Bugzilla ID:
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 Contact Information	direct E-mail : franck.leroy@certinomis.fr CA Email Alias: politiquecertification@certinomis.com CA Phone Number: +33 (0)1 56 29 72 48 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 OU = 0002 433998903 O = Certinomis 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) Example Certificate (non---SSL)	https://w3-test.certinomis.fr/ (Error code: sec_error_unknown_issuer)" : "nonce" issue, processing…

CRL URL	http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_AGENTS-crl-1.crl http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_EASY-crl-1.crl http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_PRIME-crl-1.crl http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_STANDARD-crl-1.crl
OCSP URL (Required now)	http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_AC_AGENTS http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_AC_EASY http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_AC_PRIME 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	SHA-1 is not used even for end-entity certificates, the only signature algo is sha256WithRSAEncryption : Additional CP document: http://www.certinomis.com/publi/rgs/DT-FL-1310-002-PC-PROFILS-1.0.pdf 2.2 PROFIL DES CERTIFICATS PORTEURS Signature sha256WithRSAEncryption Nevertheless some entropy is also added (160 bits) is the end-entity serial-number generation. 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 subordinates CA for issuing end-entity certificates http://www.certinomis.fr/publi/cer/AC_AGENTS.cer http://www.certinomis.fr/publi/cer/AC_EASY.cer http://www.certinomis.fr/publi/cer/AC_PRIME.cer http://www.certinomis.fr/publi/cer/AC_STANDARD.cer
Externally Operated SubCAs	None for this root and all Certinomis Roots (including the G2). CP/CPS does not forbid external subCAs.
Cross-Signing	At present, we do not expect to have any cross-certificates for the Certinomis G3 Root Certificates. However, if we need to start using the G3 Roots before they have achieved a sufficient level of distribution amongst the installed base of various software products, we may elect to issue cross-certificates to the new Roots from the existing Certinomis G2 Root.
Technical Constraints on Third-party Issuers.	There is no external third party issuer. 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.

Verification Policies and Practices

Policy Documentation	Certificate Policies (French, translations are processing). ROOT: http://www.certinomis.com/publi/rgs/DT-FL-1310-001-PC-RACINE-1.0.pdf ORGANISATION : http://www.certinomis.com/publi/rgs/DT-FL-1310-010-PC-ORGA-1.0.pdf PARTICULIER : http://www.certinomis.com/publi/rgs/DT-FL-1310-100-PC-PART-1.0.pdf SERVEUR: http://www.certinomis.com/publi/rgs/DT-FL-1310-020-PC-SERV-1.0.pdf AGENTS: http://www.certinomis.com/publi/rgs/DT-FL-1310-030-PC-AGENTS-1.0.pdf AUTORITE: http://www.certinomis.com/publi/rgs/DT-FL-1310-040-PC-AA-1.0.pdf Additional CP document: http://www.certinomis.com/publi/rgs/DT-FL-1310-002-PC-PROFILS-1.0.pdf CPS : http://www.certinomis.com/publi/rgs/PR_AE_OpC_110075.pdf RA Procedures Document – PROC (French): http://www.certinomis.com/publi/rgs/FC_AE_OPC_JUSTIFS_110207.pdf
Audits	LSTI performs the audits according to the ETSI TS 101 456 criteria for QCP/QCP+ and ETSI TS 102 042 for LCP/NCP/NCP+. The current ETSI certificate is valid until 2015.04.29, and is posted on the LSTI website at http://www.lsti-certification.fr/ ETSI list : http://www.lsti-certification.fr/images/liste_entreprise/ETSI.pdf For each entry (certificate profile from Root G2) ETSI level (LCP/NCP/QCP) is indicated. See attached document (auditor letter for Root G2) ; 2143CertinomisS.pdf Root G3 audit is done, auditor report is about to be published.
Baseline Requirements (SSL)	Added in CPs chapter 1.1 ; 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.
SSL Verification Procedures	Domain verification begins with using WHOIS to check the link between FQDN and Organisation Name. Then the domain contact is notified (a phone call to the organization main phone number and asking to talk to the domain contact) for checking the domain name recording. The domain contact is asked about the FQDN value in order to avoid mistake on sub-domain value. During the phone call to the domain owner, the RA ask if he agrees the certificate creation. Please translate section 2.1 of the CPS and section 3.2 of the CP Server into English: See attached translated documents; CertinomisTranslations CP EN.pdf & CertinomisTranslations CPS EN .pdf

Organization Verification Procedures	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. Certinomis confirms that the representative is who he claims to be as follows. 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: http://avis-situation-sirene.insee.fr/avisitu/jsp/avis.jsp 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 ORGANISATION CP.
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	Added in CPs chapter 9.6; Enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.
Network Security	Certinomis confirms the following: • Maintain network security controls that at minimum meet the CA/B Forum Network and Certificate System Security Requirements. • Check for mis-issuance of certificates, especially for high-profile domains. • Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. • Ensure Intrusion Detection System and other monitoring software is up-to-date. • 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	Yes, ETSI TS 101 456.
Document Handling of IDNs in CP/CPS	IDN certificates are not issued.
Revocation of Compromised Certificates	Yes, see Section 4.9.1 of CP documents.
Verifying Domain Name Ownership	Yes, see above.
Verifying Email Address Control	Out of scope.
Verifying Identity of Code Signing Certificate Subscriber	Out of scope
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	NA. SSL certificates are OV. SSL validity periods comply with the Baseline Requirements.
Wildcard DV SSL certificates	NA. SSL certificates are OV.
Email Address Prefixes for DV Certs	NA. SSL certificates are OV.
Delegation of Domain / Email validation to third parties	Added in CPs chapter 1.3.2 : 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	NA.
Distributing generated private keys in PKCS#12 files	The passwords are generated by a Secure Module (same as for French credit card). That password is 12 char long and used to encrypt the .p12 file for delivery. The p12 file is burned on a mini-cdrom and send to the holder by postal mail. The password is printed on a secure mail and send the day after from another geographic area.
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.