Bugzilla ID: 986854
Bugzilla Summary: Add Renewed AC Camerfirma root certificate.

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Camerfirma
Website URL	http://www.camerfirma.com
Organizational type	Private Company, Commercial CA, Regional CA in Spain
Primark Market / Customer Base	AC Camerfirma S.A. is a commercial CA issuing certificates for companies primarily in Spain. Camerfirma is the digital certification authority for Chambers of Commerce in Spain.
Inclusion in other major browsers	Yes, IE.
CA Primary Point of Contact (POC)	https://wiki.mozilla.org/CA:Information_checklist#CA_Primary_Point_of_Contact_.28POC.29 POC direct email: ramirom@camerfirma.com Email Alias: gestion_soporte@camerfirma.com CA Phone Number: 349 13 443743

Technical information about each root certificate

Certificate Name	Chambers of Commerce Root - 2008	Global Chambersign Root - 2008
Certificate Issuer Field	CN = Chambers of Commerce Root - 2008 O = AC Camerfirma S.A. Object Identifier (2 5 4 5) = A82743287 L = Madrid (see current address at www.camerfirma.com/address) C = EU	CN = Global Chambersign Root - 2008 O = AC Camerfirma S.A. Object Identifier (2 5 4 5) = A82743287 L = Madrid (see current address at www.camerfirma.com/address) C = EU
Certificate Summary	There is a "Chambers of Commerce Root - 2008" root certificate currently included in NSS, which is SHA-1 4096-bit. This new root is SHA-256 4096-bit. This root will have internally-operated subordinate CAs that issue certificates for Spanish companies and representatives. Chambers of Commerce act as RAs for end user registration.	There is a "Global Chambersign Root - 2008" root certificate currently included in NSS, which is SHA-1 4096-bit. This new root is SHA-256 4096-bit. This root will have internally-operated subordinate CAs that issue certificates for general use globally. Other companies act as RAs for end user registration.
Number of Included Roots	Can the "Chambers of Commerce Root" SHA-1 2048-bit root certificate be removed now? SHA1 Fingerprint: 6E:3A:55:A4:19:0C:19:5C:93:84:3C:C0:DB:72:2E:31:30:61:F0:B1	Can the "Global Chambersign Root" SHA-1 2048-bit root certificate be removed now? SHA1 Fingerprint: 33:9B:6B:14:50:24:9B:55:7A:01:87:72:84:D9:E0:2F:C3:D2:D8:E9

Root Cert URL	http://www.camerfirma.com/certs/root_chambers-2008_sha256.crt	http://www.camerfirma.com/certs/root_chambersign-2008_sha256.crt
SHA1 Fingerprint	CD:03:B4:68:30:48:E3:64:B8:E9:F7:ED:D9:4C:78:74:7C:39:51:CA	D6:47:D9:EA:99:4A:1B:D5:D8:C3:CF:FF:78:D6:9A:99:BD:45:CA:D4
Valid From	2011-12-07	2011-12-07
Valid To	2038-07-31	2038-07-31
Certificate Version	3	3
Certificate Signature Algorithm	SHA-256	SHA-256
Signing key parameters	4096	4096
Test Website URL (SSL)	URL to website whose SSL cert chains up to this root	URL to website whose SSL cert chains up to this root
CRL URL	URL NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS.	CRL NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS.
OCSP URL	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	e.g. DV, OV, and/or EV	
EV Policy OID(s)	1.3.6.1.4.1.17326.10.14.2.1.2 Attach screenshot to bug showing successful EV test https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	1.3.6.1.4.1.17326.10.14.2.1.2 Attach screenshot to bug showing successful EV test https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: … - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)." The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: … - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)." The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the

	Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration. This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn't an acceptable hash algorithm for certificates in this hierarchy.	Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration. This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn't an acceptable hash algorithm for certificates in this hierarchy.

CA Hierarchy information for each root certificate

CA Hierarchy	List, description, and/or diagram of all intermediate CAs signed by this root. Identify which subCAs are internally-operated and which are externally operated.
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.
Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate. If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: http://policy.camerfirma.com/ CP: CPS: Relying Party Agreement:
Audits	Audit Type: WebTrust for CA Auditor: Ernst & Young (www.ey.com/es) Audit Report: https://cert.webtrust.org/SealFile?seal=1570&file=pdf (2013.06.18) Audit Type: WebTrust for EV Auditor: Ernst & Young (www.ey.com/es) Audit Report: https://cert.webtrust.org/SealFile?seal=1573&file=pdf (2013.06.18)
Baseline Requirements (SSL)	URL to BR audit statement: https://cert.webtrust.org/SealFile?seal=1570&file=pdf The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.

SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Organization Verification Procedures	
Email Address Verification Procedures	If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Multi-factor Authentication	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
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Response 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	
OCSP	

Response 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	
CRL with critical CIDP Extension	
Generic names for CAs	
Lack of Communication With End Users	
Backdating the notBefore date	