Bugzilla ID: 844163
Bugzilla Summary: Add CSOEC root certificate

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	Conseil Supérieur de l'Ordre des Experts-Comptables (CSOEC)
Website URL	https://www.signexpert.fr
Organizational type	The Ordre des Experts-Comptables (OEC), also known as the French Institute of Certified Public Accountants, is a public body supervised administratively by the Minister of Finance which represents the French certified public accountants in public practice. The OEC consists of a national body called the Conseil Supérieur del'Ordre des Experts-Comptables (CSOEC), also known as the Certified Public Accountants National Council, and regional bodies – the Regional Councils – covering metropolitan France and the overseas departments and territories. These councils are headed by representatives elected by members of the profession. The national body and the 25 regional bodies are each considered as a separate subordinate CA issuing end-entity certificates. The regional bodies issue certificates for the certified public accountants within their region, and the national body issues certificates for the order's elected representatives.
Primark Market / Customer Base	By definition, the French Certified Public Accountants addresses the accounting services' market. The OEC's CAs cover metropolitan France and the overseas departments and territories. The Signexpert certificates are exclusively issued to the active members of the OEC. Only members of the OEC may keep, centralize, open, close, monitor, adjust and consolidate the accounts of entities to which they are not linked by an employment contract and carry out contractual audits. Beyond these regulated engagements, Certified Public Accountants provide advisory services to their clients, e.g., payroll, and to some extent tax advice and legal services. There are currently more than 18,900 individual French Certified Public Accountants and 15,600 accounting firms in France.
Impact to Mozilla Users	Mozilla users encounter Signexpert certificates through digitally signed e-mails.
Inclusion in other major CA trust lists	We have no root certificate yet included in any other major trust lists, but we have asked for inclusion in Adobe's AATL and Microsoft Root Certificate Program at the same time we started the current process with the Mozilla Foundation. The reviewing process is on its way.
CA Contact Information	CA Email Alias: signexpert@cs.experts-comptables.org Title / Department: Direction des études informatiques

Technical information about each root certificate

Certificate Name	Ordre des Experts-Comptables
Certificate Issuer Field	CN = Ordre des Experts-Comptables OU = 0002 775670003 O = Ordre des Experts-Comptables C = FR
Certificate Summary	This root signs intermediate issuing certificates. The entire PKI is operated by Keynectis Inc., and audited by LSTI.
Root Cert URL	https://www.signexpert.fr/cms/index.php/content/download/770/3228/version/1/file/AC-R.cer
SHA1 Fingerprint	82:71:9A:76:9D:88:18:2C:70:B9:C0:C9:24:73:6B:D7:A7:11:CF:C7
Valid From	2011-05-09
Valid To	2031-05-09
Certificate Version	3
Certificate Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	4096
Example Certificate (non-SSL)	https://bugzilla.mozilla.org/attachment.cgi?id=777159 (no password)
CRL URL	NextUpdate for CRLs of end-entity certs is 3 days. The CRL's end-entity certs' URL are: http://seec.experts-comptables.fr/CRL/CRL_ALSACE.crl http://seec.experts-comptables.fr/CRL/CRL_AQUIT.crl http://seec.experts-comptables.fr/CRL/CRL_AUVERGN.crl http://seec.experts-comptables.fr/CRL/CRL_B-FC.crl http://seec.experts-comptables.fr/CRL/CRL_BRETAGNE.crl http://seec.experts-comptables.fr/CRL/CRL_CHAMPAG.crl http://seec.experts-comptables.fr/CRL/CRL_CORSE.crl http://seec.experts-comptables.fr/CRL/CRL_GPE.crl http://seec.experts-comptables.fr/CRL/CRL_GUYANE.crl http://seec.experts-comptables.fr/CRL/CRL_REUNION.crl http://seec.experts-comptables.fr/CRL/CRL_LN-PCAL.crl http://seec.experts-comptables.fr/CRL/CRL_LIMOGES.crl http://seec.experts-comptables.fr/CRL/CRL_LORRAIN.crl http://seec.experts-comptables.fr/CRL/CRL_MARSEIL.crl http://seec.experts-comptables.fr/CRL/CRL_PACA.crl http://seec.experts-comptables.fr/CRL/CRL_MARTINI.crl http://seec.experts-comptables.fr/CRL/CRL_MONTPEL.crl http://seec.experts-comptables.fr/CRL/CRL_ORLEANS.crl http://seec.experts-comptables.fr/CRL/CRL_PAR-IDF.crl http://seec.experts-comptables.fr/CRL/CRL_P-LOIRE.crl http://seec.experts-comptables.fr/CRL/CRL_PIC-ARD.crl http://seec.experts-comptables.fr/CRL/CRL_POITOU.crl http://seec.experts-comptables.fr/CRL/CRL_RHO-ALP.crl http://seec.experts-comptables.fr/CRL/CRL_R-NORMA.crl

	http://seec.experts-comptables.fr/CRL/CRL_MIDI-PY.crl http://seec.experts-comptables.fr/CRL/CRL_CSOEC.crl
OCSP URL	OCSP URI in the AIA of end-entity certs: http://ocsp.experts-comptables.fr/OEC
Requested Trust Bits	Email (S/MIME)
SSL Validation Type	Not applicable – not requesting websites (SSL) trust bit.
EV Policy OID(s)	Not applicable

CA Hierarchy information for each root certificate

CA Hierarchy	The « Ordre des Experts-Comptables », OEC, (French Institute of Certified Public Accountants), is a public body supervised administratively by the Minister of Finance which represents the French certified public accountants (« expert-comptable » in french) in public practice. The OEC consists of a national body, the « Conseil Supérieur de l'Ordre des Experts-Comptables » (CSOEC, Certified Public Accountants National Council), and regional bodies – the Regional Councils – covering metropolitan France and the overseas departments and territories. These councils are headed by representatives elected by members of the profession. Each of the national body and the 25 regional bodies is considered as a separate CA issuing end-entity certificates: the regional bodies issue certificates for the certified public accountants within their region, and the national body issues certificates for the order's elected representatives. This root signs the following intermediate certificates. (see diagram below) • An intermediate cert for each of the regional CAs (shown in violet); exclusively issue certificates to public accountants. • Five intermediate certs for issuing certificates for servers or technical certificates (shown in orange) ◦ OEC-Chiffrement: is an inactive CA, reserved for the future issuance of ciphering certificates. ◦ OEC-SSL: is an inactive CA, reserved for the future issuance of SSL certificates for the OEC's servers. ◦ OEC-CC: is a CA that will (in the near future) issue signing certificates for accountants' offices. These certificates will be used for authenticating documents produced by the accountants' offices. ◦ OEC-OCSP is a technical CA that issues OCSP-signing certificates for the PKI. ◦ Horodatage is an inactive technical CA, reserved for the future issuance of timestamping certificates. • One intermediate cert for the Council's CA national body of the order (shown in blue); exclusively issues certificates to the elected members of the order's council or end-users test certificates for the PKI. These certificates are used by the council members to sign official documents, such as the CP.
Externally Operated SubCAs	The entire PKI is externally operated by Keynectis Inc. (www.keynectis.com).
Cross-Signing	All of the issuing sub-CAs are cross-signed by the following CAs. • Adobe Root CA / Keynectis CDS CA (not in Mozilla's root store) • Certplus Class 2 Primary CA (in the Mozilla root store) The cross-signing currently allows "smooth" signature verification in the following software: • Adobe Reader (for PDF files) • e-mails readers (Certplus Class 2 crosscertification) The signature creation software used by our certificate owners distinguishes between PDF signatures and other ones: when it creates a PDF signature, it includes the certification chain up to the Adobe's root CA; otherwise, it includes the "our" certification chain, that is, up to the OEC's root CA. Thus, Mozilla software will only see, verify or check our certification chain.

Hiérarchie 2012

Verification Policies and Practices

Policy Documentation	All documents are in French. Document Repository: https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification Root CA's certification policy (CP): http://www.signexpert.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf CSOEC's council members' CA's CP (signature certificates): https://www.signexpert.fr/PC/PC_ELUS.pdf CSOEC's council members' CA's CP (auth and signature certificates): https://www.signexpert.fr/PC/PC_ELUS_AS.pdf Certified accountants' CA's CP (signature certificates): https://www.signexpert.fr/PC/PC_Experts-Comptables.pdf Certified accountants' CA's CP (auth and signature certificates): https://www.signexpert.fr/PC/PC_Experts-Comptables_AS.pdf
Audits	Audit Type: ETSI/TS101456 V1.4.3 Auditor: LSTI, http://www.lsti-certification.fr/ Audit Statement: https://bug844163.bugzilla.mozilla.org/attachment.cgi?id=792857 (2012.11.26) http://www.lsti-certification.fr/images/liste_entreprise/RGS_ETSI.pdf The rows under "Conseil Supérieur de l'Ordre des Experts Comptables" correspond with this CA Hierarchy. The "Arrêté du 26 juillet 2004" indicates that the CA is also certified with respect to the French signature law. An annual audit is required to maintain a status of "Valide". The ETSI certification process is described here: http://lsti-certification.fr/index.php/les-normes-etsi/etsi-ts-101-456.html (they also mention there that the "Arrêté" has a little more requirements than the ETSI 101 456). The last part of the process is "Le suivi annuel" (the annual maintainance) : "La qualification est valide trois ans, sous réserve d'une surveillance annuelle" (The certification is valid for three years, assuming that an annual audit is performed).
Baseline Requirements	Not applicable – Not requesting the websites (SSL) trust bit
SSL Verification	Not applicable – Not requesting the websites (SSL) trust bit
Subscriber Verification Procedures	Subscriber identity verification process can be found in section "IV.2.1 Exécution des processus d'identification et de validation de la demande" (Request validation and subscriber's identification) of the certification policies. The process is as follows: Le contrôle d'Enregistrement effectue les opérations suivantes lors de la remise au demandeur du support en face-à-face (cf. IV.4) : 1. valider l'identité du futur porteur et son inscription au tableau de l'Ordre ; dans le cas des changements de nom (nom de jeune fille, mariages…), l'AE s'assurera par tout autre moyen de l'identité du demandeur à l'aide de pièces complémentaires. 2. vérifier la cohérence des justificatifs présentés, notamment par rapport au contenu de la demande ; 3. s'assurer que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation). Translation: The registration operator performs the following operations during the deliverance of the certificate, which occurs face-to-face: 1. Validate the subscriber's identity [this verification is performed with respect to the National Identity Card of the subscriber] and the fact that he/she is an actual member of the Order; should the subscriber's name had changed (spouse name…), the RA will ensure by any other means of the subscriber's identity. 2. Check the provided documents with respect to the request 3. Ensure that the subscriber's has read and approved the subscriber agreements.

Email Address Verification Procedures	The e-mail address to be included in the certificate is provided by the subscriber when he/she fills up the online subscription form. The form explicitly mentions that this e-mail address is a professional one and that it will be the one used to sign e-mails. Confirmation of the e-mail address is needed for the request to be considered complete. The email verification process can be found in section "IV.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat" (Process and responsibilities for the confirmation of a certificate request) of the certification policies. The process contains the following step: Après le paiement en ligne des frais relatifs à l'acquisition du certificat, une demande de confirmation est envoyée par e-mail. La demande n'est établie que lorsque le demandeur répond à cet e-mail. (Once the certificate's fees have been paid, a confirmation e-mail is sent [to the e-mail address that was submitted in the subscription form.) The request is complete only when the subscriber answers that confirmation e-mail. The confirmation e-mail contains an unpredictable URL that the subscriber must visit to confirm his/her subscription request. Hence, confirmation of the request can only be done by the e-mail recipient. Comment #8: The online subscription form is the same for all the issuing CAs. That web portal (www.signexpert.fr) is managed by the CSOEC, and the enrolment/renewal/revocation processes are the same for all the CAs. The OEC had to technically create one CA for each of the OEC's regional bodies because of legal questions (the OEC's structure comes from a French regulation dating back to 1945) but, for what pertains to processes, management and certificates' life-cycle, everything is actually defined, managed and controlled by the CSOEC and, of course, unified: there is no reason to have distinct processes between regions/CAs, and there is none, indeed. All the regional registration authorities use the very same web portal to manage their own "flock" of certificate owners.
Code Signing Subscriber Verification Procedures	Not applicable – Note requesting the code signing trust bit
Multi-factor Authentication	There is currently no multi-factor authentication for registration authorities, but certificate issuance is strictly limited by the Certification Policy to actual members of the French certified public accountants. The main responsibility of the OEC is to certify and maintain the list of its members as a public service. For instance, should an accountant loose his/her membership, his/her certificates will be immediately revoked. The PKI is daily synchronized with the official OEC's membership list. The contents of that list are used to fill up the certificates' DN and used as reference data during the certificates' life cycle. At the technical level, which is managed by Keynectis, and ETSI TS 101 456 certified (see above), access to the CA's interfaces is controlled by hardware tokens.
Network Security	Network security controls have been asserted by LSTI during its audit of the CA's PKI.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes, see above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	Not applicable
Revocation of Compromised Certificates	Yes
Verifying Domain Name Ownership	Not applicable

Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	Not applicable
DNS names go in SAN	Not applicable
Domain owned by a Natural Person	Not applicable
OCSP	See above.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	Not applicable
Wildcard DV SSL certificates	Not applicable
Email Address Prefixes for DV Certs	Not applicable
Delegation of Domain / Email validation to third parties	See above
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	See above
Distributing generated private keys in PKCS#12 files	Comment #5: That is not applicable to us : we provide qualified certificates. As such, the private keys are generated and stored into EAL4+ CC-evaluated hardware tokens, and we do not distribute software keys/certificate in any case (doing so would be a major violation of the ETSI/TS101456 and would immediately nullify our conformance assessment).
Certificates referencing hostnames or private IP addresses	Not applicable
Issuing SSL Certificates for Internal Domains	Not applicable
OCSP Responses signed by a certificate under a different root	No
CRL with critical CIDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	No