**Bugzilla ID:** 937589
**Bugzilla Summary:** Add Certinomis G3 (SHA256) Root Certificates

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 | Certinomis SA |
| Website URL | http://www.certinomis.fr |
| Organizational type | Commercial CA, operated by a private company held by a public company (La Poste). |
| Primark Market / Customer Base | Certinomis is a commercial CA serving a global client base, active in both the markets for SSL and End User Certificates with a focus on digital signatures. The company is a Qualified Certification Services Provider in France, and an issuer of eID for both enterprises and individuals. |
| Impact to Mozilla Users | 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. |
| Inclusion in other major browsers | Yes, the Certinomis Root Certificates are widely distributed. |
| CA Primary Point of Contact (POC) | Direct E-mail : franck.leroy@certinomis.fr<br>CA Email Alias: politiquecertification@certinomis.com<br>CA Phone Number: +33 (0)1 56 29 72 48<br>Title / Department: Franck Leroy – Chief Technical Officer |

**Technical information about each root certificate**

| | |
|---|---|
| Certificate Name | Certinomis - Root CA |
| Certificate Issuer Field | CN = Certinomis - Root CA<br>OU = 0002 433998903<br>O = Certinomis<br>C = FR |
| Certificate Summary | This SHA256 root will eventually replace the "Certinomis - Autorité Racine" G2 root certificate that was included in NSS via Bugzilla Bug #545614. |
| Root Cert URL | http://www.certinomis.fr/publi/cer/AC_Racine_G3.cer |
| SHA1 Fingerprint | 9D:70:BB:01:A5:A4:A0:18:11:2E:F7:1C:01:B9:32:C5:34:E7:88:A8 |
| Valid From | 2013-10-21 |
| Valid To | 2033-10-21 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA-256 |
| Signing key parameters | 4096 |
| Test Website URL (SSL) | https://g3-test.certinomis.com/ |

| | |
|---|---|
| CRL URL | http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_AGENTS-crl-1.crl<br>http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_EASY-crl-1.crl<br>http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_PRIME-crl-1.crl<br>http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_STANDARD-crl-1.crl<br>NextUpdate: 7 days max, but a fresh CRL every 24h and after each revocation |
| OCSP URL | http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_AC_AGENTS<br>http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_AC_EASY<br>http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_AC_PRIME<br>http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_AC_STANDARD |
| Requested Trust Bits | Websites (SSL/TLS) |
| SSL Validation Type | OV |
| EV Policy OID(s) | Not Applicable. Not requesting EV treatment. |
| Non-sequential serial numbers and entropy in cert | Comment #5: SHA-1 is not used even for end-entity certificates<br>http://www.certinomis.com/publi/rgs/DT-FL-1310-002-PC-PROFILS-1.0.pdf<br>“2.2 PROFIL DES CERTIFICATS PORTEURS … Signature sha256WithRSAEncryption”<br>Nevertheless some entropy is also added (160 bits) in the end-entity serial-number generation.<br>Dates are also unpredictable as all certificates issuance is done manually by operators. |

**CA Hierarchy information for each root certificate**

| | |
|---|---|
| CA Hierarchy | The root has signed 4 internally-operated subordinates CAs for issuing end-entity certificates.<br>http://www.certinomis.com/documents-et-liens/nos-certificats-racines<br>http://www.certinomis.fr/publi/cer/AC_AGENTS.cer<br>http://www.certinomis.fr/publi/cer/AC_EASY.cer<br>http://www.certinomis.fr/publi/cer/AC_PRIME.cer<br>http://www.certinomis.fr/publi/cer/AC_STANDARD.cer |
| Externally Operated SubCAs | Comment #5: None for this root and all Certinomis Roots (including the G2).<br>Note: The CP does not forbid external subCAs.<br><br>Regarding the Root CP, are there sections that describe who can apply for a subordinate CA?<br>http://www.certinomis.com/publi/rgs/DT-FL-1310-001-PC-RACINE-1.2.pdf section 3.2.2 Validation de l'identité d'un organisme -- Any company can contract with Certinomis in order to be a subordinate CA.<br><br>Can someone outside of Certinomis operate a subordinate CA?<br>It may be possible, but at this time, only Certinomis operates subordinate CAs of the Certinomis Root CA.<br><br>What are the rules/restrictions for such subordinate CAs, and which sections of the Root CP clarify how Baseline Requirements sections 9.7 and 17 will be met?<br>http://www.certinomis.com/publi/rgs/DT-FL-1310-001-PC-RACINE-1.2.pdf<br>[BR9.7] 4.5 USAGES DE LA BI-CLE ET DU CERTIFICAT<br>and<br>[BR17] 8.7 AUDIT DE CONFORMITE ET EVALUATIONS DES ACD |

| | |
|---|---|
| | What are the SSL verification requirements that must be enforced across all subordinate CAs?<br>As there is no external CA, sub CAs are only operated by Certinomis, then all verification are described by Certinomis' CP/CPS.<br>An external sub CA have to be set-up, its CP/CPS shall met the same level of requirements than the current Certinomis' CP/CPS. |
| Cross-Signing | This new root cross-certifies with the "Certinomis - Autorité Racine" root.<br>As in France it is now forbidden to produce sha1 and as mozilla/Microsoft/google... process is long then we decided finally to cross certify. |
| Technical Constraints on Third-party Issuers | Comment #5: There is no external third party issuer.<br>All applications are processed by Certinomis operators. When a certificate request is validated by Certinomis, the subscriber has the possibility to re-issue another certificate with the same validated informations (organization and domain names). For this feature, the subscriber need a strong authentication (based on smartcard) delivered by Certinomis and with security roles granted by Certinomis security officer.<br><br>Comment #29:<br>1) Identify who can do domain control validation: only Certinomis<br>2) Identify who can issue SSL certs: only Certinomis |

**Verification Policies and Practices**

| | |
|---|---|
| Policy Documentation | Document Repository: http://www.certinomis.com/documents-et-liens/nos-politiques<br>Root CP (French): http://www.certinomis.com/publi/rgs/DT-FL-1310-001-PC-RACINE-1.2.pdf<br>Web SSL CP (French): http://www.certinomis.com/publi/pc/DT-FL-1310-060-PC-WEB-SSL-1.2.pdf<br>SSL for private sector: http://www.certinomis.com/publi/rgs/DT-FL-1310-020-PC-SERV-1.3.pdf<br>SSL for administration sector: http://www.certinomis.com/publi/rgs/DT-FL-1310-040-PC-AA-1.3.pdf<br><br>AA et Agents<br>(requirements for French Regulation and ETSI/TS 101 042 including BR-PTC)<br>http://www.certinomis.com/publi/rgs/DT-FL-1310-040-PC-AA-1.3.pdf<br>3.2.3.3 Enregistrement d'un dispositif ou d'une application<br>See "CertinomisTranslations CP EN.pdf"<br><br>Easy CA / Prime CA / Standard CA<br>(requirements for French Regulation and ETSI/TS 101 042 including BR-PTC)<br>http://www.certinomis.com/publi/rgs/DT-FL-1310-020-PC-SERV-1.3.pdf<br>3.2.3.3 Enregistrement d'un dispositif ou d'une application<br>See "CertinomisTranslations CP EN.pdf"<br>-or-<br>(requirements for ETSI/TS 101 042 including BR-PTC only)<br>http://www.certinomis.com/publi/pc/DT-FL-1310-060-PC-WEB-SSL-1.2.pdf<br>3.2.3.3 Enregistrement d'un dispositif ou d'une application<br>See "CertinomisTranslations CP EN.pdf" |

| | |
|---|---|
| Audits | Audit Criteria: ETSI TS 102 042 v2.4.1 for LCP/NCP/NCP+/PTC-BR<br>Auditor: LSTI<br>Auditor Website: http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf<br>Auditor's Statement (G2): https://bugzilla.mozilla.org/attachment.cgi?id=8451590 (2014.06.30) |
| Baseline Requirements (SSL) | https://bugzilla.mozilla.org/attachment.cgi?id=8451590 -- ETSI TS 102 042 with PTC-BR<br><br>Server CP section 1.1: Pour les clauses applicables sur les offres serveur SSL, Certinomis se conforme à la version courante des « Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates » (BR) publié sur le site http://www.cabforum.org. En cas d'inconsistance entre ce document et les exigences BR du CABForum, les exigences BR du CABForum sont applicables.<br><br>Translation: Where applicable for SSL certificates, Certinomis conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("BR") published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document. |
| Organization Verification Procedures | See Server CP section 3.2.2<br>Machine Translation:<br>Authentication of an organization based on the verification of information provided by the latter. This information includes the name and address of the organization and the documents or references to the existence of the latter, and the domain it holds.<br>The entity shall check to ensure that the organization exists and is legally authorized to use only his name, by comparing the information provided in the application of the SSL certificate information collected from official databases of reference.<br>Information that can be verified during the authentication of the identity of the organization understand the SIREN number , the number of VAT returns , DUNS , etc. .<br>To issue the SSL certificate, it is also necessary to verify that the domain present in the request belongs to this organization, and is therefore authorized to use . Audits are performed by consulting official databases of domain names or AFNIC INTERNIC kind .<br>The AE archive all relevant information relating to that registration<br><br>Certinomis confirms that the organization exists, then Certinomis verifies that the applicant is authorized to represent the organization in question. This is done by requiring national ID cards and an authorization document signed by both the organization representative and the certificate agent. The authorization document contains the FQDN of the certificate and names the certificate manager (the person who will receive the certificate). The certificate manager must also provide a copy of the national ID card and another signed document.<br>Certinomis confirms that the representative is who he claims to be as follows.<br>When the subscriber creates an account on the Certinomis web site. Certinomis uses the INSEE database to check the name and the activity of the organization:<br>http://avis-situation-sirene.insee.fr/avisitu/jsp/avis.jsp<br>The identity of the certificate subscriber is verified by using the ID card and the extrait K-bis from the Trade |

| | |
|---|---|
| | Registry. Note that K-bis are printed on a specific paper (with watermark) that cannot be photocopied. Depending on the kind of policy, the identity of the certificate subscriber is verified by a face-to-face meeting as described in section 3.2.3.3 of the ORAGNISATION CP. |
| SSL Verification Procedures | http://www.certinomis.com/publi/rgs/PR_AE_OpC_110075.pdf<br>2.1.3.1 Dans le cas de l'utilisation d'un FQDN<br>2.1.3.3 Certificat SSL<br>See "CertinomisTranslations CPS EN .pdf"<br>Options in Baseline Requirements section 11.1.1 may be used: 3 and 5; Domain Authorization Document is always needed and some checking are done on WHOIS records. If CA has previously issued certificate for this FQDN for this applicant and that WHOIS records has not been modified, then no communication with the Domain Name Registrant is needed.<br><br>NB: There are differents policies according to enforcement of french regulation or not, but domain name validation follow the same process in any cases.<br><br>Server CP section 3.2.3: Le certificat doit toujours contenir le nom de l'entité identifiée et, éventuellement, toutes les informations complémentaires permettant d'identifier son titulaire sans ambiguïté.<br>La DPC précise les documents à fournir et les procédures d'enregistrement mises en oeuvre par l'AE, en concertation avec l'AC.<br>3.2.3.1 Enregistrement d'un dispositif ou d'une application<br>L'identification du futur dispositif (ou application) représentant une entité nécessite, d'une part, l'identification de cette entité et, d'autre part, l'identification de la personne physique responsable et du dispositif et enfin l'identité du dispositif: le RCAS<br>L'identification de l'entité et du responsable du dispositif est réalisée suivant les dispositions de l'article 3.2.2.<br>L'AE vérifie que le demandeur est autorisé à recevoir des certificats pour le dispositif ou l'application. La personne ou l'organisation qui présente une demande doit établir la preuve de son droit d'usage sur le dispositif ou l'application dont mention sera faite dans le certificat. En particulier dans le cas d'un serveur web, elle devra établir la preuve que le nom de domaine lui appartient bien.<br>For "AC Easy" subordinate CA:<br>L'AE vérifie que la demande contient les pièces suivantes :<br>· Une demande de certificat écrite, datée de moins de 3 mois, signée par le RCAS et comportant le FQDN du serveur concerné par cette demande,<br>· Une preuve de possession par l'entité du nom de domaine correspondant au FQDN du serveur.<br>L'AE vérifie la photocopie d'au moins une pièce d'identité officielle du RCAS en cours de validité comportant sa photo et sa signature.<br>L'AE conserve les pièces reçues pour l'enregistrement du dispositif, examine les pièces et documents remis avec un soin raisonnable et vérifie s'ils présentent ou non l'apparence de conformité et de validité.<br><br>Translation:<br>The RA verifies that the applicant is entitled to receive certificates for the device or application. The person |

| | |
|---|---|
| | or organization submitting an application must prove his right to use the device or application which mention will be made in the certificate. Especially in the case of a web server, it must prove that the domain name belongs to him well .<br>For "AC Easy" subordinate CA:<br>The RA verifies that the request contains the following documents:<br>- 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.<br>- A proof of possession by the entity of the domain name corresponding to the FQDN of the server.<br>The RA verifies the photocopy of at least one official ID valid containing a photograph and signature.<br>The AE keeps the documents received for device registration, examines and documents submitted with reasonable care and checks whether or not they have the appearance of compliance and validity.<br><br>Explanation:<br>The operator (RA) must verify:<br>- The link between the organization and the domain name to certify.<br>- If necessary, ask complements<br>The ownership of the domain name, on these internet web sites:<br>- http://www.networksolutions.com/whois/index.jhtml. (domains .com, ..org, .net)<br>- http://www.afnic.fr/outils/whois (domains .fr)<br>- http://www.eurid.eu (domains .eu)<br>- http://www.norid.no/domenenavnbaser/domreg.html (other countries)<br>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.<br>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.<br>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. |
| Email Address Verification Procedures | Not applicable; not requesting the email trust bit. |
| Code Signing Subscriber Verification Procedures | Not applicable; not requesting the code signing trust bit. |
| Multi-factor Authentication | Server CP section 5.2.3: Remote operators intervening within the CA system must be identified by means of strong cryptographic mechanisms. |
| Network Security | Certinomis confirms the following:<br>• Maintain network security controls that at minimum meet the CA/B Forum Network and Certificate System Security Requirements.<br>• Check for mis-issuance of certificates, especially for high-profile domains.<br>• Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.<br>• Ensure Intrusion Detection System and other monitoring software is up-to-date.<br>• Able to shut down certificate issuance quickly if we are alerted of intrusion. |

**Response to Mozilla's CA Recommended Practices** (https://wiki.mozilla.org/CA:Recommended_Practices)

| | |
|---|---|
| Publicly Available CP and CPS | Yes |
| CA Hierarchy | Yes |
| Audit Criteria | See above. |
| Document Handling of IDNs in CP/CPS | IDN certificates are not issued. |
| Revocation of Compromised Certificates | Section 4.9.1 of Server CP |
| Verifying Domain Name Ownership | Yes, see above. |
| Verifying Email Address Control | N/A |
| Verifying Identity of Code Signing Certificate Subscriber | N/A |
| DNS names go in SAN | Yes |
| Domain owned by a Natural Person | No |
| OCSP | Yes |

**Response to Mozilla's list of Potentially Problematic Practices** (https://wiki.mozilla.org/CA:Problematic_Practices)

| | |
|---|---|
| Long-lived DV certificates | SSL certificates are OV. |
| Wildcard DV SSL certificates | SSL certificates are OV. |
| Email Address Prefixes for DV Certs | SSL certificates are OV. |
| Delegation of Domain / Email validation to third parties | Server section 1.3.2: Seule l'AE Certinomis à la capacité de valider un nom de domaine internet (FQDN) en vue de l'émission d'un certificat serveur SSL/TLS reconnu publiquement dans le programme d'autorité racine des éditeurs de navigateurs internet (notamment ceux membres du CABForum http://www.cabforum.org/forum.html). Cette fonction de validation ne peut en aucun cas être déléguée à un tiers.<br>Translation:<br>Only Certinomis RA is capable of internet domain name (FQDN) validation in order to issue publicly trusted ssl/tls certificates such as internet browser software vendors CA root program (in particular those member of CABForum http://www.cabforum.org/forum.html). This capacity of validation can be delegated on no account to a third party. |
| Issuing end entity certificates directly from roots | NA – Certinomis always issues from an intermediate Issuing CA. |
| Allowing external entities to operate subordinate CAs | No |

| | |
|---|---|
| Distributing generated private keys in PKCS#12 files | Yes we do it for SSL certificates, for example for tomcat, subscribers can set the P12 file and password in config and don't have to generate key. We are also certain of the quality of the key as it is generated by our HSM.<br>The passwords are generated by a Secure Module (same as for French credit card).<br>That password is 12 char long and used to encrypt the .p12 file for delivery.<br>The p12 file is burned on a mini-cdrom and send to the holder by postal mail.<br>The password is printed on a secure mail and send the day after from another geographic area.<br><br>Server CP:<br>4.3.1 Actions of the CA regarding the delivery of the certificate [...]<br>For software certificates, when the CA generates the keys:<br>• The CD-R is inserted into the customisation tool.<br>• The PKI generates keys and certificates.<br>• The PKI generates an activation code for the certificates.<br>• The customisation tool burns the keys and certificates onto a CD-R.<br>4.3.2 Notification by the CA of the certificate's delivery to the beneficiary<br>This certificate is delivered by mail, when the certificate is stored on a CD-R. Otherwise, the certificate is sent to the beneficiary by e-mail. [...]<br>When the CA generate activation codes, the certificate cannot be used without having this code (PIN or password depending on the type of cryptographic device). It is sent directly to the beneficiary's address, by secure mail.<br>6.2.8.2 Private keys of the servers [...]<br>In the case of software, if the CA generates the activation code, the key pairs are activated via a PKCS12 password with at least 12 characters. |
| Certificates referencing hostnames or private IP addresses | Under this new CA hierarchy Certinomis doesn't issue SSL certificates with Internal Server Names and/or Reserved IP Addresses. |
| Issuing SSL Certificates for Internal Domains | Yes. Certinomis SSL issuance systems filter against an internal database of approved TLDs that are eligible to be used for domains in certificates, and that list is manually updated. The RA also alerts security officer when certificates are applied for high risk domains. |
| OCSP Responses signed by a certificate under a different root | OCSP signing certificates are issued by the CA served by the OCSP. |
| CRL with critical CIDP Extension | Certinomis CRL CIDP are not marked critical. |
| Generic names for CAs | Certinomis uses meaningful CN and OU in its CA certificates. |
| Lack of Communication With End Users | Certinomis is contactable on policy related issues at politiquecertification@certinomis.com. In addition, our website include contact forms as well as certificate problem reporting and revocation request forms that are routed to the appropriate Support teams for prompt action. |