by which personal data are taken from a Certificate Applicant Component, it confirms the identity of domain ownership and where the ability to make the request on behalf of the entity for Certificate is issued Component and formalized its contract with the FNMT-RCM for the subsequent issuance of a Component Certificate after completing the relevant validations. 64. These activities are carried out directly by the Registration Area of the FNMT-RCM. 65. To order these products should be part previously, the Electronic Community. 66. Be taken into account computing functionality planned for the DNIe in accordance with specific legislation. 67. **The body and / or entities interested in applying for a Certificate of component, must maintain contact with the pre-RCM FNMT to be provided with the information necessary for the issuance of the Certificate of component requested, and the forms to be completed .** 68. The Applicant shall make or collect the documentation to be submitted and forwards it to the FNMT-RCM. Upon receiving this documentation, FNMT-RCM checks the correctness of it, which in any case must include: □ Certificate Application Form Component perfectly completed and signed by the Applicant. □ Authorization Form Component Head or his representative to apply for the Certificate of computer components by the Applicant. □ Photocopy of National Identity, National Identity Document or Passport Alien Certificate Applicant component, with the currently valid original. There will need to produce a photocopy of the ID of the applicant provided that the application form stating the authorization FNMT-RCM to consult their personal data in the Data Verification System Identity. □ Document proving ownership of the domain name or IP address or internal document certifying the Intranet. □ If applicable, memorandum and / or copy of agreement to create and, where applicable, documentary proof of registration for the entities concerned, whether public or private. □ File PKCS # 10 certificate request Component □ In the case of a component to Sign Code for Advanced Customer Services and a generic computer component, the PKCS # 10 may be generated and inserted into the infrastructure of the FNMT-RCM following the same process as in the Pre-Application for Certificate of individuals. Documentation must accompany the Request Code generated during the Pre-Application process.
Domain Name	Comment #24: We verify domain and the organization identity (at National Trade Registry)

Ownership / Control Nombre de Dominio	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 #76: As we said, in the cases in which the Certificate includes data like domain names or IP addresses, the FNMT–RCM shall check, via the information systems that the authorised registrars for each case make available to the public, that the documentation required and validated by the Registry Office is correct. For such purpose the publications in the different official state and autonomous region gazettes shall be taken into account, as well as the public registers and the registers accessible by the FNMT-RCM of the different registry bodies of domain names and assignation of IP addresses. Translations From General CPS applicable to all FNMT's CAs: http://www.cert.fnmt.es/dpc/dgpc.pdf "155. In the cases in which the Certificate includes data like domain names or IP addresses, the FNMT–RCM shall check, via the information systems that the authorised registrars for each case make available to the public, that the documentation required and validated by the Registry Office is correct. 156. For such purpose the publications in the different official state and autonomous region gazettes shall be taken into account, as well as the public registers and the registers accessible by the FNMT-RCM of the different registry bodies of domain names and assignation of IP addresses."
Email Address Ownership / Control	Not applicable – not requesting Email trust bit at this time.
Identity of Code Signing Subscriber	As per the translations above, the certificate subscriber must already have an agreement with FNMT. FNMT consults their personal data in their Data Verification System (Sistema de Verificación de Datos de Identidad) and the subscriber must provide national identity documentation.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ Comment #24: “We verify domain and the organization identity (at National Trade Registry)”
	  ○ SSL certificates have four year of validity period.
	• Wildcard DV SSL certificates
	  ○ Comment #12: FNMT 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
	  ○ The old root signs end entity certificates directly, but the new root only signs intermediate CAs.
	• Allowing external entities to operate unconstrained subordinate CAs

	○ No. 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. • 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”