

# Mozilla - CA Program

## Case Information

Case Number	00000012	Case Record Type	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Fábrica Nacional de Moneda y Timbre (FNMT)	Request Status	Need Information from CA

## Additional Case Information

Subject	Include FNMT Root	Case Reason	New Owner/Root inclusion requested
---------	-------------------	-------------	------------------------------------

## Bugzilla Information

Link to Bugzilla Bug	<a href="https://bugzilla.mozilla.org/show_bug.cgi?id=435736">https://bugzilla.mozilla.org/show_bug.cgi?id=435736</a>
----------------------	---

## General information about CA's associated organization

Company Website	<a href="http://www.cert.fnmt.es/">http://www.cert.fnmt.es/</a>	Verified?	Verified
Organizational Type	Government Agency	Verified?	Verified
Organizational Type (Others)	Fábrica Nacional de Moneda y Timbre (FNMT) is a government agency that provides services to Spain as a national CA.	Verified?	Verified
Geographic Focus	Spain	Verified?	Verified
Primary Market / Customer Base	FNMT-RCM, through its CERES Department, provides its clients with the PKI, as well as a full catalogue of services to support the services of administrations and companies, in order to provide them with legal security and validity in a simple and comfortable manner for the citizens.	Verified?	Verified
Impact to Mozilla Users	dgpc_english.pdf: The Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (Royal Spanish Mint), (hereinafter FNMT-RCM), through the CERES (CERTificación ESpañola) (Spanish Certification) Department, in order to provide secure electronic transactions on the Internet, has since 1996 constructed the infrastructure required in order to provide electronic certification services with maximum guarantees. This infrastructure is currently fully operative and tested.	Verified?	Verified

## Response to Mozilla's list of Recommended Practices

Recommended Practices	<a href="https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices">https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices</a>	Recommended Practices Statement	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text
-----------------------	---	---------------------------------	---

box below.

**CA's Response to Recommended Practices**

- \* Use of IDNs isn't allowed
- \* All the domains, including primary name, are included in SAN
- \* We avoid use of "o" field. We use a subject like: c=ES, GivenName=<subscriber\_name>, Surname = <subscriber\_surname>, cn=<domain\_name>

**Verified?** Verified

## Response to Mozilla's list of Potentially Problematic Practices

**Potentially Problematic Practices**

[https://wiki.mozilla.org/CA:Problematic\\_Practices#Potentially\\_problematic\\_CA\\_practices](https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices)

**Problematic Practices Statement**

I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.

**CA's Response to Problematic Practices**

- \* SSL certificates issued by any SubCA chaining to "AC RAIZ FNMT-RCM" root will be valid for a maximum of 3 years
- \* SSL certs are IV/OV.
- \* We have RAs that validate information only for citizen certificates but never for SSL server certificates.
- \* There aren't third parties that issue SSL or codesigning certificates directly or indirectly.
- \* Externally-operated sub-CAs are not allowed.
- \* FNMT-RCM CA doesn't issue certificates referencing hostnames or private IP addresses.

**Verified?** Verified

## Root Case Record # 1

### Root Case Information

**Root Case No** R00000021

**Case Number** 00000012

**Request Status** Need Information from CA

**Root Certificate Name** AC RAIZ FNMT-RCM

### Additional Root Case Information

**Subject** Include "AC RAIZ FNMT-RCM" root

### Technical Information about Root Certificate

<b>O From Issuer Field</b>	FNMT-RCM	<b>Verified?</b>	Verified
<b>OU From Issuer Field</b>	AC RAIZ FNMT-RCM	<b>Verified?</b>	Verified
<b>Certificate Summary</b>	This root has internally-operated subordinate CAs.	<b>Verified?</b>	Verified
<b>Root Certificate Download URL</b>	<a href="http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt">http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt</a>	<b>Verified?</b>	Verified
<b>Valid From</b>	2008 Oct 29	<b>Verified?</b>	Verified
<b>Valid To</b>	2029 Dec 31	<b>Verified?</b>	Verified
<b>Certificate Version</b>	3	<b>Verified?</b>	Verified

<b>Certificate Signature Algorithm</b>	SHA-1	Verified?	Verified
<b>Signing Key Parameters</b>	4096	Verified?	Verified
<b>Test Website URL (SSL) or Example Cert</b>	https://www.sede.fnmt.gob.es/certificados	Verified?	Verified
<b>CRL URL(s)</b>	ldap://dapape.cert.fnmt.es/CN=CRL21,CN=AC%20Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Verified?	Verified
<b>OCSP URL(s)</b>	<a href="http://ocspape.cert.fnmt.es/ocspape/OcspResponder">http://ocspape.cert.fnmt.es/ocspape/OcspResponder</a> <a href="http://ocspap.cert.fnmt.es/ocspap/OcspResponder">http://ocspap.cert.fnmt.es/ocspap/OcspResponder</a>	Verified?	Verified
<b>Trust Bits</b>	Websites	Verified?	Verified
<b>SSL Validation Type</b>	OV	Verified?	Verified
<b>EV Policy OID(s)</b>	Not EV	Verified?	Not Applicable
<b>EV Tested</b>		Verified?	Not Applicable
<b>Root Stores Included In</b>	Apple; Microsoft	Verified?	Verified
<b>Mozilla Applied Constraints</b>	None	Verified?	Verified

### Digital Fingerprint Information

<b>SHA-1 Fingerprint</b>	B8:65:13:0B:ED:CA:38:D2:7F:69:92:94:20:77:0B:ED:86:EF:BC:10	Verified?	Verified
<b>SHA-256 Fingerprint</b>	4D:9E:BB:28:82:5C:96:43:AB:15:D5:4E:5F:96:14:F1:3C:B3:E9:5D:E3:CF:4E:AC:97:13:01:F3:20:F9:22:6E	Verified?	Verified

### CA Hierarchy Information

<b>CA Hierarchy</b>	CA Hierarchy diagram in section 7 of dgpc_english.pdf. Internally-operated subCAs: 1) "AC Componentes Informáticos" issues certificates for SSL Servers and code signing. 2) "AC Administración Pública" is an updated version of the "APE CA" in order to meet new requirements from Spanish Government about certificates of Public Administrations. 3) "APE CA" is no longer used.	Verified?	Verified
<b>Externally Operated SubCAs</b>	None, and none planned	Verified?	Verified
<b>Cross Signing</b>	None, and none planned	Verified?	Verified
<b>Technical Constraint on 3rd party Issuer</b>	* We have RAs that validate information only for citizen certificates but never for SSL server certificates. * There aren't third parties that issue SSL or codesigning certificates directly or indirectly.	Verified?	Verified

## Verification Policies and Practices

<b>Policy Documentation</b>	Documents are in Spanish, and some are translated into English.  dgpc_english.pdf = General Certification Practices Statement  dpc_english.pdf = Specific Certification Policies and Practices applicable to electronic certification and signature services for public organizations and administrations, their bodies and attached or dependent entities  dpc_components_english.pdf = Specific Certification Policy and Practices applicable to AC Software Components -- Policies specific to SSL and Code Signing certs.	<b>Verified?</b>	Verified
<b>CA Document Repository</b>	<a href="https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion">https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	English		
<b>CP</b>	<a href="https://www.sede.fnmt.gob.es/documents/11614/67070/dpc_componentes_english.pdf/">https://www.sede.fnmt.gob.es/documents/11614/67070/dpc_componentes_english.pdf/</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	English		
<b>CPS</b>	<a href="https://www.sede.fnmt.gob.es/documents/11614/137578/dpc_english.pdf/">https://www.sede.fnmt.gob.es/documents/11614/137578/dpc_english.pdf/</a>	<b>Verified?</b>	Verified
<b>Other Relevant Documents</b>	<a href="https://www.sede.fnmt.gob.es/documents/11614/67070/dgpc_english.pdf/">https://www.sede.fnmt.gob.es/documents/11614/67070/dgpc_english.pdf/</a> <a href="https://www.sede.fnmt.gob.es/documents/11614/137578/dpc_english.pdf/">https://www.sede.fnmt.gob.es/documents/11614/137578/dpc_english.pdf/</a> <a href="https://www.sede.fnmt.gob.es/documents/11614/67070/dpc_componentes_english.pdf/">https://www.sede.fnmt.gob.es/documents/11614/67070/dpc_componentes_english.pdf/</a>	<b>Verified?</b>	Verified
<b>Auditor Name</b>	PricewaterhouseCoopers	<b>Verified?</b>	Verified
<b>Auditor Website</b>	<a href="http://www.pwc.es/">http://www.pwc.es/</a>	<b>Verified?</b>	Verified
<b>Auditor Qualifications</b>	<a href="http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx">http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx</a>	<b>Verified?</b>	Verified
<b>Standard Audit</b>	<a href="https://cert.webtrust.org/SealFile?seal=1784&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1784&amp;file=pdf</a>	<b>Verified?</b>	Verified
<b>Standard Audit Type</b>	WebTrust	<b>Verified?</b>	Verified
<b>Standard Audit Statement Date</b>	12/3/2015	<b>Verified?</b>	Verified
<b>BR Audit</b>	<a href="https://cert.webtrust.org/SealFile?seal=1784&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1784&amp;file=pdf</a>	<b>Verified?</b>	Verified
<b>BR Audit Type</b>	WebTrust	<b>Verified?</b>	Verified
<b>BR Audit Statement Date</b>	12/3/2014	<b>Verified?</b>	Verified
<b>EV Audit</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit Type</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit Statement Date</b>		<b>Verified?</b>	Not Applicable

<b>BR Commitment to Comply</b>	I did not find the Commitment to Comply with the BRs in the policy documents. Please point me to where it is documented. i.e how was it disclosed to the auditors? See BRs section 8.3.	<b>Verified?</b>	Need Response From CA
<b>SSL Verification Procedures</b>	dpc_componentes_english.pdf * Section 5.3.2.2, item 48: As regards management of the lifecycle of Component Certificates, FNMT-RCM is the only authorized Registry Office, through its Registry Area. ... To check that the domain title holder's name matches the Subscriber's identity or, if appropriate, to obtain the Subscriber's authorization, which will be associated with the Component Certificate, using the means within its reach that, reasonably, make it possible to prove the title, according to the state of technology. * Section 6.1.3, item 65: If the Certificate is associated with one or more Internet domains, the Registry Office will check, on the authorized domain registrars' databases, that the title holder of the domain and the Certificate Subscriber match, and will keep proof of the inquiry.	<b>Verified?</b>	Verified
<b>EV SSL Verification Procedures</b>	Not requesting EV treatment	<b>Verified?</b>	Not Applicable
<b>Organization Verification Procedures</b>	dpc_componentes_english.pdf * Section 5.3.2.1, item 43: Checking the identity and particulars of the Certificate Applicant and the Subscriber and/or its Representative, and obtaining the representation that the Applicant is authorized by the Subscriber to file the application. ... Identification will be implemented through acceptable electronic signature certificates and the functionalities established in respect of the DNId [electronic ID document] for the above-mentioned purposes. * Section 6.1.3 item 66: The Registry Office will verify the Subscriber's personality and, if appropriate, the Representative's personality and capacity, through verification of the Electronic Signatures and Certificates used in the process and/or inquiry on the databases of the Companies Register or of trustworthy third parties.	<b>Verified?</b>	Verified
<b>Email Address Verification Procedures</b>	Not Requesting Email trust bit	<b>Verified?</b>	Not Applicable
<b>Code Signing Subscriber Verification Pro</b>	QUESTION: Are you requesting the Code Signing trust bit? If yes, please provide the audit statement regarding non-SSL certificates.	<b>Verified?</b>	Need Response From CA
<b>Multi-Factor Authentication</b>	Access to certificate issuance software is secured by using X509 certificates with private keys in a smartcard. So operators (also RA operators) need their smartcard and its associated password in order to issue certificates.	<b>Verified?</b>	Verified

<b>Network Security</b>	<p>We confirm we have performed next actions:</p> <ul style="list-style-type: none"> <li>- Maintaining network security controls that at minimum meet the Network and Certificate System Security Requirements.</li> <li>- Checking for mis-issuance of certificates, especially for high-profile domains.</li> <li>- We have review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.</li> <li>- We have updated our Intrusion Detection System and other monitoring software.</li> <li>- We will be able to shut down certificate issuance quickly if we are alerted of intrusion.</li> </ul>	<b>Verified?</b>	Verified
-------------------------	---	------------------	----------

#### Link to Publicly Disclosed and Audited subordinate CA Certificates

<b>Publicly Disclosed &amp; Audited subCAs</b>	All subCAs are disclosed in the dgpc_english.pdf document.	<b>Verified?</b>	Verified
--	--	------------------	----------