Technical information about each root certificate	
Non-sequential serial numbers and entropy in cert	We use aleatory serial numbers. Having 16 bytes = 180 entropy bits.
CA Hierarchy information for each root certificate	
CA Hierarchy	There are currently two intermediate CAs, "AC Administración Pública", APE CA and “AC Componentes Informáticos”. "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. Both have 2048 bit keys. “APE CA” is no longer used. “AC Componentes Informáticos” is a new CA that issue certificates for SSL Servers and code signing
Potential Constraints On this CA Hierarchy	Mozilla is adding the capability to apply name constraints to root certificates. Would it be reasonable to constrain certificate issuance within this CA hierarchy to certain domains, such as *.es? **NO**
Verification Policies and Practices	
Audits	Audit frecuency: Yearly Audit Type: ETSI/WebTrust Auditor: PricewaterhouseCoopers Auditores, S.L. Auditor Website: www.pwc.com/es URL to Audit Report and Management’s Assertions: https://cert.webtrust.org/ViewSeal?id=1784
Baseline Requirementes (SSL)	See Audit Report at : https://cert.webtrust.org/SealFile?seal=1784&file=pdf
Responses to CA Comunications	N/A??
SSL Verification procedures	See section 6.1 (Component certificate lifecycle management) at https://www.sede.fnmt.gob.es/documents/11614/67070/dpc_componentes_english.pdf This doc is attached at: https://bugzilla.mozilla.org/show_bug.cgi?id=435736
Code Signing Suscriber Verification	See section 6.1 (Component certificate lifecycle management) at https://www.sede.fnmt.gob.es/documents/11614/67070/dpc_componentes_english.pdf

Procedures	This doc is attached at: https://bugzilla.mozilla.org/show_bug.cgi?id=435736
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.
Network Security	We confirm we have performed next actions: • 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.
Response to Mozilla's CA Recommended Practices	
Document Handling of IDNs	Use of IDNs isn't allowed
Revocation of Compromised Certificates	Compromised certificates will be revoked. Revocation shall take effect as from the date that FNMT-RCM has evidence of any determining facts.
DNS names go in SAN	Yes. All the domains, included primary name, are included in SAN
Domain owned by a Natural Person	We avoid use of "o" field. We use a subject like: c=ES, GivenName=<suscriber_name>, Surname = <subscriber_surname>, cn=<domain_name>
Response to Mozilla's list of Potentially Problematic Practices	
Lack of Communication With End Users	we have several ways to contact us: web form, email and Call-Center
Backdating the notBefore date	No. notBefore date value is setting with the date the certificate is issued.