Print this page

Mozilla - CA Program

Case Information

Case Number	00000058	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Consejo General de la Abogacia Española (CGAE)	**Request Status**	Initial Request Received

Additional Case Information

Subject	Include new CA, CGAE, and root	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1130333

General information about CA's associated organization

Company Website	http://www.acabogacia.org/acabogacia	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Spain	**Verified?**	Verified
Primary Market / Customer Base	In its capacity as the entity regulating the Spanish Bar Associations, the National Council of Spanish Bar Associations (CGAE) has the status of public corporation, and has established its own certification system for the purpose of issuing certificates for diverse uses and different end users.	**Verified?**	Verified
Impact to Mozilla Users	Certificates are issued to end entities, including Bar members, administrative and service personnel, organisations and natural persons representing said organisation. The Primary geographical área is Spain, but some certificates are issued for other European Countries.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**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	NEED: Please review and respond to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices) - Publicly Available CP and CPS - CA Hierarchy - Audit Criteria - Document Handling of IDNs in CP/CPS - Revocation of Compromised Certificates - Verifying Domain Name Ownership - Verifying Email Address Control - Verifying Identity of Code Signing Certificate Subscriber - DNS names go in SAN - Domain owned by a Natural Person	**Verified?**	Need Response From CA

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	NEED: Please review and respond to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices) - Long-lived DV certificates - Wildcard DV SSL certificates - Email Address Prefixes for DV Certs -- If DV SSL certs, then list the acceptable email addresses that are used for verification. - Delegation of Domain / Email validation to third parties - Issuing end entity certificates directly from roots - Allowing external entities to operate subordinate CAs - Distributing generated private keys in PKCS#12 files - Certificates referencing hostnames or private IP addresses - Issuing SSL Certificates for Internal Domains - OCSP Responses signed by a certificate under a different root - SHA-1 Certificates - Generic names for CAs - Lack of Communication With End Users - Backdating the notBefore date	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Autoridad de Certificacion de la Abogacia	**Root Case No**	R00000075
Request Status	Initial Request Received	**Case Number**	00000058

Additional Root Case Information

Subject	Include Autoridad de Certificacion de la Abogacia root cert

Technical Information about Root Certificate

O From Issuer Field	Consejo General de la Abogacia NIF:Q-	**Verified?**	Verified

	2863006I		
OU From Issuer Field		**Verified?**	Verified
Certificate Summary		**Verified?**	Need Response From CA
Root Certificate Download URL	https://bugzilla.mozilla.org /attachment.cgi?id=8562410	**Verified?**	Verified
Valid From	2005 Jun 13	**Verified?**	Verified
Valid To	2030 Jun 13	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-1	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://www.icahuelva.es/ NEED: Must serve up intermediate certs along with SSL cert. Error code: sec_error_unknown_issuer	**Verified?**	Need Response From CA
CRL URL(s)	http://www.acabogacia.org /crl/acabogacia.crl http://www.acabogacia.org /crl/ACAcorporativos.crl http://www.acabogacia.org /crl/ACAcorporativosV2.crl http://www.acabogacia.org /crl/ACAtrustedV2.crl End-entity CRLS: issued every 12 hours and when they suffer a change of status.	**Verified?**	Verified
OCSP URL(s)	NEED: the AIA in end-entity certs must have the OCSP URI. OCSP URL:http://ocsp.redabogacia.org	**Verified?**	Need Response From CA
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Please consider the types of SSL certificates that need to be issued within this CA hierarchy, and if applicable provide a list of names to constrain the CA hierarchy to. Constraints may look like: *.us, *.gov.us, *.gov, *.mil	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	7F:8A:77:83:6B:DC:6D:06:8F:8B:07:37:FC:C5:72:54:13:06:8C:A4	**Verified?**	Verified
SHA-256 Fingerprint	56:07:E2:60:16:3F:49:C8:EA:41:75:A1:C0:A5:3B:13:19:5C:B7:D0:78:45:61:1E:94:3A:2F:F5:07:03:68:34	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	"Autoridad de Certificación de la Abogacía" root CA has two subordinated CAs: 1) ACA – Corporate Certificates 2014 2) ACA – Trusted Certificates 2014 Diferent end users certificates are issued by the Subordinated CAs under their own certification Policy.	**Verified?**	Verified
Externally Operated SubCAs	NEED: Response to https://wiki.mozilla.org/CA:SubordinateCA_checklist NEED Clarification. Are there any externally-operated subCAs? Do the CP/CPS documents allow there to be externally-operated subCAs in the future? If yes, please clarify how Mozilla Policy and the Baseline Requirements will be met/enforced. CPS section 1.3.2: The functions of the CSP may be exercised directly by the AC or by a delegated entity.	**Verified?**	Need Response From CA
Cross Signing	NEED Clarification. Has this root been involved in cross-signing with any other root certificates? Are there any plans to do so?	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED Clarification. Can external RAs cause the direct issuance of SSL certificates? How are external RAs constrained and/or audited/monitored? CPS section 1.3.3: RA ... Any other entity delegated by the CA upon the signing of a contract. In Spain, only Bar Associations may be Registrars for their members since said Bar Associations have the exclusive certifying capacity in respect of the status of lawyer. CPS section 3.1.9: Identity Authentication of the Registration Authority's Operators	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	Documents are in Spanish and English. Spanish versions: CPS: https://documentacion.redabogacia.org/docushare/dsweb/Get/Document-8729746/CPS_ACA_013.0.pdf Corporate Certificates CP: https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-11967 Server Certs CP: https://documentacion.redabogacia.org/docushare/dsweb/Get/Document-102302/CP3_ACA_002.pdf Corporate Trusted Certificates: https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-11968	**Verified?**	Verified

CA Document Repository	https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-1001	**Verified?**	Verified
CP Doc Language	English		
CP	https://documentacion.redabogacia.org/docushare/dsweb/Get/Document-3349164/CP3_ACA_002.0_GB.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://documentacion.redabogacia.org/docushare/dsweb/Get/Document-3349086/CPS_ACA_012.0_EN.pdf	**Verified?**	Verified
Other Relevant Documents	English versions: Corporate Certificates CP documents: https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-52979 Server Certs CP: https://documentacion.redabogacia.org/docushare/dsweb/Get/Document-3349164/CP3_ACA_002.0_GB.pdf Qualified Certs CP: https://documentacion.redabogacia.org/docushare/dsweb/Get/Document-3349169/CP_2ACA_006.0_GB.pdf	**Verified?**	Verified
Auditor Name	Ernst & Young (EY)	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1330&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	11/20/2014	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1330&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	11/20/2014	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED: The CA's CP or CPS documents must include a commitment to comply with the BRs, as described in Baseline Requirements section 8.3. Please carefully review this page with your auditor: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
EV SSL Verification Procedures	Not requesting EV treatement	**Verified?**	Not Applicable
Organization Verification Procedures	CPS section 3.1.8	**Verified?**	Verified
Email Address Verification Procedures	NEED: all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Code Signing Subscriber Verification Pro	Not requesting Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED: Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED: Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED: Provide URL to publicly disclosed and audited subCAs as per item #5 of https://wiki.mozilla.org/CA:Communications#May_13.2C_2014	**Verified?**	Need Response From CA