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.

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
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.
The root CA 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://trustcenter-crl.certificat2.com/keynectis/crl/class2keynectisca.crl Error Importing CRL to local Database. Error Code:ffffe009 ffffe009 is equivalent to -8183, "Security library: improperly formatted DER-encoded message." It means that the reply contained anything other than a valid DER-encoded CRL. Typical Resolution: Change encoding from PEM to DER. EV certificates CRL: http://trustcenter-crl.certificat2.com/keynectis/class2keynectisevca.crl Imports into Firefox without error. NextUpdate: 7 days **EV SSL CPS section 2.3 Time or Frequency of Publication** The EV certificate status is made available through CRLs. CRLs are published at least every 24 (twenty four) hours.

OCSP Responder URL	Authority Information Access Not Critical OCSP: URI: http://kvalid.keynectis.com/evssl-ocsp/ What is the maximum time until the OCSP responders are updated to reflect an end-entity revocation? http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days."
List or description of subordinate CAs operated by the CA organization associated with the root CA.	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
Subordinate CAs operated by third parties	This root does not have any subordinate CAs that are operated by third parties.
List any other root CAs that have issued cross-signing certificates for this root CA	This root has not been involved in cross-signing with any other root CAs.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV, EV 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.
EV policy OID(s)	1.3.6.1.4.1.22234.2.5.2.3.1

CP/CPS	All of the documents listed below are in English, unless otherwise noted. CPS for EV SSL CA: https://bugzilla.mozilla.org/attachment.cgi?id=382981 Also available here: https://www.keynectis.com/static/content/common/pc-dpc/DSQ_NT_KEYNECTIS_EV_SSL_CA_CPS_20090504s.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 CPS for SSL CA: https://www.keynectis.com/static/content/common/pc-dpc/DSQ_PC_PC_AC_KEYNECTIS_SSL_1.2s.pdf Keynectis Information: https://www.keynectis.com/en/support-information/pc.html CPS in French: http://www.keynectis.com/PC/CPS_KEYNECTIS_120407v1.1.pdf
AUDIT	Audit Type: ETSI 101 456 Auditor: LSTI - La Sécurité des Technologies de l'Information Auditor website: http://www.lsti.fr/ ETSI Certificate: http://www.keynectis.com/PC/Certificat_conformite_ETSI_101-456.pdf This audit expired 17th October 2008. Has a new audit been performed according to the ETSI TS 101.456 criteria? If yes, please provide link to the audit report/statement. Audit Type: WebTrust EV Readiness Auditor: KPMG Auditor website: http://www.kpmg.fr/ Audit Report and Management Assertion: https://bugzilla.mozilla.org/attachment.cgi?id=382979 (2009.05.26)

Review CPS sections dealing with subscriber verification (section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.

- - 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.
  - SSL CP section 3.2: 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.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
  - CPS section 2.3.1: For certificates with the E-mail Protection EKU (1.3.6.1.5.5.7.3.4), Keynectis verifies that the entity submitting the request controls the email account associated with the email address referenced in the certificate.
- Verify identity info in code signing certs is that of subscriber
  - Code signing trust bit isn't set, and isn't requested.

Flag Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
  - No. EV SSL CPS section 5.6:
    - The validity period of an EV certificate is 1 or 2 year(s).
    - EV certificates issued with a 2 year(s) validity period are generated using a key which is 2048 bits long for the RSA algorithm.
- 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
  - No, end-entity certificates are issued through subordinate CAs.
- Allowing external entities to operate unconstrained subordinate CAs
  - No, Subordinate CAs are internally-operated.
- Distributing generated private keys in PKCS#12 files
  - 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
  - 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
  - ?
- CRL with critical CIDP Extension
  - No, the CRLs don't have the CIDP extension.
- Generic names for CAs
  - CA is already included in NSS.

Verify Audits
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
  - Need to do. Contact information provided in bug for the WebTrust EV audit.
  - Also need to do for the WebTrust CA or the ETSI 101 456 audit.
- For EV CA's, verify current WebTrust EV Audit done.
  - WebTrust EV audit provided.
- Review Audit to flag any issues noted in the report
  - No issues noted in the WebTrust EV audit report
  - Need the other audit report.