

Mozilla - CA Program

Case Information

Case Number	00000012	Case Record Type	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Fábrica Nacional de Moneda y Timbre (FNMT)	Request Status	Ready for Public Discussion

Additional Case Information

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

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=435736
----------------------	---

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	http://www.cert.fnmt.es/	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	https://wiki.mozilla.org	Recommended Practices Statement	I have reviewed Mozilla's list of
-----------------------	---	---------------------------------	-----------------------------------

/CA:Recommended_Practices#CA_Recommended_Practices

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

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 Certificate Name	AC RAIZ FNMT-RCM	Root Case No	R00000021
Request Status	Ready for Public Discussion	Case Number	00000012

Additional Root Case Information

Subject Include "AC RAIZ FNMT-RCM" root

Technical Information about Root Certificate

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

Certificate Version	3	Verified?	Verified
Certificate Signature Algorithm	SHA-256	Verified?	Verified
Signing Key Parameters	4096	Verified?	Verified
Test Website URL (SSL) or Example Cert	https://www.sede.fnmt.gob.es/certificados	Verified?	Verified
CRL URL(s)	ldap://ldapape.cert.fnmt.es/CN=CRL164,CN=AC%20Administraci%F3n%20P%FABlica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList ;	Verified?	Verified
OCSP URL(s)	http://ocspape.cert.fnmt.es/ocspape/OcspResponder http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Verified?	Verified
Revocation Tested	http://certificate.revocationcheck.com/www.sede.fnmt.gob.es Errors resolved with POST. Error with GET appears to be an issue with the revocation checker.	Verified?	Verified
Trust Bits	Code; Websites	Verified?	Verified
SSL Validation Type	OV	Verified?	Verified
EV Policy OID(s)	Not EV	Verified?	Not Applicable
EV Tested		Verified?	Not Applicable
Root Stores Included In	Apple; Microsoft	Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	EC:50:35:07:B2:15:C4:95:62:19:E2:A8:9A:5B:42:99:2C:4C:2C:20	Verified?	Verified
SHA-256 Fingerprint	EB:C5:57:0C:29:01:8C:4D:67:B1:AA:12:7B:AF:12:F7:03:B4:61:1E:BC:17:B7:DA:B5:57:38:94:17:9B:93:FA	Verified?	Verified

CA Hierarchy Information

CA Hierarchy	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
Externally Operated SubCAs	None, and none planned	Verified?	Verified
Cross Signing	None, and none planned	Verified?	Verified

**Technical Constraint
on 3rd party Issuer**

* 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

Policy Documentation Documents are in Spanish, and some are translated into English. **Verified?** Verified

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.

CA Document Repository <https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion>

Verified? Verified

CP Doc Language English

CP https://www.sede.fnmt.gob.es/documents/11614/67070/dpc_componentes_english.pdf/

Verified? Verified

CP Doc Language English

CPS https://www.sede.fnmt.gob.es/documents/11614/137578/dpc_english.pdf/

Verified? Verified

Other Relevant Documents https://www.sede.fnmt.gob.es/documents/11614/67070/dgpc_english.pdf/
https://www.sede.fnmt.gob.es/documents/11614/137578/dpc_english.pdf/
https://www.sede.fnmt.gob.es/documents/11614/67070/dpc_componentes_english.pdf/

Verified? Verified

Updated CPS attached to bug February 2015:
<https://bug435736.bugzilla.mozilla.org/attachment.cgi?id=8565442>

Auditor Name PricewaterhouseCoopers

Verified? Verified

Auditor Website <http://www.pwc.es/>

Verified? Verified

Auditor Qualifications <http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx>

Verified? Verified

Standard Audit https://www.cert.fnmt.es/documents/11601/4379265/auditReport_en.pdf

Verified? Verified

Standard Audit Type WebTrust

Verified? Verified

Standard Audit Statement Date 5/4/2014

Verified? Verified

BR Audit	https://cert.webtrust.org/SealFile?seal=1784&file=pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	12/3/2014	Verified?	Verified
EV Audit		Verified?	Not Applicable
EV Audit Type		Verified?	Not Applicable
EV Audit Statement Date		Verified?	Not Applicable
BR Commitment to Comply	CPS section 10, item 171.	Verified?	Verified
SSL Verification Procedures	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.	Verified?	Verified
EV SSL Verification Procedures	Not requesting EV treatment	Verified?	Not Applicable
Organization Verification Procedures	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.	Verified?	Verified
Email Address Verification Procedures	Not Requesting Email trust bit	Verified?	Not Applicable
Code Signing Subscriber Verification Pro	dpc_componentes_english.pdf * Section 5.3.2.1, item 43: In the registration process, verifying the data concerning the Subscriber's legal personality and the Representative's	Verified?	Verified

capacity. These verification measures must be implemented according to the Specific Certificate Practices contained in this document and following the FNMT-RCM registration procedures. In the process for verification of the above-mentioned data, FNMT-RCM may verify said data through third parties that have the authority to attest or through public or private record and register offices.

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

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	All subCAs are disclosed in the dgpc_english.pdf document.	Verified?	Verified
--	--	------------------	----------