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, (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.
Primark Market / Customer Base	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.
Are there particular vertical market segments in which it operates?	By definition, the French Certified Public Accountants addresses the accounting services' market.
Does the CA focus its activities on a particular country or other geographic region?	The OEC's CA's exclusively cover metropolitan France and the overseas departments and territories.

Impact to Mozilla Users	Today, Mozilla users will encounter Signexpert certificates through digitally signed e-mails.
CA Contact Information	Direction des études informatiques Conseil supérieur de l'Ordre des experts-comptables 19 rue Cognacq Jay 75341 Paris Cedex 07 FRANCE
CA Email Alias:	signexpert@cs.experts-comptables.org

CA Phone Number:	
Title / Department:	Direction des études informatiques

Technical information about each root certificate	
Certificate Name	C=FR, O=Ordre des Experts-Comptables, OU=0002 775670003, CN=Ordre des Experts-Comptables
Certificate Issuer Field	The issuer's Organization Name and CN contain the order's official name. That is completed by the Organization Unit's field which, as required by the RGS certification scheme (see below), requires the OU to conform to the ISO/IEC 6523. It thus contain the issuer's International Code Designator (ICD) number and an entity number, both forming a word-wide unique registration number. The entity number is, herein, the « sirene » number of the Order, an official number given to enterprises and legal bodies by the French institute of statistics (INSEE). See *http://www.cyber-identity.com/download/ICD-list.pdf* for a presentation of the scheme.
Certificate Summary	That certificate is the root certificate for the OEC's PKI.
Root Cert URL	*https://www.signexpert.fr/cms/index.php/content/download/770/3228/version/1/file/AC-R.cer*
SHA1 Fingerprint	82719a769d88182c70b9c0c924736bd7a711cfc7
Valid From	2011-05-09
Valid To	2031-05-09
Certificate Version	3
Certificate Signature Algorithm	sha256WithRSAEncryption
Signing key parameters	RSA 4096 bits
Test Website URL (SSL)	N/A
Example Certificate (non-SSL)	-----BEGIN CERTIFICATE----- MIIHpDCCBoygAwIBAgISEicxkkOw9Oj2z64ysMHYmjfRMA0GCSqGSIb3DQEBCwUA MIGWMQswCQYDVQQGEwJGUjE9MDsGA1UECgw0Q29uc2VpbCBTdXDDqXJpZXVyIGRl IGwnT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczEXMBUGA1UECxMOMDAwMiA3 NzU2NzAwMDMxLzAtBgNVBAMTJkVsdXMgZGUgbCdPcmRyZSBkZXMgRXhwZXJ0cy1D b21wdGFibGVzMB4XDTExMDgyNjE1MzAxNFoXDTEzMDgyNjE1MzAxNFowgewxCzAJ BgNVBAYTAkZSMT0wOwYDVQQKDDRDb25zZWlsIFN1cMOpcmlldXIgZGUgbCdPcmRy ZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLDA4wMDAyIDc3NTY3MDAw MzEiMCAGA1UEDAwZRWx1IGNvbnNlaWxsZXIgc3Vww6lyaWV1cjFJMEcGA1UEBRNA MmZkNWU5Yjk1NzI0ZmVjODQ0MTlmN2YyMWRkMjUwNDExN2FhYjkzMTQxMTI4NzIx YTVjNDA2MTU3MjEwMjg4YzEWMBQGA1UEAwwNamVhbiBzYXBob3JlczCCASIwDQYJ KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKoSCTreCEFdPl1IrEPiqIMpJWFWiQJG VHEk3oktUXVsXoAHLbOxePzimleooFnJYy09NBLz7XWAGO8MeKUsepaXSgxu8ja+ 5xF9sx/7WRn/v4sSxZIt4H4aE8exsMky1fy6rTSE3ygP4APMcO2TypsqdI8tZX/1 RSAdxgGKOLHToj6iYISlukribzBG7T1K1odcR3W8HAu3XvxLqQO28YMj+O4/m3tH mMJJ3scEInA/QEkvT26XiYMdK0sG3q9JQF985qlzdGp/zUl7xBBDiUpRLUr/0K0O NvcRffUvkgyrtvgSIJGon4sxxwpu3bHlzGfgf64X5+IFTMEQTG8k4YUCAwEAAaOC A5IwggOOMAwGA1UdEwEB/wQCMAAwDgYDVR0PAQH/BAQDAgZAMCMGA1UdEQQcMBqB GGplYW4uc2FwaG9yZXNAc29nYXJleC5mcjAUBgNVHSUEDTALBgkqhkiG9y8BAQUw gcQGA1UdIASBvDCBuTCBtgYKKoF6AYElAQMGATCBpzA/BggrBgEFBQcCARYzaHR0 cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BDL1BDX0VMVVNfQVMucGRm MGQGCCsGAQUFBwICMFgaVkNlIGNlcnRpZmljYXQgZGUgbWVtYnJlIGRlIGwnT3Jk cmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlcyBzZWxvbiBsYSBwb2xpdGlxdWUgY2kt ZGVzc3VzMBMGCiqGSIb3LwEBCQIEBTADAgEBMIIBaQYDVR0fBIIBYDCCAVwwggFY oIIBVKCCAVCGM2h0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwv Q1JMX0NTT0VDLmNybIYqaHR0cDovL3d3dy5zaWduZXhwZXJ0LmZyL0NSTC9DUkxf

Technical information about each root certificate	
	Q1NPRUMuY3JshoHsbGRhcDovL2xkYXBzZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DTj1FbHVzJTIwZGUlMjBsJTI3T3JkcmUlMjBkZXMlMjBFeHBlcnRzLUNvbXB0YWJsZXMsT1U9MDAwMiUyMDc3NTY3MDAwMyxPPUNvbnNlaWwlMjBTdXBlcmlldXIlMjBkZSUyMGwlMjdPcmRyZSUyMGRlcyUyMEV4cGVydHMtQ29tcHRhYmxlcyxDPUZSP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q7YmluYXJ5P2Jhc2U/b2JqZWN0Y2xhc3M9cGtpQ0EwgYUGCCsGAQUFBwEBBHkwdzAyBggrBgEFBQcwAYYmaHR0cDovL29jc3AuZXhwZXJ0cy1jb21wdGFibGVzLmZyL09FQy8wQQYIKwYBBQUHMAKGNWh0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9jZXJ0L2NlcnRfQ1NPRUMucDdiMCIGCCsGAQUFBwEDBBYwFDAIBgYEAI5GAQEwCAYGBACORgEEMB0GA1UdDgQWBBS7UwKaVozrnRn4gk0aOxDNIkzvazAfBgNVHSMEGDAWgBTVpj3KyaPDBKDcjQGyNTGtZlgL/DANBgkqhkiG9w0BAQsFAAOCAQEAz05EH8h/02YRL1scFKPCfbXFfVxlkJIRjLMufQ1Ee1/+Zd57hArl3xjwHMhykar2nePKOAQKD//kaffkWsMFoZ6Tz6BB6WJlcBSKy8QyDWiDeUdJoYCUli06ZBjTjHTAYtp3TBXqYgJLEvGs+0oBu06JFmNNXs7Dm/j6+s8lgy0gHFQmhUdFNh8hPZSw+GMar304/ZqAnNgP43ua2wpOPvDC/gozZv1P0fPuTLnZE3hSMSKr7JLZg8JpGcXOjfMA/zcNuslTXRzb2f8/iWiOFU9gxVWxvG6dGsYXFOXjOfvTLz83RvbnGiGFzRArVd7bQZQIYf5g+YrRfmTCb0dXTA==
-----END CERTIFICATE-----
CRL URL	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 NextUpdate for CRLs of end-entity certs is 3 days after the issuance date. In the CP, the announced value is 1 day (24 hours).
OCSP URL (Required now)	OCSP URI in the AIA of end-entity certs http://ocsp.experts-comptables.fr/OEC Maximum expiration time of OCSP responses

Technical information about each root certificate	
	3 months
Requested Trust Bits	Email (Public accountants sign documents on a daily basis, including e-mails)
SSL Validation Type	Not applicable (e.g. DV, OV, and/or EV)
EV Policy OID(s)	Not applicable

CA Hierarchy information for each root certificate

The CA Hierarchy is as follows :

Below the root CA, ones find all the end-entity issuing CA's :

- in violet, there are the regional CA's. These CA exclusively issue certificates to public accountants.
- in orange, there are CA that issue servers or technical certificates (that is, not end-users certificates)
  - 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.

- in blue, the Council's CA (national body of the order). That CA 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, for instance).

Externally Operated SubCAs

The root has no subCA operated by an external third party.

The whole PKI is externally operated by Keynectis Inc. (www.keynectis.com), acting as Certificate Service Provider (CSP). Keynectis Inc. has been certified as a compliant ETSI TS 101 456 CSP by LSTI.

Cross-Signing

List all other root certificates for which this root certificate has issued cross-signing certificates.	None
List all other root certificates that have issued cross-signing certificates for this root certificate. *If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.*	The root CA is not cross-signed, however, all the issuing sub-CA's are cross-signed by the following CA's. • Adobe Root CA / Keynectis CDS CA (not in Mozilla's root store, but see below) • Certplus Class 2 Primary CA (is in the Mozilla root store) Please note that these cross-signing were only used to allow “smooth” signature verification the following softwares before we could actually apply to be ourselves included in those softwares' trusted lists : • Adobe Reader (for PDF files) • e-mails readers (Certplus Class 2 cross-certification) 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.

Verification Policies and Practices

We rely on publicly available documentation and audits of those documented processes to ascertain that the CA takes reasonable measures to confirm the identity and authority of the individual and/or organization of the certificate subscriber.

If the CP/CPS documents are not in English, then the portions of those documents pertaining to verification of the certificate subscriber ***must be translated into English****. For all of the items listed below, provide both a pointer to the original document (and section or page number of the relevant text) as well as the translated text.*

Documentation: CP, CPS, and Relying Party Agreements

The publicly accessible URLs to the document repository and the published document(s) describing how certificates are issued within the hierarchy rooted at this root, as well as other practices associated with the root CA and other CAs in the hierarchy, including in particular the Certification Practice Statement(s) (CPS) and related documents.

The following published documents are publicly available (all these documents are in french):

http://www.signexpert.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf	Root CA's certification policy (CP)
https://www.signexpert.fr/PC/PC_ELUS.pdf	CSOEC's council members' CA's certification policy (CP for signature certificates)
https://www.signexpert.fr/PC/PC_ELUS_AS.pdf	CSOEC's council members' CA's certification policy (CP for authentication and signature certificates)
https://www.signexpert.fr/PC/PC_Experts-Comptables.pdf	Certified accountants' CA's certification policy (CP for signature certificates).
https://www.signexpert.fr/PC/PC_Experts-Comptables_AS.pdf	Certified accountants' CA's certification policy (CP for authentication and signature certificates).

The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.

Not applicable to our certificates.

Audits

The publicly accessible URLs to the published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org site or elsewhere.

We need a publishable statement or letter from an auditor (who meets the requirements of the Mozilla CA Certificate Policy) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of one of:

- *ETSI TS 101 456*
- *ETSI TS 102 042*
- *WebTrust Principles and Criteria for Certification Authorities*

The CA's have been certified with respect to ETSI/TS101456 V1.4.3,"Policy Requirements for certification authorities issuing qualified certificates" with QCP public+SSCD profile on the 17th of december, 2012, by *http://www.lsti-certification.fr/*, which maintains a public list of certified CA's at the following URL : *http://lsti-certification.fr/index.php/les-normes-etsi/les-listes.html* (click on the link named "Accéder à la liste de prestataires certifiés ETSI").

Please note that LSTI has already certified several AC's that are currently included in Mozilla's

trusted anchors list (Certigna of Dhimyotis, Certinomis, etc.).

> *Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results.*

Not applicable (no SSL certificate)

> *The audit should not be more than a year old. If it is, then provide an estimate of when the updated audit report will be available. While ETSI Certificates may be valid for 3 years, it is our expectation that there is an annual renewal/review process for the ETSI Certificate to remain valid.*

Both an internal audit and a review by LSTI are planned for this year. We will inform you of the audits' results as soon as they are available.

> *Renewed root certificates also need to be included in audits. If the root certificate was created after the most recent audit, then provide an estimate of when the new audit report (that includes the operations of the new root) will be available.*

The root certificate has not been renewed since the last audit.

SSL Verification Procedures

Not applicable (Website trust bit not enabled).

Email Address Verification Procedures

> *URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate subscriber.*

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 explicitely mentions that this e-mail address is a professional one and that it will be the one used to sign e-mails. The e-mail's address must be entered twice by the subscriber. Confirmation of the e-mail's 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 adress 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 impredictable 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.

> *If subscriber identity verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity and authority of the certificate subscriber.*

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).	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.

Code Signing Subscriber Verification Procedures

Not applicable.

Multi-factor Authentication

> *Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance or specify the technical controls that are implemented by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.*

There is currently no multi-factor authentication for registration authorities, but certificate issuance is indeed strictly limited by the Certification Policy to a pre-approved domain of subscribers: as explained above, certificates are only issued to actual members of the french certified public accountants (the so-called “experts-comptables”). 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 thus daily synchronized with the official OEC's membership list. The contents of that list are used to fill up the certificates' DN and used a reference data during the certificates' life-cycle.

> *For each account that can access the certificate issuance system, do you have the log-in procedure require something in addition to username/password?*

At the technical level, which is managed by Keynectis, an ETSI TS 101 456 certified CSP (see above), access to the CA's interfaces is controled by hardware tokens.

> *Specify the form factor that you use. Examples of multi-factor authentication include smartcards, client certificates, one-time-passwords, and hardware tokens.*
>
> *This must apply to all accounts that can cause the approval and/or issuance of end-entity certificates, including your RAs and sub-CAs, unless there are technical controls that are implemented and controlled by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.*

If technical controls are used instead of multi-factor auth for any accounts, then specify what those technical controls are.

Network Security

CAs must maintain current best practices for network security, and have qualified network security audits performed on a regular basis. The CA/Browser Forum has published a document called Network and Certificate System Security Requirements which should be used as guidance for protecting network and supporting systems.

Confirm that you have done the following, and will do the following on a regular basis:

Maintain network security controls that at minimum meet the 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.

Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.

All these practices have been asserted by LSTI during its audit of the CA's.

Response to Mozilla's CA Recommended Practices

https://wiki.mozilla.org/CA:Recommended_Practices

Publicly Available CP and CPS

The CP are available at : *http://www.signexpert.fr/PC/*. All these documents are in french.

The CPS are not publicly available.

CA Hierarchy

The CA hierarchy has a single root.

Audit Criteria

OK

Document Handling of IDNs in CP/CPS

Not applicable.

Revocation of Compromised Certificates

OK

Verifying Domain Name Ownership

Not applicable.

Verifying Email Address Control

We rely on public documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met.

Section 7 of the Mozilla CA Certificate Inclusion Policy states: "for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate"

The CA's public documentation needs to provide sufficient information describing how the email address is verified to be owned/controlled by the certificate subscriber. For instance, if a challenge-response type of procedure is used, then there needs to be a brief description of the process. If public resources are used, then there should be a description of which public resources are used, what data is retrieved from public resources, and how that data is used to verify that the certificate subscriber owns/controls the email address.

The recommended way to satisfy this requirement is to perform a challenge-response type of procedure in which the CA sends email to the email address to be included in the certificate, and the applicant must respond in a way that demonstrates that they have control over that email address. For instance, the CA may send an email to the address to be included in the certificate, containing secret unpredictable information, giving the applicant a limited time to use the information within.

It is not sufficient for the CP/CPS to just say that an email is sent to the customer. The CP/CPS needs to be clear that the RA sends email to the email address to be included in the certificate. The CP/CPS needs to be clear that the email shall contain some non-predictable information that the subscriber must then use or respond with to confirm that the owner of the email address actually received the email and responded.

See above.

Verifying Identity of Code Signing Certificate

Not applicable.

Subscriber

DNS names go in SAN

Not applicable.

Domain owned by a Natural Person

Not applicable.

OCSP

OCSP responders should be set up to listen on a standard port (e.g. port 80), because firewalls may block ports other than 80/443. Firefox and some other clients do not work with HTTPS OCSP responders, and many firewalls block requests that aren't over port 80, so OCSP responders must be accessible over HTTP (not only HTTPS) on port 80.

As per the CA/Browser Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, the OCSP URI must be provided in the certificate, except when OCSP stapling is used. BR #13.2.2: "The CA SHALL update

information provided via an Online Certificate Status Protocol..." From Appendix B regarding authorityInformationAccess in Subordinate CA Certificate and Subscriber Certificate: "With the exception of stapling ... this extension MUST be present ... and it MUST contain the HTTP URL of the Issuing CA's OCSP responder..."

As per the CA/Browser Forum's Guidelines for EV Certs, CAs must provide an OCSP capability for end-entity certificates that are issued after Dec 31, 2010. Mozilla is considering technical ways to enforce this OCSP requirement such that if Firefox cannot obtain a valid response from the OCSP responder, then the certificate will not be given EV treatment. (bug 585122)

OCSP service for end-entity certs must be updated at least every four days, and OCSP responses must have a maximum expiration time of ten days.

RFC 2560, sections 2.2, 2.6, 3.2 and 4.2.2.2 define the requirements for the OCSP response signer's certificate and certificate chain. NSS enforces these requirements exactly.