NATURE DU DOCUMENT		Certinomis
Document Sécurité		
GROUPE LA POSTE		
REFERENCE	DATE	VERSION
DT-FL-1002/001	15 février 2010	1.0
Policy Information		
EMETTEUR	DESTINATAIRES	COPIES
Franck LEROY	Mozilla / Microsoft	public
CertiNomis		
CertiNomis. SA au capital de 40 000 euros. Siège social : 10 av Charles de Gaulle 94220 Charenton Le Pont – France. RCS Créteil B 433 998 903		

TABLE DES MATIERES

1 Introduction

Certinomis ask Mozilla and Microsoft to add its Root CA cert into internet products.
This document gathers all questions from Mozilla and Microsoft about Certinomis policies.

2 Matrice

General Information	**Data**
CA Name	Certinomis Company name and address : Certinomis 10 avenue Charles de Gaulle 94673 Charenton Le Pont Cedex France
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	Two contacts from your organization (first and last name, e-mail address, and phone number): François Chassery Directeur Commercial francois.chassery@certinomis.com +33 (0)1 56 29 72 62 Franck Leroy Directeur Technique franck.leroy@certinomis.com +33 (0)1 56 29 72 48 CA Email Alias: politiquecertification@certinomis.com CA Phone Number: +33 (0)1 56 29 72 48 Title / Department : Franck Leroy – Chief Technical Officer
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	https://igc-test.certinomis.com/index.php
CRL URL	ARL: http://crl.certinomis.com/AC_Racine/crl/crl-1.crl NextUpdate : 14 months, but a fresh ARL every 12 months and after each certificate use. CRL corporate : http://crl.certinomis.com/AC_CORPORATE/crl/crl-1.crl CRL 1 star: http://crl.certinomis.com/AC_1_ETOILE/crl/crl-2.crl CRL 2 stars: http://crl.certinomis.com/AC_2_ETOILES/crl/crl-2.crl NextUpdate: 7 days, but a fresh CRL every 24h and after each revocation
OCSP Responder URL	Not provided
CA Hierarchy	This root has 3 sub-CAs. "Corporate" for BtoB purpose: Class 1: Certificate issued upon verification of the e-mail (out of scope) "1 étoile" software or token, no face-to-face. ; Class 2: Certificate issued upon verification of documents "2 étoiles" only crypto token with face-to-face ; Class 3: Certificate issued on vouchers, with identity checks face to face
Externally Operated sub-CAs	None
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Only class 2 and class 3 CA.
SSL Validation Type DV, OV, and/or EV	OV
EV policy OID(s)	No EV
CP/CPS	Certificate Policy: ROOT: http://www.certinomis.com/publi/rgs/DT-FL-0905-001-PC-RACINE-1.2.pdf CLASS2 :http://www.certinomis.com/publi/rgs/DT-FL-0808-006-PC-SERV-1E-SSL-1.2.pdf CLASS3 :http://www.certinomis.com/publi/rgs/DT-FL-0808-006-PC-SERV-2E-SSL-1.2.pdf CPS: http://www.certinomis.com/publi/rgs/PR_AE_OpC_100125.pdf Additional CP/CPS document: http://www.certinomis.com/publi/rgs/DT-FL-1001-001-PC-PROFILS-1.0.pdf From web site: v1.1 soon available in v1.2 Qualified Certificate RGS-A (PRIS V2) Certificates for Professional (Authentication and Signature): (out of scope as we only ask for SSL/TLS) 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: EKU: serverAuthentication (that's it !)

	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: EKU: clientAuthentication (out of scope) 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 Out of scope ; This is another ROOT CA 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 For RGS (French qualification) we must provide 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 3 levels : 1 star, 2 stars and 3 stars (kind of class1/2/3) 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: so there are 24 available CP.
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.lsticertification.fr/index.php?option=com_content&view=article&id=58&Itemid=53&lang=en (2009.08.06)
Organization Identity Verification	Chapters are the same in any CP : 3.2.2 OV : 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.

CPS 2.1.2.1 OV :

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 organisations**

	▪ 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
Domain Name Ownership / Control	PC 3.2.3.3 DV : 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. CPS : 2.1.3.1 DV : 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 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 theses 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 contact information's 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.
Email Address Ownership / Control	Out of scope
Identity of Code Signing Subscriber	Out of scope
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 The max validity is 3 years ☐ Wildcard DV SSL certificates O No DV certificates only OV ☐ Delegation of Domain / Email validation to third parties O There is no delegation of validation ☐ Issuing end entity certificates directly from roots O The root does not issue entity certificates, only sub-CA and CRL. ☐ Allowing external entities to operate unconstrained subordinate CAs O There is no external entities. ☐ Distributing generated private keys in PKCS#12 files O Certinomis delivers PKCS#12 files but : 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.

o ☐ Certificates referencing hostnames or private IP addresses

o Only FQDN are certified

☐ 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 no critical extension

☐ Generic names for Cas

O All CA cn contains “Certinomis”

☐Lack of Communication With End Users

O Certinomis is contactable by mail/email/phone.

Root Count Restrictions : 1 root
Minimum Key Sizes for entity certificates : 1 star 1024 bits; 2 stars 2048 bits
Max Time Between Audits : 1 year