Bugzilla ID: 497917
Bugzilla Summary: Enable Keynectis root CA cert for EV SSL

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.

General Information	Data
CA Name	Keynectis/Certplus
Website URL	http://www.keynectis.com/
Organizational type	Public corporation
Primary market / customer base	Keynectis is a French commercial CA that issues certificates to the general public. Keynectis was created by merging two previous French certification operators, Certplus and PK7.
CA Contact Info	Email Address: service.clients@keynectis.com Phone Number: Department:

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	Class 2 Primary CA Note: O is Certplus
Cert summary / comments	This root is already included in NSS. The current request is to EV-enable the root. A new, internally-operated subordinate CA has been created for issuing EV SSL certificates.
Root Certificate URL	Already included in NSS. https://bugzilla.mozilla.org/attachment.cgi?id=263027
SHA-1 fingerprint	74:20:74:41:72:9C:DD:92:EC:79:31:D8:23:10:8D:C2:81:92:E2:BB
Valid from	1999-07-07
Valid to	2019-07-06
Cert Version	3
Modulus length	2048
Test Website	https://www.keynectis.com
CRL URL	KEYNECTIS Root CA CRL: http://www.certplus.com/CRL/class2.crl EV certificates CRL: http://trustcenter-crl.certificat2.com/keynectis/class2keynectisevca.crl (NextUpdate: 7 days) EV SSL CPS section 2.3: CRLs are published at least every 24 (twenty four) hours. Comment #6: CRL of our "Keynectis EV CA" is generated every 24 hours, and made valid for 7 days.
OCSP Responder URL	Authority Information Access: OCSP: URI: http://kvalid.keynectis.com/evssl-ocsp/ Comment #6: The OCSP service is updated every hour, and OCSP responses have an expiration date/time equal to that of the CRL (thus, max 7 days for the "Keynectis EV CA")

CA Hierarchy	This root has two internally-operated subordinate CAs: 1) Class 2 KEYNECTIS CA, issues SSL certificates 2) KEYNECTIS Extended Validation CA, issues EV SSL certificates
Externally Operated sub-CAs	This root does not have any subordinate CAs that are operated by third parties.
Cross-signing	This root has not been involved in cross-signing with any other root CAs.
Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type(s)	OV, EV
EV policy OID(s)	1.3.6.1.4.1.22234.2.5.2.3.1
CP/CPS	Keynectis Information: https://www.keynectis.com/en/support-information/pc.html CPS (French): http://www.keynectis.com/PC/CPS_KEYNECTIS_120407v1.1.pdf EV SSL CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=387860 EV SSL CPS (French): https://www.keynectis.com/static/content/common/pc-dpc/DSQ_NT_KEYNECTIS_EV_SSL_CA_CPS_20090504s.pdf SSL CPS (French): https://www.keynectis.com/static/content/common/pc-dpc/DSQ_PC_PC_AC_KEYNECTIS_SSL_1.2s.pdf Root CA Certification Policy: https://www.keynectis.com/static/content/common/pc-dpc/DSQ_CP_RCA_0.6.pdf SSL CA Certificate Policy: https://www.keynectis.com/static/content/common/pc-dpc/DSQ_CP__KEYNECTIS_SSL_CA_CP_1.1s.pdf
AUDIT	Audit Type: ETSI 101 456 Auditor: LSTI - La Sécurité des Technologies de l'Information, http://www.lsti.fr/ ETSI Certificate: http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=58&Itemid=53&lang=fr Audit Type: WebTrust EV Readiness Auditor: KPMG, http://www.kpmg.fr/ Audit Report and Management Assertion: https://bugzilla.mozilla.org/attachment.cgi?id=382979 (2009.05.26) > From: Paling, Patrick <Paling.Patrick@kpmg.nl> > Subject: RE: Verifying Authenticity of Audit Report provided by Keynectis > Date: Friday, July 31, 2009, 1:45 AM > Kathleen, > I hereby confirm that KPMG Advisory NV performed the EVpoint-in-time > audit for Keynectis and issued the report referred to in the URL below. > Please do not hesitate to contact me in case you have any further questions. > Best regards, > Patrick From Patrick (KPMG): The CAB Forum also allows ETSI TS 102042 and TS 101456 as a basis for WebTrust EV SSL.
Organization Validation	SSL CPS section 3.2.2 Authentication of an organization identity

	Authentication of an organization identity is based on the verification of information provided by the organization. This information includes the organization name, the address of the organization and documentation or references of the existence of the organization, the domain name it owns. The entity that proceeded to the verification checks that the organization is legally entitled to the exclusive use of its name, by mapping the information provided in the SSL certificate application, Club SSL or ISP SSL contract with information retrieved from official database documentation (database issued from government agencies or competent authorities), that confirms the existence of the organization. That database documentation contains trusted information that is filled by the trusted source that registers the legal company. Information that is subject to verification during the authentication of the organization identity includes the SIREN number, VAT declaration number, DUNS… For the purpose of SSL certificate delivery, the verification also requires to check that the domain name featured in the request belongs to that organization, which is therefore entitled to use it. In this way, verifications are made against domain name database. EV SSL CPS section 3.2: Applicant's existence and identity are verified, including; • Applicant's legal existence and identity, and • Applicant's physical existence (business presence at a physical address), and • Applicant's operational existence (business activity), and • Verification of Applicant's Domain Name. The entity that proceeded to the verification checks that the organization is legally entitled to the exclusive use of its name, by mapping the information provided in the EV certificate application, Club EV or ISP EV contract with information retrieved from official database documentation (Qualified Independent Information Source, Qualified Government Information Source, Qualified Government Tax Information Sources), that confirms the existence of the organization. That database documentation contains trusted information that is filled by the trusted source that registers the legal company.
Domain Name Verification	Keynectis verifies domain control by communicating with the Administrative Contact listed in WHOIS. (CPS section 6.1.3) Google Translations of parts of CPS Section 6.1.3: To avoid errors and fraudulent issuance of SSL certificates, the process is based on the principle of the "separation of duties." The person who performs the authentication cannot proceed with the Audit and vice versa. The process should operate with a buddy (Person 1 / 2 person) who distribute the tasks as follows: • Validation of receiving the order (Person 1) • Verifying the existence of the company and its coordinates (Person 1) • Verification that the company owns the domain name (Person 1) • Verifying the identity of the technical contact and membership of the company whose name has been given in the application (person 2)

	• Verify that the administrator of the domain is aware of the request and does not object (person 2). The authentication procedure determines the precise identity of an organization that makes a request SSL certificate. Authentication is one of the two stages of the validation process, the other being the audit. This step"authentication"establishes that: • The organization indicated in the CSR exists and it has a legal right to exclusive use of its name • The domain of the application it belongs so it can use • The technical contact has the right to apply for it belongs to the organization or corporation mandated by the holder of the domain name which was authorized to apply e The validation of the SSL certificate request is accepted after the 3 following checks with all given an acceptable response by the rule. This is a preliminary step in investigations of administrative error which will be followed by a step telephone checks. 1. The organization's name in the DN is similar (but not necessarily exactly the same) to that of owner of the domain (relationship capital between 2 organizations, applications by a host on behalf of the organization). 2. The owner of the domain name has not blocked the certificate request (24h) after sending the mail informing him of a request from the technical contact. 3. The organization specified in the certificate request (CSR) is related to the owner domain. SSL CPS section 1.3.4, Owner of Domain Name (ODN): The ODN is the legal entity that holds the domain name to include in an SSL certificate delivered by KEYNECTIS SSL CA. The domain name is managed by a domain name administrator. An "Authentication" step enables KEYNECTIS SSL CA to ascertain that: • The organization mentioned in the Certificate Signing Request (CSR) exists and is legally entitled to the exclusive use of its name; • The domain name featured in the request belongs to that organization, which is therefore entitled to use it; • There is either an SSL administrator (refer to § 1.3.6 below) acting as the SSL certificate Applicant or a technical contact (refer tp § 1.3.5 below), acting as the SSL certificate Applicant, who is entitled to submit the request since he belongs to the ODN organization, or a company appointed by the ODN organization, and which authorized him to send the request. SSL CPS section 3.2.2, Authentication of an organization identity: For the purpose of SSL certificate delivery, the verification also requires to check that the domain name featured in the request belongs to that organization, which is therefore entitled to use it. In this way, verifications are made against domain name database. SSL CPS section 3.2.5, Validation of Authority: An applicant authority is checked during the registration and validation process of SSL certificates requests he proceeds to. The authentication of an applicant is based on a request sent to the ODN, whether he or she authorize or not the applicant to act as an applicant for the domain name

	he or she made the SSL certificate request for. • A TC authorization is verified during the retrieval of the SSL certificate by presentation of a retrieval code that was transmitted to the RA during the registration process. The retrieval code is only known from the applicant who transmits it to the TC prior to the retrieval of the SSL certificate. • AN SSL administrator authorization is also based on a document provided by the organization that gives evidence that the SSL administrator is appointed by the organization to this position.

Domain Name Verification for EV	EV SSL CPS section 3.2.2.4, Verification of an Entity Domain Name:
	For the purpose of EV certificate delivery, the verification also requires to check that the domain name featured in the request belongs to the Applicant, which is therefore entitled to use it. In this way, verifications are made against domain name database in order to verify Applicant is a registered holder, or has exclusive control, of the domain name to be included in the EV Certificate. Checks on domain names are such that the KEYNECTIS EV CA confirms such domain name satisfies the following requirements:
	• The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN) approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);
	• Domain registration information in the WHOIS is public and shows the name, physical address, and administrative contact information for the organization. For Government Entity Applicants, the CA relies on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.
	• Applicant:
	  • is the registered holder of the domain name; or
	  • has been granted the exclusive right to use the domain name by the registered holder of the domain name;
	• Applicant is aware of its registration or exclusive control of the domain name.
	• In case an EV Certificate request is made for a domain name containing mixed character KEYNECTIS EV CA visually compares the domain name with mixed character sets with known high risk domains. If a similarity is found then the EV Certificate Request is flagged as High Risk. The CA performs appropriate additional authentication and verification to be certain that Applicant and the target in question are the same organization.

Email Address Verification	CPS section 2.3.1: Keynectis verifies that the entity submitting the request controls the email account associated with the email address referenced in the certificate.
Code Signing Identity Verification	Not Applicable – Code Signing trust bit is not enabled.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  o SSL certs are OV and EV
	  o SSL CPS section 4.1.2: Duration of the SSL certificate (1 or 2 year(s))

	◦ EV SSL CPS section 5.6: The validity period of an EV certificate is 1 or 2 year(s). • Wildcard DV SSL certificates ◦ Not found. • Delegation of Domain / Email validation to third parties ◦ **Yes, KEYNECTIS delegates domain validation to third parties.** ◦ EV SSL CPS: ▪ KEYNECTIS EV customer service acts as an RA for EV certificates. ▪ EV Administrators act as RA for the Club EV and the ISP EV offers, (refer to § 1.3.8 below). ◦ EV SSL CPS section 1.3.8, EV administrator: An EV administrator is a person authorized by the EV customer to act as EV certificate approver or requester for Club EV and ISP EV offers. The EV administrator may also revoke certificates on behalf of the EV customer he or she is authorized to act for. The EV administrator act as an RA service. When a KEYNECTIS EV customer owns its RA services it has to first contract with the KEYNECTIS EV CA. The contract mentions that: ▪ The organization is responsible for internal authentication and all checks necessary to validate EV certificates in accordance with the present CP; ▪ The organization, acting as an RA, implements relevant parts of the present CPS; ▪ The organization has to inform the KEYNECTIS EV CA , in a reasonable and safe delay, of any changes related to the identity and the position of its representatives toward KEYNECTIS EV CA; ▪ Its EV administrator uses electronic certificates on smartcards to authenticate with the KEYNECTIS EV CA website when proceeding to EV certificate application and validation; ▪ Its RA services are subject to KEYNECTIS EV CA audits. ▪ An organization that owns its RA service also relies on TC for technical aspects of the EV certificate lifecycle management. ◦ EV SSL CPS section 1.3.8.1, EV administrator for Club EV offer: In case of a Club EV offer, the EV administrator is acting as an applicant for the organization that owns the domain names. For the Club EV offer, the EV administrator acts as an RA and manages RA services for the KEYNECTIS EV CA. In this perspective, the EV administrator is in charge of: ▪ Filling the EV certificate requests on behalf of the EV customer ▪ Transmitting the EV certificate retrieval codes to the appropriate technical contact ▪ Revoking the EV certificate ▪ Authenticate to the KEYNECTIS EV CA as necessary. ◦ EV SSL CPS section 1.3.8.2, EV administrator for ISP EV offer: In case of the ISP EV offer, the EV

	administrator is acting as an applicant for the ISP which himself is acting on behalf of organizations owning the domain names. For the ISP EV offer, the EV administrator acts as an RA and manages RA services for the KEYNECTIS EV CA. In this perspective, the EV administrator is in charge of: ▪ Filling the EV certificate requests on behalf of the (ODN) hosted entities ▪ Transmitting the EV certificate retrieval codes to the appropriate technical contact ▪ Revoking the EV certificate ▪ Authenticate to the KEYNECTIS EV CA as necessary. • Issuing end entity certificates directly from roots o No, end-entity certificates are issued through subordinate CAs. • Allowing external entities to operate unconstrained subordinate CAs o No, Subordinate CAs are internally-operated. • Distributing generated private keys in PKCS#12 files o No. EV SSL CPS section 3.2: KEYNECTIS EV CA ensures that the customer requesting an EV certificate owns the private key corresponding to the public key to be certified, using CSR on PKCSs#10 format. • Certificates referencing hostnames or private IP addresses o No. EV SSL CPS section 3.1: The Common Name is the Fully Qualified Domain Name (FQDN). It is the name of the website to be secured. Therefore, the Common Name is all that follows http://, including the extension. The Common Name can never be an IP address. • OCSP Responses signed by a certificate under a different root o No • CRL with critical CIDP Extension o CRLs import into Firefox without error. • Generic names for CAs o CA is already included in NSS.