ORDRE DES EXPERTS-COMPTABLES

Conseil Supérieur

PKI DISCLOSURE STATEMENT – "SIGNATURE & AUTHENTICATION"

FOR THE THE ACCOUNTING PROFESSION

Version 1.0

May, 2016

OID n° 1.2.250.1.165.1.10.1.1

Signature numérique de Jean Saphores

VERSION HISTORY

Date	Updates	Version
April, 2016	First draft	1.0-alpha
May, 2016	Published version	1.0

Authors	Organisation
Stéphane GASCH	CSOEC
Samuel LACAS	SEALWeb
Jean SAPHORES	CSOEC

I INTRODUCTION

This document constitutes the PKI disclosure statement for the "Signexpert" certificates.

II TSP CONTACT INFO

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

Direction des études informatiques
Conseil supérieur de l'Ordre des experts-comptables
19 rue Cognacq Jay
75341 Paris Cedex 07

Revocation requests can be made:

a) Online, on the Signexpert web site (www.signexpert.fr), using his/her personal account

b) By contacting the CSOEC by phone (0890 46 16 16) or e-mail (hotline@signexpert.fr)

c) Directly on the certification services operator:

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

d) 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 1.2.250.1.165.1.11.1.1	Certificates for the creation of EU-advanced seals	Exclusively issued to certified accounting firms.

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 certificates are exclusively issued to certified public accountants firms. They provide an advanced 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.

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 (certified public accountant)	http://ocsp2.experts-comptables.fr/OEC-ACUNIQUE http://seec.experts-comptables.fr/cert/cert_signature_et_authentification.p7b
Élu de l'Ordre (elected official of the Order)	

	OCSP Responder & issuing CA certificate
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.

Personnal 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, personnal 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.

Expert-Comptable (certified public accountant)	ETSI EN 101 456 ETSI EN 319401, ETSI EN 319411-1, ETSI EN 319411-2 (after July 2016, the 1st)
Élu de l'Ordre	

(elected official of the Order)	
Cachet Cabinet (accounting firm's seal)	No certification

The French Trusted List is available at the following URL:

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