Bugzilla ID: 545614
Bugzilla Summary: Add Certinomis 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.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	Certinomis
Website URL	http://www.certinomis.com
Organizational type	Commercial CA
Primary market / customer base	Certinomis is a commercial CA that delivers certificates to the general public in France, and is the Certificate Service Provider of "La Poste" the French Postal Service.
CA Contact Information	CA Email Alias: Please provide an email alias that includes the people in your company who should receive correspondence from Mozilla in regards to root certificates. An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. CA Phone Number: A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. Title / Department: If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?

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

Info Needed	Data
Certificate Name	Certinomis - Autorité Racine
Cert summary / comments	
Root certificate URL	http://www.certinomis.com/publi/rgs/ac-racine-g2.cer
SHA-1 fingerprint	2e:14:da:ec:28:f0:fa:1e:8e:38:9a:4e:ab:eb:26:c0:0a:d3:83:c3
Valid from	2008-09-17
Valid to	2028-09-17
Cert Version	3
Modulus length / key length	4096

Test Website	For testing purposes, please provide a URL to a website whose SSL cert chains up to this root. Note that this can be a test site.
CRL URL	ARL: http://crl.certinomis.com/AC_Racine/crl/crl-1.crl CRL for end-entity certs: NextUpdate:
OCSP Responder URL	Not provided
CA Hierarchy	This root has 3 sub-CAs. Are these all internally operated? "1 étoile" software or token, no face-to-face. (Class 1: Certificate issued upon verification of the e-mail) "2 étoiles" only crypto token with face-to-face (Class 2: Certificate issued upon verification of documents) "Corporate" for BtoB purpose. (Class 3: Certificate issued on vouchers, with identity checks face to face)
Externally Operated sub-CAs	Does this root have any subordinate CAs that are operated by external third parties? For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. Also, see https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List any other root CAs that have issued cross-signing certificates for this root CA
Requested Trust Bits	Please indicate which trust bits you would like to enable for this root. One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing
SSL Validation Type DV, OV, and/or EV	Do you perform identity/organization verification for all SSL certificates? Is it ever the case for SSL certs that the ownership of the domain name is verified, but the identity/organization of the subscriber is not verified?
EV policy OID(s)	Not EV
CP/CPS	All documents are in French. -- from bug -- Certificate Policy: http://www.certinomis.com/publi/rgs/DT-FL-0905-001-PC-RACINE-1.2.pdf http://www.certinomis.com/publi/rgs/DT-FL-0808-006-PC-SERV-1E-SSL-1.2.pdf CPS: http://www.certinomis.com/publi/rgs/PR_AE_OpC_100125.pdf Additional CP document: http://www.certinomis.com/publi/rgs/DT-FL-1001-001-PC-PROFILS-1.0.pdf -- from website -- Certinomis Certificate Policies: http://www.certinomis.com/qui_politiques_certification.php

	Qualified Certificate RGS-A (PRIS V2) Certificates for Person (Authentication and Signature): http://www.certinomis.com/publi/rgs/DT-FL-0808-004-PC-ORGA-1E-M-1.1.pdf http://www.certinomis.com/publi/rgs/DT-FL-0808-014-PC-ORGA-2E-M-1.1.pdf Certificates for Server Authentication: http://www.certinomis.com/publi/rgs/DT-FL-0808-006-PC-SERV-1E-SSL-1.1.pdf http://www.certinomis.com/publi/rgs/DT-FL-0808-007-PC-SERV-2E-SSL-1.1.pdf Certificates of Server for Customer Authentication: http://www.certinomis.com/publi/rgs/DT-FL-0808-008-PC-SERV-1E-CLT-1.1.pdf http://www.certinomis.com/publi/rgs/DT-FL-0808-018-PC-SERV-2E-CLT-1.1.pdf Non-Qualified Certificates Certificates of Person or Servers (Corporate): http://www.certinomis.com/publi/pc/pol_corporate_1.pdf Certificates of Server (SSL): https://www.certinomis.com/publi/pc/pol_certinomisssl_1.pdf What is the relation between the CP/CPS documents listed in the bug versus the documents that are provided at http://www.certinomis.com/qui_politiques_certification.php?
AUDIT	Audit Type: ETSI 101 456 Auditor: LSTI http://www.lsti-certification.fr Audit Document: http://www.certinomis.com/publi/rgs/8035_OC_TS_101_456_ex1F.pdf Listed on LSTI website: http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=58&Itemid=53&lang=en (2009.08.06)
Organization Identity Verification	Please provide translations into English of the sections of the CP/CPS documents pertaining to Verification of Identity and Organization. Please also list the documents and section or page numbers where the original text can be found.
Domain Name Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text.
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements:

	• for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text.
Identity of Code Signing Subscriber	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; If you are also requesting that the Code Signing trust bit be enabled, please provide the specific document(s) and section or page numbers where the procedures for code signing certs are described. Please provide translations into English of the sections of the CP/CPS documents that describe the identity verification procedures for code signing certs. Please also list the corresponding document(s) and section or page numbers containing the original text.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information and translations into English of the CP/CPS where relevant. • Long-lived DV certificates o • Wildcard DV SSL certificates o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o

	• Certificates referencing hostnames or private IP addresses o • Issuing SSL Certificates for Internal Domains o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs o