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: politiquecertification@certinomis.com CA Phone Number: +33 (0)1 56 29 72 48 Title/Department: Chief Technical Officer

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	This root has internally-operated subordinate CAs: "Certinomis AC 1 étoile" (OV verification for SSL), "Certinomis AC 2 étoiles" (EV like verification for SSL), "Certinomis - Autorité de Test" (for internal testing only), "Certinomis Corporate" (discontinued).
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	https://class2.test-certinomis.com/ -- The ssl cert is signed by a subCA with CN=Certinomis AC 1 étoile https://class3.test-certinomis.com/ -- The ssl cert is signed by a subCA with CN=Certinomis AC 2 étoiles
CRL URL	ARL: http://crl.certinomis.com/AC_Racine/crl/crl-1.crl CRL 1 star: http://crl.certinomis.com/AC_1_ETOILE/crl/crl-2.crl (NextUpdate: 7 days) CRL 2 stars: http://crl.certinomis.com/AC_2_ETOILES/crl/crl-2.crl (NextUpdate: 7 days)

OCSP Responder URL	Not supported
CA Hierarchy	This root has the following internally-operated subCAs: ▪ Certinomis AC 1 étoile -- OV verification for SSL ▪ Certinomis AC 2 étoiles -- EV like verification for SSL ▪ Certinomis - Autorité de Test -- Internal use only for test purpose ▪ Certinomis Corporate -- certs are no longer signed by this subCA, it has been discontinued
Externally Operated sub-CAs	None
Cross-Signing	None
Requested Trust Bits	Websites
SSL Validation Type	OV
EV policy OID(s)	Not requesting EV at this time.
CP/CPS	All documents are in French. CPS: http://www.certinomis.com/publi/rgs/PR_AE_OpC_100125.pdf Root CP: http://www.certinomis.com/publi/rgs/DT-FL-0905-001-PC-RACINE-1.2.pdf CP Serveur SSL 1 étoile: http://www.certinomis.com/publi/rgs/DT-FL-0808-006-PC-SERV-1E-SSL-1.2.pdf CP Serveur SSL 2 étoiles: http://www.certinomis.com/publi/rgs/DT-FL-0808-016-PC-SERV-2E-SSL-1.2.pdf Document repository: http://www.certinomis.com/publi/rgs/ RGS (French qualification) requires a different CP for each usage, each level and for each type of holder. There are 3 types of holder: particular, professional/agent and server There are now 2 verification levels: OV, and EV-like (DV-only has been discontinued) There are about 4 usages: authentication, signature, encipherment and serverAuth. Certinomis delivers for the moment only 1 and 2 stars certificates, but for all public and all usage there are 24 documents.
AUDIT	Audit Type: ETSI 101 456 Auditor: LSTI http://www.lsti-certification.fr ETSI Certificate: 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	Comment #15: There is also a pre-check of the identity of the organization when the subscriber create its account on certinomis web site. We use the INSEE database to check the activity of the organization: http://avis-situation-sirene.insee.fr/avisitu/jsp/avis.jsp Comment #16: Certinomis attached part of another document to the bug, which is the section of their RA process documentation dealing with when the organization is a new customer. It includes checking the existence of the organization on the SIRENE directory: http://avis-situationsirene.insee.fr/avisitu/jsp/avis.jsp. The RA must retrieve the exact name from the directory and verify that the facility exists and is not closed. https://bugzilla.mozilla.org/attachment.cgi?id=498112

	Translation from CPS section 2.1.2.1: As a rule, the organization must bring the proof of its existence and of its registration number (unique number identification from a trade register or all other official up-to-date lists.) This proof takes the form of a supporting document. Generally, for a corporation, this is a copy of the extract ‘k-bis’ delivered by the transplants of courts of commerce of the seat of the corporation. A list of supporting document accepted is available in a supplementary procedure: FC_AE_OPC_JUSTIFS Extract from FC_AE_OPC_JUSTIFS: **1. A company registered at the French Trade Register** _ An original K-Bis certificate of incorporation dated less than 3 months, delivered by the registry _ One valid copy of your company’s articles of association, bearing the signature of its representatives **2. French organisations registered at the SIRENE Register** _ a situation notice from the SIRENE register justifying your registration number _ a copy of the articles of association / minutes of the General Assembly, or any other valid document bearing the signatures of the organisation’s representatives _ **ELECTED REPRESENTATIVES :** a copy of the minutes / the debate leading to the election of the Mayor, the Chairman, etc. This copy is to bear your organisation’s stamp and mention « certified true copy » _ **APPOINTED REPRESENTATIVES :** a copy of the official gazette or bulletin attesting to this appointment (if the page contains a lot of text, please highlight the line involved). **3. European organizations** _ copy of the document awarding your organisation its Intra-community VAT Identification Number _ copy of the registration at a trade and company register, « certified true copy » _ a copy of the articles of association / minutes of the General Assembly, or any other valid document bearing the signatures of the organisation’s representatives Translation from “CP Serveur SSL 1 étoile” section 3.2.2: Note: Translations from “CP Serveur SSL 2 étoile” section 3.2.2 are basically the same. The Registration Authority verifies the organization identity, the legal representative identity and identity of all persons designated by the representative, directly or indirectly, to represent the organization to the CA or the RA. The legal representative and these persons are the certificate “agents”. In lack of designation, the legal representative is the unique certificate agent. At the time of the registration, the organization must bring the proof of its existence, the proof of the identity of its legal representative as well as the mandate chain conferring the power to the certificate agents.

	The CA or the RA archives all pertinent documents relating to this recording. The RA verifies that the request contains the following documents: · A written request of certificate, signed, and dated back to less than 3 months, by a legal representative of the entity or by the certificate agent · A signed mandate, and dated back to less than 3 months, by a legal representative of the organization or by the certificate agent designating the future holder to which the certificate must be delivered. This mandate must be signed for acceptance by the future certificate holder · A copy of the status of the organization, in course of validity, carrying signature of its representatives, or for an association a verbal process of the general assembly carrying the signature of its representatives, · A document, valid at the recording, carrying the number SIREN of the organization (k-bis extract or a situation notice from the SIRENE register justifying the registration number) or, another valid piece testifying the unique identification of the company that will figure in the certificate or, for the administrations a valid document at the recording, carrying delegation of responsible authority of the administrative structure. The RA preserves the documents received for the recording of the holder, examines the given pieces and documents with a reasonable care and verifies if they appear to be conformant and valid. Translation from “CP Serveur SSL 1 étoile” section 3.2.3.1: The identification of the future carrier (person) representing an entity requires, first, identification of the entity and, secondly, the identification of the individual. The identification of the entity is performed under the terms of Article 3.2.2. The RA verifies the photocopy of at least one official ID of the recipient being validity with his photo and signature, preceded by the words "certified copy true to the original "dated less than three (3) months from the date of filing of documents deemed to be the date in the postmark. The EA maintains the documents received for registration of the beneficiary, and examines parts documents provided with reasonable care and checks whether or not present the appearance of compliance and validity. Translation from “CP Serveur SSL 1 étoile” section 3.2.3.2: An RA is caused to establish a registration dossier for a Mandatory Certification to meet the following requirements: · Using the back of the MC data as reference for the identification of the entity all recipients presented by the MC. · Possibly, of a certificate to the MC for it to sign files registration of beneficiaries of the entity they represent and transmit the form mail. The identification of future attorney representing an entity certification requires, first, identification of the entity and, secondly, the identification of the individual. The identification of the entity is performed under the terms of Article 3.2.2. The RA verifies that the application contains the following parts: • A warrant signed and dated within 3 months by a legal representative of the entity designating the MC. This warrant

	must be signed by the MC for acceptance • A commitment signed and dated within 3 months of the MC, with HQ, to perform properly and independently controls the records of applicants, • A commitment signed and dated within 3 months of the MC to report his departure to EI entity, • A formal identity document valid MC with a photo ID (such as national identity card, passport or stay), which is presented to EI which retains a copy. The RA verifies the photocopy of at least one official ID of the recipient being validity with his photo and signature, preceded by the words "certified copy true to the original "dated less than three (3) months from the date of filing of documents deemed to be the date in the postmark. The EA maintains the documents received for registration of the beneficiary, and examines parts documents provided with reasonable care and checks whether or not present the appearance of compliance and validity.
Domain Name Ownership / Control	Translation of CPS section 2.1.3.1: The certificate's common name (CN) must be a FQDN. (Fully Qualified Domain Name). A FQDN starts with a hostname (www, ftp…) et ends with an extension (.com, .eu, .fr, .org etc.). This is the internet address to access to the server, with no directory or files (not a full URL) ex. : www.certinomis.com , www.test-certinomis.com are FQDN. On the other hand, www.certinomis.com/faq is not acceptable (directory). The following chars are forbidden within a FQDN : slash(/), comma(,) spaces (and other like tab). Dash(-) and dot (.) are accepted. The operator (RA) must verify: 1. The link between the organization and the domain name to certify, if needed, ask complements. 2. The ownership of the domain name, on these internet web sites: ▪ http://www.networksolutions.com/whois/index.jhtml. (domains .com, .org, .net) ▪ http://www.afnic.fr/outils/whois (domains .fr) ▪ http://www.eurid.eu (domains .eu) ▪ http://www.norid.no/domenenavnbaser/domreg.html (other countries) If the identified organization is not the owner of the domain, the recorded owner of the domain must provide an authorization of usage of domain name to the identified organization. The domain's contact information must be up-to-date. If not the domain owner must update them. When done, he must notify the operator for checking the domain name recording and then the operator can validate the certificate request. In addition, if the request is done under the form of a request accompanied with a CSR, this one is checked by the back office tool in order to verify the proof of possession of the private key. Translation from "CP Serveur SSL 1 étoile" section 3.2.3.3: The identification of the future device (or application) representing a corporation needs, on one hand, the identification of this entity and, on the other hand, the identification of the physical person in charge of the device and at last the identity of the device.

	The identification of the entity and person in charge of the device is realized following the disposals of the item 3.2.3.1 and if the entity designates a certificate agent, following disposals of the item 3.2.3.2. RA verifies that the requester is authorized by his company to receive certificates for the device or the application. The person or the organization that presents a request must establish the proof of his right of usage on the device or the application that will have the requested certificate. In particular in the case of a web server, the person will have to establish the proof that the domain name belongs to him. RA verifies that the request contains the following documents: · A written request of certificate, dated back to less than 3 months, signed by a legal representative of the entity or by the certificate agent, containing the server FQDN. · A signed mandate, and dated back to less than 3 months, by a legal representative of the organization or by the certificate agent designating the future holder to which the certificate must be delivered. This mandate must be signed for acceptance by the future certificate holder. · A proof of possession by the entity of the domain name corresponding to the FQDN of the server. The RA preserves the documents received for the recording of the holder, examines the given pieces and documents with a reasonable care and verifies if they appear to be conformant and valid.
Email Address Ownership / Control	Not applicable – not requesting the email trust bit.
Identity of Code Signing Subscriber	Not applicable – not requesting the code signing trust bit.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV. The max validity of SSL certs is 3 years. • Wildcard DV SSL certificates o SSL certs are OV. • Delegation of Domain / Email validation to third parties o There is no delegation of validation to third parties. • Issuing end entity certificates directly from roots o The root does not directly sign end entity certs. The root signs sub-CAs and the CRL. • Allowing external entities to operate unconstrained subordinate CAs o All of the sub-CAs are internally operated. • Distributing generated private keys in PKCS#12 files o Translation from “CP Serveur SSL 1 étoile” section 6.1.2: In the case where the key pair is

	generated at the CA private key is transmitted to the head of server securely, to ensure confidentiality and integrity. The private key is transmitted to the carrier within a PKCS #12, protected by a password passes, consisting of 12 alphanumeric characters, the PKCS #12 and the password being transmitted by two different mailings. o Certinomis delivers PKCS#12 files: ▪ The process is qualified; use of a SSCD with no copy of keys ▪ The delivery is secured; the PKCS12 is burned on a CD sended by mail. ▪ The password (12 chars long) is delivered with secure mailer. ▪ These operations are differed in space and time. • Certificates referencing hostnames or private IP addresses o Only FQDN allowed • Issuing SSL Certificates for Internal Domains o Only registered domains are certified. • OCSP Responses signed by a certificate under a different root o No OCSP • CRL with critical CIDP Extension o The CRLs import into a Firefox browser without error. • Generic names for CAs o Root CN contains the company name.