Bugzilla ID: 401262
Bugzilla Summary: Add Certicámara S.A. root CA cert

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	**Data**
CA Name	Certicámara S.A. Sociedad Cameral de Certificación Digital - Certicámara S.A.
Website URL (English version)	www.certicamara.com http://www.certicamara.com/index.php?option=com_content&task=category&sectionid=10
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Commercial
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	Sociedad Cameral de Certificación Digital - Certicámara S.A. is a commercial CA primarily serving the Colombia and Andean Region.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**	**Data**
Certificate Name	Certificado Empresarial Clase-A	AC Raíz Certicámara S.A.
Cert summary / comments	This is the original root which expires in 2011. Certicámara requests that this root also be added to the NSS database because they have a significant number of customers that use it, and their certificates expire in 2010. End entity certificates have been issued directly from this root, rather than using an offline root and issuing certs through a subordinate CA.	This is a new root CA certificate authorized by Industry and Commerce Department of Colombia, to replace the Certificado Empresarial Clase-A root certificate. This root has one internally operated subordinate CA.
The root CA certificate URL	http://www.certicamara.com/certicamara.crt	http://www.certicamara.com/ac_offline_raiz_certicamara.crt
SHA-1 fingerprint.	8b:1a:11:06:b8:e2:6b:23:29:80:fd:65:2e:61:81:37:64:41:fd:11	CB:A1:C5:F8:B0:E3:5E:B8:B9:45:12:D3:F9:34:A2:E9:06:10:D3:36
Valid from	5/23/2001	11/27/2006
Valid to	5/23/2011	4/2/2030

Cert Version	3	3
Modulus length	2048	4096
CRL URL	http://www.certicamara.com/certicamara.crl http://www.certicamara.com/certs/certicamara.crl	http://www.certicamara.com/repositoriorevocaciones/ac_raiz_certicamara.crl
CRL update frequency for end-entity certificates	CPS page 27: The CRLs generated by Certicámara have a validity period of 3 days. Certicámara reissues and publishes the CRL every time when a certificate is revoked or before CRL expiration, if there are no revocation requests.	
OCSP Responder URL	Not applicable	Not applicable
List or description of subordinate CAs operated by the CA organization associated with the root CA.	None	One subordinate CA, internally operated: http://www.certicamara.com/ac_online_subordinada_certicamara.crt URL of certificate hierarchy diagram: http://www.certicamara.com/certificate_hierarchy_diagram.jpg
For subordinate CAs operated by third parties, if any:	None	None
List any other root CAs that have issued cross-signing certificates for this root CA	None	None
Requested Trust Bits One or more of: • Websites • Email • Code Signing	Websites Email Code	Websites Email Code
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • DV • OV	OV CPS page 45: Verification of identity and representation Additional terms of the general part of the certification practice statement, the Bank of Registration confirm the legal capacity to act for and on behalf of the person or legal entity's State. This check is done by checking the certificate of existence and legal representation the legal person, the nomination paper or any equivalent. CPS page 46: Certicámara verifies the domain name referenced in the certificate or petition using a query to a whois service,	

	may request additional documentation Certicámara that proves the authenticity of the applicant's control over the domain to be secured by digital certificate issued by Certicámara. If the ownership and control of a domain name changes, Subscriber must notify the changes and has the sole responsibility of the unauthorized use of the SSL certificate issued for the domain, additionally has the responsibility to request the revocation of the certificate SSL domain if the property or any of the attributes certified Certicámara is changed. From Certicámara: The verification performed to issue SSL certificates chaining up is ORGANIZATIONALLY VALIDATED (OV), establishing to Certicámara to verify that the organization attribute is verified to be that associated with the certificate subscriber. Certicámara verifies the domain name referenced in the certificate/request by use whois services, also Certicámara can request additional documentation that probe the authenticity of the requester control over the domain to be secured by a digital certificate issued by Certicámara. If ownership and control of a domain name changes, the subscriber must notify to Certicámara that changes and have the entirely responsibility of unauthorized use of the SSL certificate issue for the domain, also have the responsibility of request the revocation of the issued SSL certificate when the ownership or any other attribute changes	
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable.	https://www.superfinanciera.gov.co	https://www.certicamara.com/index.php Need to also install the subordinate-CA: http://www.certicamara.com/ac_online_subordinada_certicamara.crt
CP/CPS	Certification Practices Statement (CPS) – in Spanish http://www.certicamara.com/templates/cc/images/dpc/DPCMarzo_09.pdf Certicámara Documentation http://www.certicamara.com/index.php?option=com_content&task=category&sectionid=22	
AUDIT	Audit Type (WebTrust, ETSI etc.): WebTrust Auditor: Deloitte & Touche Auditor Website: www.deloitte.com Audit Document URL(s): https://cert.webtrust.org/SealFile?seal=750&file=pdf (3/31/2008)	

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL
    - CPS page 46: Certicámara verifies the domain name referenced in the certificate or petition using a query to a whois service, may request additional documentation Certicámara that proves the authenticity of the applicant's control over the domain to be secured by digital certificate issued by Certicámara. If the ownership and control of a domain name changes, Subscriber must notify the changes and has the sole responsibility of the unauthorized use of the SSL certificate issued for the domain, additionally has the responsibility to request the revocation of the certificate SSL domain if the property or any of the attributes certified Certicámara is changed.
    - From Certicámara:
        - "The owner of this kind of digital certificate is the person that is included into the digital certificate and was confirm through its legal representative that has the owner rights over determinate domain in Internet. The SSL certificates bring a technical security to the domains which are establishing a communication."
        - "The verification performed to issue SSL certificates chaining up is ORGANIZATIONALLY VALIDATED (OV), establishing to Certicámara to verify that the organization attribute is verified to be that associated with the certificate subscriber. Certicámara verifies the domain name referenced in the certificate/request by use whois services, also Certicámara can request additional documentation that probe the authenticity of the requester control over the domain to be secured by a digital certificate issued by Certicámara."
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - From Certicámara: Certicámara verifies the associated email address provided by the requester through a verification process based on an email confirmation message replayed by the requester with personal and confidential information. Then, this information is validated in a personal or impersonal (phone) way. Also in the CPS we include the following text: "Every requester must provide to registration entity a valid and effective e-mail address that must be hastened in the digital certificate request form appropriate field.
    - CPS page 19: All Applicants must provide the repository a valid email address and force, which must be processed in the space provided on the application form provision of digital certification. NETWORKING AND COMMUNICATIONS TO BE MADE BY MEANS OF MAIL E CERTICÁMARA and Subscriber shall be given THROUGH THE E-MAIL ADDRESS PROVIDED BY THE SUBSCRIBER IN APPLICATION FORM FOR PROVISION OF DIGITAL CERTIFICATES. EL SUBSCRIBER IS RESPONSIBLE FOR THE VALIDITY AND EFFECT OF THE MAIL ACCOUNT ELECTRONIC CERTICÁMARA DELIVERED TO THE RECEIPT OF CORRECT INFORMATION AND COMMUNICATIONS. All applicants must marshal, along with the form of provision of certification services digital certificate digital connection, a copy of your certificate of citizenship or documents equivalent.
- Verify identity info in code signing certs is that of subscriber
    - From Certicámara: Certicámara in addition of the basis verify process; include the following translated text:"3.1. Identity verification -- In addition to the established in the general section of this CPS, the registration entity must check the identity of the requester-subscriber through the review of the request documentation given by requester to demonstrate the information about qualifies as entity or person that demonstrates their activities as development, design, programming, maintenance, distribution of software, applications, source code or object code, or affinities."

- CPS page 49, Verification of identity: In addition to the provisions of part of this certification practice statement, the Bank of Registration as a professional will check the applicant's qualification-subscriber through the revision of the content and the nature of the documentation submitted by the applicant to prove his quality professional entitled.

Flag Problematic Practices (COMPLETE)
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
  - SSL certs are OV
  - CPS page 46: Certicámara issues certificates to validate organizational OV, which is possible by the issuance of licenses long term, but the validity period should not exceed three (3) years from the date of emission.
- Wildcard DV SSL certificates
  - SSL certs are OV
  - Certicámara issued wildcard certificates off of the old root, but as of 2008 they do not issue any more wildcard certs. Certicámara does validate the organizational identity (OV) for SSL certs.
- Issuing end entity certificates directly from roots
  - End entity certificates were directly issued from the old root rather than using an offline root and issuing certs through a subordinate CA. This has been fixed with the new root.
    - **The Certificado Empresarial Clase-A root issues end entity certificates directly.**
    - The new AC Raíz Certicámara S.A. root issued a subordinate CA to issue end entity certificates.
- Allowing external entities to operate unconstrained subordinate CAs
  - No
- Distributing generated private keys in PKCS#12 files
  - No
  - CPS page 45: The Subscriber shall at all times to ensure the confidentiality of the private key, regardless of use of the hardware of the digital certificate. To this end, shall take all measures necessary for access to the hardware of the digital certificate is strictly restricted.
- Certificates referencing hostnames or private IP addresses
  - Not found
- OCSP Responses signed by a certificate under a different root
  - No OCSP
- CRL with critical CIDP Extension
  - CRLs imported without error into Firefox

Verify Audits (COMPLETE)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - On WebTrust site
- For EV CA's, verify current WebTrust EV Audit done.
    - Not applicable
- Review Audit to flag any issues noted in the report
    - COMPLETE