



**PKI disclosure statement - Signexpert & Seal
for the the accounting profession**

**Déclarations de l'IGC – Signexpert et Cachet
Cabinet pour la profession Expert-Comptable**

Version 1.3

Juin 2018

OID n° 1.2.250.1.165.1.10.1.1

CSOEC - ECMA		June 2018
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.3

VERSION HISTORY

Date	Nam/Nom	Updates / mise à jour	Version
April, 2016	Samuel LACAS	First draft / première version	1.0-alpha
February, 2017	Samuel LACAS	Title, “Cachet” qualification and CA address / ajustement titre et adresse de l’AC	1.1
March/Mars 2017	Mathieu JORRY	Version bilingue et ajustements mineurs	1.2
Juin 2018	Fabrice FAIVRE	Modification des url de révocation des certificats	1.3

Authors	Organisation
Samuel LACAS	SEALWeb
Mathieu JORRY	ECMA
Fabrice FAIVRE	ECMA

Classification : Public		Page
	ECMA properties /Propriétés d’ECMA	2/11

CSOEC - ECMA		June 2018
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.3

I INTRODUCTION

This document constitutes the PKI disclosure statement for the “Signexpert” and “Seal” certificates.

II TSP CONTACT INFO

The name, location and relevant contact information for the CA/PKI (name of responsible person, address, website, info mail, fax, etc.), including clear information on how to contact the TSP to request a revocation.

ECMAssociation - Signexpert
Conseil supérieur de l'Ordre des experts-comptables
19 rue Cognacq Jay
75341 Paris Cedex 07

Revocation requests can be made:

- Online, on the Signexpert web site (www.signexpert.fr), using his/her personal account
- By contacting the CSOEC by phone (0890 46 16 16) or e-mail (hotline@signexpert.fr)
- Directly on the certification services operator:

Expert-Comptable	https://kregistration-user.certificat2.com/OEC/ACUNIQUE/EC-SIGNAUTH:/
Élu de l'Ordre	https://kregistration-user.certificat2.com/OEC/ACUNIQUE/ELU-SIGNAUTH:/
Cachet Cabinet	https://kregistration-user.certificat2.com/OEC/ACUNIQUE/CACHET2016:/

- By going in person to a CROEC/CDOEC office, with an official I.D.

III CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE

A description of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage.

Any limitations on its use.

Whether the policy is for certificate issued to the public.

CP being applied (including OID and short summary).

There are three kinds of Signexpert certificates.

Expert-Comptable (certified public accountant)	PGS-OEC Politique de Certification - Signature & Authentification 1.2.250.1.165.1.10.1.1	Authentication & Signature EU- qualified certificates	Exclusively issued to certified public accountants.
Élu de l'Ordre (elected official of the Order)	PGS-OEC Politique de certification Élus de l'Ordre des experts- comptables 1.2.250.1.165.1.10.11.1	Authentication & Signature EU- qualified certificates	Exclusively issued to elected officials of the French Order of certified public accountants (Conseil de l'Ordre des experts- comptables)
Cachet Cabinet (accounting firm's seal)	Politique de certification « Cachet Serveur » de la profession comptable 1.2.250.1.165.1.11.2.1	Certificates for the creation of EU- qualified seals	Exclusively issued to certified accounting firms.

Classification : Public		Page
	ECMA properties /Propriétés d'ECMA	3/11

CSOEC - ECMA		June 2018
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.3

III.1 Expert-Comptable (certified public accountant) certificates

These EU-qualified certificates are exclusively issued to certified public accountants. They provide a “high assurance level” electronic identification means and a “qualified certificate for electronic signatures” (both in the sense of the eIDAS Regulation (*Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market*)) to their owner.

Besides the accountant's legal identity, the validation process checks the accountant's public certification (as maintained by the Order according to French laws) and its legal area of practice.

III.2 Élu de l'Ordre (elected official of the Order) certificates

These EU-qualified certificates are exclusively issued to elected officials of the french Order of certified public accountants. They provide a “high assurance level” electronic identification means and a “qualified certificate for electronic signatures” (both in the sens of the eIDAS Regulation) to their owner.

These certificates are directly issued by the Order following the elections.

III.3 Cachet Cabinet (accounting firm's seal) certificates

These EU-qualified certificates are exclusively issued to certified public accountants firms. They provide a qualified certificate for electronic seals (in the sense of the eIDAS Regulation).

Besides the accountant's legal identity, the validation process checks the accountant's public certification and that of his/her firm (as maintained by the Order according to French laws).

IV RELIANCE LIMITS

The reliance limits, if any.

There are no specific reliance limits on the Signexpert certificates.

Indication that the certificate is only for use with digital signatures or seals.

See previous section.

The period of time which registration information and TSP event are maintained (and hence are available to provide supporting evidence).

Registration information is kept 10 years.

Certificates, CRL and OCSP responses are kept at least eight years after their expiration date.

Technical logs are kept 7 years.

V OBLIGATIONS OF SUBSCRIBERS

The description of, or reference to, the critical subscriber obligations.

The subscriber's obligations [...], including whether the policy requires use of a secure cryptographic device.

In the following, “the owner” is:

- Expert-Comptable/Élu de l'Ordre: the physical person (certified accountant) whose identity is in the issued certificate (“subject”).
- Cachet Cabinet: the physical person (certified accountant) related to the accounting firm whose identity is in the issued certificate (“subject”).

Upon registration, the owner must provide genuine and exact information to the TSP.

The owner must retrieve his/her Signexpert token within two months following its production by the TSP.

Classification : Public		Page
	ECMA properties /Propriétés d'ECMA	4/11

CSOEC - ECMA		June 2018
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.3

When applicable, the owner must renew the certificates during the available period (usually, the 45 days preceding the certificate's expiration date).

The owner shall use the key pair in accordance with any limitations expressed in the present PDS.

The owner shall prevent unauthorized use of his/her subject's private key.

The owner shall maintain the subject's private key under the subject's sole control. In particular, he/she must not share the subject's private key activation code (PIN) with anyone.

The owner shall only generate and use the subject's private key(s) for cryptographic functions within the secure cryptographic device. Doing such ensures that the subject keys are generated using an algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP, and that key length and algorithm are as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP during the validity time of the certificate.

The owner shall notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

- the subject's private key has been lost, stolen, potentially compromised;
- control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; or
- inaccuracy or changes to the certificate content.

Following compromise, the owner will immediately and permanently discontinue to use the subject's private key.

The owner will no longer use the subject's private key once he/she has been informed of its revocation or that of the issuing CA.

VI CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

The extent to which relying parties are obligated to check certificate status, and references to further explanation.

Information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate.

Certificate users must, before relying on the certificate, check the revocation status of the certificate chain using one of the following methods.

	CRL distribution point
Expert-Comptable (certified public accountant)	http://seec.experts-comptables.fr/CRL/CRL_signature_et_authentification.crl http://www.signexpert.fr/CRL/CRL_signature_et_authentification.crl http://trustcenter-crl.certificat2.com/CRL/CRL_signature_et_authentification.crl
Élu de l'Ordre (elected official of the Order)	
Cachet Cabinet (accounting firm's seal)	http://seec.experts-comptables.fr/CRL/CRL_cachet.crl http://www.signexpert.fr/CRL/CRL_cachet.crl http://trustcenter-crl.certificat2.com/CRL/CRL_cachet.crl

	OCSP Responder & issuing CA certificate
Expert-Comptable	http://ocsp.experts-comptables.fr/OEC-ACUNIQUE

Classification : Public		Page
	ECMA properties /Propriétés d'ECMA	5/11

CSOEC - ECMA		June 2018
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.3

(certified public accountant)	http://seec.experts-comptables.fr/cert/cert_signature_et_authentification.p7b
Élu de l'Ordre (elected official of the Order)	
Cachet Cabinet (accounting firm's seal)	http://ocsp.experts-comptables.fr/OEC-ACCACHET http://seec.expert-comptables.fr/cert/cert_cachet.p7b

VII LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.

Limitations of liability.

No specific limitation.

VIII APPLICABLE AGREEMENTS

Identification and references to applicable agreements, CPS, CP and other relevant documents ; CP being applied.

See section III.

IX PRIVACY POLICY

A description of and reference to the applicable privacy policy.

The period of time during which registration information is retained.

Personal data is managed by the TSP and its information systems according to the French and European regulation, in particular, the EU Data Protection Act.

Registration information is, among others, personal data.

See above for the retention time of registration information.

X REFUND POLICY

A description of and reference to the applicable refund policy.

Not applicable.

XI APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

Statement of the choice of law, complaints procedure and dispute resolution mechanisms (anticipated to often include a reference to the International Chambers of Commerce's arbitration services).

The procedures for complaints and dispute settlements.

The applicable legal system.

The applicable legal system is the French one.

XII TSP AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT

Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.

If the TSP has been certified to be conformant with a CP, and if so through which scheme.

The link toward the Trusted List of the country within which the TSP is operated.

Classification : Public		Page
	ECMA properties /Propriétés d'ECMA	6/11

CSOEC - ECMA		June 2018
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.3

Expert-Comptable (certified public accountant)	ETSI EN 101 456 ETSI EN 319401, ETSI EN 319411-1, ETSI EN 319411-2 (after July 2016, the 1 st)
Élu de l'Ordre (elected official of the Order)	
Cachet Cabinet (accounting firm's seal)	ETSI EN 102 042 ETSI EN 319401, ETSI EN 319411-1, ETSI EN 319411-2 (after July 2016, the 1 st)

The French Trusted List is available at the following URL:

<http://references.modernisation.gouv.fr/sites/default/files/TSL-FR.xml>

Classification : Public		Page
	ECMA properties /Propriétés d'ECMA	7/11



I INTRODUCTION

Ce document constitue les « Déclarations de l'IGC » pour les certificats de la gamme « Signexpert » et le « Cachet cabinet ».

II CONTACT

ECMAssociation - Signexpert
Conseil supérieur de l'Ordre des experts-comptables
19 rue Cognacq Jay
75341 Paris Cedex 07

Une demande de révocation peut être déposée en utilisant l'un des moyens suivants :

- En contactant l'A.E. nationale (CSOEC) par téléphone (0890 46 16 16) ou par courriel (hotline@signexpert.fr)
- En se connectant sur le Portail Web de *Signexpert* (www.signexpert.fr). Dans ce cas, le porteur s'identifie sur son compte selon la même procédure que lors d'une demande initiale ; le portail envoie alors une demande de confirmation aux adresses courriels saisies, que le porteur doit valider pour confirmer sa demande de révocation.
- En personne, auprès du CSOEC ou d'un CROEC/CDOEC
- Depuis le portail web client de l'OSC, 24h/24 et 7j/7 :

Expert-Comptable	https://kregISTRATION-user.certificat2.com/OEC/ACUNIQUE/EC-SIGNAUTH:
Élu de l'Ordre	https://kregISTRATION-user.certificat2.com/OEC/ACUNIQUE/ELU-SIGNAUTH:
Cachet cabinet	https://kregISTRATION-user.certificat2.com/OEC/ACUNIQUE/CACHET2016:

III TYPE DE CERTIFICAT, PROCEDURES DE VALIDATION ET UTILISATION

Expert-Comptable	PGS-OEC Politique de Certification - Signature & Authentification 1.2.250.1.165.1.10.1.1	Certificats qualifiés de signature électronique	Émis exclusivement à l'attention des experts-comptables inscrits au tableau de l'Ordre.
Élu de l'Ordre	PGS-OEC Politique de certification Élus de l'Ordre des experts-comptables 1.2.250.1.165.1.10.11.1	Certificats qualifiés de signature électronique	Émis exclusivement à l'attention des élus de l'Ordre (Conseil de l'Ordre des experts-comptables)
Cachet Cabinet	Politique de certification « Cachet Serveur » de la profession comptable 1.2.250.1.165.1.11.2.1	Certificats qualifiés de création de cachet électronique	Émis exclusivement à des cabinets d'expertise comptable.

III.1 Certificats Signexpert

Ces certificats sont des certificats qualifiés de signature électronique au sens du *Règlement (UE) N° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et*

CSOEC - ECMA		March/Mars 2017
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.2

les services de confiance pour les transactions électroniques au sein du marché intérieur (dit « Règlement eIDAS ») et ne sont délivrés qu'aux experts-comptables inscrits au tableau de l'Ordre.

III.2 Élu de l'Ordre

Ces certificats sont des certificats qualifiés de signature électronique au sens du « Règlement eIDAS » et ne sont délivrés qu'aux élus de l'Ordre en exercice.

III.3 Cachet Cabinet

Ces certificats sont des certificats qualifiés de cachet électronique au sens du « Règlement eIDAS » et ne sont délivrés qu'aux cabinets d'exercice comptable dûment inscrits au tableau de l'Ordre.

IV LIMITATIONS DE GARANTIE

Les dossiers d'enregistrement sont conservés 10 ans.

Les certificats, LCR et réponses OCSP sont conservées au moins huit ans après leur date d'expiration.

Les traces techniques sont conservées 7 ans.

V OBLIGATIONS DES PORTEURS

Dans ce qui suit, "le propriétaire" est :

- Expert-Comptable / Élu de l'Ordre : la personne physique dont l'identité figure dans le certificat délivré (« sujet » ou « subject »).
- Cachet Cabinet : la personne physique (comptable agréée) liée à l'entreprise comptable dont l'identité figure dans le certificat délivré (« sujet » ou « subject »).

Lors de l'inscription, le propriétaire doit fournir des informations authentiques et exactes au TSP.

Le propriétaire doit récupérer son jeton Signexpert dans les deux mois suivant sa production par le TSP.

Le cas échéant, le propriétaire doit renouveler les certificats pendant la période disponible (habituellement, les 45 jours précédant la date d'expiration du certificat).

Le propriétaire doit utiliser la paire de clés conformément aux limites exprimées dans le présent PDS.

Le propriétaire doit empêcher l'utilisation non autorisée de la clé privée de son sujet.

Le propriétaire doit maintenir la clé privée du sujet sous le contrôle exclusif du sujet. En particulier, il ne doit pas partager le code d'activation de clé privée (NIP) du sujet avec n'importe qui.

Le propriétaire ne doit générer et utiliser que la (les) clé (s) privée (s) du sujet pour les fonctions cryptographiques dans le dispositif cryptographique sécurisé. Cela garantit que les clés de sujet sont générées à l'aide d'un algorithme tel que spécifié dans ETSI TS 119 312 pour les utilisations de la clé certifiée comme identifié dans le CP, et que la longueur et l'algorithme de la clé sont tels que spécifiés dans ETSI TS 119 312 pour les utilisations de La clé certifiée identifiée dans le CP pendant la durée de validité du certificat.

Le propriétaire doit notifier le TSP dans un délai raisonnable, si l'une des situations suivantes se produit jusqu'à la fin de la période de validité indiquée dans le certificat :

- la clé privée du sujet a été perdue, volée, potentiellement compromise ;
- le contrôle de la clé privée du sujet a été perdu en raison du compromis des données d'activation (par exemple, du code PIN) ou d'autres raisons ; ou
- inexactitude ou modification du contenu du certificat.

Classification : Public		Page
	ECMA properties /Propriétés d'ECMA	9/11

CSOEC - ECMA		March/Mars 2017
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.2

Suite au compromis, le propriétaire cessera immédiatement et en permanence d'utiliser la clé privée du sujet.

Le propriétaire n'utilisera plus la clé privée du sujet une fois qu'il a été informé de sa révocation ou de l'autorité de certification émettrice.

VI STATUT DU CERTIFICAT ET CONTRÔLE DES OBLIGATIONS DES PARTIES PRENANTES

Les utilisateurs du certificat doivent, avant de se fier au certificat, vérifier l'état de révocation de la chaîne de certification en utilisant l'une des méthodes suivantes.

	Point de distribution des LCR (Liste des Certificats Révoqués)
Expert-Comptable (certified public accountant)	http://seec.experts-comptables.fr/CRL/CRL_signature_et_authentification.crl http://www.signexpert.fr/CRL/CRL_signature_et_authentification.crl http://trustcenter-crl.certificat2.com/CRL/CRL_signature_et_authentification.crl
Élu de l'Ordre (elected official of the Order)	
Cachet Cabinet (accounting firm's seal)	http://seec.experts-comptables.fr/CRL/CRL_cachet.crl http://www.signexpert.fr/CRL/CRL_cachet.crl http://trustcenter-crl.certificat2.com/CRL/CRL_cachet.crl

	Répondeur OCSP & certificate de l'AC émettrice
Expert-Comptable	http://ocsp.experts-comptables.fr/OEC-ACUNIQUE
Élu de l'Ordre	http://seec.experts-comptables.fr/cert/cert_signature_et_authentification.p7b
Cachet Cabinet	http://ocsp.experts-comptables.fr/OEC-ACCACHET http://seec.expert-comptables.fr/cert/cert_cachet.p7b

Classification : Public		Page
	ECMA properties /Propriétés d'ECMA	10/11

CSOEC - ECMA		March/Mars 2017
Signexpert	PKI disclosure statement - Signexpert & Seal Déclarations de l'IGC – Signexpert et Cachet Cabinet	v. 1.2

VII LIMITE DE GARANTIE ET AVERTISSEMENT / LIMITATION DE RESPONSABILITE

Aucune limitation spécifique.

VIII ACCORDS APPLICABLES

Voir la section III

IX POLITIQUE DE CONFIDENTIALITÉ

Les données personnelles sont gérées par le TSP et ses systèmes d'information selon la réglementation française et européenne, en particulier la loi sur la protection des données de l'UE.

L'information d'enregistrement est, entre autres, les données personnelles.

Voir ci-dessus pour le temps de conservation des informations d'enregistrement.

X POLITIQUE DE REMBOURSEMENT

N'est pas applicable.

XI DROIT APPLICABLE, PLAINTES ET RÈGLEMENT DES DIFFÉRENDS

Le système juridique applicable est le système français.

XII TSP ET NORMES APPLICABLES, MARQUES DE CONFIANCE ET AUDIT

Expert-Comptable	ETSI EN 101 456
Élu de l'Ordre	ETSI EN 319401, ETSI EN 319411-1, ETSI EN 319411-2 (after July 2016, the 1 st)
Cachet Cabinet	ETSI EN 102 042 ETSI EN 319401, ETSI EN 319411-1, ETSI EN 319411-2 (after July 2016, the 1 st)

La liste de confiance française est disponible à l'URL suivante:

<http://references.modernisation.gouv.fr/sites/default/files/TSL-FR.xml>

Classification : Public		Page
	ECMA properties /Propriétés d'ECMA	11/11