Mozilla - CA Program

Case Information

Case Number	00000005	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Certinomis	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Included renewed root	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=937589

General information about CA's associated organization

Company Website	http://www.certinomis.fr	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)	Commercial CA, operated by a private company held by a public company (La Poste).	**Verified?**	Verified
Geographic Focus	France	**Verified?**	Verified
Primary 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.	**Verified?**	Verified
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.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Recommended Practices	Document Handling of IDNs in CP/CPS -- IDN certificates are not issued. Revocation of Compromised Certificates -- Section 4.9.1 of Server CP	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* Delegation of Domain / Email validation to third parties -- Translation from Server CP section 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. * 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. 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. Server CP section 4.3.1, Actions of the CA regarding the delivery of the certificate [...] For software certificates, when the CA generates the keys: • The CD-R is inserted into the customisation tool. • The PKI generates keys and certificates. • The PKI generates an activation code for the certificates. • The customisation tool burns the keys and certificates onto a CD-R. 4.3.2 Notification by the CA of the certificate's delivery to the beneficiary 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. [...] 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. 6.2.8.2 Private keys of the servers [...] 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 -- 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.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Case No	R00000007	**Case Number**	00000005
Request Status	Ready for Public Discussion	**Root Certificate Name**	Certinomis - Root CA

Additional Root Case Information

Subject	Include SHA-256 Certinomis - Root CA

Technical Information about Root Certificate

O From Issuer Field	Certinomis	**Verified?**	Verified
OU From Issuer Field	0002 433998903	**Verified?**	Verified
Certificate Summary	This SHA256 root will eventually replace the “Certinomis - Autorité Racine” G2 root certificate that was included in NSS via Bugzilla Bug #545614.	**Verified?**	Verified
Root Certificate Download URL	http://www.certinomis.fr/publi /cer/AC_Racine_G3.cer	**Verified?**	Verified
Valid From	2013 Oct 21	**Verified?**	Verified
Valid To	2033 Oct 21	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://g3-test.certinomis.com/	**Verified?**	Verified
CRL URL(s)	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 NextUpdate: 7 days max, but a fresh CRL every 24h and after each revocation	**Verified?**	Verified
OCSP URL(s)	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	**Verified?**	Verified

	/INSTANCE_SHA2 /ocsp/OCSP_AC_STANDARD		
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not requesting EV treatement.	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	9D:70:BB:01:A5:A4:A0:18:11:2E:F7:1C:01:B9:32:C5:34:E7:88:A8	**Verified?**	Verified
SHA-256 Fingerprint	2A:99:F5:BC:11:74:B7:3C:BB:1D:62:08:84:E0:1C:34:E5:1C:CB:39:78:DA:12:5F:0E:33:26:88:83:BF:41:58	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The root has signed 4 internally-operated subordinates CAs for issuing end-entity certificates. http://www.certinomis.com/documents-et-liens/nos-certificats-racines 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	**Verified?**	Verified
Externally Operated SubCAs	Comment #5: None for this root and all Certinomis Roots (including the G2). Root CP section 3.2.2 Validation de l'identité d'un organisme -- Any company can contract with Certinomis in order to be a subordinate CA. At this time, only Certinomis operates subordinate CAs of the Certinomis Root CA. If 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.	**Verified?**	Verified
Cross Signing	This new root cross-certifies with the “Certinomis - Autorité Racine” root. 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.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Comment #5: There is no external third party issuer. All applications are processed by Certinomis operators. When a certificate request is validated by Certinomis, the	**Verified?**	Verified

	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. Comment #29: 1) Identify who can do domain control validation: only Certinomis 2) Identify who can issue SSL certs: only Certinomis		

Verification Policies and Practices

Policy Documentation	Documents are in French. See "CertinomisTranslations CP EN.pdf" AA et Agents (requirements for French Regulation and ETSI/TS 101 042 including BR-PTC) http://www.certinomis.com/publi/rgs/DT-FL-1310-040-PC-AA-1.3.pdf 3.2.3.3 Enregistrement d'un dispositif ou d'une application Easy CA / Prime CA / Standard CA (requirements for French Regulation and ETSI/TS 101 042 including BR-PTC) http://www.certinomis.com/publi/rgs/DT-FL-1310-020-PC-SERV-1.3.pdf 3.2.3.3 Enregistrement d'un dispositif ou d'une application -or- (requirements for ETSI/TS 101 042 including BR-PTC only) http://www.certinomis.com/publi/pc/DT-FL-1310-060-PC-WEB-SSL-1.2.pdf 3.2.3.3 Enregistrement d'un dispositif ou d'une application	**Verified?**	Verified
CA Document Repository	http://www.certinomis.com/documents-et-liens/nos-politiques	**Verified?**	Verified
CP Doc Language	French		
CP	http://www.certinomis.com/publi/pc/DT-FL-1310-060-PC-WEB-SSL-1.2.pdf	**Verified?**	Verified
CP Doc Language	French		
CPS	http://www.certinomis.com/documents-et-liens/nos-politiques	**Verified?**	Verified
Other Relevant Documents	Root CP (French): http://www.certinomis.com/publi/rgs/DT-FL-1310-001-PC-RACINE-1.2.pdf Server CP (French): http://www.certinomis.com/publi/pc/DT-FL-1310-060-PC-WEB-SSL-1.2.pdf SSL for private sector: http://www.certinomis.com/publi/rgs/DT-FL-1310-020-PC-SERV-1.3.pdf SSL for administration sector: http://www.certinomis.com/publi/rgs/DT-FL-1310-040-PC-AA-1.3.pdf	**Verified?**	Verified
Auditor Name	LSTI	**Verified?**	Verified

Auditor Website	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	**Verified?**	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	**Verified?**	Verified
Standard Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	6/30/2014	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8451590	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	6/30/2014	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	Server CP section 1.1	**Verified?**	Verified
SSL Verification Procedures	Translation of Server CP section 3.2.3: 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 . For “AC Easy” subordinate CA: The 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 proof of possession by the entity of the domain name corresponding to the FQDN of the server. Explanation: The RA must verify: - link between the organization and the domain name to certify. - ownership of the domain name, on these internet web sites: - www.networksolutions.com/whois/index.jhtml. (domains .com, ..org, .net) - www.afnic.fr/outils/whois (domains .fr) - www.eurid.eu (domains .eu) - 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.	**Verified?**	Verified

EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	See Server CP section 3.2.2 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 ORAGNISATION CP.	**Verified?**	Verified
Email Address Verification Procedures	Not requesting the Email trust bit.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Not requesting the Code Signing trust bit.	**Verified?**	Not Applicable
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.	**Verified?**	Verified
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.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.certinomis.com/documents-et-liens/nos-certificats-racines	**Verified?**	Verified