ORDRE DES EXPERTS-COMPTABLES

Conseil Supérieur

POLITIQUE DE CERTIFICATION « AUTHENTIFICATION FORTE »

POUR LES AC DE LA PROFESSION COMPTABLE

(AC CROEC)

Version 6.75

septembre 2015

OID n° 1.2.250.1.165.1.2.x.7.6

Signature numérique de Jean Saphores

HISTORIQUE DES VERSIONS

Date	Évolutions	Edition / révision
20/04/2010	Refonte de la PC suite à la parution du RGS (par TPC)	v5.0
03/05/2010	Intégration d'éléments propres à la profession comptable	v5.1
17/05/2010	Dernière révision avant transmission à la DEI	V5.1fin
12/04/2011	Refonte suite à contractualisation avec l'OSC	v5.2
17/06/2011	Intégration des gabarits	5.5
01/07/2011	Procédure de remise en masse et validation	6.0
08/2012	Révision Corse et Audit R.G.S.	6.32
09/2012	Revue R.G.S.	6.33
09/2012	Précisions sur le rôle des AE en région	6.40
08/2013	Précisions sur le renouvellement Modification du vocabulaire (A.E. et A.R.)	6.6
09/2014	Arrêt du renouvellement et passage à des certificats de 3 ans	6.7
05/2015	SGMAP remplace DGME et ajout de l'adresse des LCR Signexpert	6.75
09/2015	Changement de vocabulaire (réémission de certificat) – remarque LSTI	6.81

Contributeurs	Organisation
Stéphane GASCH	CSOEC
Thierry PIETTE-COUDOL	Avocat
Samuel LACAS	SEALWeb
Jean SAPHORES	CSOEC

TABLE DES MATIÈRES

TABLE DES MATIÈRES 3
I Introduction 8
I.1 Présentation générale 8
I.2 Identification du document 8
I.2.1 Transfert de compétence de la région PACAC 9
I.3 Entrée en vigueur du document 9
I.4 Entités intervenant dans l'ICP et responsabilités 9
I.4.1 Le Prestataire de services de certification électronique 9
I.4.2 Autorité de certification (AC) 10
I.4.3 Autorité d'enregistrement (AE) 11
I.4.4 Agent de remise (AR) 11
I.4.5 Opérateur de certification (OC/OSC) 11
I.4.6 Porteurs de certificats 12
I.4.7 Utilisateurs de certificat 12
I.4.8 Mandataire de certification 12
I.5 Usage des certificats 13
I.5.1 Domaines d'utilisation applicables 13
I.5.2 Domaines d'utilisation interdits 14
I.6 Gestion de la PC 14
I.6.1 Entité gérant la PC 14
I.6.2 Point de contact 14
I.6.3 Entité déterminant la conformité d'une DPC avec cette PC 14
I.6.4 Procédures d'approbation de la conformité de la DPC 14
I.7 Définitions et abréviations 14
I.7.1 Abréviations 14
I.7.2 Définitions 15
II Responsabilités concernant la mise à disposition des informations devant être publiées 20
II.1 Entités chargées de la mise à disposition des informations 20
II.2 Informations devant être publiées 20
II.3 Délais et fréquences de publication 20
II.4 Contrôle d'accès aux informations publiées 20
III Identification et authentification 21
III.1 Nommage 21
III.1.1 Types de noms 21
III.1.2 Nécessité d'utilisation de noms explicites 21
III.1.3 Pseudonymisation des porteurs 23
III.1.4 Règles d'interprétation des différentes formes de nom 23
III.1.5 Unicité des noms 23
III.1.6 Identification, authentification et rôle des marques déposées 23
III.2 Validation initiale de l'identité de la structure professionnelle d'exercice du porteur 23
III.2.1 Méthode pour prouver la possession de la clé privée 23
III.2.2 Validation de l'identité d'un organisme 23
III.2.3 Validation de l'identité d'un individu 23
III.2.4 Informations non vérifiées du porteur 24
III.2.5 Validation de l'autorité du demandeur 24
III.2.6 Certification croisée d'AC 24
III.3 Identification et validation d'une demande de délivrance d'un certificat suite au changement de biclé (réémission) 25
III.4 Identification et validation d'une demande de révocation 25
IV Exigences opérationnelles sur le cycle de vie des certificats 27
IV.1 Demande de certificat 27

IV.1.1 Origine d'une demande de certificat 27
IV.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat 27
IV.2 Traitement d'une demande de certificat 27
IV.2.1 Exécution des processus d'identification et de validation de la demande 27
IV.2.2 Acceptation ou rejet de la demande 28
IV.2.3 Durée d'établissement du certificat 28
IV.3 Délivrance du certificat 28
IV.3.1 Actions de l'AC concernant la délivrance du certificat 28
IV.3.2 Notification par l'AC de la délivrance du certificat au porteur 28
IV.4 Acceptation du certificat 28
IV.4.2 Démarche d'acceptation du certificat 28
IV.4.3 Publication du certificat 29
IV.4.4 Notification par l'AC aux autres entités de la délivrance du certificat 29
IV.5 Usages de la biclé et du certificat 29
IV.5.1 Utilisation de la clé privée et du certificat par le porteur 29
IV.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat 29
IV.6 Renouvellement d'un certificat 29
IV.7 Réémission d'un certificat 30
IV.8 Modification du certificat 30
IV.9 Révocation et suspension des certificats 30
IV.9.1 Causes possibles d'une révocation 30
IV.9.2 Origine d'une demande de révocation 31
IV.9.3 Procédure de traitement d'une demande de révocation 31
IV.9.4 Délai de traitement par l'AC d'une demande de révocation 32
IV.9.5 Exigences de vérification de la révocation par les utilisateurs de certificats 32
IV.9.6 Fréquence d'établissement des LCR 32
IV.9.7 Délai maximum de publication d'une LCR 33
IV.9.8 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats 33
IV.9.9 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats 33
IV.9.10 Autres moyens disponibles d'information sur les révocations 33
IV.9.11 Exigences spécifiques en cas de compromission de la clé privée 33
IV.9.12 Suspension de certificats 33
IV.10 Fonction d'information sur l'état des certificats 33
IV.10.1 Caractéristiques opérationnelles 33
IV.10.2 Disponibilité de la fonction 35
IV.11 Fin de la relation entre le porteur et l'AC 35
IV.12 Séquestre de clé et recouvrement 35
IV.13 Certificats de test 35
V Mesures de sécurité non techniques 36
V.1 Mesures de sécurité physique 36
V.2 Mesures de sécurité procédurales 36
V.2.1 Rôles de confiance 36
V.2.2 Nombre de personnes requises par tâches 37
V.2.3 Identification et authentification pour chaque rôle 37
V.2.4 Rôles exigeant une séparation des attributions 37
V.3 Mesures de sécurité vis-à-vis du personnel 37
V.4 Procédures de constitution des données d'audit 37
V.4.1 Informations enregistrées pour chaque événement 38
V.4.2 Imputabilité 38
V.4.3 Événements enregistrés par l'AE 38
V.4.4 Événements enregistrés par l'AC 38
V.4.5 Événements divers 39

V.4.6 Processus de journalisation 39
V.4.7 Protection d'un journal d'événements 39
V.4.8 Copies de sauvegarde des journaux d'événement 39
V.4.9 Procédure de collecte des journaux (interne ou externe) 39
V.4.10 Anomalies et audit. 39
V.5 Archivage des données 40
V.5.1 Types de données à archiver 40
V.5.2 Période de conservation des archives 40
V.5.3 Protection des archives 41
V.5.4 Procédure de sauvegarde des archives 41
V.5.5 Exigences d'horodatage des données 41
V.5.6 Système de collecte des archives 41
V.5.7 Procédures de récupération et de vérification des archives 41
V.6 Changement de clé d'AC 41
V.7 Reprise suite à compromission et sinistre 41
V.8 Fin de vie de l'ICP 42
V.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC 42
V.8.2 Cessation d'activité affectant l'AC 42
VI Mesures de sécurité techniques 44
VI.1 Génération et installation de biclés 44
VI.1.1 Génération des biclés 44
VI.1.2 Transmission de la clé privée à son propriétaire 44
VI.1.3 Transmission de la clé publique à l'AC 44
VI.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats 44
VI.1.5 Tailles des clés 44
VI.1.6 Vérification de la génération des paramètres des biclés et de leur qualité 44
VI.1.7 Objectifs d'usage de la clé 44
VI.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 45
VI.2.1 Standards et mesures de sécurité pour les modules cryptographiques 45
VI.2.2 Contrôle de la clé privée de l'AC par plusieurs personnes 45
VI.2.3 Séquestre de la clé privée 45
VI.2.4 Copie de secours de la clé privée 45
VI.2.5 Archivage de la clé privée 45
VI.2.6 Transfert de la clé privée vers / depuis le module cryptographique 45
VI.2.7 Stockage de la clé privée dans un module cryptographique 45
VI.2.8 Méthode d'activation de la clé privée 45
VI.2.9 Méthode de désactivation de la clé privée 45
VI.2.10 Méthode de destruction des clés privées 46
VI.2.11 Autres aspects de la gestion des biclés 46
VI.3 Données d'activation 46
VI.3.1 Génération et installation des données d'activation 46
VI.3.2 Protection des données d'activation 46
VI.3.3 Procédure de déblocage du support 47
VI.4 Mesures de sécurité des systèmes informatiques 47
VI.5 Mesures de sécurité liées au développement des systèmes 47
VI.6 Mesures de sécurité réseau 47
VI.7 Horodatage / Système de datation 47
VII Profils des certificats, OCSP et des LCR 48
VII.1 Certificats de porteurs 48
VII.1.1 Régions, OID et DN des A.C. 49
VII.2 Liste de Certificats Révoqués 51
VII.3 Certificat des réponses OCSP 52
VII.4 Certificats des A.C. émettrices 52

VII.4.1 CROEC d'Alsace 53
VII.4.2 CROEC d'Aquitaine 54
VII.4.3 CROEC d'Auvergne 55
VII.4.4 CROEC de Bourgogne Franche-Comté 56
VII.4.5 CROEC de Bretagne 58
VII.4.6 CROEC de Champagne 59
VII.4.7 CROEC de Corse 60
VII.4.8 CROEC de Guadeloupe 61
VII.4.9 CROEC de Limoges 62
VII.4.10 CROEC de Lorraine 63
VII.4.11 CROEC de Montpellier 64
VII.4.12 CROEC de Paris Île-de-France 65
VII.4.13 CROEC de Picardie-Ardennes 66
VII.4.14 CROEC de Poitou Charente Vendée 67
VII.4.15 CROEC de Rhône-Alpes 68
VII.4.16 CROEC de Rouen Normandie 69
VII.4.17 CROEC de Toulouse Midi-Pyrénées 70
VII.4.18 CROEC des Pays de Loire 71
VII.4.19 CROEC d'Orléans 72
VII.4.20 CROEC du Nord Pas-de-Calais 73
VII.4.21 CROEC Marseille Provence Alpes Côte-d'Azur 74
VII.4.22 CROEC Marseille Provence Alpes Côte-d'Azur Corse 76
VII.4.23 CROEC de la Réunion 77
VII.4.24 CROEC de la Martinique 78
VII.4.25 Comité départemental de la Guyane 79
VIII Audit de conformité et autres évaluations 81
VIII.1 Fréquences et / ou circonstances des évaluations 81
VIII.2 Identités / qualifications des évaluateurs 81
VIII.3 Relations entre évaluateurs et entités évaluées 81
VIII.4 Sujets couverts par les évaluations 81
VIII.5 Actions prises suite aux conclusions des évaluations 81
VIII.6 Communication des résultats 81
IX Autres problématiques métiers et légales 82
IX.1 Tarifs 82
IX.1.1 Tarifs pour la fourniture ou le renouvellement de certificats 82
IX.1.2 Tarifs pour accéder aux certificats 82
IX.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats 82
IX.1.4 Tarifs pour d'autres services 82
IX.1.5 Politique de remboursement 82
IX.2 Responsabilité financière 82
IX.3 Confidentialité des données professionnelles 82
IX.3.1 Périmètre des informations confidentielles 82
IX.3.2 Informations hors du périmètre des informations confidentielles 82
IX.3.3 Responsabilités en termes de protection des informations confidentielles 82
IX.4 Protection des données personnelles 83
IX.4.1 Politique de protection des données personnelles 83
IX.4.2 Informations à caractère personnel 83
IX.4.3 Informations à caractère non personnel 83
IX.4.4 Responsabilité en termes de protection des données personnelles 83
IX.4.5 Notification et consentement d'utilisation des données personnelles 83
IX.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives 83
IX.4.7 Autres circonstances de divulgation d'informations personnelles 83
IX.5 Droits sur la propriété intellectuelle et industrielle 83

IX.6 Interprétations contractuelles et garanties 83
IX.7 Limite de garantie 83
IX.8 Limite de responsabilité 83
IX.9 Indemnités 83
IX.10 Durée et fin anticipée de validité de la PC 83
IX.10.1 Durée de validité 83
IX.10.2 Fin anticipée de validité 84
IX.10.3 Effets de la fin de validité et clauses restant applicables 84
IX.11 Notifications individuelles et communications entre les participants 84
IX.12 Amendements à la PC 84
IX.13 Dispositions concernant la résolution de conflits 84
IX.14 Juridictions compétentes 84
IX.15 Conformité aux législations et réglementations 84
IX.16 Transfert d'activités 84
X Annexe 1 : Documents cités en référence 85
X.1 Législation et réglementation 85
X.2 Documents techniques 85
X.3 Autres documents 85
XI Annexe 2 : Exigences de sécurité du module cryptographique de l'AC 86
XI.1 Exigences sur les objectifs de sécurité 86
XI.2 Exigences sur la qualification 86
XII Annexe 3 : Exigences de sécurité du dispositif d'authentification et de signature 87
XII.1 Exigences sur les objectifs de sécurité 87
XII.2 Exigences sur la qualification 87

I INTRODUCTION

I.1 Présentation générale

Le Conseil Supérieur de l'Ordre des Experts-Comptables a décrit dans sa *Politique Générale de Sécurité* (PGS-OEC) les diverses fonctions de sécurisation à mettre en œuvre lors des échanges électroniques avec les administrations comme avec ses autres partenaires professionnels. Parmi les fonctions et instruments de sécurisation figurent l'authentification la signature électronique dont conditions et modalités de d'organisation et fonctionnement sont décrites dans un document de type « Politique de Certification ». Le présent document constitue cette Politique.

Ce document constitue une Politique de Certification mise en œuvre par une Autorité de Certification de l'Ordre des Experts Comptables (OEC) pour les membres de l'Ordre. Elle réunit l'ensemble des obligations et engagements des différents acteurs relatifs à la délivrance et l'usage des certificats numériques de personnes physiques dans le cadre de leur activité réglementé d'Experts Comptables.

Le présent document se réfère à la *Politique Générale de Sécurité* (PGS) de l'OEC et met en œuvre un niveau de sécurité deux étoiles (ci-après "**") selon la typologie en vigueur dans le *Référentiel Général de Sécurité* de l'Administration (RGS).

Cette politique de certification couvre la délivrance de certificats de signature et d'authentification. Ces certificats sont distribués à des utilisateurs finaux pour sécuriser des applications à l'aide d'un dispositif sécurisé d'authentification et de de création de signature (noté DSCS).

Toute AC de l'OEC souhaitant être qualifiée doit mettre en œuvre la présente PC dont la structure est totalement conforme au RFC3647.

I.2 Identification du document

La présente PC est dénommée *PGS-OEC Politique de Certification - Authentification* forte. Elle est identifiée par son numéro d'identifiant d'objet (OID), ainsi que par le nom, numéro de version, et la date de mise à jour.

Le présent document décrit les politiques de certification des autorités de certification (AC) des CROEC et CDOEC de l'Ordre. Formellement, chacune de ces politiques est identifiée par un OID distinct, rappelé dans le tableau ci-dessous.

Région	OID de la P.C.
Alsace	1.2.250.1.165.1.2.**1**.7.6
Aquitaine	1.2.250.1.165.1.2.**2**.7.6
Auvergne	1.2.250.1.165.1.2.**3**.7.6
Bourgogne Franche-Comté	1.2.250.1.165.1.2.**4**.7.6
Bretagne	1.2.250.1.165.1.2.**5**.7.6
Champagne	1.2.250.1.165.1.2.**6**.7.6
Corse	1.2.250.1.165.1.2.**24**.7.6
Guadeloupe	1.2.250.1.165.1.2.**7.**7.6
Guyane	1.2.250.1.165.1.2.**8**.7.6
La Réunion	1.2.250.1.165.1.2.**9**.7.6
Lille Nord Pas-de-Calais	1.2.250.1.165.1.2.**10**.7.6
Limoges	1.2.250.1.165.1.2.**11**.7.6
Lorraine	1.2.250.1.165.1.2.**12**.7.6
Marseille, PACA	1.2.250.1.165.1.2.**25**.7.6
Marseille, PACAC	1.2.250.1.165.1.2.**13**.7.6

Martinique	1.2.250.1.165.1.2.**14**.7.6
Montpellier	1.2.250.1.165.1.2.**15**.7.6
Orléans	1.2.250.1.165.1.2.**16**.7.6
Paris Ile-de-France	1.2.250.1.165.1.2.**17**.7.6
Pays de Loire	1.2.250.1.165.1.2.**18**.7.6
Picardie-Ardennes	1.2.250.1.165.1.2.**19**.7.6
Poitou Charentes Vendée	1.2.250.1.165.1.2.**20**.7.6
Rhône-Alpes	1.2.250.1.165.1.2.**21**.7.6
Rouen Normandie	1.2.250.1.165.1.2.**22.7**.6
Toulouse Midi-Pyrénées	1.2.250.1.165.1.2.**23**.7.6

Le type de service RGS correspondant est (PC Type signature et authentification OID : 1.2.250.1.165.1.3.1.1) :

Service	**Niveau de sécurité**	**Type de certificat**
Signature et authentification	**	Entreprise ou Administration

Les exigences relatives aux certificats d'entreprise ou d'administration étant similaires, la même PC peut être utilisée pour ces deux types de certificats.

La PC est complétée par une *Déclaration des Pratiques de Certification* correspondante référencée par un numéro d'OID. La *Politique de Certification* et la *Déclaration des Pratiques de Certification* identifiées ci-dessus sont désignés dans la suite du document respectivement sous le nom de "PC" et de "DPC".

I.2.1 Transfert de compétence de la région PACAC

Depuis la version (6.0) de ce document, l'OID 1.2.250.1.165.1.2.13.1.6 désigne la politique de certification du CROEC de Marseille Provence Alpes Côte-d'Azur Corse. Ce CROEC est remplacé par les CROEC de Corse et de Provence Alpes Côte-d'Azur à la date du 1er octobre 2012. Par décret ministériel, ce dernier est le successeur, « à compétence territoriale réduite », du Conseil Régional de Marseille Provence Alpes Côte-d'Azur Corse, et a été « investi de l'ensemble des droits et obligations » de celui-ci. Le SIREN est, par ailleurs, inchangé.

Afin d'assurer la continuité de service des A.C., la population des porteurs PACAC a été partitionnée pour rattachement aux A.C. PACA et Corse. Les A.E. de ces deux structures ont autorité pour renouveler les certificats PACAC correspondants.

I.3 Entrée en vigueur du document

La présente P.C. (version) s'applique à partir du.

I.4 Entités intervenant dans l'ICP et responsabilités

I.4.1 Le Prestataire de services de certification électronique

Dans le cadre de cette PC, ***le rôle de PSCE assuré au niveau national par le Conseil Supérieur de l'Ordre des Experts-Comptables (CSOEC).*** Au titre de l'Ordonnance n° 45-2138 du 19 septembre 1945 portant institution de l'ordre des experts-comptables et règlementant le titre et la profession d'expert-comptable, le CSOEC est l'organe de direction et de gestion des membres de l'Ordre des experts-comptables. Il a seule qualité pour représenter la profession et exercer, devant toutes les juridictions, tous les droits réservés à la partie civile. Il est composé des présidents de 23 Conseils régionaux et de membres élus.

En tant que PSCE, le CSOEC comporte plusieurs AC, au minimum autant que de CROEC et que de CDOEC.

Le PSCE est identifié dans tout certificat dont il a la responsabilité au travers des AC ayant émis ce certificat et qui sont elles-mêmes directement identifiées dans le champ "*issuer*" du certificat.

I.4.2 Autorité de certification (AC)

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (ICP).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des biclés et des certificats.

Dans le cadre de ce document, ***les AC sont les CROEC et les CDOEC de l'Ordre ; on parlera de CROEC/CDOEC pour désigner les AC émettrices de certificats***.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine, la décomposition fonctionnelle d'une ICP qui est retenue dans la présente PC est la suivante :

Fonction d'enregistrement (AE)	AE technique
Fonction de génération des certificats	AC et OSC
Fonction de génération des éléments secrets du porteur	AC et OSC
Fonction de remise au porteur	Agent de remise
Fonction de publication	AC (documents, certificats d'AC) et OSC (LCR)
Fonction de gestion des révocations	AE Nationale et OSC
Fonction d'information sur l'état des certificats	OSC (OCSP, LCR)

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, notamment un OSC, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'ICP sont les suivantes :

- Être une entité juridique au sens de la loi française.
- Être en relation par voie réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'ICP et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.

- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels, notamment l'AC doit mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'ICP et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre pour atteindre un niveau de sécurité (**). Elle élabore sa DPC en fonction de cette analyse.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences de la présente PC, notamment en termes de fiabilité, de qualité et de sécurité. A ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure.
- Générer, et renouveler lorsque nécessaire, ses biclés et les certificats correspondants (signature de certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

I.4.3 Autorité d'enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du futur porteur de certificat. Pour cela, l'AE assure les tâches suivantes :

- la prise en compte et la vérification des informations du futur porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'ICP suivant l'organisation de cette dernière et les prestations offertes ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur y compris lors des échanges de ces données avec les autres fonctions de l'ICP (notamment, elle respecte la législation relative à la protection des données personnelles).

La fonction d'AE est partagée entre l'AE « nationale » (CSOEC) et l'AE « technique » ; voir I.3.2 pour la façon dont les responsabilités sont réparties.

En effet, une majorité des procédures de gestion des certificats (délivrance, révocation, etc.) est dématérialisée et s'appuient sur une autorité d'enregistrement technique tierce, en charge du système d'information des AE ; se référer à la DPC pour plus de détail.

I.4.4 Agent de remise (AR)

Les agents de remise (AR) sont des personnels des CROEC/CDOEC chargés de la remise en face-à-face des supports. Bien que rattachés à un CROEC/CDOEC, les AR ne sont pas limités à l'AC de leur organisme et peuvent délivrer les supports pour toutes les AC régionales.

I.4.5 Opérateur de certification (OC/OSC)

Se référer à la DPC.

I.4.6 Porteurs de certificats

Dans le cadre de la présente PC, un porteur de certificat ne peut être qu'un Expert-comptable personne physique (*cf.* 0), à l'exception des EC pourvus d'un mandat électoral qui bénéficient de certificats spécialisés.

Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle il a un lien réglementaire.

Le porteur respecte les conditions qui lui incombent telles que définies dans la présente PC.

I.4.7 Utilisateurs de certificat

La présente PC traitant de certificats de signature et d'authentification, un utilisateur de certificat peut être notamment :

- Un service de l'administration accessible par voie électronique aux usagers (application, serveur Internet, base de données, etc.), sous la responsabilité d'une personne physique ou morale, qui utilise un certificat et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat. L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.
- Un agent (personne physique) destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'authentifier l'origine de ce message ou de ces données transmises par le porteur du certificat. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager destinataire d'un message ou de données provenant d'un agent et qui utilise un certificat et un dispositif de vérification d'authentification afin d'authentifier l'origine de ce message ou de ces données transmises par le porteur du certificat.
- Un service de l'administration accessible par voie électronique aux usagers (application, serveur Internet, base de données, etc.), sous la responsabilité d'une personne physique ou morale, qui utilise un certificat et un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat. L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.
- Un agent (personne physique) destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager destinataire d'un message ou de données provenant d'un agent et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données transmises par le porteur du certificat.

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document fournis par l'AC. En particulier, l'AC respecte ses responsabilités envers les utilisateurs qui ont « raisonnablement » confiance dans un certificat, selon les dispositions de l'article 33 de la *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

I.4.8 Mandataire de certification

La fonction de mandataire de certification n'est pas utilisée dans l'ICP de l'OEC.

I.5 Usage des certificats

I.5.1 Domaines d'utilisation applicables

Dans le cadre de la présente PC, il s'agit d'utiliser des applications qui demandent une authentification du porteur ou une signature électronique de celui-ci de document pourvu d'un effet légal ou réglementaire.

I.5.1.1 Biclés et certificats des porteurs

La présente PC traite des biclés et des certificats à destination des catégories de porteurs identifiées au chapitre I.3.3 ci-dessus, afin que ces porteurs puissent s'authentifier ou signer électroniquement des données (documents ou messages) dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées au chapitre I.3.4 ci-dessus. Une telle signature électronique apporte, outre l'authentification du signataire et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu juridique de ces données. À noter qu'en matière de signature électronique,

- le RGS est imposé par une administration partenaire, en qualité d'Autorité Administrative de l'Ordonnance du 8 décembre 2005 précitée, dans ses échanges électroniques avec les membres de l'OEC ;
- le RGS est imposé par l'OEC, en qualité d'Autorité Administrative de l'Ordonnance du 8 décembre 2005 précitée, dans ses échanges électroniques avec les services des administrations, les agents des administrations et les autres partenaires non administratifs

Les certificats de signature objets de la présente PC sont utilisés au niveau (**) par des applications pour lesquelles les risques de tentative d'usurpation d'identité sont forts.

Enfin, certaines applications d'échanges dématérialisés de la sphère publique peuvent nécessiter des certificats à des fins de tests ou de recette, différents des certificats "de production" fournis et gérés par l'AC. Dans certains cas, une AC spécifique "de test" pourra être mise en place ; des certificats de test pourront aussi être émis.

I.5.1.2 Biclés et certificats d'AC et de composantes de l'ICP

La hiérarchie d'A.C. du CSOEC est la suivante :

L'A.C. de l'Ordre des Experts-Comptables est la racine de la hiérarchie. En-dessous, se trouvent trois types d'A.C. subalternes :

- L'A.C. des élus de l'OEC (bleu)
- Des A.C. techniques (orange)
- Des A.C. régionales et départementales (violet)

Pour des détails à propos des A.C. régionales « Marseille PACA/PACAC » et Corse, voir I.2.1.

I.5.1.2.1 Certificats d'AC

Pour tous ces certificats, AC racine comprise, une unique biclé est utilisée pour la signature des certificats porteurs et de la L.C.R. sous la responsabilité de l'AC.

I.5.1.2.2 Certificats de composante

Se référer à la DPC.

I.5.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des biclés et des certificats sont définies au chapitre IV.5 ci-dessous. L'AC respecte ces restrictions et impose leur respect par ses porteurs et ses utilisateurs de certificats.

À cette fin, elle communique à tous les porteurs et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

I.6 Gestion de la PC

I.6.1 Entité gérant la PC

La PC est gérée par le CSOEC. Cette fonction est dévolue au CSOEC par le Règlement Intérieur de l'Ordre des Experts-Comptables.

Comme mentionné en I.2, la présente PC est un modèle unique, reprise à l'identique par chaque AC de la profession au niveau des CROEC et des CDOEC.

I.6.2 Point de contact

La rédaction, la modification et la diffusion de la PC est confiée à la Direction des Études Informatiques (DEI) du CSOEC.

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

I.6.3 Entité déterminant la conformité d'une DPC avec cette PC

Le CSOEC agissant comme PSCE confie à la DEI le soin et la responsabilité finale pour déterminer la conformité de la DPC avec la PC.

I.6.4 Procédures d'approbation de la conformité de la DPC

La DPC sera déclarée conforme à la DPC l'issue d'un processus d'approbation élaboré par le CSOEC.

Toute mise à jour de la DPC suivra le processus d'approbation mis en place et sera publiée, conformément aux exigences du paragraphe II sans délai.

I.7 Définitions et abréviations

I.7.1 Abréviations

Les abréviations utilisées dans la présente PC sont les suivantes :

A.C. Autorité de Certification

A.E.	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CDOEC	Conseil départemental de l'Ordre des experts-comptables
CEN	Comité Européen de Normalisation
CRL	Liste des Certificats Révoqués *(Certificate revocation list)*
CRLDP	*Point de Distribution de la Liste des Certificats Révoqués (Distribution Point of the Certificate revocation list)*
CSOEC	Conseil Supérieur de l'Ordre des Experts-Comptables
CROEC	Conseil Régional de l'Ordre des Experts-Comptables
DCS	Dispositif de Création de Signature
DN	*Distinguished Name* (nom distinctif)
D.P.C.	Déclaration des Pratiques de Certification
EC	Expert-Comptable
ETSI	*European Telecommunications Standards Institute*
I.C.P.	Infrastructure à Clés Publiques
LCR	Liste des Certificats Révoqués
OSC	Opérateur de Service de Certification
OC	Opérateur de Certification
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier* (identifiant d'objet)
P.C.	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
SGMAP	Secrétariat Général pour la Modernisation de l'Action Publique
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
URL	*Uniform Resource Locator* (adresse universelle)

I.7.2 Définitions

Les termes utilisés dans la présente PC sont les suivants :

Agent - Personne physique agissant pour le compte d'une autorité administrative.

Agent de remise (AR) : Agent d'un CROEC/CDOEC chargé de la vérification de l'identité du demandeur (face-à-face) et de la remise en mains propres du support.

Autorité d'Enregistrement (AE) : Fonction ou entité chargée de la vérification que les demandeurs ou les porteurs de certificat sont identifiés, que leur identité est authentique et que les contraintes liées à l'usage d'un certificat sont remplies conformément à la politique de certification.

Différentes AE se répartissent les tâches incombant à cette fonction :

- L'AE technique (portail Signexpert) contrôle l'inscription professionnelle du demandeur sur le tableau régional géré par le CROEC/CDOEC auquel il appartient et valide la demande

- L'AE nationale gère les demandes de révocation

La remise en mains propres du support est effectuée par l'AR (*qv.*).

Autorité de Certification (AC) : L'AC assure les fonctions suivantes :

- rédaction des documents de spécifications de l'ICP, notamment la PS et la/les PC,
- mise en application de la PC ;
- gestion des certificats (de leur cycle de vie) ;
- choix des dispositifs cryptographiques et gestion des données d'activation ;
- publication des certificats valides et des listes de certificats révoqués ;
- conseil, information ou formation des acteurs de l'ICP ;
- maintenance et évolution de la PC et de l'ICP ;
- journalisation et archivage des événements et informations relatives au fonctionnement de l'ICP, à son niveau ;

L'AC est une composante de l'ICP de l'OEC au niveau de chaque CROEC/CDOEC. Elle est chargée de la relation directe avec l'EC demandeur de certificat, notamment en ce qui concerne l'existence de son inscription sur le tableau régional professionnel. En conséquence, le certificat du porteur contient l'indication de l'AC en toutes lettres.

Les 23 CROEC/CDOEC de la profession sont les suivants :

1. CROEC d'Alsace
2. CROEC d'Aquitaine
3. CROEC d'Auvergne
4. CROEC de Bourgogne Franche-Comté
5. CROEC de Bretagne
6. CROEC de Champagne
7. CROEC de Corse
8. CROEC de Guadeloupe
9. CDOEC de la Guyane
10. CROEC de Limoges
11. CROEC de Lorraine
12. CROEC de Montpellier
13. CROEC de Paris Île-de-France
14. CROEC de Picardie-Ardennes
15. CROEC de Poitou Charente Vendée
16. CROEC de Rhône-Alpes
17. CROEC de Rouen Normandie
18. CROEC de Toulouse Midi-Pyrénées
19. CROEC des Pays de Loire
20. CROEC d'Orléans

21. CROEC du Nord Pas-de-Calais
22. CROEC Marseille Provence Alpes Côte-d'Azur (ou « CROEC Marseille Provence Alpes Côte-d'Azur Corse », voir I.2.1)
23. CROEC de la Réunion
24. CROEC de la Martinique

Les 23 CROEC et l'unique CDOEC entraînent la création de 24 AC, auxquelles on ajoutera une AC supplémentaire au niveau du CSOEC pour ses besoins propres.

Une autorité racine au niveau du CSOEC sert de sommet à l'arborescence de l'ICP.

Autorité de Certification Racine (ou **AC Racine**) **:** désigne l'entité de plus haut niveau dans l'infrastructure à Clé publiques et qui certifie les autorités de certification filles. Dans le cadre des présentes, l'AC Racine est celle de l'Ordre des Experts-Comptables. À ce titre, les AC des CROEC/CDOEC peuvent être qualifiées d'AC « filles » ou « subalternes ».

Autorités administratives - Ce terme générique, défini à l'article 1 de l'Ordonnance n° 2005-1516 du 8 décembre 2005, désigne les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif, notamment l'Ordre des Experts-Comptables.

Certificat électronique - Fichier électronique attestant qu'une biclé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et le biclé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Le certificat électronique délivré par une AC de l'OEC comporte pour information en matière d'identification de l'AC mention « AC-CROEC de… » (respectivement, « AC-CDOEC de… »), car la vérification de l'appartenance à la profession du demandeur de certificat est uniquement de la compétence d'un Conseil Régional (ou départemental) de l'Ordre des Experts-Comptables (CROEC/CDOEC).

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'ICP. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Déclaration des pratiques de certification (DPC) - La DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Dispositif d'authentification et de création de signature électronique (DACS) : un matériel et/ou un logiciel destiné à générer un biclé cryptographique et à mettre en œuvre la clé privée pour générer une authentification ou une signature électronique. Le DACS est dit "sécurisé" (DSCS) lorsqu'il satisfait aux exigences définies au I de l'article 3 du décret n° 2001-272 du 30 mars 2001.

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Expert-comptable (EC) : personne inscrite au tableau de l'Ordre ou à sa suite, salarié autorisé à exercer la profession d'expert-comptable.

Identificateur d'objet (OID) - identificateur alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifique. Dans le cadre de

l'ICP, les identificateurs OID servent notamment à identifier chacune des politiques, ainsi que les algorithmes de chiffrement acceptés.

Infrastructure à Clés Publiques (**ICP**) : désigne un ensemble de moyens organisationnels, techniques (matériels et logiciels), humains, documentaires et contractuels pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'ICP génère, distribue, gère et archive les Certificats. Chacune des composantes de l'ICP est décrite dans la Politique de certification définissant le niveau de confiance confié à chacune d'entre elles.

Opérateur de Service de Certification (OSC) : composante de l'ICP disposant d'une plate-forme lui permettant de générer et émettre des certificats auxquels une communauté d'utilisateurs fait confiance.

Online Certificate Status Protocol **(OSCP)** : protocole de l'ICP par lequel un certificat est validé (non révocation) en ligne. Le protocole fait l'objet de la norme RFC 2560.

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Portail web client : désigne un site web sous la responsabilité du CSOEC sur lequel chaque Porteur (i) effectue ses demandes d'émission, de renouvellement et de révocation de Certificats, (ii) suit en ligne l'état de ses demandes, (iii) recueille la documentation relative à l'utilisation de ses Certificats et (iv) télécharge le Progiciel de signature sur son poste informatique.

Ce site peut être assuré par le CSOEC lui-même ou être confié par lui à une des organisations spécialisées de l'Ordre des Experts-Comptables.

Prestataire de services de certification électronique (PSCE) - Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "*issuer*" du certificat.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Qualification d'un prestataire de services de certification électronique - Le *Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005* décrit la procédure de qualification d'un PSCE. Il s'agit d'un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC pour un niveau de sécurité donné et correspondant au service visé par les certificats.

Qualification d'un produit de sécurité - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le RGS. La procédure de qualification des produits de sécurité est décrite dans le Décret du 8 décembre 2005 précité. Le RGS

précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Support : désigne un support physique contenant la Clé privée et le (ou les) certificat(s) électronique(s) (d'authentification et de signature), protégés à l'aide d'un code PIN, et permettant des opérations cryptographiques. Le Support est remis à chaque Porteur en face-à-face par la composante de l'AC dont il dépend chargée de l'Enregistrement.

SUPRA : Ce numéro identifie de façon unique chaque Expert Comptable inscrit au Tableau de l'Ordre. Ce numéro est délivré à la première inscription de la personne physique à l'Ordre et n'est plus modifié par la suite, même en cas de pluri-adhésion. Rappelons aussi qu'une personne physique peut détenir plusieurs certificats, avec un même SUPRA, mais dans ce cas, les SIRET seront différents.

II RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

II.1 Entités chargées de la mise à disposition des informations

L'AC met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats à destination des porteurs et des utilisateurs de certificats (cf. chapitre I.3.1 ci-dessus).

Les méthodes de mise à disposition et les adresses correspondantes sont précisées ci-après.

II.2 Informations devant être publiées

L'AC a pour obligation de publier au minimum les informations suivantes à destination des porteurs et utilisateurs de certificats :

- La politique de certification, établie par le PSCE et couvrant l'ensemble des rubriques du RFC3647
- la liste des certificats révoqués
- les certificats de l'AC, en cours de validité
- le certificat de l'AC Racine et son empreinte cryptographique (SHA-256)
- la PC de l'AC Racine

L'AC a également pour obligation de publier sur un modèle établi par le PSCE, à destination des porteurs de certificats, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.). Ces conditions générales font notamment partie intégrante du dossier d'enregistrement.

Le moyen utilisé pour la publication de ces informations, sauf pour les LCR / LAR (cf. chapitre IV.10), est libre et précisé plus loin dans la PC. Il garantit l'intégrité, la lisibilité, la compréhensibilité et la clarté des informations publiées.

La D.P.C. est exclusivement accessible à un membre de l'Ordre sur demande de sa part au point de contact identifié en I.6.2.

II.3 Délais et fréquences de publication

Les informations liées à l'ICP (nouvelle version de la PC, formulaires, etc.) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. En particulier, toute nouvelle version sera communiquée au porteur lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent avoir une disponibilité de 24 h sur 24.

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants et les systèmes les publiant doivent avoir la même disponibilité.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres IV.9 et IV.10.

II.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'ICP, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

III IDENTIFICATION ET AUTHENTIFICATION

III.1 Nommage

III.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat conforme à la norme X.509, l'AC émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un "*Distinguished Name*" (DN) de type X.501.

III.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats sont explicites.

Le DN du porteur est construit à partir des nom et prénom de son état civil tels que contenus dans le tableau de l'Ordre.

Ces éléments sont vérifiés par l'AE à partir des documents d'identité joints au dossier. Les noms d'épouse ou d'usage sont acceptés dès lors qu'ils figurent sur ces documents d'identité.

III.1.2.1 Identité des A.C émettrices

Les AC émettrices sont identifiables par leurs DN, comme suit.

DN de l'AC	Entité
C=FR, O=CROEC d'Alsace, OU=0002 778867796, CN=Ordre des Experts-Comptables - région Alsace	CROEC d'Alsace
C=FR, O=CROEC d'Aquitaine, OU=0002 781846464, CN=Ordre des Experts-Comptables - région Aquitaine	CROEC d'Aquitaine
C=FR, O=CROEC d'Auvergne, OU=0002 779186311, CN=Ordre des Experts-Comptables - région Auvergne	CROEC d'Auvergne
C=FR, O=CROEC de Bourgogne Franche-Comté, OU=0002 778212951, CN=Ordre des Experts-Comptables - région Bourgogne Franche-Comté	CROEC de Bourgogne Franche-Comté
C=FR, O=CROEC de Bretagne, OU=0002 777733700, CN=Ordre des Experts-Comptables - région Bretagne	CROEC de Bretagne
C=FR, O=CROEC de Champagne, OU=0002 775611718, CN=Ordre des Experts-Comptables - région Champagne	CROEC de Champagne
C=FR, O=CROEC de Corse, OU=0002 752406082, CN=Ordre des Experts-Comptables - région Corse	CROEC de Corse
C=FR, O=CROEC de Guadeloupe, OU=0002 348367988, CN=Ordre des Experts-Comptables - région Guadeloupe	CROEC de Guadeloupe
C=FR, O=CDOEC de Guyane, OU=0002 508714565, CN=Ordre des Experts-Comptables - comité Guyane	CDOEC de Guyane
C=FR, O=CROEC de La Réunion, OU=0002 322951443, CN=Ordre des Experts-Comptables - région La Réunion	CROEC de La Réunion
C=FR, O=CROEC de Lille Nord Pas-de-Calais, OU=0002 380182212, CN=Ordre des Experts-Comptables - région Lille Nord Pas-de-Calais	CROEC de Lille Nord Pas-de-Calais
C=FR, O=CROEC de Limoges, OU=0002 380183319, CN=Ordre des Experts-Comptables - région Limoges	CROEC de Limoges
C=FR, O=CROEC de Lorraine, OU=0002 380188185, CN=Ordre des Experts-Comptables - région Lorraine	CROEC de Lorraine
C=FR, O=CROEC de Marseille PACAC, OU=0002 782825046, CN=Ordre des Experts-Comptables - région Marseille PACA	CROEC de Marseille PACA
C=FR, O=CROEC de Marseille PACAC, OU=0002 782825046, CN=Ordre des Experts-Comptables - région Marseille PACAC	CROEC de Marseille PACAC
C=FR, O=CROEC de Martinique, OU=0002 382052538, CN=Ordre des Experts-Comptables - région Martinique	CROEC de Martinique

DN de l'AC	Entité
C=FR, O=CROEC de Montpellier, OU=0002 776038077, CN=Ordre des Experts-Comptables - région Montpellier	CROEC de Montpellier
C=FR, O=CROEC d'Orléans, OU=0002 775501364, CN=Ordre des Experts-Comptables - région Orléans	CROEC d'Orléans
C=FR, O=CROEC de Paris Ile-de-France, OU=0002 784854408, CN=Ordre des Experts-Comptables - région Paris Ile-de-France	CROEC de Paris Ile-de-France
C=FR, O=CROEC de Pays de Loire, OU=0002 332603604, CN=Ordre des Experts-Comptables - région Pays de Loire	CROEC de Pays de Loire
C=FR, O=CROEC de Picardie-Ardennes, OU=0002 780601803, CN=Ordre des Experts-Comptables - région Picardie-Ardennes	CROEC de Picardie-Ardennes
C=FR, O=CROEC de Poitou-Charentes-Vendée, OU=0002 311146385, CN=Ordre des Experts-Comptables - région Poitou-Charentes-Vendée	CROEC de Poitou-Charentes-Vendée
C=FR, O=CROEC de Rhône-Alpes, OU=0002 779893890, CN=Ordre des Experts-Comptables - région Rhône-Alpes	CROEC de Rhône-Alpes
C=FR, O=CROEC de Rouen Normandie, OU=0002 781121850, CN=Ordre des Experts-Comptables - région Rouen Normandie	CROEC de Rouen Normandie
C=FR, O=CROEC de Toulouse Midi-Pyrénées, OU=0002 776949596, CN=Ordre des Experts-Comptables - région Toulouse Midi-Pyrénées	CROEC de Toulouse Midi-Pyrénées

Conformément au R.G.S., le DN de ces AC est construit comme suit :

- le champ `C` désigne le pays de l'AC
- le champ `O` désigne l'organisme (ici, CROEC ou CDOEC, selon les cas)
- le champ `OU` contient le SIRET de l'organisme
- le champ `CN` contient le nom INSEE de l'organisme

III.1.2.2 Identité des porteurs

Le DN des certificats porteurs est construit comme suit :

- Le champ `C=FR` désigne la France
- Le champ `O` désigne l'organisme de rattachement du porteur, à savoir son cabinet d'exercice professionnel, tel qu'inscrit au registre du commerce
- Le champ `OU` est contient le SIREN de ce même organisme, précédé de la chaîne « 0002 »
- Le champ `Title` contient le titre du porteur tel qu'il apparaît dans le tableau de l'Ordre. Deux possibilités : « Expert-comptable » ou « Autorisé à exercer la profession d'expert-comptable »
- Le champ `CN` contient le prénom et le nom du porteur (dans cet ordre) tels qu'ils apparaissent dans le tableau de l'Ordre.
- Le champ `serialNumber` contient un numéro unique d'identification, propre au porteur. Ce champ est calculé à partir du numéro SUPRA du porteur et est utilisé par les applications du métier pour identifier le porteur.

  Ce numéro apparaît ainsi dans tous les certificats attribués au porteur par les AC du CSOEC.

III.1.2.3 Certificats de test

Les certificats de test sont identifiables par le fait que leur `CN` contient le mot « `TEST` », précédant un prénom et un nom fictifs. Tous les autres champs (à l'exception des informations d'AC, comme les champs `Issuer`, AIA, AKI, etc.) sont susceptibles de différer des profils des certificats porteurs décrits au chapitre VII.1.

CES CERTIFICATS NE SONT PAS ATTRIBUES A DES EXPERTS-COMPTABLES DANS LE CADRE DE LEUR EXERCICE PROFESSIONNEL ET NE DOIVENT EN AUCUN CAS ETRE CONSIDERES COMME TELS.

III.1.3 Pseudonymisation des porteurs

La présente politique n'autorise pas l'utilisation de pseudonymes dans ses certificats.

III.1.4 Règles d'interprétation des différentes formes de nom

Voir III.1.2 ci-dessus.

III.1.5 Unicité des noms

Le DN du champ "*subject*" de chaque certificat de porteur permet d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC.

Ce DN respecte les règles d'homonymie au sein du domaine de l'AC.

Dans chaque certificat X509v3, l'AC émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un "*Distinguished Name*" (DN) de type X.501

L'unicité des noms au sein de la présente AC est assurée par le `serialNumber` du DN (y compris pour les certificats de test).

L'anonymat ou le pseudonyme des porteurs ne sont pas supportés par la présente AC.

III.1.6 Identification, authentification et rôle des marques déposées

L'AC est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom. Les litiges pouvant survenir dans les noms apparaissant dans les certificats ne peuvent porter que sur le cabinet de rattachement, cet aspect étant déjà traité au niveau de l'inscription au Tableau de l'Ordre.

III.2 Validation initiale de l'identité de la structure professionnelle d'exercice du porteur

La demande initiale est saisie sur une application Web en liaison avec les tableaux régionaux de l'Ordre. L'identité du demandeur est issue de ce référentiel, sans possibilité de changement, y compris pour l'adresse d'exercice professionnel concernée par le certificat. En cas d'anomalie sur cette adresse, l'Expert Comptable doit, préalablement à sa demande de certificat, faire procéder à la rectification des informations auprès de l'Ordre.

L'inscription au tableau de l'Ordre est nécessaire et suffisante pour la présente validation.

III.2.1 Méthode pour prouver la possession de la clé privée

Sans objet, car la biclé est tirée en central.

III.2.2 Validation de l'identité d'un organisme

Voir ci-dessous.

III.2.3 Validation de l'identité d'un individu

III.2.3.1 Enregistrement d'un porteur

L'enregistrement du futur porteur (personne physique) rattaché à une entité nécessite l'identification de cette entité et, l'identification de la personne physique et la preuve du rattachement de la personne physique à l'entité.

L'identité du porteur est vérifiée lors d'un face à face physique avec un A.R.

Le dossier d'enregistrement, déposé soit directement auprès de l'AE via la signature en ligne sur le portail Signexpert, soit par numérisation du dossier papier, comprend au moins :

- Une pièce d'identité officielle en cours de validité (carte nationale d'identité ou passeport).

- La copie du formulaire de demande de certificat, signée par le porteur. Ce formulaire est constitué sur la base des informations provenant du tableau de l'Ordre et de la demande déposée sur le portail ;

Remarque :

- La qualité d'expert-comptable du demandeur (E.-C. inscrit dans le CROEC/CDOEC) est établie à partir du tableau de l'Ordre : seuls les membres de l'Ordre peuvent effectuer une demande sur le portail.
- De même, l'existence de l'entité de rattachement et son numéro SIREN, tel qu'il figurera dans le certificat, est établie à partir du tableau de l'Ordre. Cette entité n'ayant pas de relation hiérarchique vis-à-vis du demandeur, le dossier d'enregistrement ne nécessite pas de mandat particulier.

L'AE garde une copie de la pièce d'identité présentée à l'A.R. Elle archive l'ensemble des documents constituants la demande de certificat, à savoir :

- une copie de la pièce d'identité présentée
- la copie du formulaire de demande de certificat, signée par le porteur lors de la remise du support
- l'attestation d'acceptation du certificat signée par le porteur lors de la remise de la carte à puce (support du certificat et des clés)

La signature de l'attestation d'acceptation du certificat par le porteur est considérée comme la preuve de la possession du support de la clé privée. Cette signature est possible à tout moment mais sera conseillée au moment du retrait.

III.2.3.2 Enregistrement d'un Mandataire de Certification

Sans objet.

III.2.3.3 Enregistrement d'un porteur via un MC

Sans objet

III.2.4 Informations non vérifiées du porteur

La présente PC ne formule pas d'exigence spécifique sur le sujet.

III.2.5 Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique.

III.2.6 Certification croisée d'AC

Seul le comité de pilotage peut prendre la décision de procéder à une certification croisée d'une A.C. Signexpert.

À ce jour, les certificats d'A.C. sont certifiés par les deux A.C. supplémentaires suivantes, pour des raisons techniques de reconnaissance des certificats de la profession par les logiciels du marché :

CertPlus Classe 2	CN = Class 2 Primary CA O = Certplus C = FR	URL=http://www.certplus.com/CRL/Class2.crl
	SKI	e3 73 2d df cb 0e 28 0c de dd b3 a4 ca 79 b8 8e bb e8 30 89

KEYNECTIS CDS CA	CN = KEYNECTIS CDS CA OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR	URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_CDS_CA.crl
	SKI	9f 22 78 d7 71 1b de 33 b0 7f c9 20 7a a9 a8 e0 4e 62 e3 fb

III.3 Identification et validation d'une demande de délivrance d'un certificat suite au changement de biclé (réémission)

À compter du 1er octobre 2014, avant l'expiration de ces certificats, le possesseur d'une clé Signexpert peut demander en ligne (cf. ci-dessous) l'émission de nouveaux certificats semblables sur une nouvelle clé (réémission), à condition que la clé en sa possession lui ait été remise en mains propres (III.2.3). Autrement dit, une telle demande n'est possible qu'une fois ; un certificat « réémis » ne peut pas l'être une seconde fois.

Il n'est pas possible d'effectuer une telle demande si le certificat de la clé Signexpert correspondante a été révoqué : suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande est identique à la procédure d'enregistrement initial ou doit être une procédure offrant un niveau de garantie équivalent.

Note : cette procédure remplace le « renouvellement » des versions 6.6 et précédentes de cette P.C.

La réémission d'un nouveau certificat ne peut se faire qu'avec changement de la biclé correspondante (cf. chapitre IV.6).

La demande de réémission du certificat s'effectue en ligne, depuis l'espace personnel du demandeur, sur le portail Signexpert.

L'AC s'assure que :

- les informations du dossier d'enregistrement initial sont toujours valides
- le certificat à réémettre existe et est toujours valide

Dans l'affirmative, un nouveau support est envoyé par courrier postal recommandé à l'adresse du cabinet du demandeur (adresse ordinale).

Le portail Signexpert prévient par *courriel*, à intervalles réguliers, tous les porteurs qui sont en période de réémission.

Une réémission de certificat ne peut être réalisé que dans les 45 derniers jours de validité du certificat concerné.

Remarque : conformément au I.2.1, une fois le transfert de compétences effectif, la réémission des certificats de la région PACAC (certificats d'OID 1.2.250.1.165.1.2.13.1.6) donnera lieu à la production d'un nouveau certificat pour le même porteur mais produit par l'une des deux nouvelles A.C.

III.4 Identification et validation d'une demande de révocation

Le porteur peut demander la révocation de son certificat par différents moyens :

a) En contactant l'AE nationale (CSOEC) par téléphone ou par courriel

b) Depuis son espace personnel sur le Portail Web de *Signexpert* : il s'identifie avec les mêmes identifiants que ceux utilisés lors d'une demande initiale de certificat.

c) Depuis le portail web client de l'O.S.C. : le porteur s'identifie à l'aide du code de révocation choisi lors de sa demande de certificat.

d) Auprès de son CROEC/CDOEC : le porteur peut se présenter directement muni d'une pièce d'identité.

e) Une demande de révocation peut également être faite par courrier ou par télécopie auprès du CROEC/CDOEC. Elle est alors signée par le demandeur et le service de gestion des révocations s'assure de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

Dans tous les cas, le demandeur est formellement authentifié par la vérification de son identité et de son autorité par rapport au certificat à révoquer.

IV EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

IV.1 Demande de certificat

IV.1.1 Origine d'une demande de certificat

Les personnes habilitées à déposer une demande de certificat auprès de chaque CROEC/CDOEC sont les experts-comptables inscrits au tableau dudit CROEC/CDOEC.

L'AE assure la validation de la demande de certificat en s'appuyant sur le tableau de l'Ordre et sur les documents présentés.

Une demande de certificat n'oblige en rien l'AC à émettre un certificat. Un refus doit cependant être motivé.

IV.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

L'expert-comptable se connecte au site Portail Web Client. Il peut alors choisir de demander un certificat pour une de ses inscriptions au tableau pour laquelle aucune demande n'est déjà en cours. Le processus pourra être réitéré pour les autres inscriptions.

Les informations suivantes font partie de la demande de certificat :

- le nom du porteur à utiliser dans le certificat ;
- les données personnelles d'identification du porteur ;
- le CROEC/CDOEC d'inscription du demandeur
- les données d'identification de l'entité professionnelle.

Ces données proviennent du tableau de l'Ordre : l'expert-comptable confirme l'exactitude de ces informations. Toujours sur le portail Web, il procède ensuite à la saisie…

1. des questions de révocation
2. de l'adresse de facturation
3. de l'adresse courriel de confirmation de la demande.

Après le paiement en ligne des frais relatifs à l'acquisition du certificat, une demande de confirmation est envoyée par courriel. La demande n'est établie que lorsque le demandeur répond à cet courriel.

Une demande de génération du certificat et de la biclé est générée par l'AC vers la fonction adéquate de l'ICP (*cf.* chapitre I.3.1).

IV.2 Traitement d'une demande de certificat

IV.2.1 Exécution des processus d'identification et de validation de la demande

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'A.R. 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).

Il est conservé une trace des justificatifs d'identité présentés :

- pour les pièces au format papier, sous la forme d'une photocopie signée à la fois par le futur porteur et par l'A.R.

- pour les pièces au format électronique, celles-ci sont conservées sous une forme ayant valeur légale.

IV.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, la composante chargée de l'enregistrement en informe le porteur en en justifiant le rejet.

IV.2.3 Durée d'établissement du certificat

La durée d'établissement du certificat (délai entre la réception de la demande et l'émission du certificat) est d'au plus 35 jours.

IV.3 Délivrance du certificat

IV.3.1 Actions de l'AC concernant la délivrance du certificat

À la réception d'une demande en provenance du portail, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au porteur auprès de l'OSC.

Chez l'OSC, le processus de génération du certificat est lié de manière sécurisée au processus de génération de la biclé : l'ordonnancement des opérations est assuré ainsi que l'intégrité et l'authentification des échanges entres les composantes. La clé privée est protégée en intégrité et en confidentialité tout au long de son cycle de vie : le support est remis en mains propres au porteur, tandis que les données d'activation lui sont transmises par un canal distinct (voir ci-dessous).

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées ci-après.

IV.3.2 Notification par l'AC de la délivrance du certificat au porteur

La remise du certificat se fait en mains propres (face-à-face).

Le certificat complet et exact est mis à la disposition de son porteur.

IV.4 Acceptation du certificat

En parallèle au tirage de la biclé par l'AC et à la confection du certificat, l'E.-C. demandeur recevra à son domicile sous correspondance sécurisée en courrier simple le code PIN d'activation de sa (ou ses) carte(s). L'adresse utilisée est l'adresse professionnelle d'inscription au tableau de l'Ordre.

La carte est envoyée au CROEC/CDOEC dont dépend l'expert-comptable.

IV.4.1.1 Cas particulier d'une remise en masse

Le conseil de l'Ordre peut procéder à la remise des supports et des certificats en mains propres dans le cadre de ses congrès nationaux ou toute manifestation organisée ou animée par les conseils régionaux. Dans le cas des congrès nationaux, le support n'est pas envoyé au CROEC/CDOEC dont dépend le porteur, mais à l'A.C., dont un représentant sera présent au congrès.

Le cas échéant, en fonction des modalités d'organisation des remises en masse, le code PIN d'activation des cartes pourra être transmis aux porteurs par un autre moyen que le courrier postal. Dans tous les cas, les codes d'activation seront transmis de manière séparée, dans le temps et dans l'espace, des supports, et par un canal assurant l'identité du destinataire.

IV.4.2 Démarche d'acceptation du certificat

L'expert-comptable demandeur se rend alors au siège du CROEC/CDOEC dont il dépend ou, le cas échéant, dans un lieu fixé par celui-ci.

L'expert-comptable demandeur dispose d'un délai de deux mois pour venir prendre possession de sa clé soit auprès de son CROEC/CDOEC (demande initiale), soit de la Poste (réémission). Ce délai court à partir de la date à laquelle sa clé est disponible auprès de l'entité concernée. Passé ce délai, dit « **délai de délivrance** », sa clé peut être détruite et ses certificats, révoqués par l'Autorité de Certification.

Au cours d'un face à face, il présente une pièce d'identité en cours de validité. Si elle correspond à la demande de certificat et aux informations enregistrées dans l'annuaire de la profession, alors le certificat peut être délivré.

Dans le cas où une discordance est notée, le certificat est immédiatement révoqué par l'AE et la carte détruite.

Sinon, la carte contenant les clés et le certificat est remise au porteur. Il visualise alors le contenu du certificat avec l'AR et signe : la demande de certificat, le document d'acceptation du certificat, les conditions générales d'utilisation et le bordereau de remise de la carte physique.

IV.4.2.1 Cas particulier d'une remise en masse

Les demandes font l'objet d'une vérification dans la demi-journée précédant la remise physique, et non lors de la remise (vérification de l'inscription du porteur dans l'annuaire de la profession).

L'A.E. peut être quelqu'un extérieur au CROEC, dûment habilitée pour l'occasion : la liste des A.E. présentes est validée par le CSOEC. De plus, dans le cadre d'un congrès national, la présence d'une A.E. nationale est requise afin de permettre les révocations nécessaires, le cas échéant.

IV.4.3 Publication du certificat

Le certificat fait l'objet d'une publication dans les annuaires techniques du système d'information de l'Ordre.

La publication ne peut avoir lieu qu'après acceptation du contenu du certificat par celui-ci. Son acceptation de publication est dans les Conditions Générales d'Utilisation, elle est cosubstancielle à la demande.

IV.4.4 Notification par l'AC aux autres entités de la délivrance du certificat

L'AC informe les autres entités de l'ICP de la délivrance du certificat si nécessaire.

IV.5 Usages de la biclé et du certificat

IV.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service d'authentification et de signature (*cf.* chapitre I.5.1.1). Cette contrainte est portée à la connaissance des porteurs par l'AC, notamment dans l'accord contractuel qui les lie. Il y est rappelé que :

- Les porteurs doivent respecter strictement les usages autorisés des biclés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.
- Les porteurs s'engagent également à ne plus utiliser leur biclé ou leur certificat dès la perte ou la suspension de la qualité d'expert-comptable ou après révocation ou expiration du certificat.

L'usage autorisé de la biclé du porteur et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés. Cet usage est explicité dans les conditions générales d'utilisation et/ou le contrat porteur. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du porteur par l'AC avant d'entrer en relation contractuelle.

IV.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Les utilisateurs de certificats seront informés par l'AC qu'ils doivent respecter strictement les usages autorisés des certificats et que dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6 Renouvellement d'un certificat

Dans le cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la biclé correspondante. Comme l'AC génère les biclés des porteurs, elle garantit qu'un certificat correspondant à une biclé existante ne peut pas être renouvelé au sens du RFC3647.

IV.7 Réémission d'un certificat

Le déclenchement de la fourniture d'un nouveau certificat du porteur peut-être automatique, à l'initiative du porteur, ou par l'entité, pour un porteur qui lui est rattaché. La notion de réémission est décrite en III.3.

La demande et l'émission du nouveau certificat s'effectuent en ligne. La demande est authentifiée sur la base du certificat courant ou d'un certificat d'authentification conforme à la politique [PC_AS], en cours de validité.

Le processus de réémission est le suivant :

1. Le porteur s'authentifie sur le portail Signexpert et accède à son espace personnel
2. S'il est en période de réémission, le portail lui propose d'effectuer sa demande de réémission en ligne. S'il accepte,
    a. un récapitulatif de ces certificats lui est présenté. Le cas échéant, le porteur peut mettre à jour son adresse *courriel* (en cas de changement, une confirmation de cette adresse sera nécessaire avant de pouvoir procéder à l'émission des nouveaux certificats).
    b. Le porteur saisit l'adresse de livraison du code PIN.
    c. le porteur signe (en ligne) sa demande de réémission et l'acceptation des CGU
3. le porteur reçoit sa nouvelle clé et ses certificats par courrier recommandé à l'adresse ordinale de son cabinet.

Les délais d'établissement (IV.2.3) et de délivrance (IV.4.2) sont les mêmes que pour une demande initiale.

IV.8 Modification du certificat

La modification du certificat n'est pas admise.

IV.9 Révocation et suspension des certificats

IV.9.1 Causes possibles d'une révocation

IV.9.1.1 Certificats de porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le porteur ou l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur;
- la clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- le porteur ou une entité autorisée (représentant légal de l'entité) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur ou de son support) ;
- le décès du porteur ou la cessation d'activité de l'entité du porteur ;
- le porteur n'est plus membre de l'Ordre dans les conditions d'émission du certificat ;

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné est révoqué.

L'AC peut, à sa discrétion, révoquer un certificat lorsqu'un porteur ne respecte pas les obligations énoncées dans la présente politique de certification.

IV.9.1.2 Certificats d'une composante de l'ICP

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR) :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif)
- Cessation d'activité de l'entité opérant la composante.

IV.9.2 Origine d'une demande de révocation

IV.9.2.1 Certificats de porteurs

Les personnes ou entités qui peuvent demander la révocation d'un certificat de porteur sont les suivantes :

- le porteur au nom duquel le certificat a été émis ;
- l'AC émettrice du certificat
- Une fois le transfert de compétences de la région PACAC effectif (cf. I.2.1), ces certificats (OID 1.2.250.1.165.1.2.13.7.6) pourront être révoqués par les A.C. PACA et Corse
- le CSOEC par l'intermédiaire de l'AC.

Le porteur est informé des personnes et entités susceptibles d'effectuer une demande de révocation pour son certificat.

IV.9.2.2 Certificats d'une composante de l'ICP

Les demandes de révocation des certificats de composantes sont émises par le CSOEC. La liste des personnes habilitées à ce faire au CSOEC est précisée dans la D.P.C.

IV.9.3 Procédure de traitement d'une demande de révocation

IV.9.3.1 Révocation d'un certificat de porteur

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

a) En contactant l'AE nationale (CSOEC) par téléphone ou par courriel

b) En se connectant sur le Portail Web de *Signexpert*

c) Depuis le portail web client de l'OSC, 24h/24 et 7j/7.

d) Auprès de son CROEC/CDOEC : le porteur peut se présenter directement muni d'une pièce d'identité.

e) Une demande de révocation peut également être faite par courrier ou par télécopie auprès du CROEC/CDOEC

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- l'identité du porteur du certificat utilisée dans le certificat (nom, prénom, ...) ;
- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,...) ;
- éventuellement, la cause de révocation.

Une fois la demande authentifiée et contrôlée, l'AC révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la publication sur l'état des certificats. L'information de révocation est diffusée au minimum via une LCR signée par l'AC. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC.

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il doit également être informé de la révocation effective de son certificat. L'entité professionnelle est informée de la révocation de tout certificat des porteurs qui lui sont rattachés.

L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

IV.9.3.2 Révocation d'un certificat d'une composante de l'ICP

Les demandes de révocation des certificats de composante se font sur le portail client de l'O.S.C. La demande est authentifiée conformément aux procédures de l'O.S.C. (demande signée manuscrite ou électroniquement).

IV.9.3.3 Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

IV.9.4 Délai de traitement par l'AC d'une demande de révocation

IV.9.4.1 Révocation d'un certificat de porteur

Toute demande de révocation est traitée en urgence.

Les demandes de révocation sont immédiatement traitées :

a) par le CROEC/CDOEC saisi par le porteur qui, après validation de l'identité, demande à l'AE Nationale de procéder à la révocation.

b) par le porteur lui-même sur le site de la profession

c) par l'O.S.C. saisi par le porteur

Il s'écoule au maximum 12 heures entre la demande de révocation par le porteur et la publication de la nouvelle LCR prenant en compte cette demande. Dans ce cas, la publication est biquotidienne;

La durée maximale d'indisponibilité par interruption de service (panne ou maintenance) ainsi que la durée maximale totale d'indisponibilité par mois est fixée dans le contrat PSCE-OSC et les modalités en sont précisées dans la DPC.

IV.9.4.2 Révocation d'un certificat d'une composante de l'ICP

Toute demande de révocation est traitée en urgence.

Les demandes de révocation sont immédiatement traitées par l'O.S.C. saisi par le CSOEC.

La durée maximale d'indisponibilité par interruption de service (panne ou maintenance) ainsi que la durée maximale totale d'indisponibilité par mois est fixée dans le contrat PSCE-OSC et les modalités en sont précisées dans la D.P.C.

IV.9.5 Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

IV.9.6 Fréquence d'établissement des LCR

La LCR est mise à jour biquotidiennement et publiée via HTTP et LDAP. Une LCR est valable au maximum 72 heures.

IV.9.7 Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai de 30 minutes suivant sa génération.

IV.9.8 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

L'A.C. se réserve la possibilité d'ouvrir un service OCSP accessible à l'adresse indiquée dans les certificats. Dans le cas de l'ouverture du service, l'A.C. s'engage à respecter les exigences d'intégrité, de disponibilité et de délai de publication décrites dans la présente P.C.

IV.9.9 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Cf. chapitre IV.9.6 ci-dessus.

IV.9.10 Autres moyens disponibles d'information sur les révocations

Sans objet.

IV.9.11 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences du chapitre IV.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée fera l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

Quant au porteur, l'AC impose par voie contractuelle qu'en cas de compromission de sa clé privée du porteur ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

IV.9.12 Suspension de certificats

La suspension de certificats n'est pas autorisée dans la présente PC.

IV.10 Fonction d'information sur l'état des certificats

IV.10.1 Caractéristiques opérationnelles

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du certificat de l'AC Racine.

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR. Ces LCR sont des LCR au format V2, publiées aux URL suivantes :

Autorité de certification	URL HTTP
CROEC d'Alsace	`http://seec.experts-comptables.fr/CRL/CRL_ALSACE.crl`
CROEC d'Aquitaine	`http://seec.experts-comptables.fr/CRL/CRL_AQUIT.crl`
CROEC d'Auvergne	`http://seec.experts-comptables.fr/CRL/CRL_AUVERGN.crl`
CROEC de Bourgogne Franche-Comté	`http://seec.experts-comptables.fr/CRL/CRL_B-FC.crl`

Autorité de certification	URL HTTP
CROEC de Bretagne	http://seec.experts-comptables.fr/CRL/CRL_BRETAGNE.crl
CROEC de Champagne	http://seec.experts-comptables.fr/CRL/CRL_CHAMPAG.crl
CROEC de Corse	http://seec.experts-comptables.fr/CRL/CRL_CORSE.crl
CROEC de Guadeloupe	http://seec.experts-comptables.fr/CRL/CRL_GPE.crl
CDOEC de Guyane	http://seec.experts-comptables.fr/CRL/CRL_GUYANE.crl
CROEC de La Réunion	http://seec.experts-comptables.fr/CRL/CRL_REUNION.crl
CROEC de Lille Nord Pas-de-Calais	http://seec.experts-comptables.fr/CRL/CRL_LN-PCAL.crl
CROEC de Limoges	http://seec.experts-comptables.fr/CRL/CRL_LIMOGES.crl
CROEC de Lorraine	http://seec.experts-comptables.fr/CRL/CRL_LORRAIN.crl
CROEC de Marseille PACA	http://seec.experts-comptables.fr/CRL/CRL_PACA.crl
CROEC de Marseille PACAC	http://seec.experts-comptables.fr/CRL/CRL_MARSEIL.crl
CROEC de Martinique	http://seec.experts-comptables.fr/CRL/CRL_MARTINI.crl
CROEC de Montpellier	http://seec.experts-comptables.fr/CRL/CRL_MONTPEL.crl
CROEC d'Orléans	http://seec.experts-comptables.fr/CRL/CRL_ORLEANS.crl
CROEC de Paris Île-de-France	http://seec.experts-comptables.fr/CRL/CRL_PAR-IDF.crl
CROEC de Pays de Loire	http://seec.experts-comptables.fr/CRL/CRL_P-LOIRE.crl
CROEC de Picardie-Ardennes	http://seec.experts-comptables.fr/CRL/CRL_PIC-ARD.crl
CROEC de Poitou-Charentes-Vendée	http://seec.experts-comptables.fr/CRL/CRL_POITOU.crl
CROEC de Rhône-Alpes	http://seec.experts-comptables.fr/CRL/CRL_RHO-ALP.crl
CROEC de Rouen Normandie	http://seec.experts-comptables.fr/CRL/CRL_R-NORMA.crl
CROEC de Toulouse Midi-Pyrénées	http://seec.experts-comptables.fr/CRL/CRL_MIDI-PY.crl

Les CRL sont aussi accessibles via une adresse Signexpert dont l'adresse suit la convention suivante :

http://www.signexpert.fr/CRL/CRL_**Région**.crl

Par exemple, l'adresse de la LCR de l'A.C. du CROEC de Rhône-Alpes est la suivante :

http://www.signexpert.fr/CRL/CRL_**RHO-ALP**.crl

Les CRL sont aussi accessibles par un annuaire LDAP V3 dont l'adresse suit la convention suivante :

ldap://ldapseec.experts-comptables.fr/DN_de_l'AC?certificaterevocationlist;binary?base?objectclass=pkiCA

Par exemple, l'adresse de la LCR de l'A.C. du CROEC de la Réunion est la suivante :

ldap://ldapseec.experts-comptables.fr/C=FR,O=CROEC%20de%20La%20Réunion,OU=0002%20322951443,CN=Ordre%20des%20Experts-Comptables%20-%20région%20La%20Réunion?certificaterevocationlist;binary?base?objectclass=pkiCA

Le cas échéant, une A.C. dédiée est en charge de la production des certificats de signature des réponses OCSP. Le tableau ci-dessous explicite les moyens d'identifier cette A.C. (voir chapitre VII pour plus de détails).

Champ	**Valeur**
Serial Number	11:20:52:57:8a:7a:42:86:a0:95:70:aa:3f:95:3b:e0:48:13
Subject	C=FR, O=Conseil Supérieur de l'Ordre des Experts-Comptables, OU=0002 775670003, CN=Ordre des Experts-Comptables – OCSP
X509v3 Subject Key Identifier	CC:05:0D:2F:CF:AA:B5:CC:DA:B6:71:36:87:FA:77:F2:EC:AC:41:2C

IV.10.2 Disponibilité de la fonction

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 2 heures et une durée maximale totale d'indisponibilité par mois de 8 heures.

Le cas échéant, le temps de réponse du serveur de vérification en ligne du statut d'un certificat (OCSP) à la requête reçue est inférieur à 10 secondes.

IV.11 Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier est révoqué.

IV.12 Séquestre de clé et recouvrement

Il n'est procédé à aucun séquestre ni recouvrement des clés privées des porteurs.

Il n'est procédé à aucun séquestre ni recouvrement des clés d'AC.

IV.13 Certificats de test

Les certificats de test (cf. III.1.2.3) et leurs supports sont produits et gérés par l'OSC en accord avec l'AC, dans le cadre de campagnes de test définies et formalisées. Les certificats de test sont révoqués et leurs supports détruits, dès lors que la campagne de test est terminée.

V MESURES DE SECURITE NON TECHNIQUES

V.1 Mesures de sécurité physique

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'ICP. C'est pourquoi elles sont précisées dans la DPC, notamment sur les points suivants :

- Situation géographique et construction des sites
- Accès physique
- Alimentation électrique et climatisation
- Vulnérabilité aux dégâts des eaux
- Conservation des supports
- Mise hors service des supports
- Sauvegardes hors site

V.2 Mesures de sécurité procédurales

V.2.1 Rôles de confiance

L'AC distingue au moins les cinq rôles fonctionnels de confiance suivants :

Responsable de sécurité : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.

Responsable d'application : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'ICP au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

Ingénieur système : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.

Opérateur : Un opérateur au sein d'une composante de l'ICP réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.

Contrôleur : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'ICP et aux politiques de sécurité de la composante.

Un même rôle fonctionnel peut être tenu par différentes personnes.

De manière générale, des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification. Ces rôles sont décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'ICP sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Lorsqu'appropriées, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'AC. L'AC doit implémenter techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre. Ces descriptions figurent dans la DPC.

V.2.2 Nombre de personnes requises par tâches

Le nombre de personnes requises par tâches selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, est précisé dans la DPC.

V.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'ICP doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment que :

- son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'ICP.

Ces contrôles sont décrits dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante.

V.2.4 Rôles exigeant une séparation des attributions

Les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur
- contrôleur et tout autre rôle
- ingénieur système et opérateur

V.3 Mesures de sécurité vis-à-vis du personnel

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'ICP. C'est pourquoi elles sont précisées dans la DPC, notamment sur les points suivants :

- Qualifications, compétences et habilitations requises
- Procédures de vérification des antécédents
- Exigences en matière de formation initiale
- Exigences et fréquence en matière de formation continue
- Fréquence et séquence de rotation entre différentes attributions
- Sanctions en cas d'actions non autorisées
- Exigences vis-à-vis du personnel des prestataires externes
- Documentation fournie au personnel

V.4 Procédures de constitution des données d'audit

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'ICP. C'est pourquoi elles sont précisées dans la DPC en ce qui concerne la journalisation d'événements.

V.4.1 Informations enregistrées pour chaque événement

Toutes les opérations effectuées par l'AC ou l'AE sont journalisées automatiquement avec les éléments d'authentification des opérateurs et horodatage local afin d'être en mesure de fournir une preuve de la certification en justice. Les éléments suivants sont mémorisés pour chaque événement :

- Type d'opération.
- Destinataire de l'opération.
- Nom du demandeur de l'opération.
- Nom de l'opérateur.
- Nom des personnes présentes (s'il y en a d'autres).
- Lieu de l'opération.
- Date et heure de l'opération.
- Cause de l'événement.
- Résultat de l'événement (échec ou réussite).
- Date et heure de journalisation.

V.4.2 Imputabilité

L'imputabilité d'une action revient à la personne, à la composante, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure dans l'un des champs du journal d'événements.

V.4.3 Événements enregistrés par l'AE

L'AE enregistre et sauvegarde les événements suivants :

- Les dossiers de demandes de certificat
- Les dossiers de demandes de révocation
- Toutes les relations avec l'AC
- Tous les accès aux fonctions ayant trait aux opérations d'enregistrement.

V.4.4 Événements enregistrés par l'AC

La fonction de journalisation de l'AC doit consister à enregistrer tous les événements et notamment :

- Tous les événements ayant trait à la sécurité des systèmes informatiques utilisés,
- Démarrage et arrêt des systèmes informatiques,
- Démarrage et arrêt des applications,
- Opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou. modifier les privilèges système d'Utilisateurs privilégiés (Utilisateurs maîtres de l'ICP, responsables de sécurité, gestionnaires),
- Génération des clés de ses composantes,
- Chargement, déchargement du dispositif contenant la clé de l'AC, insertion et retrait de la carte cryptographique,
- Création et révocation de certificats,
- Opérations pour initialiser, extraire, valider et invalider des porteurs, et pour mettre à jour ou récupérer leurs clés,

- Opérations d'écriture dans l'annuaire des certificats et des LCR.
- Requêtes et réponses OCSP (si le service est mis en œuvre)

V.4.5 Événements divers

L'environnement d'exploitation fait lui aussi l'objet d'une journalisation des événements :

- Accès physiques aux locaux et matériels protégés.
- Opérations de maintenance et de changements de la configuration des systèmes.
- Les changements de personnel.
- Le suivi des dossiers et supports physiques.
- Le suivi des opérations de sauvegarde et d'archivage.
- Les actions de destruction des supports contenant des clés, des données d'activation ou des renseignements personnels sur les porteurs.

V.4.6 Processus de journalisation

Le processus de journalisation est effectué en tâche de fond et permet un enregistrement en temps réel des opérations effectuées. Il est incontournable au sens de l'exploitation. Il n'est pas modifiable.

La journalisation des opérations d'origine manuelle porte mention des deux dates (exécution et saisie) qui sont proches (quelques heures).

V.4.7 Protection d'un journal d'événements

L'écriture dans les journaux d'événements est automatique, elle est une conséquence des contrôles des droits d'accès. Les enregistrements ne sont pas modifiables a posteriori et le système de signature séquentiel assure ce contrôle.

Les journaux d'événements sont protégés en intégrité et horodatés selon des modalités précisées dans la DPC.

V.4.8 Copies de sauvegarde des journaux d'événement

Des sauvegardes mensuelles sur supports non réinscriptibles sont effectuées. Des précisions sont fournies dans la DPC sur les modalités de sauvegarde.

V.4.9 Procédure de collecte des journaux (interne ou externe)

La collecte des journaux commence au démarrage des systèmes concernés par les événements à enregistrer et se termine aux arrêts de ces systèmes.

V.4.10 Anomalies et audit.

Les responsables des traitements de journalisation prennent toutes les mesures nécessaires, au regard de l'état de l'art, pour détecter toute tentative de violation de l'intégrité du système de gestion des certificats, y compris les équipements physiques, l'environnement d'exploitation et le personnel. Pour assurer ce contrôle les journaux d'événements journaliers sont contrôlés afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux de l'AC sont examinés périodiquement par un responsable qui en fait la revue à partir d'un résumé d'exploitation joint dans lequel les éléments importants sont analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées. L'AC est susceptible d'approfondir ou de faire approfondir toute période présentant des anomalies potentielles.

Des rapprochements ponctuels sont effectués de façon au plus hebdomadaire entre les journaux de l'AE et ceux de l'AC pour vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

Les anomalies détectées à l'occasion de ces contrôles réguliers ou ponctuels donnent lieu à la mise en œuvre des actions de recherche pour identifier les conséquences éventuelles des anomalies :

- Validité des certificats concernés par l'événement.
- Sécurité globale de l'ICP.
- Sécurité partielle de l'ICP (analyse des composantes).
- Non-respect de la PC.

V.5 Archivage des données

Les opérations d'archivage sont réalisées suivant *Les Recommandations pour l'archivage sécurisé*, en date du 12 juillet 2000, par le groupe de travail commun du Conseil Supérieur de l'Ordre des Experts-Comptables et de l'association IALTA France et (http://www.edificas.org).

V.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont prises par l'AC. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'ICP.

Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- la PC ;
- la DPC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- les journaux d'événements des différentes entités de l'ICP.

V.5.2 Période de conservation des archives

V.5.2.1 Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi française.

La durée de conservation des dossiers d'enregistrement pendant 10 ans est portée à la connaissance du porteur. Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat est tenu à disposition des autorités habilitées par l'AC. Ce dossier, complété par les mentions consignées par l'AE, permet de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

V.5.2.2 Certificats et LCR émis par l'AC

Les certificats de clés de porteurs et d'AC, ainsi que les LCR produites, sont archivés pendant au moins dix ans après leur expiration.

V.5.2.3 Journaux d'événements et autres

La durée d'archivage des journaux d'événements et autres est de dix ans

V.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

La DPC expose les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes, qui est équivalent au niveau de protection des archives, est précisé dans la DPC.

V.5.5 Exigences d'horodatage des données

Le chapitre VI.8 précise les exigences en matière de datation ou d'horodatage.

V.5.6 Système de collecte des archives

La DPC décrit le système de collecte des archives, interne ou externe, qui doit respecter les exigences de protection des archives concernées.

V.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à 72 heures, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'ICP qui ne peut récupérer et consulter que les archives de la composante considérée).

V.6 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC est supérieure à celle des certificats qu'elle signe. Au regard de la date de fin de validité de ce certificat, son renouvellement est demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle biclé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats. Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

V.7 Reprise suite à compromission et sinistre

Les procédures de remontée et de traitement des incidents et des compromissions ainsi que de reprise seront précisées dans la DPC.

En cas de compromission ou de sinistre, l'AC s'engage à informer :

- tous les porteurs
- les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords
- toute autre entité précisée dans la DPC

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC s'engage à :

- informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats.
- révoquer tout certificat concerné.

V.8 Fin de vie de l'ICP

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où elle serait en faillite ou, pour d'autres raisons, serait incapable de couvrir ces coûts par elle-même, autant que possible et en fonction des contraintes de la législation applicable en matière de faillite.

V.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC :

1) Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).
2) Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente politique.

En particulier :

1) Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire et, au moins, 1 (un) mois auparavant.
2) L'AC communique au point de contact identifié sur le site :

   http://www.modernisation.gouv.fr

   les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité.
   Elle y présente notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue.
   L'AC communiquera au SGMAP et à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus.
   L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.
3) L'AC tient informées le SGMAP et l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

V.8.2 Cessation d'activité affectant l'AC

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la

publication des LCR conformément aux engagements pris dans la présente politique. L'AC stipule dans ses pratiques les dispositions prises en cas de cessation de service. Celles-ci incluent :

- la notification des entités affectées
- le transfert de ses obligations à d'autres parties
- la gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés

Lors de l'arrêt du service, l'A.C. :

a. s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats
b. prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante
c. révoque son certificat
d. révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité
e. informe (par exemple par récépissé) tous les porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3)

VI MESURES DE SECURITE TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'ICP, notamment par des dispositions spécifiques de la DPC.

VI.1 Génération et installation de biclés

VI.1.1 Génération des biclés

VI.1.1.1 Clés de l'AC

Ces questions sont traitées dans d'autres documents de spécifications de l'ICP.

VI.1.1.2 Clés porteurs générées par l'AC

La génération des clés des porteurs est effectuée dans un environnement sécurisé (cf. chapitre V). Les biclés des porteurs sont générées dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif de création de signature et d'authentification destiné au porteur sans que l'AC n'en garde aucune copie.

VI.1.1.3 Clés porteurs générées par le porteur

Sans objet

VI.1.2 Transmission de la clé privée à son propriétaire

La clé privée générée par l'AC est transmise au porteur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission se fait directement dans le dispositif de création de signature et d'authentification destiné au porteur.

Une fois remise, la clé privée est maintenue sous le seul contrôle du porteur.

L'AC ne conserve ni ne duplique cette clé privée.

VI.1.3 Transmission de la clé publique à l'AC

Sans objet

VI.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

Le certificat de l'AC CSOEC et des AC CROEC/CDOEC sont téléchargeables sur le site Internet du CSOEC (http://www.experts-comptables.fr/)

VI.1.5 Tailles des clés

La taille des biclés des AC 2048 bits.

La taille des biclés des porteurs est de 2048 bits.

VI.1.6 Vérification de la génération des paramètres des biclés et de leur qualité

L'équipement de génération de biclés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la biclé. Les paramètres et les algorithmes de signature sont documentés au chapitre VII.

VI.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR ou de réponses OCSP (voir chapitre I.4.1.).

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature et d'authentification.

VI.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

VI.2.1 Standards et mesures de sécurité pour les modules cryptographiques

VI.2.1.1 Modules cryptographiques de l'AC

Ces questions sont traitées dans d'autres documents de spécifications de l'ICP.

VI.2.1.2 Dispositifs d'authentification et de création de signature des porteurs

Les dispositifs d'authentification et de création de signature des porteurs, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences du chapitre XII.

L'AC s'assure que :

- la préparation des dispositifs est contrôlée de façon sécurisée par le prestataire de service ;
- les dispositifs sont stockés et distribués de façon sécurisée ;
- les désactivations et réactivations des dispositifs sont contrôlées de façon sécurisée.

VI.2.2 Contrôle de la clé privée de l'AC par plusieurs personnes

Ces questions sont traitées dans d'autres documents de spécifications de l'ICP.

VI.2.3 Séquestre de la clé privée

L'A.C. ne séquestre en aucun cas les clés privées des porteurs.

VI.2.4 Copie de secours de la clé privée

L'A.C. ne conserve aucune copie de secours des clés privées des porteurs.

VI.2.5 Archivage de la clé privée

Les clés privées des porteurs ne doivent en aucun cas être archivées ni par l'AC ni par aucune des composantes de l'ICP.

VI.2.6 Transfert de la clé privée vers / depuis le module cryptographique

Le transfert de la clé privée du porteur vers le support cryptographique se fait conformément aux exigences du chapitre VI.1.1.2 ci-dessus.

Pour les clés privées d'AC, tout transfert se fait sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.7 Stockage de la clé privée dans un module cryptographique

Voir ci-après.

VI.2.8 Méthode d'activation de la clé privée

VI.2.8.1 Clés privées d'AC

Ces questions sont traitées dans d'autres documents de spécifications de l'ICP.

VI.2.8.2 Clés privées des porteurs

L'activation de la clé privée du porteur est contrôlée via des données d'activation (cf. chapitre VI.4) et permet de répondre aux exigences définies dans le chapitre XII.

VI.2.9 Méthode de désactivation de la clé privée

VI.2.9.1 Clés privées d'AC

Ces questions sont traitées dans d'autres documents de spécifications de l'ICP.

VI.2.9.2 Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur doivent permettre de répondre aux exigences définies dans le chapitre XII.

VI.2.10 Méthode de destruction des clés privées

VI.2.10.1 Clés privées d'AC

Ces questions sont traitées dans d'autres documents de spécifications de l'ICP.

VI.2.10.2 Clés privées des porteurs

Les clés privées des porteurs étant générées par l'AC dans un module cryptographique hors du dispositif d'authentification et de création de signature, la méthode de destruction de ces clés privées après leur exportation hors du module cryptographique permet de répondre aux exigences définies dans le chapitre XII.

En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée permet de répondre aux exigences définies dans le chapitre XII.

VI.2.10.3 Niveau de qualification du module cryptographique et des dispositifs d'authentification et de création de signature

Ces exigences sont précisées aux chapitres XI et XII.

VI.2.11 Autres aspects de la gestion des biclés

VI.2.11.1 Archivage des clés publiques

Les clés publiques des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

VI.2.11.2 Durées de vie des biclés et des certificats

Les biclés et les certificats des porteurs couverts par la présente PC ont une durée de vie d'au maximum trois ans.

La fin de validité d'un certificat d'AC est postérieure à la fin de vie des certificats porteurs qu'elle émet.

VI.3 Données d'activation

VI.3.1 Génération et installation des données d'activation

VI.3.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

Ces questions sont traitées dans d'autres documents de spécifications de l'ICP.

VI.3.1.2 Génération et installation des données d'activation correspondant à la clé privée du porteur

Comme l'AC génère la clé privée du porteur, elle a l'obligation de transmettre au porteur les données d'activation correspondantes par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données. Notamment, la remise de la donnée d'activation est séparée dans le temps ou dans l'espace de la remise de la clé privée.

VI.3.2 Protection des données d'activation

VI.3.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

Ces questions sont traitées dans d'autres documents de spécifications de l'ICP.

VI.3.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Comme les données d'activation des dispositifs d'authentification et de création de signature des porteurs sont générées par l'AC, elles sont protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs.

VI.3.3 Procédure de déblocage du support

Dans le cas où le porteur a bloqué son support suite à la saisie erronée de plusieurs codes PIN, il a la possibilité de demander à l'A.E. nationale le code de déblocage de celui-ci.

L'AE nationale contacte directement le porteur et s'assure avec celui-ci :

- Que le support a bien été remis au porteur
- Que le porteur est en possession de son support et est bien à l'origine de la demande
- Que le porteur déclare n'avoir pas modifié son code PUK
- Que l'adresse d'expédition contenue dans le référentiel de l'Ordre est correcte

L'AE adresse ensuite une demande d'émission de code PUK à l'A.C.

VI.4 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques prises par l'AC sont décrites dans la DPC.

VI.5 Mesures de sécurité liées au développement des systèmes

Les mesures de sécurité liées au développement des systèmes prises par l'AC sont décrites dans la DPC.

VI.6 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'ICP.

L'AC s'assure que les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

De plus, les échanges entre composantes au sein de l'ICP peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

VI.7 Horodatage / Système de datation

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'ICP d'événements liés aux activités de l'ICP (cf. chapitre V.4). Les modalités d'application sont définies dans la DPC.

VII PROFILS DES CERTIFICATS, OCSP ET DES LCR

VII.1 Certificats de porteurs

Les certificats des porteurs sont émis suivant le profil ci-dessous. Dans ce profil, certains éléments dépendent de l'A.C. émettrice (région) et du porteur (voir sections suivantes).

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	AC Région, Département ou CSOEC
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (3 ans après la date d'émission du certificat)
Subject	C=FR O=Cabinet ou entité OU=0002 SIREN Title= « Autorisé à exercer la profession d'expert-comptable » ou « Expert-Comptable » (voir III.1.2.2) Serialnumber=Code unique de l'expert-comptable CN=Prénom NOM
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1
Key size	2048
Signature (algorithm & OID)	SHA256WithRsaEncryption
Authority Key Identifier	Identification de la clé publique de l'A.C. émettrice (voir ci-dessous)
keyIdentifier	issuerName+serialNumber
Subject Key Identifier	Identification de la clé publique du porteur
Key Usage (critical)	contentCommitment, digitalSignature
Certificate Policies (critical)	
policyIdentifier	1.2.250.1.165.1.2.*x*.7.6 (le *x* dépend de l'A.C., voir ci-dessous)
policyQualifier-cps	http://seec.experts-comptables.fr/PC/PC_Experts-Comptables_AS.pdf
policyQualifier-unotice	Ce certificat de membre de l'Ordre des Experts-Comptables selon la poilitique ci-dessus
Subject Alternative Name	
rfc822Name	Adresse courriel du porteur
Basic Constraint (critical)	CA:False
Extended Key Usage	CDS PKI =1.2.840.113583.1.1.5 1.2.840.113583.1.1.9.2
CRL Distribution Points	
distributionPoint	http://seec.experts-comptables.fr/CRL/CRL_Région.crl
distributionPoint	http://www.signexpert.fr/CRL/CRL_Région.crl
distributionPoint	ldap://ldapseec.experts-comptables.fr/DN_de_l'AC?certificaterevocationlist;binary?base?objectclass=pkiCA

Champ	Description
Authority Information Access	
ocsp	`http://ocsp.experts-comptables.fr/OEC`
caIssuer	`http://seec.experts-comptables.fr/cert/cert_`Région`.p7b`

VII.1.1 Régions, OID et DN des A.C.

Ces informations apparaissent dans les champs *policyIdentifier*, *CRL Distribution Points* et *Authority Information Access* des certificats porteurs. Pour les CRLDP, on peut aussi se référer au tableau du IV.10.1.

AC	Région	OID (policyIdentifier)
C=FR O=CROEC d'Alsace OU=0002 778867796 CN= Ordre des Experts-Comptables – région Alsace	ALSACE	1.2.250.1.165.1.2.1.7.6
C=FR O=CROEC d'Aquitaine OU=0002 781846464 CN=Ordre des Experts-Comptables – région Aquitaine	AQUIT	1.2.250.1.165.1.2.2.7.6
C=FR O=CROEC d'Auvergne OU=0002 779186311 CN=Ordre des Experts-Comptables – région Auvergne	AUVERGN	1.2.250.1.165.1.2.3.7.6
C=FR O=CROEC de Bourgogne Franche-Comté OU=0002 778212951 CN= Ordre des Experts-Comptables – région Bourgogne Franche-Comté	B-FC	1.2.250.1.165.1.2.4.7.6
C=FR O=CROEC de Bretagne OU=0002 777733700 CN=Ordre des Experts-Comptables – région Bretagne	BRETAGNE	1.2.250.1.165.1.2.5.7.6
C=FR O=CROEC de Champagne OU=0002 775611718 CN=Ordre des Experts-Comptables – région Champagne	CHAMPAG	1.2.250.1.165.1.2.6.7.6
C=FR O=CROEC de Corse OU=0002 752406082 CN=Ordre des Experts-Comptables - région Corse	CORSE	1.2.250.1.165.1.2.24.7.6
C=FR O=CROEC de Guadeloupe OU=0002 348367988 CN=Ordre des Experts-Comptables – région Guadeloupe	GPE	1.2.250.1.165.1.2.7.7.6
C=FR O=CDOEC de Guyane OU=0002 508714565 CN=Ordre des Experts-Comptables – comité Guyane	GUYANE	1.2.250.1.165.1.2.8.7.6

AC	Région	OID (policyIdentifier)
C=FR O=CROEC de La Réunion OU=0002 322951443 CN=Ordre des Experts-Comptables – région La Réunion	REUNION	1.2.250.1.165.1.2.9.7.6
C=FR O=CROEC de Lille Nord Pas-de-Calais OU=0002 380182212 CN=Ordre des Experts-Comptables – région Lille Nord Pas-de-Calais	LN-PCAL	1.2.250.1.165.1.2.10.7.6
C=FR O=CROEC de Limoges OU=0002 380183319 CN= Ordre des Experts-Comptables – région Limoges	LIMOGES	1.2.250.1.165.1.2.11.7.6
C=FR O=CROEC de Lorraine OU=0002 380188185 CN=Ordre des Experts-Comptables – région Lorraine	LORRAIN	1.2.250.1.165.1.2.12.7.6
C=FR O=CROEC de Marseille PACAC OU=0002 782825046 CN=Ordre des Experts-Comptables – région Marseille PACAC	MARSEIL	1.2.250.1.165.1.2.13.7.6
C=FR O=CROEC de Marseille PACA OU=0002 782825046 CN=Ordre des Experts-Comptables – région Marseille PACA	PACA	1.2.250.1.165.1.2.25.7.6
C=FR O=CROEC de Martinique OU=0002 382052538 CN=Ordre des Experts-Comptables – région Martinique	MARTINI	1.2.250.1.165.1.2.14.7.6
C=FR O=CROEC de Montpellier OU=0002 776038077 CN=Ordre des Experts-Comptables – région Montpellier	MONTPEL	1.2.250.1.165.1.2.15.7.6
C=FR O=CROEC d'Orléans OU=0002 775501364 CN=Ordre des Experts-Comptables – région Orléans	ORLEANS	1.2.250.1.165.1.2.16.7.6
C=FR O=CROEC de Paris Ile-de-France OU=0002 784854408 CN=Ordre des Experts-Comptables – région Paris Ile-de-France	PAR-IDF	1.2.250.1.165.1.2.17.7.6
C=FR O=CROEC de Pays de Loire OU=0002 332603604 CN=Ordre des Experts-Comptables – région Pays de Loire	P-LOIRE	1.2.250.1.165.1.2.18.7.6

AC	Région	OID (policyIdentifier)
C=FR O=CROEC de Picardie-Ardennes OU=0002 780601803 CN=Ordre des Experts-Comptables – région Picardie-Ardennes	PIC-ARD	1.2.250.1.165.1.2.19.7.6
C=FR O=CROEC de Poitou-Charentes-Vendée OU=0002 311146385 CN=Ordre des Experts-Comptables – région Poitou-Charentes-Vendée	POITOU	1.2.250.1.165.1.2.20.7.6
C=FR O=CROEC de Rhône-Alpes OU=0002 779893890 CN=Ordre des Experts-Comptables – région Rhône-Alpes	RHO-ALP	1.2.250.1.165.1.2.21.7.6
C=FR O=CROEC de Rouen Normandie OU=0002 781121850 CN=Ordre des Experts-Comptables – région Rouen Normandie	R-NORMA	1.2.250.1.165.1.2.22.7.6
C=FR O=CROEC de Toulouse Midi-Pyrénées OU=0002 776949596 CN=Ordre des Experts-Comptables – région Toulouse Midi-Pyrénées	MIDI-PY	1.2.250.1.165.1.2.23.7.6

VII.2 Liste de Certificats Révoqués

Chacune des A.C. maintient et publie sa propre L.C.R., conformément au profil ci-dessous.

Champ	Valeur
Version	V2
Issuer DN	DN de l'A.C. émettrice, cf. Liste des A.C.
ThisUpdate	AAAA/MM/JJ HH:MM:SS Z (date d'émission de la CRL)
NextUpdate	AAAA/MM/JJ HH:MM:SS Z (3 jours après date d'émission)
Signature (algorithm & OID)	SHA256WithRsaEncryption
CRL Extension	
CRLNumber	Numéro de la CRL
AKI	Identification de la clé publique de l'A.C. émettrice (voir ci-dessous)
CRL Entry Extension	
Revocation Reason	Défini lors de la révocation (champ optionnel)
Distribution point	
HTTP	Cf. Liste des A.C. (IV.10.1, p. 33)
LDAP	Cf. Liste des A.C. (IV.10.1, p. 33)

VII.3 Certificat des réponses OCSP

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	C=FR O=Conseil Supérieur de l'Ordre des Experts-Comptables OU=0002 775670003 CN=Ordre des Experts-Comptables - OCSP
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (12 mois après la date d'émission du certificat)
Subject	C=FR O=CSOEC OU=0002 775670003 OU=par Keynectis CN=OCSP-AAAA-n (année d'émission du certificat et numéro d'ordre du certificat)
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1
Key size	2048
Signature (algorithm & OID)	SHA256WithRsaEncryption
Authority Key Identifier	CC:05:0D:2F:CF:AA:B5:CC:DA:B6:71:36:87:FA:77:F2:EC:AC:41:2C
Subject Key Identifier	Identification de la clé publique de la plate-forme
Key Usage (critical)	digitalSignature
Certificate Policies (critical)	
policyIdentifier	1.2.250.1.165.1.9.1.1
policyQualifier-cps	http://seec.experts-comptables.fr/PC/PC_OCSP.pdf
policyQualifier-unotice	Ce certificat technique de l'Ordre des Experts-Comptables selon la politique ci-dessus
Subject Alternative Name	
Basic Constraint (critical)	CA:False
Extended Key Usage	OCSPSigning
OCSP No Check	null

VII.4 Certificats des A.C. émettrices

Les certificats d'A.C. émettrices sont conformes au profil ci-dessous. Les valeurs susceptibles de varier (numéro de série, DN, etc.) sont fournies ci-après, pour chacune des A.C.

Champ	Valeur
Version	3 (0x2)
Serial Number	(numéro de série du certificat, voir ci-dessous)
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR, O=Ordre des Experts-Comptables, OU=0002 775670003, CN=Ordre des Experts-Comptables
Validity	
Not Before	May 10 00:00:00 2011 GMT

Champ	Valeur
Not After	Dec 31 01:00:00 2019 GMT
Subject	(voir ci-dessous)
Subject Public Key Info	
Public Key Algorithm	rsaEncryption
Public-Key	(2048 bit)
Modulus	(module de la clé publique, voir ci-dessous)
Exponent	65537 (0x10001)
X509v3 extensions	
X509v3 Key Usage (critical)	Certificate Sign, CRL Sign
X509v3 Certificate Policies	
Policy	X509v3 Any Policy
CPS	http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf
X509v3 Basic Constraints (critical)	CA:TRUE, pathlen:0
X509v3 CRL Distribution Points	
Full Name	URI:http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl
X509v3 Subject Key Identifier	(identifiant de la clé publique, voir ci-dessous)
X509v3 Authority Key Identifier	keyid:81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56
Signature Algorithm	sha256WithRSAEncryption

VII.4.1 CROEC d'Alsace

Champ	Valeur
Serial Number	11:20:9f:da:09:32:1d:d7:f9:a2:77:39:06:53:42:22:00:f4
Subject	C=FR, O=CROEC d'Alsace, OU=0002 778867796, CN=Ordre des Experts-Comptables - région Alsace
Modulus	00:be:df:0b:f4:3b:ac:a7:ae:34:cc:74:07:e9:ae: 26:65:42:21:ba:9b:ba:04:8f:2b:ed:c1:dc:d2:6d: 07:17:ea:02:29:9f:7e:c5:a6:2e:0d:ff:21:d9:16: f7:d0:c1:df:56:cb:83:97:5e:9f:6f:fd:02:b4:5a: 7d:48:5b:5b:15:7b:5f:a2:69:ac:8f:d6:e6:74:56: ce:6b:17:20:9f:e2:f6:57:0d:72:d3:63:89:c1:38: e1:1f:7e:bc:57:90:f0:f6:ea:b2:aa:13:5e:e3:c4: 5c:96:7e:4c:ed:43:14:ad:42:38:3a:36:bf:8a:7f: df:65:bb:b1:07:3f:e1:c5:a0:28:2e:34:e8:09:2f: 59:8c:6a:2c:2d:90:42:d9:35:fe:85:56:c9:72:6e: 74:f7:94:59:be:32:40:60:b5:ab:e8:b0:a7:99:6b: 03:1f:25:59:97:60:e5:d5:4d:cf:52:af:e3:58:61: 5c:8d:6a:e2:64:0b:83:6b:01:a7:5d:c6:8f:1b:d2: d8:10:86:64:1a:64:fc:10:4f:41:12:67:01:cb:38: 7a:e8:a4:19:85:25:29:4a:56:ec:04:b0:76:36:96: c8:d9:4b:bc:40:c6:c4:f7:95:6c:c4:15:0e:41:73: 41:ce:ff:77:6d:eb:bf:2e:79:49:08:0e:9a:32:ea: f0:b5
X509v3 Subject Key Identifier	1A:72:1C:48:D6:EE:41:68:E6:3E:DA:46:A1:CA:EB:9B:AA:88:9D:A1

Champ	Valeur
Signature Algorithm	ae:36:09:8c:30:dd:f3:89:fc:7c:57:3c:4e:7b:cb:4f:ed:d2: 0b:c0:76:74:69:c0:68:d1:43:cf:ff:81:40:2f:0c:0a:40:f1: 52:ad:95:21:4c:47:58:c3:5a:02:ab:cd:6b:eb:47:9a:b2:32: 2f:40:6d:36:e7:c2:7b:6b:34:df:87:e0:8c:f0:c6:45:0f:89: fa:b4:34:8e:d0:e5:48:c0:52:a8:71:c2:0f:fd:7d:30:63:82: eb:ee:47:71:0c:d6:2c:46:05:8f:1f:22:0b:17:22:e4:19:83: 80:22:c5:24:73:3f:d9:07:ae:b3:c0:a8:f6:29:a8:33:db:19: 74:c3:4b:0f:ba:11:5b:de:df:75:9d:17:18:a7:41:72:44:c9: 7b:87:fa:96:cc:47:f8:02:b2:b3:1f:ad:e1:c3:4c:d0:9b:ec: 96:8c:20:90:94:69:93:1e:77:55:00:fd:53:ad:c7:43:3f:41: dd:de:35:b4:bf:c9:49:38:da:b9:be:7d:f7:6b:8b:6a:1d:7b: 6a:9f:6f:16:de:a7:6d:7b:78:93:c9:2b:c5:52:b0:31:63:e0: 58:4a:5f:b2:e1:ef:4f:70:73:29:79:3d:00:f1:c5:ab:67:05: 2a:bf:18:32:1e:82:4d:53:f0:67:14:ea:94:f3:cf:dd:a5:ed: 7c:f8:08:1e:f9:45:05:90:86:42:a0:12:8a:89:0e:bd:51:08: 83:f8:85:42:19:21:f1:3c:7b:42:7d:88:ff:6c:f1:f3:5f:6a: 3e:5b:24:54:4a:44:73:86:18:a3:b7:ff:49:ce:1c:9c:e4:16: 1d:22:ce:f2:0c:a6:2e:5f:ae:65:09:8a:96:eb:49:89:a2:2b: 4d:0f:47:4a:f4:66:e2:0a:66:da:5b:c5:7c:6f:44:98:b6:ce: 5d:fa:76:8a:6c:00:a0:9a:98:48:62:3d:4b:4e:82:10:c2:70: 95:21:5e:69:5f:d0:04:57:31:ce:f9:88:a7:8c:c9:2d:84:b0: 85:72:71:1b:07:72:8c:bd:64:b9:27:d9:38:57:56:0b:3c:8a: e4:e6:76:e8:96:60:c3:80:86:68:8b:22:6b:70:68:55:2e:c1: b8:bb:02:7a:b1:10:a2:2f:78:9d:61:de:66:9b:06:38:6e:fe: 37:34:92:b1:af:65:dc:05:f9:2e:91:e3:e0:03:ac:41:b2:5a: a0:0a:cb:a2:a5:25:26:7c:67:f0:08:6c:17:18:09:43:28:7a: bb:41:bc:d3:9c:75:24:53:a7:b7:2c:9e:95:af:4b:3e:4e:54: 57:96:48:4b:10:5c:7b:be:a1:db:01:77:4e:14:22:41:b7:28: d0:77:1e:dd:20:d8:94:a5

VII.4.2 CROEC d'Aquitaine

Champ	Valeur
Serial Number	11:20:15:2d:b3:e2:53:ff:c3:a7:76:fe:e1:be:bb:c0:4b:14
Subject	C=FR, O=CROEC d'Aquitaine, OU=0002 781846464, CN=Ordre des Experts-Comptables - région Aquitaine
Modulus	00:c1:fe:43:28:bd:31:1f:55:54:1d:fe:fc:5e:60: 12:6c:69:0d:e7:7b:19:38:32:0c:c7:5f:05:b5:84: b4:5e:77:7a:ac:10:01:7f:56:81:f3:69:fa:11:33: 3d:7b:46:40:95:51:8d:76:4d:4b:6c:bc:8e:4b:5a: b5:7f:ed:a8:9c:83:35:2a:f9:e1:5c:f1:d9:c3:ff: 24:1d:75:0d:e7:df:8b:0f:86:17:be:1f:6c:c8:a0: c6:48:77:6c:29:83:d6:3f:a5:7f:cc:df:2e:97:e5: f7:6a:1b:a7:60:05:55:4d:b5:1a:2e:71:70:94:5a: 43:48:03:c7:a7:c6:90:d4:bf:48:06:66:01:a8:d2: 42:d1:8d:67:62:2e:33:90:59:ad:58:4a:7a:77:00: ad:58:cb:2f:a3:b2:84:5d:d4:7c:d9:48:8c:49:f9: 00:de:e1:55:34:e8:c2:18:2c:f9:d5:1d:c7:7a:52: 4f:9f:85:aa:90:25:65:d9:fc:ab:e3:00:f5:07:b3: 16:38:33:ba:85:2a:4c:6b:37:94:09:76:08:21:06: 55:62:92:76:e2:4f:13:93:bb:1d:c7:bd:62:2a:40: 64:bc:7c:1a:5b:40:ed:fd:2b:7c:b2:b9:7a:45:25: fe:58:1a:52:42:c1:da:68:30:7d:c6:f8:5d:0f:4f: 93:79

Champ	Valeur
X509v3 Subject Key Identifier	2C:31:DD:9E:E2:A5:03:A8:D3:6A:67:7E:AA:24:EA:53:E5:CF:F7:8E
Signature Algorithm	84:d0:dd:9b:62:db:73:8f:1f:35:ba:49:1a:fa:1d:4f:72:33:9f:bb:51:f8:e4:11:68:b5:14:6b:94:a2:f3:f3:d6:ea:20:25:3e:ff:0e:e7:f4:ac:40:b9:f6:cf:3f:be:8e:39:d7:df:51:f4:9e:9c:22:73:93:2d:4a:fc:38:f0:1e:b7:06:b1:d4:a7:81:73:2e:59:32:47:17:99:0b:16:78:a8:b1:79:76:ca:ca:10:64:7f:ce:10:5e:4e:d3:6d:11:c6:a0:c9:82:eb:f4:10:b7:a7:7a:3a:8a:25:71:d6:ad:a7:a7:0a:55:ec:a9:eb:87:1c:fa:e1:4f:4c:4b:b4:a9:5a:3d:2b:c0:06:c0:e4:43:43:f2:2f:28:98:55:9b:7b:00:0f:21:b6:0c:f1:e6:f2:e5:1d:59:da:28:96:20:9a:7c:8a:eb:1b:16:f1:6d:fe:48:b4:c0:8a:7f:34:b3:d6:45:f2:75:31:ec:6e:d0:eb:87:00:f1:0a:0b:95:94:2c:34:b5:94:97:65:91:2a:17:0b:c6:28:66:37:a8:52:c8:33:07:6b:37:b9:b8:f7:07:2d:4b:fd:c6:19:66:6b:d4:ec:5e:c6:5a:ef:d0:0a:43:cf:66:8e:b5:e5:f0:bb:3f:af:04:b3:bd:64:ad:c1:16:35:55:e0:41:67:53:b6:65:a1:26:ba:8d:10:8b:2e:f8:40:96:4c:3b:97:77:fe:21:0f:d7:9c:11:ae:24:f9:d9:3b:e3:35:48:4f:51:5d:91:af:e8:45:ec:44:97:1b:5b:81:00:9b:60:a6:d5:43:5c:5d:6f:61:b3:9d:ad:0f:f4:a4:c1:49:f6:0a:32:f5:bf:cf:d2:0d:d5:93:dc:43:27:d0:5a:fb:1f:cb:6d:f4:df:10:c1:70:15:08:e9:3b:64:87:a1:06:19:aa:7f:2f:c0:34:7a:a8:22:cb:0a:df:c3:d5:2e:89:ad:a9:4c:54:54:31:d4:3f:02:9d:1e:fc:6a:73:6a:50:71:f8:f3:73:9c:85:95:58:30:b2:60:97:06:6b:d0:ff:7d:c3:f5:cb:60:af:49:b7:1c:01:74:c7:28:34:f6:51:9d:a9:ef:03:ec:d2:48:77:91:f3:c3:b6:66:77:ae:60:b2:d0:36:94:2d:1f:c3:46:9a:38:59:ce:67:31:85:38:60:61:5b:20:e9:f7:dd:6f:38:f7:54:11:ff:77:4d:ee:9d:df:8a:82:25:e5:95:3b:28:41:c2:a9:d3:5d:71:32:63:72:fa:07:b0:79:33:00:e8:92:fe:74:5d:08:e7:b8:b3:d7:06:87:b1:99:21:89:58:93:bf:c9:ab:51:53:15:28:e3:a7:6d

VII.4.3 CROEC d'Auvergne

Champ	Valeur
Serial Number	11:20:41:e3:8a:59:d2:06:fa:1a:ab:80:89:f7:fe:c9:b6:da
Subject	C=FR, O=CROEC d'Auvergne, OU=0002 779186311, CN=Ordre des Experts-Comptables - région Auvergne

Champ	Valeur
Modulus	00:b9:ab:2c:7b:3c:af:a3:35:c2:0f:16:18:8a:2f: 66:38:3d:4b:37:6a:cf:8f:92:7c:5f:ac:a8:0c:9e: a1:95:e0:f0:f9:15:e3:e7:a0:d9:33:bc:a1:81:ca: 4c:b4:d1:d3:a8:1b:c9:69:06:3f:93:c8:f8:10:14: 78:10:41:48:a6:31:75:af:4c:be:90:ce:c7:92:a6: 28:b8:47:ef:48:70:22:dd:77:1e:37:5c:f1:39:4e: 5c:66:42:50:0a:8b:e5:74:68:fd:c5:58:97:9d:f1: e8:9c:e9:5a:92:8f:95:d7:8e:db:f1:7f:d2:5d:ca: bc:55:6a:d6:83:dd:b6:23:a4:de:3e:ad:ae:7c:65: e3:42:c1:f9:4e:dd:64:5c:96:e6:08:32:a6:e3:cc: 81:cc:6b:d5:b0:29:9c:45:c3:a1:00:ff:49:61:e0: 4d:f0:07:6e:fc:5d:7f:4b:9b:e2:a2:e4:56:42:73: 47:73:f3:d1:f7:a0:0b:b5:7b:98:49:77:8b:79:e9: 77:3c:87:57:89:08:3b:ff:3c:fe:13:ee:f9:18:88: e2:32:f0:58:09:72:9c:82:44:59:0b:50:e2:43:ec: 6e:01:a4:67:c6:a0:b0:63:4f:c4:00:f9:12:78:78: 73:8a:0a:d6:48:92:04:b9:b2:0e:84:0f:06:26:02: ce:47
X509v3 Subject Key Identifier	3E:70:9F:F6:56:E2:2A:EC:66:EC:28:3E:B6:04:B0:D3:AA:6B: 7F:A4
Signature Algorithm	17:ba:10:88:31:2d:a5:af:e0:a4:0c:08:70:eb:a4:2c:9c:fc: 29:5a:97:01:6b:fa:a4:d9:54:74:2b:16:67:4a:ac:22:97:ee: 55:48:f0:7b:4b:29:5e:8a:05:e0:94:a2:ac:b0:c1:22:77:c2: 90:a2:4f:69:bb:83:4e:b8:cc:18:9f:44:fa:d3:7c:b3:8d:3b: a0:e2:13:80:ef:a4:18:3f:6b:d3:ae:a0:87:6a:38:30:93:0b: e5:4e:6e:bf:2f:2d:e8:a8:55:c1:9c:20:9b:af:5b:a8:39:5f: 9b:75:3c:07:cc:89:49:6d:24:13:83:a7:ac:b4:a4:15:e9:e2: e9:be:69:cd:76:1b:1a:60:c0:88:22:f3:45:f2:3d:b2:fa:5d: d3:3a:9d:21:83:51:5b:6a:bc:33:97:7b:cd:65:5d:e0:f5:b2: 74:d0:c5:71:6a:77:a9:a1:0b:a7:6a:8b:ff:01:fa:f3:35:3d: 3c:63:1c:05:83:1c:0a:88:15:2e:a9:56:be:05:6e:a7:ee:d5: 55:4a:20:13:18:a3:d6:11:2d:91:05:ad:b7:3e:7c:3c:4c:f5: 0a:02:03:d2:ff:58:aa:7f:49:08:a8:f0:03:d0:5d:8f:52:ab: 85:79:9f:73:4d:58:b5:af:a4:2f:32:09:95:72:8a:9d:72:eb: 9d:46:36:03:5f:3b:1c:5c:73:85:7e:41:f2:3d:aa:e1:4d:3b: 64:03:2a:b8:9c:e1:a1:60:7b:98:cc:97:18:ce:2b:41:03:7b: 4e:a3:70:d6:92:30:29:58:3a:6f:00:07:7d:0c:0c:4b:be:c5: 6f:cc:55:82:25:43:1d:32:38:5d:52:36:0a:5b:52:a6:df:11: 1b:31:a1:97:15:64:6c:e9:54:db:a6:a3:20:2f:d7:3d:5e:1f: 5f:83:58:08:fb:25:20:06:cd:85:1b:5a:21:46:67:83:7b:d3: 44:0b:83:d1:c5:5b:7a:38:8b:17:e1:f1:a2:84:1f:5b:5e:b0: ec:45:79:03:37:27:44:86:53:33:7b:8f:e7:f4:4c:a2:1a:59: 0c:b4:83:a6:30:1b:ea:d8:61:0d:6e:85:2c:99:7a:48:15:57: 68:f5:cd:7b:06:9d:1b:0b:bc:c1:50:6e:5d:35:aa:59:77:c1: ca:ed:5b:17:5c:a8:a7:56:34:62:19:36:77:a3:fc:6a:63:da: 8c:02:c6:6c:57:ce:93:59:ad:02:d7:be:37:c2:69:4f:ec:7f: 21:81:9c:5d:3f:dd:2a:93:ec:27:13:78:a6:e4:03:8b:ee:a1: b5:48:b7:f2:f3:2a:a9:0c:e8:e8:48:5d:42:4c:a2:e0:7d:24: 5b:f2:4e:41:ae:46:0a:3f

VII.4.4 CROEC de Bourgogne Franche-Comté

Champ	Valeur
Serial Number	11:20:6e:0c:7c:40:5c:b0:50:3b:b3:3a:a3:1b:3f:d5:50:96

Champ	Valeur
Subject	C=FR, O=CROEC de Bourgogne Franche-Comté, OU=0002 778212951, CN=Ordre des Experts-Comptables - région Bourgogne Franche-Comté
Modulus	00:ae:39:76:80:d4:a4:b3:e8:17:62:8f:7d:84:95: 65:f8:d8:99:f0:d8:90:3a:56:a7:d0:6a:8d:e3:c7: 71:27:95:d0:53:ba:71:c3:d7:c9:8e:62:51:8f:6b: 26:cf:46:a9:b1:b1:8e:21:40:58:90:68:4f:46:28: 96:c4:9d:d1:2e:75:9e:ca:7a:a3:40:36:f4:9c:1c: c6:b6:91:b1:eb:e6:e0:4a:ab:7e:db:21:f9:89:43: dc:17:1e:ae:f6:f6:3e:26:bf:17:17:0a:b0:a9:8a: c7:56:48:c3:9b:b8:b1:d7:bb:61:41:c0:16:7a:92: 65:fe:e3:da:c0:92:ed:97:29:21:e2:56:6c:d3:e5: 5a:07:f8:ff:4f:a4:7f:92:d9:01:e1:cc:02:f5:d0: b2:c4:4b:25:f6:2e:09:5b:d3:8e:fa:be:e5:9a:a4: 60:2e:58:cf:ef:aa:fb:07:93:97:cc:dd:eb:d4:38: 13:3c:69:6c:45:43:9a:1e:68:bb:58:48:fe:f5:de: 59:09:2c:4d:b9:85:01:cc:bc:75:98:62:a5:68:fd: 33:1c:6c:6e:f5:2e:54:3d:f8:cd:ef:ad:3b:76:6a: 1e:1b:a3:10:41:d3:b6:f6:1d:af:c8:05:e4:82:b2: 39:1b:8a:7e:48:54:fd:f8:7a:af:22:81:8a:1b:2e: 76:75
X509v3 Subject Key Identifier	3F:81:5A:90:61:51:B5:F7:60:E7:05:B8:99:D6:74:F9:6E:E7: 87:71
Signature Algorithm	53:b6:9b:e2:10:de:82:9b:fe:1d:bd:24:54:27:6c:e0:b3:6c: 54:dc:b9:8a:37:78:c2:18:22:ec:ee:ca:b3:e5:64:7e:54:2f: 8d:18:77:63:61:11:9b:44:42:e5:73:01:9c:12:19:9e:2a:4c: 1f:2a:f7:d0:4b:5e:a3:86:2a:3b:90:fb:07:54:05:c0:ea:13: 11:a7:31:ed:3a:db:97:94:13:55:dc:2b:ba:9a:51:dd:90:c7: 68:b9:6e:08:4d:68:16:79:c5:f7:ef:95:b2:0a:55:10:48:b0: d5:5f:99:10:08:48:80:0f:f0:48:31:c7:8f:b3:ed:d2:d5:be: 8d:7c:2b:dc:12:0e:98:96:1c:f9:ac:0f:d5:ca:9e:76:6d:4b: ab:e2:0a:b6:98:bc:a3:0c:ec:f6:7d:46:a9:b3:7a:08:3e:4a: fb:84:c4:1a:82:b0:db:40:75:52:a3:12:e4:69:0e:f2:4f:62: 7a:fa:30:75:f4:72:b7:c9:67:b0:63:00:7e:9f:7d:57:2b:ce: 31:33:89:f4:98:1b:f4:bf:3d:22:7c:6a:75:19:e9:a4:a4:2e: f3:e8:24:39:13:b3:be:ac:54:0b:f8:2c:0a:ef:4d:69:d5:79: 0b:30:6b:f8:52:de:dd:52:64:c1:03:4e:32:be:8c:17:d6:33: 4f:04:83:d4:86:a2:34:1e:19:63:35:43:2c:d2:04:7c:fc:3c: e6:af:3a:1c:5a:54:15:49:de:f5:af:9c:1a:bc:e8:60:3f:11: ca:e5:98:d7:ca:1e:af:78:32:e5:82:45:e0:3e:e6:6b:81:7c: 1c:ae:72:3e:a3:8b:19:50:6d:c7:2f:6d:53:c7:49:b4:74:b7: 5f:48:92:4a:21:7e:8f:22:60:7b:05:fa:06:a7:6c:c4:1d:cd: e7:95:8b:f2:5a:70:ca:fd:60:7b:a1:17:b5:7a:b4:28:4a:d6: c6:01:72:5b:51:5f:44:ee:10:fd:95:f4:97:9e:70:09:0b:e5: 46:b8:c4:53:bc:46:5c:ea:22:89:81:ef:ee:3e:3a:ff:c5:83: 53:dc:8c:0e:e8:fe:51:33:c3:df:c2:39:55:db:96:25:6f:eb: 7d:66:ad:9b:71:98:3a:22:ac:b9:85:8b:d1:d2:5f:ea:4d:36: 10:9c:d2:e8:38:4e:b7:52:ee:88:4e:6e:2d:6d:a5:56:8c:8d: 0c:53:dc:d8:6b:05:b2:ad:63:00:e4:f0:a0:00:e1:fb:39:84: 3d:0b:19:ba:63:d6:f1:23:53:42:50:f0:85:18:09:fa:33:58: 1b:73:00:0d:2a:d7:cc:77:da:88:75:14:d6:42:a9:21:17:a2: fe:31:f5:20:c0:da:84:18

VII.4.5 CROEC de Bretagne

Champ	Valeur
Serial Number	11:20:2b:ab:bd:62:5d:4d:5c:7c:c7:ef:92:eb:19:48:d2:f3
Subject	C=FR, O=CROEC de Bretagne, OU=0002 777733700, CN=Ordre des Experts-Comptables - région Bretagne
Modulus	00:9c:fc:f7:0a:29:70:9c:ea:51:d4:66:e1:85:aa: 71:22:e1:fc:56:1e:3a:ff:70:5b:34:23:cd:fa:30: 18:0d:13:b9:5f:85:e2:6d:29:76:d6:a6:5f:a1:27: 6e:a0:33:d4:67:c1:a9:cd:51:51:b7:6e:4d:fc:1e: 12:8c:74:3a:f6:e6:28:18:20:a1:0b:0a:72:68:e1: 81:96:4a:91:7f:fe:4c:7f:50:06:73:1e:4a:a3:2d: dc:30:2b:1a:d4:b4:3c:71:52:fc:29:b3:e5:b9:2a: 15:43:b2:3d:31:ae:d6:8c:30:cd:68:7c:d9:d7:28: a4:2c:d9:01:3a:9e:76:91:76:f9:98:a7:7d:4e:8b: 2f:67:12:da:0f:f0:d0:ee:93:ad:3f:48:0a:fe:40: 22:dc:07:d8:09:e6:fe:29:5e:97:25:a4:30:7d:d2: db:8f:99:1f:ae:42:16:6b:16:2c:9c:fa:0d:d0:5e: 79:84:9c:6e:93:44:a2:e9:98:fb:fe:c2:0e:59:ea: eb:ce:45:ca:74:7a:d5:3d:40:75:4c:3b:c9:fb:27: e0:ae:64:83:78:b4:0f:8e:c3:30:fd:d2:77:6c:ce: 0f:3a:4f:93:97:c4:f6:79:45:a0:c5:aa:40:91:7a: 70:79:9c:4d:df:a8:66:69:0d:ee:20:1e:70:b1:26: 1a:f9
X509v3 Subject Key Identifier	4B:79:AC:43:D6:34:89:ED:B8:DC:24:E8:9D:36:01:EC:2C:88:A5:3E
Signature Algorithm	61:87:76:34:92:9f:77:b0:bc:e4:ad:df:a1:1c:0d:68:9e:06: aa:d9:e6:eb:a6:fe:19:33:49:3a:1d:12:c9:c8:42:87:98:9f: 06:f8:4e:2b:6f:14:33:50:90:7e:16:c9:b5:ba:e0:db:9c:7b: 7e:1d:e7:07:a5:9b:5b:c5:72:bf:41:c4:ba:c9:9b:e5:f8:8a: 44:4e:c7:b3:5e:51:f3:75:91:73:b9:7f:8b:2d:a4:67:c3:70: 9f:d5:fa:58:8b:55:4a:db:cd:e3:f9:e2:36:85:86:bf:70:a6: 09:41:26:db:cb:75:91:fa:41:db:df:d6:c2:7e:13:80:4c:8d: c1:8a:b0:8e:0f:55:90:71:e4:38:87:bf:d8:88:ad:86:fc:03: 02:2f:e6:c6:1a:6a:b7:e5:24:e8:5d:87:8d:19:cf:5a:78:8a: 83:71:39:54:6e:16:25:fe:5b:75:44:07:66:69:ed:e9:d1:20: 2b:90:91:2d:04:45:9e:41:02:2a:d7:b7:a3:ae:6d:cb:8d:12: fd:83:87:e3:86:63:a5:ab:19:32:38:78:d5:9f:b7:8f:5c:3e: 17:43:e8:ca:a7:51:ef:6a:bd:87:db:41:15:7f:0a:3c:4b:a3: 42:e6:24:e3:f2:df:c8:79:55:59:f2:65:fb:0c:62:cc:e8:8a: 00:2e:a7:9a:12:e8:d2:a4:18:e7:41:87:b2:f3:38:d8:d7:a0: 4d:aa:5d:7a:c8:38:7e:07:88:9d:59:2f:b6:4d:35:2a:93:a4: 63:60:5c:93:9c:b4:30:c0:de:a0:d9:15:f6:c5:90:c2:f0:8e: 3f:13:14:68:e8:f0:0d:81:7a:c5:5f:7d:92:86:91:bd:b8:55: 9a:51:22:88:9a:2c:a6:59:56:47:e8:f6:b1:e7:cb:76:18:57: 54:80:f4:14:50:8f:90:b3:a1:bd:c7:13:d7:94:f6:29:76:b7: 94:1f:c0:c0:4d:46:9e:4a:e8:ae:01:3c:c4:c6:0e:05:e7:d4: 63:8a:b3:dc:b9:e0:fc:37:b9:f2:d1:1c:15:ae:44:df:25:eb: 7f:39:0f:dd:03:36:35:89:df:b5:ce:30:a0:38:47:dd:a0:82: a0:5c:06:25:1f:18:ac:5f:9d:af:08:39:68:6a:2e:0f:88:c9: 61:8b:ff:16:6e:29:d6:a7:42:9f:e9:d2:c4:9f:64:cf:92:a7: 2e:96:0f:de:3a:cf:b6:2e:7c:d7:ab:f0:a0:99:ac:dd:a4:18: d1:16:8f:9a:e0:9e:e1:66:bf:a5:77:98:24:a4:24:2c:b8:d8: 44:01:1b:13:38:64:c0:c6:eb:a5:cd:e3:38:3e:82:29:ba:04: 55:be:61:47:34:23:0d:dd

VII.4.6 CROEC de Champagne

Champ	Valeur
Serial Number	11:20:03:c9:a5:5d:9e:e5:e8:bd:53:64:d6:bc:f4:bf:89:ac
Subject	C=FR, O=CROEC de Champagne, OU=0002 775611718, CN=Ordre des Experts-Comptables - région Champagne
Modulus	00:dc:68:39:df:1f:43:4e:66:95:ad:e1:bd:06:1c: fd:21:68:29:40:c9:f1:ab:2c:6b:7d:a2:a5:d1:4b: 59:ce:a6:90:f0:c1:7c:81:a7:fb:f5:71:78:ff:dc: f6:d7:47:69:b8:e2:cd:20:a8:aa:3b:d5:92:8a:08: 6e:ce:31:44:37:13:79:80:a8:5a:bd:1f:cd:1c:fe: 61:92:5d:8f:bf:3d:30:b5:65:e8:11:b0:1a:d6:8d: 90:84:20:3b:e0:7f:1e:4d:9d:d5:e0:f8:55:24:4c: 9d:50:5d:00:cb:6c:d8:3a:c2:e7:4f:a4:8c:96:e9: 71:be:13:d0:c1:af:80:02:fc:24:f4:dc:7c:a1:5a: 53:60:14:eb:2c:02:16:dc:6b:7a:d4:65:70:a4:64: 27:03:8f:46:13:f2:99:0c:82:22:9f:20:ad:45:96: 7f:92:d4:9c:c7:01:25:a0:cf:d0:9a:d0:e4:00:d5: c9:48:92:18:9a:1e:4d:6c:9a:57:cd:71:9e:10:ea: 29:e8:38:fe:03:a1:d2:10:59:2c:14:0f:e7:d7:2f: 3d:91:1b:89:5c:bf:f0:54:8a:3f:0d:84:6e:cc:18: 04:1f:9a:bb:fa:99:59:21:5e:ae:88:2c:4d:7b:0b: 91:d3:3d:b6:aa:55:a4:7b:d2:aa:2b:8a:00:59:4a: 82:e7
X509v3 Subject Key Identifier	4B:E2:F0:D5:2E:FE:11:DC:F5:6F:F2:84:47:29:60:74:49:2C: 9F:69
Signature Algorithm	67:6d:2f:b1:db:a8:52:db:9c:30:62:9b:ae:f9:66:16:e4:41: 3b:56:75:40:ff:fe:8a:47:fc:48:61:2f:8e:c2:08:7f:c4:8f: 8f:2f:be:bc:8e:66:24:78:63:09:e2:f1:ca:39:db:66:90:8b: b9:d5:74:49:db:b3:b5:83:b9:fd:49:37:64:ef:76:6c:16:c2: 0b:d5:4d:81:6c:99:f3:a2:25:76:62:c3:30:54:ed:21:2d:e4: 9e:ab:8b:12:58:bf:e7:52:76:28:2e:f6:38:e1:3d:6a:16:c9: 9c:b1:e3:a0:2f:8f:d0:dc:42:0d:6c:d1:de:08:a4:5f:87:01: 21:7a:d8:2e:77:1c:cb:52:f0:b9:89:e5:f1:63:71:4f:44:05: d7:61:01:46:a4:57:24:e7:de:ad:c7:d2:5c:c4:df:9e:47:2f: 30:bf:88:a4:26:47:71:36:f3:53:aa:20:ff:f5:ea:a3:c5:c2: 42:f3:d0:c5:f2:4d:0b:c9:63:ed:74:1c:6c:a6:b4:1b:04:3a: 0d:11:c7:ea:e8:6f:f0:f1:bb:4c:bb:99:16:bc:f4:bb:5e:37: de:92:75:42:68:7e:17:aa:55:63:5f:b8:64:b6:c0:3c:7a:ed: 02:1f:c7:c5:22:31:9b:25:09:89:c7:f5:ab:00:15:64:38:eb: e2:ec:65:16:6a:b8:21:90:c3:40:40:fe:63:3a:9b:0c:b8:37: d9:8e:a2:da:21:7c:e9:83:d3:38:7b:2c:99:58:d1:24:3b:a9: ba:12:6f:65:c8:94:6e:c5:7f:9f:78:ef:e8:2e:d8:4f:53:06: ce:3f:8b:7e:21:ae:09:54:f6:f5:f1:f5:5d:b2:ac:f0:00:72: 8b:76:5c:18:44:88:dd:db:02:e0:58:8e:27:0e:00:c9:74:83: 60:cb:3d:f6:fa:7e:8e:8f:8b:08:2d:c8:60:d1:b8:50:a3:a1: a3:dd:89:df:98:15:eb:58:d6:a2:f3:c1:e9:a4:ea:07:f6:3e: d6:5f:00:a1:1a:e2:bf:f7:10:67:f7:5c:28:9a:e6:fd:5e:73: 0b:c2:01:c5:a0:8d:ee:93:f7:ab:73:26:92:4e:99:5f:9a:48: 72:c6:e5:f8:5b:9f:c1:08:97:dd:61:47:e4:e4:89:2f:9d:2e: ff:93:e5:fc:aa:f3:75:8c:1a:70:00:fb:3f:43:44:87:08:bf: e3:51:b4:5a:e0:84:dd:0b:cb:c7:65:00:cd:0d:50:8b:d4:99: 2a:aa:93:eb:57:ce:82:d0:29:7b:42:6c:5a:0a:4c:2c:5c:c7: ba:de:c1:e2:eb:45:08:d3:76:c6:ef:11:38:d2:7d:84:d0:d2: e8:d9:6f:01:3e:40:39:3b

VII.4.7 CROEC de Corse

Remarque : la période de validité de cette biclé est différente des autres (cf. I.2.1).

Champ	Valeur
Serial Number	11 20 a0 81 93 7e 29 9c ca 8f 43 03 59 ed ae 83 b6 f1
Subject	C=FR, O=CROEC de Corse, OU=0002 752406082, CN=Ordre des Experts-Comptables - région Corse
Validity	
Not Before	Sep 25 00:00:00 2012 GMT
Not After	Dec 31 00:00:00 2019 GMT
Modulus	00:c5:f6:d1:30:49:04:81:45:b7:05:6f:68:64:87: 85:9a:29:e9:32:ec:8f:8b:f5:22:52:89:f4:1d:0b: 88:39:9d:a2:41:86:c1:ab:54:7c:e1:6f:ff:ea:e0: 98:d9:57:8c:ea:b7:08:b3:63:ee:31:ef:4e:ad:fa: 84:c3:62:28:a8:b7:14:63:d2:f8:ff:a4:22:97:dc: 9c:64:c6:36:bb:34:88:d7:55:3b:ee:8a:29:f4:d7: dd:a7:5f:40:0b:70:d0:d8:bc:ad:93:b5:db:96:b4: 20:75:0c:d2:a8:09:52:80:f9:96:fb:c6:ac:7f:b0: 23:e3:0e:23:c2:88:5b:d3:e3:1c:e7:57:1f:e5:60: 6b:92:3a:b5:1a:90:c6:c6:86:23:87:4a:4d:76:f4: 40:62:f5:0a:58:86:9c:c6:9e:dd:3b:00:53:01:e1: 3c:17:0a:43:3f:ec:77:36:e4:bf:d0:4e:f5:1e:c8: 30:56:66:94:df:bf:2a:c2:53:87:9f:de:e4:6e:4f: 0f:20:02:7f:18:dc:f9:75:d7:37:6d:fc:b6:05:c3: 37:95:05:f8:56:17:d4:18:dc:ac:60:22:21:5d:65: 4d:f6:c4:9f:cc:5c:23:06:7b:b6:03:73:11:ef:ef: 88:0d:e1:52:1c:5b:56:a0:5a:c2:bc:1f:99:5c:31: 71:95
X509v3 Subject Key Identifier	bb:b6:00:e6:04:6e:7b:ca:5e:bc:35:ba:b2:df:9f:e2:ca:21:93:f1

Champ	Valeur
Signature Algorithm	1e:7b:83:97:4b:b4:f4:ed:9b:da:20:89:8e:58:5d:0d:ce:23: 74:b9:ca:ee:97:d1:f9:d8:68:fd:7b:bc:43:12:08:6c:bb:4b: 85:e5:6c:65:b0:be:b4:ab:1e:58:14:93:7d:e1:91:86:5c:18: 9c:19:d8:d9:ea:c6:69:4f:bd:3b:30:32:95:94:5f:a9:cc:e5: 6d:28:80:cb:e9:e3:8f:68:43:f2:c3:1d:a2:63:1a:b5:9a:be: d0:60:ef:10:00:ff:a8:4f:1a:e9:23:40:05:13:a6:83:58:ef: ab:21:bc:77:55:e0:8a:67:e7:d7:a3:6c:13:cd:2c:55:3c:14: 3f:d7:85:fc:a3:93:96:8b:22:0b:b3:75:45:00:34:40:38:fa: 4e:e3:25:4d:e9:1e:de:23:0b:cb:ec:85:5b:0b:ce:29:a1:7d: 52:6d:7c:09:0e:33:dc:13:38:77:dc:33:1b:bc:9e:81:75:ae: 81:60:56:f8:80:ce:c6:8b:e2:d1:d8:af:a6:65:28:67:a3:63: 0f:46:f8:94:ba:e1:0b:d6:d4:d8:3a:6a:47:7f:14:a7:b8:cc: b1:73:49:5c:d3:ac:93:23:ed:b6:e4:47:9e:43:bf:94:4d:fd: ee:0d:c2:90:19:c7:c2:77:14:ba:75:98:c4:c8:ae:cf:32:9a: f2:14:c2:10:c5:02:8e:e4:1e:a6:e1:cb:38:c4:8f:c7:e0:ad: 01:ce:c5:f1:63:a7:ee:90:b1:67:1a:c4:fe:b4:e3:27:4c:cf: 30:6b:a3:f3:51:f3:d9:93:47:58:e6:a1:2f:a6:6a:b9:b3:1a: 4c:3c:71:f9:78:0b:63:ab:7f:c7:03:36:bb:bf:16:bf:d4:ea: c1:3b:02:e4:16:83:1e:fd:b7:f1:60:a5:58:44:aa:a1:6f:7a: 77:f6:0d:89:e0:b8:59:04:d1:bf:75:be:d3:bb:ea:64:c3:e7: 03:9f:a9:47:e9:1b:e4:2e:47:4e:cb:8e:5c:34:7e:2d:9c:6b: d3:8a:9d:55:ef:0a:46:20:86:13:b1:68:c3:82:93:88:b1:a4: 20:8f:c3:ae:a1:fb:a5:21:87:3a:8d:12:8e:7d:48:c5:22:8c: 2b:3f:7a:e8:e6:75:9b:64:c3:ab:9d:58:9c:64:56:51:46:95: 8b:66:83:53:c0:a0:d9:e9:d5:3c:47:c8:32:1a:30:6b:47:d2: 4c:8c:b6:e8:33:63:34:27:a3:70:e5:2d:9a:f6:d8:39:fb:c7: 49:cd:8c:b5:ae:64:ed:53:db:ca:0d:d9:6f:4c:0d:6d:fb:e9: dc:4e:40:dc:17:a6:04:d2:19:0e:28:ac:9b:ca:90:5f:9c:62: 94:5f:30:44:85:12:4c:ae

VII.4.8 CROEC de Guadeloupe

Champ	Valeur
Serial Number	11:20:b2:38:79:d2:e8:9e:68:bb:5c:a7:ac:4c:56:09:4c:e1
Subject	C=FR, O=CROEC de Guadeloupe, OU=0002 348367988, CN=Ordre des Experts-Comptables - région Guadeloupe

Champ	Valeur
Modulus	00:c0:05:ab:f6:fd:fb:0d:86:53:a6:df:f5:1c:10: 5a:9a:3e:f9:4b:ee:fa:8b:7d:ca:b2:41:24:10:a2: 83:9f:ce:65:a1:7b:f0:37:09:ec:64:b4:4b:f1:82: 89:5c:74:e0:6d:80:63:e6:29:1a:ef:94:6e:30:24: d1:41:a0:e2:78:10:7e:96:3e:99:1b:64:76:17:d9: 00:e5:25:3c:47:95:ed:f3:ed:22:16:54:f8:6a:d7: c5:df:a5:ee:93:7b:17:69:37:46:fb:3f:44:26:86: 0e:8b:2b:77:39:7a:b0:1b:35:dc:f0:25:59:50:94: 19:b7:33:82:36:28:db:35:1c:3f:9d:0c:c5:cd:2c: 7e:36:a1:76:a8:2f:3b:50:d2:ce:d0:98:32:0d:84: e8:15:e2:e4:36:77:3f:8d:10:0f:60:ce:2f:69:4b: 0e:05:6d:0e:cc:45:eb:8e:15:13:45:fe:b7:cd:86: a2:73:17:6b:90:d3:06:26:8a:2f:2c:5f:28:dd:00: fe:f9:c2:2c:ee:52:5a:c8:31:11:99:9a:c8:d0:82: c8:e6:6d:23:21:13:ff:14:81:2c:49:a8:85:43:33: 28:81:21:5a:f7:e7:71:df:bf:f2:7e:51:e3:87:ef: bc:a8:cf:63:f4:7d:5a:d5:b7:cf:be:9b:4b:55:b6: 37:49
X509v3 Subject Key Identifier	6F:61:A6:3A:45:28:5D:AA:0E:EC:11:72:52:42:3B:EE:79:49: 1D:E9
Signature Algorithm	6a:69:b8:c5:3e:e9:86:fb:5e:8e:07:10:47:85:fa:97:56:3c: de:8e:18:cb:87:11:42:3e:71:23:f9:24:5d:f8:8c:4b:8d:49: e8:c9:28:00:c8:ea:48:67:1d:db:25:b7:d5:a2:dc:74:64:dc: 6c:8e:79:00:2e:97:99:6d:f5:07:4a:30:35:1e:24:e0:30:f7: 29:d3:1d:9d:99:47:e5:1b:a2:74:28:77:9e:89:90:9e:4b:e0: 23:da:4b:99:da:ba:11:63:82:ea:9d:ba:4e:42:e7:23:7e:35: 90:cf:b9:34:3d:cb:af:b4:70:b6:58:b3:df:85:c0:15:64:cc: af:0f:7c:2d:53:ba:b6:a7:b6:7f:7c:91:bb:dc:17:16:17:63: b9:42:b9:6f:d9:66:a1:af:a7:b8:09:90:f0:0d:48:f3:8f:84: 0b:3b:a7:cd:a2:56:de:a6:68:ea:18:51:e6:90:2e:b9:99:0b: fe:23:7b:71:dc:9d:fc:3b:b7:15:ba:a6:84:4d:f4:bb:ea:13: 4d:f3:3c:cb:26:40:8d:05:de:7f:fc:23:95:aa:f9:99:4b:01: 89:cc:ef:fe:d8:26:79:f8:97:86:95:de:a0:82:a0:7c:13:5f: d8:52:d3:43:98:b9:5f:66:92:4c:69:10:f6:de:a8:35:c6:a1: 04:08:0d:db:78:c2:9a:04:53:12:c4:ba:bd:fe:78:90:ba:68: 13:ff:2f:bd:e1:ad:4d:1b:3a:94:18:e7:8f:40:8d:d3:5a:7e: 2d:a2:f7:6f:17:59:fc:9b:18:aa:3c:87:04:08:83:20:99:39: 5b:50:bd:aa:55:12:88:2d:c5:34:6c:7d:93:ad:1b:55:7c:3a: c1:f5:22:f2:c2:d7:8e:9a:53:93:07:f3:f9:9e:e4:40:92:d2: 49:cf:fa:e3:7d:9f:00:49:bb:d9:f5:13:b6:3e:18:2c:79:bc: fa:6c:48:23:72:4a:16:00:47:22:7c:4b:69:bb:c3:ca:3c:9d: a7:79:69:ff:44:ff:af:14:55:44:38:ef:6a:12:3e:1f:a1:44: 26:61:22:a4:7a:32:34:74:0b:e4:2c:46:b4:7e:85:c4:e1:8a: 05:77:c9:42:df:f6:fd:7b:35:aa:8d:91:bf:13:3e:79:02:2c: ac:a1:83:fd:5a:6a:9a:16:b0:e5:52:25:06:62:27:50:f7:ed: fe:79:58:18:6b:d2:7e:0a:9b:bb:85:6e:a5:ee:4e:e6:ab:77: 32:0d:96:59:6b:8c:c9:38:93:8a:5e:6c:ea:fe:b8:ca:93:b4: 98:85:51:c1:8b:13:4f:4d:57:8c:3d:7c:8b:e0:9d:a8:71:32: 88:37:62:f8:2c:39:4d:10

VII.4.9 CROEC de Limoges

Champ	Valeur
Serial Number	11:20:b2:8d:49:df:ec:33:59:31:fd:9c:08:03:15:d7:48:9a
Subject	C=FR, O=CROEC de Limoges, OU=0002 380183319, CN=Ordre des Experts-Comptables - région Limoges

Champ	Valeur
Modulus	00:df:cc:6a:57:9f:1b:bd:08:61:d4:59:64:e7:23: 68:b4:3d:c5:e6:6c:34:cc:64:a9:c4:bf:ea:c2:f5: 01:d2:38:5c:e4:92:b3:08:2f:ec:e9:12:b0:40:47: 6f:84:d9:73:d0:7c:ee:29:1e:23:a0:35:9c:52:88: c1:e9:23:ae:10:89:34:f9:e9:29:d9:ab:f8:ab:4f: fd:e7:ed:cb:ec:db:ee:c1:bf:66:c2:60:80:02:26: 44:25:c6:a5:2c:d6:92:e5:2a:9c:b5:88:ab:24:07: fa:bc:75:32:b2:f8:31:fa:96:22:3c:2d:f6:e6:99: a0:09:fb:48:6d:08:8e:1d:97:30:15:7f:93:60:07: 1d:cd:23:2d:60:e5:88:58:52:cc:a0:f3:7e:eb:5a: 56:b8:12:d1:b4:33:a3:ac:70:78:5c:b7:11:ee:33: 73:a8:40:50:7a:72:03:f8:fc:28:bb:ea:41:7f:3c: b6:bb:6f:94:0d:c3:40:b7:e1:90:e1:d1:f5:6a:af: 40:8a:5d:e1:b2:c7:7e:87:69:7f:4f:52:64:b1:da: 41:ce:e9:cd:4b:ec:86:cf:f2:ee:06:b6:90:93:03: a4:52:37:a1:9f:03:d3:d4:68:f3:6b:00:08:34:d6: 76:eb:d0:ad:7b:81:b1:7c:c5:79:d3:40:ae:e4:c6: f1:2f
X509v3 Subject Key Identifier	52:BF:C8:76:6A:7F:95:37:C1:F9:DF:33:80:5F:96:39:9C:D9: 30:1A
Signature Algorithm	0b:38:f3:80:c5:f1:aa:4c:7c:4e:6b:3d:65:ed:19:66:d7:84: 05:c2:dd:14:2e:7f:a1:7e:7a:0f:40:92:cb:ab:91:85:c1:20: 7c:90:3c:b6:d5:32:f9:a5:60:99:b3:fe:f1:fc:8f:83:6f:85: 11:90:1b:de:06:70:e6:b6:4f:50:f8:50:9f:08:63:ae:80:b4: 58:8c:0e:03:8a:82:b3:dd:9e:95:57:6e:42:17:43:a2:d7:63: b4:4b:f7:3e:63:f7:fa:f0:cf:16:3b:69:4b:07:3f:2d:9b:4a: 4a:19:ac:d0:43:a3:9c:f9:a1:ac:f1:00:e2:14:d3:a3:51:d7: b4:54:17:f9:36:a0:a8:00:92:b8:87:22:fc:0e:5a:bf:1b:92: 40:c6:24:b3:82:11:34:77:48:14:56:69:ad:3e:62:27:a0:72: 22:f5:27:d3:72:fb:ea:fe:e4:b2:4d:26:24:ee:9e:90:3e:b0: ea:08:77:cb:0c:2a:59:de:17:1d:7f:db:62:b2:76:54:8b:c4: 03:78:c7:d2:60:4b:39:d8:eb:35:6c:bb:a3:52:a0:f3:d7:08: c1:25:0c:aa:c6:0e:98:8c:9e:05:d7:5d:0d:74:f3:02:7b:7d: de:30:4b:20:7c:1f:6d:63:3d:7c:8f:e3:ed:67:80:51:f0:df: 02:49:7c:d6:57:4c:2b:b3:0e:8c:6e:2d:4b:b8:7b:4b:76:38: 71:53:80:a4:fa:f6:b6:4d:6d:fd:3e:ed:bc:8c:31:5f:cc:ed: bd:21:82:c9:0e:ed:15:8f:11:ce:7c:fe:16:a1:22:3e:dd:57: 13:ee:cb:25:46:3c:dc:d4:7c:89:a6:5b:fe:5e:ca:06:25:5c: 22:b4:7a:aa:4a:ad:64:68:1a:64:bb:18:e4:d2:13:88:42:f1: 5c:ef:ba:e4:8a:5a:2e:fa:2e:3d:81:bf:b7:09:b0:01:c1:65: 1c:e4:c7:16:09:76:1a:d3:ec:8f:6f:d1:ac:2e:4f:d7:dd:a9: cb:3a:4f:81:5f:32:a5:71:f7:c0:9c:80:d1:d9:be:df:89:c4: f6:ac:06:d8:35:32:86:89:e8:1f:12:19:e8:54:53:8e:33:06: 44:36:a9:57:94:87:2d:81:64:37:3a:b4:b1:53:8d:a5:33:01: 00:81:2c:e6:0f:37:fc:bf:13:86:c5:36:c6:a8:f7:cf:97:02: e9:c5:4f:aa:ec:6c:47:d5:b7:97:34:32:ce:54:7f:19:c2:43: 47:51:86:1c:3c:eb:14:73:f7:db:f3:0c:be:53:7b:c9:56:1b: df:c2:f1:42:3b:b4:8d:6d:5a:b8:ce:ec:8d:dd:19:f8:ea:4d: d3:fc:7d:05:46:b5:f7:b9

VII.4.10 CROEC de Lorraine

Champ	Valeur
Serial Number	11:20:36:09:a4:4f:03:cf:1d:10:c2:81:28:cd:cd:48:f1:8c
Subject	C=FR, O=CROEC de Lorraine, OU=0002 380188185, CN=Ordre des Experts-Comptables - région Lorraine

Champ	Valeur
Modulus	00:a2:48:76:77:43:20:1d:93:45:3e:9c:1d:19:b4: f5:f5:ff:c8:db:c5:50:3e:d0:3b:71:d9:3f:78:65: 1d:fb:1a:b8:12:0b:5e:91:a2:1b:d2:13:d7:00:11: 7a:26:13:c5:24:82:61:f7:84:e3:a2:77:d4:9c:4c: 5f:c3:06:d6:6b:d7:7f:04:df:5c:46:80:15:f6:c4: 4f:fe:7b:01:01:be:05:aa:c6:6a:53:97:16:b8:55: ad:39:b0:ca:ab:6a:eb:6f:19:2e:19:34:9f:c7:20: d3:89:c3:7c:84:34:18:09:09:69:58:7b:f3:92:9f: e0:35:2d:a0:40:e7:4f:d2:95:1a:82:15:3d:7f:02: 98:fe:f4:e8:59:aa:be:b9:8a:c8:e6:c6:96:44:ab: 6b:67:e8:be:24:94:b4:a0:30:63:cb:50:29:25:8e: 5d:c6:a6:dc:58:53:65:94:64:6d:fb:f3:0a:22:a5: 4b:d0:f3:e6:2a:30:d4:10:c0:1b:2c:90:b7:7c:01: a3:59:e8:91:11:06:3b:a8:7c:4e:7e:26:94:70:fe: 43:d1:e3:8a:93:ec:4f:33:87:5e:57:b7:56:9e:21: ce:3b:69:b0:2e:e8:a6:62:80:cf:70:14:09:64:06: 1f:94:f3:3a:0f:00:66:9e:72:67:98:11:b1:a0:0a: 6d:d1
X509v3 Subject Key Identifier	59:3D:71:E7:B8:E6:83:B7:05:E4:07:AA:C1:F3:15:4E:47:1F: 87:3F
Signature Algorithm	04:1d:11:c8:af:9a:3f:05:52:bf:70:1d:de:88:b1:cb:8e:c6: ea:2c:c7:bb:c3:b6:85:0f:e5:a7:db:8b:97:d7:53:a4:f7:43: 6b:32:3a:db:c2:31:99:58:f2:63:fc:f4:09:d6:3c:f5:4c:76: 33:49:bb:c8:42:71:4e:54:44:48:07:b4:ad:64:ab:a3:d3:45: 69:0f:4c:42:9c:a6:d0:a5:95:46:1e:b0:d7:40:fc:e8:37:26: 1c:8a:46:53:80:be:c7:79:51:e0:0c:55:96:ff:a3:cd:5a:35: 7e:f4:ed:3b:16:1f:a3:f7:4a:3c:94:5b:3f:a8:a6:7e:57:1a: 5d:6e:00:86:48:61:2a:f9:55:44:90:1b:62:ea:25:df:e3:6d: 46:68:1f:d0:cd:9d:9e:8f:d1:f8:00:8d:1e:5c:dc:f3:e0:86: 3c:3f:0e:0e:bf:03:e8:e8:35:ec:cb:53:bc:a4:ff:32:bd:06: 9a:47:79:55:93:54:ec:3e:30:15:d9:2f:bb:bd:cf:ba:ce:9c: ae:2b:1e:de:91:03:50:8f:93:7a:8d:79:fb:66:af:a9:c5:4d: 70:e8:d2:09:65:25:1f:04:e1:98:57:ab:07:cb:29:45:1c:0d: 43:80:15:bb:54:ad:aa:92:32:ed:89:b7:02:3a:47:e6:9d:03: 63:de:c1:ed:c5:b0:eb:ae:5c:fb:ca:0b:3b:5c:da:4c:b3:1a: 6b:de:cf:76:7f:a9:d4:70:8a:9e:25:65:d7:e7:79:76:f5:50: e4:50:95:d2:8e:81:7a:53:e3:79:e1:0b:1e:0b:2b:29:dd:2c: dd:e8:d6:84:ea:d5:3e:36:d1:6a:a1:b9:bc:0f:88:ba:f5:50: a1:1e:82:db:e3:92:56:d7:f5:b7:77:46:21:2a:f0:e4:a6:6a: 1c:74:c9:b3:eb:2c:dc:da:f6:0b:1e:9c:c6:8a:d5:43:54:5f: 47:e9:bd:99:f0:e4:9b:4f:dd:95:b9:20:70:5a:f4:5a:88:6a: b5:e4:5c:3c:64:46:6a:5e:80:f0:73:4a:04:25:63:94:38:a2: d2:f2:24:12:23:3b:3b:07:31:68:d1:22:c3:8f:97:36:30:e5: 74:88:ec:43:ef:96:c5:63:12:4e:e2:a2:5b:22:e7:5b:d7:11: 04:db:c5:01:57:98:a6:7d:4b:96:5d:cc:74:f6:1f:bb:b1:81: 92:9a:92:3a:11:a2:47:c3:28:fe:08:f4:a9:f3:23:9a:1b:c1: 6c:fe:6f:50:65:58:7e:d0:d7:f8:53:60:68:df:1e:25:9b:2a: 88:67:72:54:9d:34:a3:79:6b:d8:7b:09:bc:fd:0d:ab:2c:57: 12:b9:aa:d8:c9:c9:ca:88

VII.4.11 CROEC de Montpellier

Champ	Valeur
Serial Number	11:20:0d:c2:06:5c:a2:53:3e:66:35:1a:9e:57:b9:c2:a8:58

Champ	Valeur
Subject	C=FR, O=CROEC de Montpellier, OU=0002 776038077, CN=Ordre des Experts-Comptables - région Montpellier
Modulus	00:ce:a7:23:7e:88:61:f5:a9:1e:c3:bd:c2:fe:db: 36:6f:bc:ec:84:05:71:5c:b1:f1:b0:75:16:0f:4d: df:8a:cc:36:4b:a6:3a:7c:5b:28:56:5a:fa:d0:ac: 33:5c:80:66:d6:57:84:a2:5b:77:31:1e:41:30:12: 1a:77:62:6c:05:b9:51:cd:e4:8f:ec:62:45:f7:29: 47:fc:4d:81:09:f6:4d:12:de:b9:73:e3:f6:7d:50: b1:5d:ce:14:a3:71:ba:44:e6:b0:ba:09:07:6f:c4: 13:38:18:6d:1f:e0:2d:8a:ac:10:2a:5e:e7:04:37: 00:99:93:50:53:a0:b7:f5:3b:89:36:65:56:e5:34: b1:b8:7a:af:77:41:b6:19:e4:37:c5:27:b8:89:63: 4b:a9:eb:94:fc:61:35:8f:e2:19:0c:f3:97:c8:44: c2:ff:09:05:55:5c:1e:67:a9:37:1d:aa:9e:3f:fd: 3c:62:c9:9a:f7:89:7d:4a:91:d4:48:11:39:95:3c: 48:85:8c:3b:b6:ff:c4:15:b6:9e:15:92:3f:30:4e: 7c:96:43:56:02:06:11:09:6f:48:26:c9:b8:41:e7: fa:2e:ca:51:5e:06:ef:59:01:a2:a5:82:8e:70:9b: 6d:7a:43:fa:66:1f:53:f1:25:dd:0c:97:33:2f:03: 7e:71
X509v3 Subject Key Identifier	60:4D:B1:66:22:83:5A:25:54:A9:E8:7B:1D:08:45:1C:6F:05: 7F:91
Signature Algorithm	48:4a:8d:47:5a:82:5e:ef:99:29:91:e3:db:61:fe:f2:4e:ab: 52:21:fa:fc:7a:4c:c3:fa:c5:38:85:d4:dd:22:e0:45:46:59: de:57:3d:39:fe:5a:f5:10:d0:72:08:27:e8:62:6a:4d:ee:e2: 69:39:7d:a7:35:16:b1:53:36:e5:db:cf:17:03:3b:fc:79:f8: bf:29:ca:78:79:4d:f1:65:e5:51:b8:41:b7:7f:57:f2:63:ee: 52:26:6a:24:12:21:3d:65:d3:df:95:72:0b:a0:65:fc:49:70: 3b:1c:5a:00:4d:01:85:65:ef:85:4e:3f:fb:a3:fd:7d:16:3c: 74:53:5a:0a:cc:0b:93:3e:37:e0:4d:85:f6:66:e7:31:77:6c: 8a:78:62:27:85:35:61:42:e0:3c:91:e3:0e:a4:40:83:09:2a: fd:aa:04:6c:40:bb:22:e3:3f:31:52:4e:7e:ba:30:38:30:de: bc:07:25:19:0f:0f:07:6a:11:a1:e5:37:12:68:94:2b:a0:70: 4f:17:d7:40:10:f5:5b:fc:12:5d:0a:0e:dd:72:22:43:e2:1a: 7d:6a:31:10:0f:1e:5e:de:e7:1c:ff:eb:0f:69:9d:19:db:0b: dd:cf:d4:15:bb:ff:7d:e7:b9:12:0f:9e:f7:ff:dc:74:4f:fa: e5:5b:d2:ee:00:4f:1a:7d:f1:6a:d9:a0:e6:27:01:00:82:b8: 2c:5c:77:42:8c:3c:08:2e:d8:c0:e1:63:b8:b4:cc:02:cc:9e: a8:d1:42:0c:95:5d:c1:71:c1:e2:6f:03:94:9f:06:dc:89:f4: 93:ab:d1:58:36:c2:18:86:d1:34:31:b7:49:63:81:8f:bb:7d: 28:7a:86:d1:ce:cc:f6:d3:34:62:2c:6a:bf:3a:7c:31:88:36: f1:3c:c7:04:db:7a:a6:5b:03:53:ef:5b:a5:14:f4:ca:1d:b4: e4:6b:2c:44:73:69:c3:c3:22:53:45:66:61:cc:d6:52:65:29: 0d:f4:a7:3c:12:30:1b:cf:8c:44:e9:6e:33:7e:8a:49:f6:1a: c2:e6:6e:a4:f5:84:d9:dd:38:28:dd:51:cc:4f:09:53:3f:94: 9a:94:f2:4d:cd:f8:46:fa:12:d5:d8:1b:b4:89:07:d5:d8:ee: 15:ba:63:df:46:43:64:8e:65:5f:6d:c8:c2:54:8e:ac:13:a2: bc:dd:7d:6d:23:06:1e:a1:4e:20:3d:3a:8d:45:aa:2b:84:10: 9c:cc:dd:7e:25:d3:b8:fb:6b:fe:1f:90:82:8e:21:be:ab:82: 1a:61:84:b4:44:f5:65:e7:a0:a8:d9:b3:b6:14:1e:41:76:99: a2:16:89:32:56:aa:bd:69

VII.4.12 CROEC de Paris Île-de-France

Champ	Valeur
Serial Number	11:20:8f:4a:47:7f:5a:c6:0e:55:b8:59:a9:d1:c8:69:eb:97

Champ	Valeur
Subject	C=FR, O=CROEC de Paris Ile-de-France, OU=0002 784854408, CN=Ordre des Experts-Comptables - région Paris Ile-de-France
Modulus	00:b2:e4:51:c9:4a:3c:cd:f0:98:22:a4:20:7c:c9: 43:1f:48:b9:6f:ff:5f:33:b6:26:08:58:5d:b7:ad: 36:f6:90:88:a2:17:a3:f1:b5:0e:42:2e:99:41:a0: d6:91:38:50:31:0a:ff:48:af:1a:70:48:0a:4f:ec: 48:cb:6d:1d:87:5f:5c:ea:a2:66:7a:03:c5:9e:66: 5e:2a:08:83:ad:5a:51:f8:5d:cf:79:ff:9e:8b:e2: 1e:34:a1:5c:8c:d3:07:6a:de:6c:7d:22:4f:ee:c8: 44:d0:42:34:93:21:11:58:e1:d1:02:5b:63:f2:d8: d5:ab:64:97:92:7e:f0:03:8c:40:76:f3:3b:8a:90: 23:16:22:96:1a:32:25:85:45:48:8c:66:09:6b:12: ac:7c:ed:ad:1b:a3:a7:4a:1b:68:ce:2a:63:77:db: eb:4e:ea:1f:42:f0:97:79:3b:11:06:3a:5a:38:72: f5:85:db:7f:5f:c5:88:d8:49:b3:5b:16:97:1b:cb: dd:be:bd:dc:09:ff:2a:ed:95:5f:a9:a1:3a:03:3d: ee:34:b1:2e:a5:a7:e5:4e:02:c0:f3:3c:ac:a7:2d: 64:0a:5f:8c:3f:92:79:aa:fe:fe:f2:ad:17:00:80: 97:e3:96:8d:1c:5b:fb:4a:47:63:fa:d7:94:b3:57: aa:c5
X509v3 Subject Key Identifier	87:49:DC:E9:D8:7C:AC:EC:64:06:FA:01:75:73:0D:2B:1C:E7: BB:EC
Signature Algorithm	0a:ff:48:01:50:0b:b9:ea:e5:ec:97:e3:18:f2:df:d4:d6:48: fb:3d:f0:8b:95:1d:1e:6d:91:44:a7:22:ed:ca:6a:78:68:91: 3f:d3:19:ed:76:72:d7:ba:73:91:1f:9a:5a:11:b6:d1:9e:f7: 2c:04:c9:90:a5:f3:10:e7:76:30:98:46:b2:e9:a9:a9:5b:cd: 00:67:75:83:6c:7c:6c:d7:84:b8:59:d3:7f:dc:5f:79:92:73: 9c:e4:e1:0b:a9:07:22:be:25:16:8e:1f:b0:dc:de:aa:54:99: c6:d5:3f:50:df:36:d3:c8:4d:41:e3:07:81:38:77:4a:c5:8b: 14:ad:41:86:da:b4:0d:2f:e2:7f:55:15:92:74:54:a2:8a:a9: 41:c1:88:8b:7d:7b:56:aa:05:29:1d:ca:24:b8:80:ba:a9:7a: 93:da:8e:82:68:2d:63:e8:20:de:eb:a9:58:2b:0b:fd:d2:8e: 1b:ca:9e:87:f5:a4:23:24:29:76:bc:b2:84:0c:54:99:e8:1a: e3:37:40:f3:d1:af:b0:72:99:01:3f:86:ee:2c:97:44:25:d0: 20:e5:1f:fa:50:d8:ea:bf:d8:45:58:aa:48:58:cd:e6:2c:21: b9:1b:76:2e:6f:94:88:c3:d1:f2:be:e2:28:a0:32:84:40:32: 71:a7:06:a2:e0:d9:9e:81:b8:38:e7:ff:e5:05:0a:b2:44:35: bf:01:90:e9:1a:18:11:56:51:aa:40:4d:7b:f3:fb:80:b7:f6: 2e:d1:12:e1:ee:96:43:6e:d4:e1:06:24:3d:c9:48:ca:27:9d: 86:5a:c8:0a:5f:24:c7:3b:46:fc:99:b8:d7:e9:7e:2a:7e:de: eb:aa:55:f4:81:83:3f:6a:06:11:cc:f6:08:40:f2:83:8b:c7: 97:f9:6a:c2:e9:bd:23:c2:de:7a:72:7e:cd:54:0c:f2:00:97: bf:cf:4d:c3:5f:64:e8:b9:1f:08:b9:74:58:e9:36:d7:0d:b7: f5:cf:15:57:56:da:43:6d:05:12:21:c4:b4:86:f1:11:70:93: 03:a5:d4:5f:86:75:3f:79:ac:b2:73:c1:4f:a3:be:7f:bc:c4: b8:e2:62:7f:69:14:99:b7:e3:99:72:8b:f0:9f:bd:62:d6:d1: bc:a6:08:2e:c8:80:78:57:f8:19:16:ad:3a:94:4d:31:7f:25: 7c:60:74:f9:9e:34:a4:26:0e:ff:a7:de:a4:82:fd:d9:fb:86: 1d:d9:06:0a:55:7f:f2:7b:86:7a:e1:f0:71:b7:08:a5:bd:aa: f9:06:7e:1f:3a:67:b6:1c:f5:ea:4c:45:c4:28:84:9a:19:49: 5c:f4:f6:78:c1:88:1c:cf

VII.4.13 CROEC de Picardie-Ardennes

Champ	Valeur
Serial Number	11:20:ca:16:93:7a:7c:26:e5:69:d0:44:0b:86:dc:84:3b:86

Champ	Valeur
Subject	C=FR, O=CROEC de Picardie-Ardennes, OU=0002 780601803, CN=Ordre des Experts-Comptables - région Picardie-Ardennes
Modulus	00:b6:8f:1d:5f:eb:0b:4f:b4:b5:0e:cb:ab:82:cf: 3c:de:0c:55:06:0e:8c:7c:ce:22:8e:53:0c:f8:24: 04:9a:0f:ae:28:8a:a2:25:f4:41:e5:6f:b0:95:97: 18:3a:6b:22:e3:7d:ca:b8:c8:48:9d:4a:90:73:ed: 2c:19:08:6d:6b:47:dd:77:18:6d:1c:b5:92:94:d7: 86:f3:20:c7:d8:fd:86:3b:4a:26:15:fc:df:a7:99: bd:13:2a:49:56:e8:a7:76:f6:5b:b1:b2:03:9f:db: 96:75:a9:6e:8a:62:9c:f0:21:3e:09:77:f0:a7:b3: bb:4f:80:64:19:f9:5f:73:97:d1:0e:7b:b2:7c:8a: 5c:34:4f:fe:54:1f:77:c3:43:11:2d:09:6a:fd:62: 23:e1:83:15:3e:7f:73:8a:3c:34:85:21:f7:34:a0: 7e:d2:29:d2:0f:a0:98:72:6e:bd:50:87:b6:92:20: c8:0d:b2:f0:7e:d1:ab:7b:af:a7:da:ef:30:3b:13: 4e:23:0a:18:6b:18:ff:67:94:8b:fd:a4:74:24:b6: 1b:ca:eb:1a:cc:e6:34:e0:15:39:45:ef:f4:29:02: 60:c8:87:f8:dd:54:7c:1c:0f:c3:8f:6e:5f:33:be: 74:8b:ca:5f:fe:78:72:77:18:1a:5c:2b:5b:15:ff: 84:5b
X509v3 Subject Key Identifier	A1:58:4F:E7:20:20:E4:96:CE:AA:99:AE:F1:A3:59:63:1B:CD: 2F:F7
Signature Algorithm	16:dc:40:79:b2:95:04:08:50:38:d2:c1:04:d9:b9:9e:f3:2d: 85:6b:46:d4:8b:13:4d:84:c3:07:3e:03:c3:67:29:4d:19:ae: 64:ef:c7:c3:bc:3b:4f:9a:5f:43:2b:61:94:6c:5c:8c:72:d4: 2a:f7:3c:4a:f7:47:f9:69:05:8f:5a:1e:d6:a8:6c:4d:af:c1: 13:8b:b1:8e:67:da:d4:d6:f9:80:bc:0d:47:d5:96:42:1a:12: 8b:d8:7a:98:4c:a2:5a:f3:46:18:1c:46:7b:e4:93:c0:33:4c: c0:a0:b4:91:e1:8e:ef:ea:86:3f:01:ff:e7:b1:60:a6:ea:e7: 77:42:4a:22:79:60:e8:29:c1:96:8e:d8:f2:9d:38:96:4a:e5: 91:d6:85:89:07:56:96:cd:d9:11:cf:1f:a2:1e:97:cb:ba:ce: 46:d1:55:c4:ef:1e:6d:41:d8:c0:3b:45:8c:05:07:6f:11:46: 76:9e:c4:2c:50:37:75:80:31:dd:ef:5c:0c:de:82:b4:ab:9c: 1f:6a:3f:6c:ca:6b:ad:43:60:ac:e3:e4:fe:c6:39:6e:74:ee: f1:b1:d6:27:3e:de:c8:16:1b:f1:2c:e5:d8:99:ce:ce:77:5e: dd:75:63:e4:25:d9:82:09:37:15:6b:22:ff:8c:7b:4d:08:cc: 96:66:9d:8f:32:3f:6d:1e:21:00:21:46:90:b7:97:d9:c5:63: 2a:93:67:75:d2:9b:58:ab:3c:64:46:cf:b9:7d:e7:bc:13:23: 03:f6:43:58:93:02:eb:a6:5f:70:b3:b6:54:b6:4e:cc:b8:bb: 17:31:a1:0d:87:1f:66:98:71:38:6a:5f:bc:2e:b7:d9:a5:95: 84:9f:d8:34:47:2a:89:25:b7:33:3f:0f:26:20:24:3d:ce:e7: 65:30:03:ad:ee:a9:99:a0:ce:fd:a7:d0:f0:ed:4f:72:2e:01: cc:13:e9:08:22:d0:af:09:86:7f:a9:63:e6:24:d6:49:be:90: bd:c7:e5:ba:82:e1:5d:85:03:65:72:65:3e:81:61:eb:fc:46: 05:61:d3:90:1b:ac:48:94:92:d2:e1:b3:18:df:31:14:26:be: b7:1d:64:8d:49:f3:42:f1:fb:c8:c3:ec:e6:71:1f:5a:cc:1b: a2:28:6c:07:ee:39:83:61:b2:e8:9d:5f:78:11:10:01:02:83: ba:dc:67:42:22:cf:c5:da:f4:b9:f1:06:88:23:9e:1d:4b:3d: e8:2b:11:0e:18:de:84:06:5a:46:0f:c3:59:0c:83:90:89:f8: 19:e3:a4:b1:2d:d3:32:0a:f9:04:3b:cd:9a:88:8f:51:50:82: 4c:32:86:ee:4f:6b:2c:72

VII.4.14 CROEC de Poitou Charente Vendée

Champ	Valeur
Serial Number	11:20:2f:53:f4:c6:40:30:76:de:93:2a:9c:88:5e:5d:a4:bb

Champ	Valeur
Subject	C=FR, O=CROEC de Poitou-Charentes-Vendée, OU=0002 311146385, CN=Ordre des Experts-Comptables - région Poitou-Charentes-Vendée
Modulus	00:cb:b2:a5:52:0b:1a:62:38:b8:26:35:41:af:d9: b8:3c:ac:a6:83:02:0e:b6:00:d5:9e:e3:88:60:22: 96:89:91:28:d8:8f:12:67:42:0f:08:b3:26:05:79: 58:1f:bb:f3:51:71:98:cf:bd:fd:2e:c9:e0:3b:a9: 3e:03:52:b4:1f:a7:b3:99:b2:76:71:a2:1e:e5:fd: 16:9a:d8:1c:6a:51:55:d4:af:1e:a3:3a:bf:7c:c1: 12:3f:4f:91:a2:32:9c:38:2d:2f:b2:6f:67:3a:12: 62:3e:63:3b:4b:dd:ba:dc:07:90:4b:1a:16:48:a0: 67:ad:71:72:53:7e:b4:cd:9a:5d:13:5c:c0:0c:7a: 22:bb:af:65:cd:6f:e9:d1:c6:9a:cf:65:89:3c:80: 48:75:bc:ae:f9:fe:e3:65:51:75:69:e5:66:bb:2c: 0c:4a:8f:33:cc:91:57:a5:87:cb:fd:3c:7b:a6:35: 46:ce:a3:e1:7f:d6:be:a3:9e:c0:db:09:c0:87:84: 98:93:2d:67:67:dc:39:66:2d:8c:b7:08:15:f6:9a: 1c:ab:b2:f3:fb:cc:6e:e4:0a:5b:9f:8f:1a:e2:78: 43:c3:4a:26:83:54:b6:d6:f6:c7:5b:ac:88:7b:f0: 72:d5:4e:a9:4d:be:b6:cb:f8:72:59:c9:6d:5b:78: ae:35
X509v3 Subject Key Identifier	A0:8A:F3:F6:0F:D2:F0:1A:15:F1:2A:85:D9:DA:45:04:1C:8B: D1:2D
Signature Algorithm	1a:8d:22:af:d4:05:f9:7c:33:fc:80:1e:e3:cd:79:89:80:48: fc:16:79:03:bd:a7:fa:87:6b:4b:2e:c1:cd:8b:6e:0f:3c:c5: 4f:69:82:e5:f6:54:62:7d:d4:06:88:09:fe:89:c0:7f:d0:1a: cb:7d:72:7e:ea:4f:3e:71:d7:a3:e6:b3:43:df:c8:a8:91:27: e9:7d:fc:ce:87:e0:86:42:52:9c:a8:2e:fd:8c:1e:9d:cf:b1: 1f:20:5d:a4:36:de:8b:bc:50:f5:4f:e9:a9:67:ee:6d:f3:78: ea:9e:05:6d:d6:d7:9a:19:8d:31:42:1b:67:be:ab:2e:52:ec: d3:c6:04:04:94:29:5a:45:f2:93:2d:bf:ec:43:28:db:e3:c9: 1c:5a:20:01:eb:fb:ac:bf:4b:4b:4d:c8:70:d8:bd:35:a9:ba: d0:38:a7:fc:29:23:5e:2b:41:2e:5e:71:b2:ca:31:ae:dd:ba: 3d:41:e8:67:bf:94:3c:f2:ba:0a:9b:88:d6:3d:28:e7:1d:d5: 54:f0:24:89:86:91:ca:11:e6:74:77:fd:dc:61:2c:7d:7b:0e: f0:82:d9:aa:10:28:cd:f5:95:7a:7d:51:85:5d:ac:51:3e:fc: 9e:ba:ac:b4:29:99:3c:96:60:70:49:87:a8:ad:8b:e9:10:5f: fc:9d:d8:e3:b5:c6:37:44:bd:16:23:36:ba:34:cd:6d:7a:9a: 20:63:74:a7:75:00:e1:92:03:1c:d9:3b:87:68:f5:ae:7f:33: f6:5e:80:c0:4a:e7:72:46:3a:b1:09:64:c0:67:c7:e8:19:c1: f2:3a:b9:b0:d9:dd:04:1a:e1:5d:40:96:72:dd:09:44:13:9c: 84:68:6d:f5:d8:b3:4f:64:0c:d9:51:02:d5:4c:58:6a:b8:27: ab:99:07:e8:bb:72:0b:6e:bf:c0:2e:46:66:b8:7c:fb:45:e7: f2:4c:3a:88:39:28:5f:23:f7:71:e5:c7:8e:bf:ad:9b:45:b0: 23:32:15:44:96:ab:a3:d7:38:5f:6c:03:be:ed:98:e9:17:7a: 32:2f:68:6a:ae:b8:ba:66:89:bb:d9:ed:98:b6:1f:37:5b:d2: 1c:37:6a:0d:c4:72:ae:80:e2:83:b4:55:77:27:95:ce:9d:52: 74:e6:48:1c:ee:e2:7a:ef:58:91:69:f7:1a:34:7b:ef:bd:97: 6d:c7:77:eb:53:a9:91:a0:ce:6d:f9:dd:b6:10:1b:f7:e9:98: 57:c3:1f:92:2e:31:64:c9:de:b1:9d:a7:c4:b7:3a:c0:98:ca: a1:ca:71:a9:ed:3d:3d:a7:91:b4:c3:0e:8f:61:36:05:32:00: 77:f7:1b:fc:3c:fc:2a:e2

VII.4.15 CROEC de Rhône-Alpes

Champ	Valeur
Serial Number	11:20:17:5f:e4:07:46:c9:8e:d0:7f:5a:2e:6d:1b:b1:ab:e1

Champ	Valeur
Subject	C=FR, O=CROEC de Rhône-Alpes, OU=0002 779893890, CN=Ordre des Experts-Comptables - région Rhône-Alpes
Modulus	00:ec:ab:02:f4:0f:93:3b:51:9a:9d:ca:7b:be:f8: c5:08:b9:69:d1:17:c7:b6:7a:6e:80:90:e3:aa:fb: da:87:38:8c:40:d7:2e:ef:cb:d5:c1:b2:aa:18:a8: a3:07:cc:cd:17:2d:25:d0:dd:1b:f4:37:b8:13:40: e8:7c:eb:51:a3:67:d7:3f:89:43:28:4b:ab:66:3f: 29:60:45:70:b5:e6:c0:12:c3:e1:04:3a:0e:3f:e8: 8c:56:c8:c3:c3:e5:e0:a4:87:01:50:4f:f1:28:c2: 25:7e:97:bd:47:d1:65:75:ea:16:54:0a:97:94:9e: dc:a9:d0:33:cc:a7:a6:c4:7a:76:83:ad:65:1a:bf: 76:40:95:7d:87:3f:e1:5e:07:61:e0:5a:cc:a1:9d: 90:64:6c:06:49:1b:d4:df:72:68:c0:08:b0:0a:f9: ea:01:7f:1e:ef:a8:37:7f:cf:31:03:4f:78:c6:7c: 19:f9:44:7b:65:12:ee:e1:e2:3a:a9:46:66:0c:85: 35:57:bc:c8:1e:7a:ed:57:84:bf:c2:50:05:91:46: ee:10:82:2e:49:b2:01:e0:61:28:22:e0:b5:b5:0d: 5e:95:2d:7d:67:9f:19:e4:0c:13:63:cd:a6:c6:d6: 03:cc:24:c5:b4:87:1a:7a:5a:0f:a0:40:66:e3:8d: 39:3f
X509v3 Subject Key Identifier	A1:58:4F:E7:20:20:E4:96:CE:AA:99:AE:F1:A3:59:63:1B:CD:2F:F7
Signature Algorithm	67:1c:5d:ef:f5:80:d6:f0:df:68:ba:83:24:cf:d4:7a:99:98: 65:89:58:b4:0f:a1:f1:ef:98:e6:ef:eb:d5:23:85:59:9b:29: 83:c1:a1:a0:e9:96:40:74:37:27:67:3f:1f:65:fb:55:2b:14: ea:f5:aa:0b:8d:8b:06:19:d4:53:79:b3:34:28:6f:d6:4d:e9: 77:30:cb:58:58:81:a3:12:9e:37:6b:36:dc:ad:f5:35:47:d7: 93:3b:ee:69:7a:c2:8e:e3:5e:9b:54:de:c0:1d:e8:d7:87:17: ca:79:a0:b9:d4:25:5e:43:79:32:7e:68:d3:7f:ee:1c:ca:23: e9:40:61:ac:22:8c:23:75:1d:95:e8:78:78:f0:b9:4a:85:48: 7e:7a:df:85:96:cb:6e:33:05:c9:71:b7:d5:8f:e2:70:86:a7: 7d:2c:36:cf:c0:3d:aa:85:9c:9e:8b:e0:34:ae:88:b3:70:0e: e5:c6:1c:35:72:b3:36:c2:17:2e:e4:06:4b:10:eb:1d:2a:37: c0:5a:f6:ad:96:85:f2:e9:42:ba:5b:2b:16:2c:5c:9c:98:f4: 7d:f1:a4:40:63:46:34:52:0c:cd:10:af:b6:9e:c5:ec:5a:de: 0f:d9:b7:91:26:e2:a1:86:7b:61:09:37:cc:44:8a:e3:17:93: b7:44:9f:aa:01:c0:fd:55:22:a4:91:73:92:cc:d9:99:d8:60: 80:c9:cb:79:e9:83:b8:c7:7a:43:3e:f0:ea:8e:a5:81:6a:25: 9c:1c:9a:fb:09:d2:cd:dc:d8:50:c2:1a:99:33:03:c8:03:29: 64:33:57:66:16:16:65:30:76:40:28:8b:f6:a6:2f:d6:da:9e: c6:99:86:d4:ad:3d:50:f7:e4:da:08:c1:1e:2b:9e:d3:88:2d: 05:93:e3:74:bf:48:74:fb:06:52:21:0c:7d:c7:c1:03:e7:cb: 46:fd:fa:39:de:0a:6c:72:81:48:25:41:8d:84:aa:4b:e7:38: 37:1c:a3:05:5a:5e:e9:e7:b0:3c:b2:04:4a:77:0f:0d:6f:35: c5:40:ad:a7:34:f3:15:8f:09:24:a8:1a:38:5a:fa:72:03:c4: 33:2f:bc:36:8e:bf:b6:02:d8:ce:41:9d:10:9e:4f:13:27:e2: 86:93:67:4b:7e:7d:60:c6:f3:7b:3b:f2:17:32:0f:d0:48:94: f9:37:c2:ef:93:e3:a2:1d:ea:56:c2:e8:c1:27:9d:57:00:a6: a9:e8:e0:b3:a5:a3:f1:af:f8:b4:3d:ee:31:59:2c:6a:ef:9d: 19:57:88:c1:dc:aa:0d:90:99:c5:94:92:e3:88:47:57:74:18: 27:09:00:79:97:78:70:8c

VII.4.16 CROEC de Rouen Normandie

Champ	Valeur
Serial Number	11:20:b3:4d:7f:19:08:ef:55:82:93:c5:1e:a7:19:d6:99:44

Champ	Valeur
Subject	C=FR, O=CROEC de Rouen Normandie, OU=0002 781121850, CN=Ordre des Experts-Comptables - région Rouen Normandie
Modulus	00:b2:21:f9:40:7f:09:3e:e7:97:15:d4:9f:a5:14: f4:9b:9f:2e:75:2a:3f:71:5f:eb:60:e9:15:3a:36: f7:c0:01:dd:56:9d:9a:a5:45:3b:bd:bf:5f:3f:77: b8:3b:c5:85:0d:04:7b:40:a8:ad:80:8b:66:5b:6f: c7:50:c9:c2:d1:8a:f1:4e:63:42:59:d0:e2:3f:9c: 06:07:89:92:e2:c9:88:33:64:81:46:33:0e:83:de: 31:8f:1f:c8:66:13:92:78:7b:58:1a:05:a4:91:2b: f4:b6:f6:d8:14:35:99:2a:ee:42:a8:ce:e0:a9:2d: ee:10:3a:3f:7d:85:37:de:42:e1:6c:80:e3:ee:94: 28:af:65:4b:28:c5:64:dd:db:c2:12:e1:ad:61:63: 1d:ac:d0:8d:cb:a6:cf:67:54:1a:f7:47:e6:7a:a5: fb:7e:a5:54:1b:70:f6:ef:a8:98:9c:8d:0a:14:f7: 59:c7:b2:76:f3:d3:53:46:ee:b4:7f:ca:14:42:3b: 20:10:cf:b5:a6:3b:73:70:dd:8f:57:f7:22:37:fa: 95:e3:64:00:c5:4d:eb:b3:73:3e:85:97:b8:76:48: ff:73:b3:42:e4:0d:c7:90:80:a1:80:02:c5:21:0e: 2a:7c:81:8e:dc:53:5f:51:e9:66:ed:36:4d:81:af: d0:2d
X509v3 Subject Key Identifier	A7:02:19:91:9D:ED:6A:42:CB:F3:62:D1:25:58:C4:5F:34:3E: 5C:8F
Signature Algorithm	bd:3b:d2:c1:fe:c4:d9:83:06:19:fa:23:8a:bb:67:bf:af:9f: 24:ee:4d:e8:1d:77:f8:55:b6:73:0b:d3:30:1a:8f:bf:04:ff: 23:33:84:0c:59:55:89:97:2d:f3:6a:5f:64:1f:42:85:b1:3a: 5c:b1:f2:7a:bc:3f:eb:26:6b:0a:e8:a8:fc:a0:42:1b:93:ae: ee:f0:9d:b3:81:bb:8f:38:02:bb:38:81:86:68:25:10:c3:e5: 8f:92:0b:12:a0:25:23:3d:b7:18:5b:43:7b:aa:ea:30:d6:c6: 01:b2:2b:b1:1f:1d:9b:e8:62:9f:43:c6:86:66:5b:f8:cc:6d: 64:75:09:ee:41:13:83:63:b6:3e:dc:8e:05:98:f8:e5:70:8c: f0:a6:ac:cf:6b:11:51:6d:cf:65:9a:f6:37:00:a3:af:92:22: dc:8a:c3:d2:90:31:0a:73:a9:1d:48:ef:fe:2a:5d:0f:04:68: 8d:fc:f3:13:c4:6e:91:d9:1d:df:dc:59:0c:1c:07:81:e5:02: f5:c0:f3:4e:f3:85:ef:35:63:57:75:d9:32:1b:41:b5:0f:bb: f9:5e:95:5f:7a:55:21:a3:f6:91:20:3d:8b:ae:63:08:8f:eb: 1a:6d:e7:8a:46:2c:bd:74:80:f5:c1:e7:6d:66:87:a4:49:43: b7:4a:cd:e8:e0:d0:6f:70:21:3d:bf:da:47:ac:79:02:6e:d6: f6:ff:4a:b6:46:b6:c6:95:b5:bc:7c:fe:c2:4d:bb:a3:5f:54: 8c:d7:7c:49:dd:a9:d6:93:0a:7f:a3:dc:50:30:0d:1c:2e:00: 68:01:d4:49:9d:97:ab:c0:fb:79:7d:2c:09:e1:b3:dc:53:35: 94:a4:b0:be:0a:9c:2b:81:a6:a9:0b:46:8f:31:f1:fe:72:af: 2d:57:ce:75:2c:99:1d:74:d5:ce:09:7d:ec:c1:ad:92:42:63: f4:43:ba:b1:16:a2:04:57:9d:51:a5:52:91:f4:7f:52:57:7a: 9a:b4:c9:f6:0d:86:47:0a:61:42:38:55:1a:81:22:76:0f:ef: e3:1d:08:b5:fe:9e:ea:d1:54:fb:66:bb:4d:39:da:c1:17:5c: ac:91:b2:d0:13:5c:fa:84:c2:10:0d:61:66:d3:d6:95:ba:88: 25:7f:d1:8a:a9:74:55:0c:71:d2:45:96:1c:17:63:0b:94:63: 98:10:96:97:56:d2:80:4d:c1:9d:0a:f8:60:53:a5:b1:38:48: a7:4b:fd:17:8f:3a:ca:5b:ab:dc:51:e5:d4:b0:32:0d:d9:fc: f5:62:ed:27:b5:84:20:0b:2c:09:79:c9:57:26:cc:d3:4c:5b: 5e:09:62:8c:97:16:3f:21

VII.4.17 CROEC de Toulouse Midi-Pyrénées

Champ	Valeur
Serial Number	11:20:e3:5d:57:2d:b2:13:ac:d7:07:6e:5e:6c:7d:2d:af:78

Champ	Valeur
Subject	C=FR, O=CROEC de Toulouse Midi-Pyrénées, OU=0002 776949596, CN=Ordre des Experts-Comptables - région Toulouse Midi-Pyrénées
Modulus	00:b3:26:75:00:87:48:8b:b7:f8:e8:02:79:a2:72: d1:98:06:e2:20:45:18:1e:90:67:26:a1:6d:6b:94: 39:40:cb:32:a0:03:24:86:bc:6f:a7:52:f0:69:4e: 2d:ce:ce:ba:f7:4b:05:b0:f0:a1:27:69:6c:19:98: 3e:a6:25:17:23:88:4c:45:82:b5:0f:71:9d:22:e5: 15:3c:82:0d:74:ac:ed:be:94:f9:3f:92:f5:ed:b4: 45:4a:54:4b:dc:fc:7f:e9:e8:5f:f3:9a:9a:12:c3: 9c:af:e1:fb:13:8c:92:41:41:88:15:6a:74:ad:dc: b7:63:ae:34:1f:d6:4e:60:42:0e:d9:c0:c0:62:3f: bf:ad:a2:83:8e:75:3c:a1:90:c8:9d:37:fc:1a:d9: 25:6e:e1:f9:ba:c2:04:50:ea:c3:ff:9b:b5:c1:21: 83:ff:26:c4:00:57:95:cf:d8:b3:88:07:ae:50:df: 3c:7d:58:06:65:10:87:50:a1:c3:79:ae:ed:d4:a3: 2a:73:60:1a:3e:c8:67:b2:6d:18:f6:4c:5d:63:79: 97:9d:21:e8:5b:34:29:2f:5b:c9:2b:19:33:d7:85: bb:57:6e:1b:12:07:e7:1a:e9:94:60:66:ff:e5:f1: e3:79:96:3c:44:2e:b4:f7:85:8f:71:ad:1b:cd:d2: 27:93
X509v3 Subject Key Identifier	B0:BA:CE:8C:4A:E4:19:D6:77:82:50:64:8B:C9:6F:7E:01:49: DD:79
Signature Algorithm	83:98:24:4b:2f:73:40:de:e5:88:0a:af:89:9b:1e:83:70:e2: 9e:8c:93:b6:fa:e8:38:0a:ee:4a:6f:ff:0e:e7:b8:3b:bb:5c: bb:e0:c2:9e:84:f3:65:e8:a6:ab:45:e5:c7:32:3e:a1:c6:68: 6c:e5:3a:bc:3a:5b:5e:b2:a1:29:e0:bf:9f:1d:2b:df:3c:86: d7:da:c1:d2:6b:c2:c2:a5:a7:c6:5d:9b:11:7a:36:03:8e:3f: 20:2e:be:86:a5:3d:62:0f:cf:b7:24:5c:8d:a1:f6:d5:5d:a6: 25:1e:5c:bb:8b:7b:bb:3d:21:64:5b:ae:3b:4f:0d:77:f2:df: 4b:50:bb:03:25:5f:5c:c9:53:1d:21:b3:3e:2f:dc:08:8a:7f: 24:b9:ef:5e:a7:e7:0c:7e:20:fe:be:68:8b:7e:cb:6f:fb:04: 88:f8:53:91:50:43:65:78:62:dd:ad:fb:d8:60:a0:72:cf:bc: cd:89:e9:66:ae:b8:09:5e:ef:20:b8:bd:90:d6:e5:46:a5:df: fa:9c:94:10:18:83:53:9a:46:10:db:b3:2d:44:28:11:5d:60: 6f:d6:66:21:cf:76:62:14:14:0f:49:5a:b1:d5:a9:e7:06:d0: 28:3a:87:d2:14:27:97:40:4c:81:91:d1:85:4d:4d:8b:1e:0e: d6:83:d8:70:de:cb:25:20:79:99:bc:3b:d3:9c:20:d2:87:41: 93:4d:bf:65:43:8f:f8:e9:8d:3e:10:3b:4e:fb:2f:aa:35:59: 08:85:7c:d7:4a:dc:2f:96:92:08:21:17:b4:9c:3f:7f:8c:6b: 4d:41:fd:0f:b7:5c:97:ba:0f:01:fe:3f:6a:28:b4:f5:37:b6: bb:5d:c1:90:a0:98:7f:d1:5b:12:32:88:31:13:a0:df:21:79: 9e:33:c1:ef:36:3e:af:b0:f3:5a:ba:d7:88:42:9e:43:61:cc: 28:11:a7:9a:6a:3e:99:7c:c7:61:4c:0d:54:49:02:27:8a:5f: 14:21:1a:ef:74:47:9f:a9:d0:2d:a3:d1:43:2c:d8:5b:d7:c1: 81:7a:12:5e:42:b8:fe:a7:fc:a1:7a:6a:ec:e8:06:cd:cf:a8: 90:fe:c9:0e:04:35:51:ac:a8:08:3e:75:f0:5a:2c:1c:40:99: d8:3e:93:9d:eb:49:e9:c5:f0:b2:2e:dd:5c:32:18:ae:11:3d: bd:08:22:ec:ca:1c:1d:a1:68:da:00:ee:c5:0b:f0:67:02:46: ea:4a:d0:e3:05:18:46:a0:88:ad:ad:32:61:a1:db:fa:4d:44: db:48:03:46:f5:c7:73:f2:41:e0:57:bc:06:28:c7:48:c9:a5: 15:bd:9a:39:39:4e:ec:e3

VII.4.18 CROEC des Pays de Loire

Champ	Valeur
Serial Number	11:20:62:38:1c:6c:8e:fc:5e:db:a5:90:e7:1e:7a:49:30:74

Champ	Valeur
Subject	C=FR, O=CROEC de Pays de Loire, OU=0002 332603604, CN=Ordre des Experts-Comptables - région Pays de Loire
Modulus	00:d5:64:44:b8:43:ad:38:74:c3:08:52:23:f8:66: cf:33:b3:d6:6c:91:be:57:ed:a4:45:23:9e:3e:59: e8:bc:3e:53:b3:41:96:28:5f:b5:76:b2:cc:ce:cb: 24:27:98:65:39:6d:e8:0d:65:57:9f:78:2f:a8:51: 17:d2:57:d1:e8:1b:10:f3:8c:dd:61:84:b4:6b:ca: 00:8f:1d:52:f7:4b:11:d4:35:01:b3:7f:3a:d3:c0: 56:ab:8e:fa:15:65:01:eb:f3:3f:8c:3d:75:98:0a: 1b:eb:92:8c:7e:92:cf:6f:80:87:e1:7a:62:4f:2a: 4e:49:a7:83:1c:70:26:02:84:9e:b2:ea:48:04:cf: 27:ad:e0:35:1a:43:ca:ac:31:59:49:be:84:13:c0: cf:ca:43:0e:d5:64:e8:05:d4:37:cd:78:24:2e:52: 65:28:99:48:25:31:b9:4c:25:fd:89:c8:eb:4b:2a: ee:ef:c5:70:2d:62:a4:2b:b0:bf:fc:92:b1:d8:21: b9:d8:a2:1e:b5:a8:d3:bb:5d:0c:e5:87:06:de:bd: b1:a3:b1:68:2f:1c:e0:e7:9d:0c:2b:be:ae:84:75: a2:3b:26:a1:aa:c2:2c:d0:a1:c9:8a:d5:d4:d7:a5: aa:4c:92:e1:63:60:b8:6f:fc:2d:fd:f4:73:c0:7e: 1e:71
X509v3 Subject Key Identifier	87:01:9D:D0:56:21:F8:B4:79:D6:1B:AD:38:F6:0E:E9:C2:EF: CB:52
Signature Algorithm	08:c2:d3:94:fd:3f:1d:27:2e:b5:a9:6c:f1:c1:13:35:58:27: 67:b7:2e:0b:de:3d:05:55:fc:ac:9b:2f:2a:f0:c4:80:86:15: c6:4e:4b:e4:da:58:f9:f5:bd:0a:fb:17:8b:99:38:02:5a:2e: 22:65:63:e5:0a:15:54:34:81:e6:47:b1:b4:59:60:f7:50:b1: 0e:a8:c8:0b:23:79:70:90:02:4b:76:77:b2:61:a0:3f:a8:82: 60:12:f2:fe:12:0a:5a:e0:08:b0:73:ad:b6:09:05:13:96:1c: 28:5f:f7:05:a2:83:92:5c:8e:0d:ea:43:12:7c:1b:1f:f0:7c: bb:6f:4c:b2:00:2f:d5:8b:5e:23:49:7f:50:fc:1a:1e:5d:a9: 09:31:fe:4b:10:e3:03:0b:08:6b:af:5b:a9:82:18:f9:ae:0c: 9c:e4:fd:5c:d6:26:77:c5:b2:1f:f4:9b:d7:2a:ca:6a:42:81: f3:ac:f9:25:33:dd:c7:c8:8e:f3:c7:08:e3:de:ed:9e:ad:74: 35:b6:24:f6:d5:b3:08:f6:a9:98:70:1d:0e:f4:93:7e:08:59: 7e:cf:36:e1:1b:c3:fe:10:a7:ea:c5:15:6e:07:17:a4:63:a0: e7:5e:ee:d0:b6:52:7b:a8:e2:df:f8:8f:6a:d9:34:fe:f8:95: f5:a0:ed:65:09:6d:66:24:aa:69:87:70:fa:6f:91:40:36:a1: 3f:2c:be:0b:b0:a2:ac:55:c7:71:10:0c:6b:2d:18:03:66:4b: cf:80:fc:6d:d4:74:1a:0f:c7:6e:85:67:53:19:c2:19:f4:ce: 02:29:ae:fa:ab:03:08:69:1e:9d:4d:aa:73:29:c7:1d:64:35: b2:a5:77:37:dc:e1:bf:0c:e9:ef:3d:ac:2f:24:9c:b8:0d:14: 49:f7:a8:9c:ed:aa:ab:89:16:30:c5:42:80:b1:2d:30:62:0e: 0f:78:62:36:86:8c:15:6c:6d:4b:78:c4:4d:72:c1:65:46:fa: c9:a0:1f:c6:66:e7:27:7a:90:07:84:aa:68:c3:92:41:46:9d: a6:66:b2:92:15:46:71:51:0f:e3:47:33:38:4b:cd:bd:6d:37: 70:de:81:eb:c4:34:c6:85:f7:e9:17:07:84:33:43:0c:8a:e8: 58:0c:0d:5a:f9:ec:c2:bd:f4:bf:2b:a3:b0:a6:ae:84:59:05: e2:bd:24:43:73:31:f3:53:36:bd:d0:a2:6f:95:08:ef:a3:f6: 3f:dc:78:62:3e:1a:b1:3b:b3:ee:ea:b1:42:93:cb:90:93:31: e6:68:ad:26:f4:fa:e5:c3:5d:fc:c9:e9:d8:d2:5a:88:b1:6f: 2e:44:5c:61:51:c5:3b:7a

VII.4.19 CROEC d'Orléans

Champ	Valeur
Serial Number	11:20:8f:4a:47:7f:5a:c6:0e:55:b8:59:a9:d1:c8:69:eb:97

Champ	Valeur
Subject	C=FR, O=CROEC d'Orléans, OU=0002 775501364, CN=Ordre des Experts-Comptables - région Orléans
Modulus	00:b8:57:25:23:62:93:7c:e1:ee:a7:4a:3f:88:4a: 01:23:fc:96:14:78:a6:5c:c0:f8:dc:e4:c5:f7:a8: 09:a2:8e:3c:e3:c2:2c:dd:af:98:13:c6:20:1b:7e: 3d:3f:06:29:df:de:c9:b3:86:4e:c8:b1:01:5a:c5: 7f:c1:f2:3f:11:48:80:27:17:80:fc:28:b0:b5:cc: 6d:ff:b7:7d:f2:96:51:6a:1f:d5:8c:b8:ec:b3:3a: 3c:69:ef:cc:b0:fd:13:e1:e5:f0:db:ed:83:00:a2: 1e:96:2c:76:27:aa:11:ea:81:c6:3a:e3:92:5e:49: 1f:d1:5e:96:cf:c1:5b:a0:e8:e8:8c:58:fc:a1:f5: f8:8c:ea:3d:22:aa:51:c9:16:ab:8e:59:d5:8b:1b: 68:1c:f7:47:01:77:29:d8:d9:fa:71:e9:e3:72:01: 00:a7:e9:f9:77:c8:27:e2:8e:db:12:85:f3:51:03: 0a:d3:27:f1:2f:50:11:fe:72:be:dd:50:4a:17:33: 25:6b:5f:a3:be:f4:0e:ff:34:4f:24:41:da:1d:21: 4a:4e:73:51:d1:e5:63:72:57:7b:bd:ee:70:9d:a8: 3c:d9:ce:7f:2d:e2:9f:9d:22:33:6f:6d:35:73:4e: 4a:a4:46:02:61:a6:e6:cf:ff:16:36:34:70:82:5e: 5c:99
X509v3 Subject Key Identifier	66:37:E9:35:66:E6:28:9D:B2:35:04:41:D7:88:3C:77:AC:F4: 81:33
Signature Algorithm	1f:46:cf:c2:f9:6c:a7:b2:45:87:a2:f8:e4:bb:a5:4d:79:32: e1:32:f2:d0:61:c2:d9:33:0b:ea:b7:d2:39:a2:6b:fb:b8:60: b0:27:4a:03:41:99:11:18:f2:6e:05:5a:61:e6:ea:a4:13:2d: e3:a7:59:f4:fd:62:fe:be:a1:65:55:0b:7c:c4:af:01:d2:d3: 22:6a:e9:81:40:53:0c:02:22:67:e7:b6:b3:71:9f:6e:ff:a0: 6f:90:33:0f:35:31:a2:55:14:cf:d4:c2:69:af:cc:a9:d7:dd: 58:93:ae:7f:6c:aa:54:85:ba:ea:7c:24:8f:9a:4e:bb:73:af: 45:ea:15:47:e7:41:0c:7f:a7:df:9b:15:3e:32:51:9a:ed:26: 5a:09:53:b5:0e:61:08:a9:55:e5:0c:6a:1c:c3:03:06:d4:26: 21:7a:f1:6c:68:5d:f5:84:1a:40:53:42:ab:9d:fa:06:9a:d4: 2d:11:6e:d0:76:c1:ad:ad:f1:cd:90:01:17:ba:72:ba:38:4a: 2a:a4:50:0e:53:54:c2:6b:db:32:3b:b3:2c:84:36:f1:44:1b: 34:b4:da:e0:b6:ee:13:cd:3c:11:1d:ce:4e:a0:60:81:61:67: 5e:9d:2b:5f:3e:97:0b:8d:1d:f4:a2:7f:13:31:c7:34:c1:82: cb:d7:f0:92:da:8b:00:61:6c:28:60:73:42:eb:42:55:b1:63: ce:7a:08:96:27:74:7f:50:b5:2e:b8:02:88:4f:78:c5:60:22: 19:76:dc:79:05:c6:75:b4:00:d9:2e:37:47:ef:15:91:ca:64: 73:f7:15:89:ef:a1:dd:f1:2e:31:b1:ac:9c:42:43:3f:14:b1: c7:f9:91:c1:90:ff:66:50:0d:8d:26:b6:28:1e:ae:d9:5d:83: de:b7:e6:24:d6:7b:ed:5a:ce:a4:82:c5:a0:92:32:57:d5:05: 80:72:5f:b4:88:b8:48:11:56:85:f6:92:4e:46:06:08:67:ac: d3:9a:95:69:54:8b:c2:4e:2d:a8:40:2f:9c:78:d2:4d:a1:7e: 22:d2:e1:46:41:00:e5:97:55:c0:be:34:36:b2:6b:6b:f7:73: 51:8c:73:81:bb:90:7c:ba:29:96:b0:07:06:63:e7:04:ee:d6: 79:fb:ab:8b:eb:24:4d:7c:f4:50:6c:3a:fe:c1:e9:d3:8f:17: 71:f7:de:86:51:b3:96:59:c4:64:71:98:8a:a9:f5:6b:da:8d: c8:49:58:cc:a4:aa:37:1b:38:ba:5e:b7:0b:dc:49:2f:95:93: 99:88:47:f8:b5:0d:3e:ac:fb:2f:69:10:02:a3:06:3f:2f:c5: ef:66:1f:b8:42:ce:93:e6

VII.4.20 CROEC du Nord Pas-de-Calais

Champ	Valeur
Serial Number	11:20:d5:0f:29:43:03:15:ca:2a:4c:17:b3:72:dc:38:3e:87

Champ	Valeur
Subject	C=FR, O=CROEC de Lille Nord Pas-de-Calais, OU=0002 380182212, CN=Ordre des Experts-Comptables - région Lille Nord Pas-de-Calais
Modulus	00:bb:00:91:3f:1b:46:7c:ae:52:e0:1b:b7:e8:f3: ee:35:2a:1f:1a:c2:71:df:56:f3:15:6e:49:d1:af: 23:cc:cd:cb:05:1f:fc:f1:82:d3:1a:f0:d2:6b:71: e7:51:ba:c4:2a:b5:23:74:08:a3:03:df:fb:2d:67: 48:a2:4b:4f:cd:7c:72:f1:c0:ed:4b:75:05:16:2b: 7d:bf:47:38:6f:55:5e:55:f9:f4:00:2d:ab:d5:ee: b7:79:dc:fc:6f:02:15:14:a4:51:89:02:55:d3:84: 8b:49:cf:5a:5c:aa:dc:10:10:b5:3e:e9:cb:53:e1: a3:68:57:bd:d6:78:29:0a:59:c7:c0:f8:ff:1a:22: 92:54:fc:a9:3a:37:04:3d:78:b8:10:66:c8:88:59: 79:bd:fa:b9:a5:b0:e0:01:99:73:62:80:6c:ad:94: 82:e8:90:06:cf:d8:67:68:33:69:8a:68:0d:93:67: 02:d9:14:7e:ac:c8:f4:30:5a:a3:f1:ce:84:50:c9: 2e:92:79:4e:a0:27:bf:eb:f0:ff:ae:ac:81:6d:18: 6d:70:82:1f:3b:32:82:9d:c1:6a:3b:4d:ab:03:ba: 2c:26:f8:4b:c7:fa:e9:64:b1:b3:af:cb:2a:42:9e: 8e:43:df:7b:91:c7:b1:c3:64:b1:22:15:32:f0:5b: aa:6b
X509v3 Subject Key Identifier	10:EC:81:AD:4E:45:ED:99:38:BD:97:23:6B:05:E2:36:5F:D7: 2B:EC
Signature Algorithm	54:8b:f2:62:a4:29:56:e6:f0:24:09:69:57:0e:f8:10:09:61: bd:16:8f:ab:0b:f3:66:c5:3d:7a:46:64:54:3a:4d:05:4b:01: b5:bc:a9:81:4f:35:69:0d:fb:5b:15:d0:03:8a:a2:3c:68:af: e9:d3:77:2e:4a:7c:c2:02:ce:6f:e5:cd:94:21:d2:a1:2d:88: c1:ee:fe:35:70:d1:32:c2:e3:27:d2:d3:55:f9:50:88:dd:cd: e5:0c:b7:19:fb:c3:22:cd:ce:dc:60:7e:05:d1:20:61:67:3e: 38:d2:83:d2:6e:66:48:37:fa:34:1d:79:5f:21:2a:fd:4d:9e: de:8a:8d:5e:74:6a:15:3f:a4:4c:fc:6e:e4:8a:e8:4b:c8:51: cb:19:db:7d:f8:e3:d4:4a:d6:33:ff:e2:d5:5d:91:39:93:fd: dc:ff:30:91:c3:c3:26:22:39:af:64:44:d4:06:59:ec:82:ff: 60:dd:7c:be:3e:d9:7d:8f:b3:48:99:13:56:1a:c0:2f:2b:0b: 24:0a:46:a1:6d:5f:8f:66:ce:d4:98:4c:11:b0:5f:3c:4c:6e: 18:d3:94:f2:1f:9d:94:d8:56:a3:ba:0f:fc:56:82:66:9f:d7: 86:51:48:12:a6:16:0e:ca:1a:ca:04:ed:3d:e6:5b:4d:dd:2d: 85:d9:39:7c:10:7a:90:db:48:2d:b2:c1:85:7e:ed:7b:26:57: 06:6f:d6:07:c6:4e:9b:ed:04:e6:67:96:e0:02:f1:85:f9:1b: 6b:1a:37:04:0f:e4:e1:50:56:79:a0:b7:77:a4:e5:c5:63:f9: 12:a5:e0:17:75:54:2e:b8:58:0d:4f:9b:a9:a2:fc:98:44:f2: 47:93:4b:c8:b1:ab:80:69:78:2e:c7:10:74:bf:f1:45:7c:63: 47:9b:56:cd:ed:bd:81:a0:6a:47:e6:f8:f3:01:57:67:dd:e6: 5b:21:96:17:33:5a:b9:7f:be:2a:03:6c:b2:4d:10:84:da:c4: 46:f2:6d:4a:9f:22:08:60:8b:a2:45:85:87:0b:d1:34:a2:0d: fc:55:91:bf:9c:f9:24:74:6b:c5:a4:f3:d7:d8:34:e6:29:0f: bb:20:14:9e:1e:82:81:e0:76:fd:ed:57:0e:3e:8f:12:ab:f6: 8c:b9:e0:a1:4e:3c:97:c6:0f:4f:b7:a8:47:bb:a1:bd:2e:ba: 0d:25:33:f0:98:ea:e2:66:99:5f:89:74:9a:c9:1f:ac:df:d9: 4f:ec:5d:3b:89:7e:0a:a7:3d:cc:b2:b0:77:2c:64:d4:e7:3c: f6:50:57:8f:e5:2f:bc:c9:f0:cb:41:a3:2b:4f:5e:e7:35:8b: 23:b6:cf:b5:ce:7c:d9:e5

VII.4.21 CROEC Marseille Provence Alpes Côte-d'Azur

Remarque : la période de validité de cette biclé est différente des autres (cf. I.2.1).

Champ	Valeur
Serial Number	11:20:ac:42:c6:09:21:09:bf:c2:7a:88:07:fb:ae:77:17:9d
Subject	C=FR, O=CROEC de Marseille PACA, OU=0002 782825046, CN=Ordre des Experts-Comptables - région Marseille PACA
Validity	
Not Before	Sep 25 00:00:00 2012 GMT
Not After	Dec 31 00:00:00 2019 GMT
Modulus	00:de:50:f0:f2:be:f1:e4:d4:30:2c:4e:5b:39:84: 25:43:c0:be:9b:23:88:80:26:0e:c3:b1:ba:4e:28: d6:f0:31:fd:a2:f0:3f:67:8b:07:28:26:fa:76:a2: 95:22:25:29:e5:d5:33:af:2c:c8:b1:60:69:12:4b: 78:99:30:d0:fa:87:15:07:85:d6:f0:3c:2b:1c:be: 56:af:9b:a1:75:a6:b7:db:10:7d:33:5a:0e:be:bf: ee:b7:49:67:a9:c7:e5:08:95:67:2a:ef:da:24:29: 78:84:8a:06:d2:ea:af:eb:45:3c:6f:2b:cb:db:21: ee:5e:55:59:ae:24:b1:ab:11:8c:88:7c:fc:8c:24: 93:37:87:e6:c2:6a:cd:5d:5a:d5:88:e8:c3:31:91: 67:18:e6:ce:d3:d3:ef:95:2d:00:e1:46:5b:3e:96: fb:45:0e:cc:16:30:90:53:1e:d5:76:07:0c:69:79: 75:06:db:ac:66:21:10:f2:ff:93:66:a1:2d:5e:c5: 2d:ca:f3:d0:c6:a0:a6:5d:98:13:20:4b:54:20:32: b6:c7:18:84:49:e6:fd:73:20:ea:b1:d7:63:81:4d: 43:f3:3c:dd:1e:53:c5:3e:bb:5a:a8:ab:91:40:ee: 9d:cd:b2:84:85:09:e5:ed:6a:92:d9:ba:95:63:c3: d6:9f
X509v3 Subject Key Identifier	8C:B3:F2:CC:9D:74:9A:AE:55:13:DE:05:D6:5B:E4:5D:0D:7A: 87:81

Champ	Valeur
Signature Algorithm	16:38:ac:fe:40:4e:1c:13:2a:7c:eb:ce:7b:9d:67:05:14:53: 3c:cb:df:d9:bd:3e:13:89:c8:4f:7f:51:13:00:b3:ea:a2:90: a8:bd:47:df:49:52:e1:a1:4a:91:a1:9b:e5:11:f1:2f:7c:87: cb:87:f1:22:8c:65:a0:91:8e:4f:e9:e7:59:e7:c6:b5:f0:38: df:2d:fc:4c:e3:0b:84:4d:24:8c:de:5a:b6:73:c9:d5:13:f7: 25:9b:6a:21:2c:4f:02:bd:6c:73:b3:6d:71:93:af:ab:7e:80: 41:3d:16:29:9c:48:d2:e7:4a:fd:63:ac:1e:58:f0:28:23:56: 46:8b:f8:c0:2a:66:11:cb:04:75:63:38:50:3c:9b:b1:e5:0d: 52:2f:67:58:b4:20:e1:28:8f:40:8e:49:e4:bd:71:0f:db:8a: e4:fe:c3:66:15:8a:40:09:8d:f6:7a:7d:dc:aa:b9:0e:59:55: 89:2a:26:70:af:60:ef:65:e0:cb:14:47:cb:aa:c3:47:7b:9c: 5f:38:24:dc:e0:de:c4:ca:bf:db:2e:8f:3b:d2:29:09:60:4c: c3:1c:36:3c:d5:15:a8:8a:f8:05:5d:e7:96:33:d0:df:23:38: b5:e8:95:1c:e2:4c:48:98:01:f3:0f:0f:a6:60:87:8d:60:04: 90:61:e1:47:64:e4:fb:68:4d:cf:12:ea:9e:47:71:70:40:54: 73:ae:12:62:1a:6b:7e:6c:8f:32:6e:58:4d:73:81:5c:e4:77: fd:29:3c:f4:48:1c:99:c5:a8:bd:68:0e:67:ec:bf:15:a1:a2: 39:d9:de:23:84:00:5e:61:c4:f3:3e:6a:ec:09:5e:7d:ae:bd: ab:58:bd:76:b3:3e:26:cf:4f:d6:5a:5f:b7:d0:14:04:31:16: 4a:cc:75:ff:32:03:55:d9:79:3e:9f:02:d7:49:79:3b:ee:8b: 91:b8:8d:a5:d0:04:e0:79:ed:c3:e5:82:dd:42:a1:52:c1:d9: 34:e8:dc:6f:b1:23:d3:94:6d:de:76:a7:47:02:54:19:cd:ec: 6e:66:67:09:68:57:7c:8b:db:19:af:02:9c:84:a0:f1:71:41: 47:90:ef:73:60:8b:2c:44:e3:d8:b4:75:f3:67:7d:55:2d:56: c1:8e:f6:ea:6c:ae:e0:08:ab:71:b9:60:2c:88:ea:78:80:c8: 3a:f2:c2:40:eb:24:51:bd:90:2d:a3:ec:bd:41:a0:3a:6f:1a: a9:c7:7b:e3:6d:96:90:2b:79:b8:e1:dd:96:6f:03:d3:6e:0d: 59:28:9c:06:3b:57:73:57:86:72:77:cc:e1:5e:a3:77:6b:11: 16:7d:72:75:d8:1e:3e:d6

VII.4.22 CROEC Marseille Provence Alpes Côte-d'Azur Corse

Champ	Valeur
Serial Number	11:20:fa:43:b5:de:6b:db:6d:11:75:95:79:56:40:44:63:3c
Subject	C=FR, O=CROEC de Marseille PACAC, OU=0002 782825046, CN=Ordre des Experts-Comptables - région Marseille PACAC

Champ	Valeur
Modulus	00:ae:03:6b:20:58:9e:db:92:20:8b:3b:4d:0b:b9: 52:fc:de:ff:70:0b:06:ba:f6:64:3e:a3:66:39:01: 62:1e:a7:52:7c:f6:2d:b8:0f:f0:b1:1a:80:19:5a: 77:08:d8:67:65:bd:6c:72:31:f7:ed:d9:f9:4e:a1: 9c:fa:a3:e5:0c:2e:33:ce:61:87:53:5e:fe:43:41: ac:e8:e5:31:dd:c3:d5:f5:3a:9e:9d:7d:3e:f8:79: 2f:31:1e:f5:bb:88:4a:15:23:dd:cf:9e:20:f6:53: eb:17:7c:cd:31:dc:60:3d:e7:5b:aa:d1:09:11:68: 52:ca:bc:3b:af:fe:b4:b4:98:9e:24:bf:43:6f:e8: 8a:92:c5:cf:37:6d:5a:2e:cb:a8:36:0d:f7:13:46: 26:2a:d6:0b:3f:e7:c2:77:2c:12:d8:5e:43:35:69: 95:97:50:aa:3f:ac:72:3c:2c:02:1f:fc:a6:89:98: 74:2e:88:83:6c:2a:5c:46:32:0b:3d:d1:8b:69:7a: da:fb:a0:2e:9f:0d:e2:98:9d:00:ac:ba:2f:c2:e1: 54:68:4b:8a:64:fb:18:d3:01:62:eb:8d:92:90:82: 99:6c:d8:09:9a:61:9a:d1:f5:8b:9c:8a:18:1d:c8: 95:23:16:d9:a0:60:da:ce:d6:f3:9b:47:d3:49:bf: 2f:5d
X509v3 Subject Key Identifier	59:3D:71:E7:B8:E6:83:B7:05:E4:07:AA:C1:F3:15:4E:47:1F: 87:3F
Signature Algorithm	03:96:95:ac:9d:6c:c4:be:2d:65:fa:42:31:b0:80:e4:44:c1: 65:95:73:f4:20:52:98:0e:72:65:7b:53:82:ef:c1:e1:36:d1: cf:a7:ce:c0:70:b5:27:f9:48:0d:3c:94:4e:aa:36:57:9e:f7: b6:50:72:7b:70:bf:40:fe:fb:38:79:f7:dd:23:da:38:97:13: a1:71:67:68:6b:6e:46:d3:0c:8a:02:bc:b9:f0:fd:77:a2:be: 00:f3:a1:b5:db:06:7a:14:9b:26:50:80:b7:c0:40:63:8c:7d: 5e:44:8f:b1:6f:c1:39:7e:f6:30:c5:93:76:64:26:6e:93:6a: c8:ef:06:0c:f2:9c:dc:70:ac:54:ac:4c:50:73:a5:c0:6d:2e: 69:3c:ca:db:79:d5:38:7c:f6:83:07:c0:ff:c7:e2:a9:06:2a: 8e:00:1d:a6:4c:0e:3b:30:1d:19:f4:58:3d:5e:a5:80:01:69: 2a:06:6f:eb:97:3f:63:39:1a:2f:4b:80:d3:1f:42:6a:eb:1e: dd:6e:dc:ab:f5:30:bd:c7:5f:0a:c3:bb:58:12:37:90:8a:8f: 40:cd:f2:e2:02:25:4b:4a:54:30:d3:3f:4f:6e:5f:12:f3:f9: 3f:92:fe:e7:a9:5a:99:68:53:0b:38:27:de:c5:14:d0:b9:d2: 81:6b:d5:4d:d0:a4:a7:21:e9:5d:48:69:83:8b:c7:d8:23:25: d2:59:87:58:0b:e3:0b:50:36:57:d2:8c:9d:d1:a6:04:cb:29: 27:05:ba:9b:ac:5a:42:28:a3:41:2b:ba:e8:71:68:c6:64:e9: d3:59:7f:ab:97:d5:3d:2d:f0:72:af:5e:58:19:a4:77:40:3b: 5f:97:37:9b:a4:b4:42:de:ef:94:f1:3e:0e:4e:5b:92:06:3f: 21:49:90:62:32:fc:dc:8d:61:65:4f:c6:40:47:53:99:a1:74: 5a:44:e8:c2:da:97:6d:7f:70:8d:dd:90:77:2e:51:a2:47:68: 7a:13:fa:4e:b7:07:a1:f7:46:c3:7a:25:e3:dc:19:4e:ca:a5: 7d:ec:f3:05:7b:ac:bc:2e:7d:ee:62:40:82:59:70:3a:57:dd: 13:93:01:36:da:ef:4b:e8:8a:46:26:83:b8:3c:14:ca:74:b0: 05:7d:d1:04:af:e2:ec:25:cb:ea:ae:e1:ff:e1:53:eb:fb:a7: d7:4e:55:15:bb:e3:bc:39:67:3e:41:66:a9:f2:c5:93:ce:40: 2a:d4:a5:3a:7d:cd:22:e5:1a:d8:38:03:ec:5a:96:ae:ad:cf: ce:56:0d:cf:56:9c:78:8a:4a:86:33:98:1c:05:44:e5:09:96: f7:24:76:18:83:86:fc:59

VII.4.23 CROEC de la Réunion

Champ	Valeur
Serial Number	11:20:b2:8d:49:df:ec:33:59:31:fd:9c:08:03:15:d7:48:9a
Subject	C=FR, O=CROEC de La Réunion, OU=0002 322951443, CN=Ordre des Experts-Comptables - région La Réunion

Champ	Valeur
Modulus	00:bf:d7:20:14:c3:45:ee:4c:8e:9d:15:80:b1:8e: 56:e9:85:43:49:bb:ff:37:fb:69:df:c7:4a:02:6d: 8a:f1:44:cc:78:c0:ae:24:25:7f:46:21:f0:3e:7a: a7:00:ae:32:55:76:fb:5b:02:f9:04:0c:d9:8c:a7: 34:14:8b:99:68:97:a1:c8:0d:f1:e9:17:0e:42:7a: 64:55:6b:be:2f:be:2d:fd:cf:5b:fa:39:ca:8f:2d: 71:00:af:b6:b2:af:82:26:6c:50:fb:53:f8:09:51: 84:47:7f:da:28:74:22:20:be:dd:cb:79:2a:b0:20: c2:90:0a:4a:17:1e:2c:c0:71:f0:4b:bf:76:e6:09: 98:61:3b:38:fb:e2:1d:50:4f:e4:a9:5c:48:1b:14: 3a:c5:7b:49:aa:70:59:ac:ed:f1:20:aa:8f:b9:07: da:15:17:fc:96:d0:ae:65:62:e0:c6:9f:5d:4a:85: ba:25:e0:85:de:54:5c:5a:03:3e:ae:e6:47:ee:9c: c4:0d:d1:df:c5:22:64:e6:64:a4:d2:50:23:e8:62: 51:da:61:27:fc:a8:a8:ea:82:82:da:96:96:21:4b: 02:34:14:c9:ca:79:48:aa:23:66:a1:b9:14:ae:18: 24:98:c7:cf:a4:98:20:d1:4e:e2:0c:3f:9b:a7:10: c5:dd
X509v3 Subject Key Identifier	7D:FF:03:04:97:75:18:A3:BD:26:03:AB:9B:A4:79:A4:3A:54: 8A:89
Signature Algorithm	66:d0:49:e8:51:85:d7:59:aa:a0:9a:1d:f5:12:e5:0a:e5:48: 65:91:04:c1:7e:a5:1b:f4:26:d6:1f:76:19:28:a3:29:70:e1: 30:c0:51:74:b1:3a:0a:9a:70:17:62:83:94:23:7c:8b:16:0f: 49:a4:3e:f4:4a:88:1c:60:33:d1:74:ba:c5:43:02:cb:67:a6: 5b:6d:d7:77:d5:ea:3d:d0:33:59:7b:50:b6:d1:21:46:93:5c: 9c:47:cd:0a:be:37:14:5b:cf:ed:c2:fd:56:91:2c:51:c7:98: d1:5e:a9:ac:f1:d1:63:11:de:a8:1d:be:7a:c7:93:42:c2:42: bd:6f:6c:11:05:76:f3:02:68:b1:82:89:d8:aa:22:99:f2:14: dc:0e:3d:61:47:b2:18:07:89:27:4b:f6:6d:d2:78:7b:0b:91: 09:99:dd:22:9e:6b:fb:96:d1:3a:7b:59:ee:0d:3a:19:78:71: 70:dc:d3:aa:25:98:4d:56:c2:30:c9:81:50:05:91:ff:9b:77: fa:b6:f9:8a:b3:74:fc:02:28:76:65:f8:d1:8a:50:b4:d9:eb: aa:de:71:9f:7a:03:43:b4:87:50:c2:c9:e1:6d:45:55:96:2f: 5d:70:c4:4e:1b:87:9c:12:2f:38:e6:e2:40:c9:d3:70:92:ac: 9a:d1:41:cf:40:61:8d:88:0f:67:01:2a:5e:aa:54:65:a1:13: da:cc:19:3f:7c:1e:06:8d:83:3d:b6:89:be:81:05:6d:ac:f1: 15:af:35:3d:54:b8:7f:a7:a0:08:35:ca:88:d4:fa:29:6a:e0: 9f:5a:7a:f4:bd:40:83:d8:15:6d:ba:27:f0:8e:23:58:ca:7f: 7b:56:39:a4:d2:68:81:cc:97:8a:87:51:49:60:9a:34:74:2e: f6:ee:42:86:fe:27:46:30:5a:1b:74:6b:49:fc:2d:ad:d0:bd: f8:7b:f2:51:f9:9f:92:93:b7:fd:fe:cf:80:81:25:ff:46:51: 51:19:e2:bc:5f:e1:c7:7d:d3:e7:d2:a9:58:f9:b8:a1:bb:82: a4:65:aa:59:6d:c4:f9:46:1b:a7:a3:73:3c:97:ce:16:3e:30: 3a:17:ae:52:78:15:1d:3e:8b:f9:3a:12:ca:82:ae:59:a7:b9: e6:f9:01:6c:1d:04:c2:98:46:d5:38:ad:69:38:a8:d4:85:97: 7d:eb:6b:e0:29:7f:ca:2b:c9:9b:82:3e:92:2a:7d:7f:ee:dd: 20:43:34:3f:af:23:6b:f1:d2:01:b8:a7:93:80:0e:fb:b8:36: 14:11:44:61:47:c2:8b:84:9a:a9:b8:c7:00:15:d1:a2:28:30: 64:f4:a9:66:b8:f2:e6:a1

VII.4.24 CROEC de la Martinique

Champ	Valeur
Serial Number	11:20:fa:43:b5:de:6b:db:6d:11:75:95:79:56:40:44:63:3c
Subject	C=FR, O=CROEC de Martinique, OU=0002 382052538, CN=Ordre des Experts-Comptables - région Martinique

Champ	Valeur
Modulus	00:d5:7a:ec:02:17:23:1e:d6:37:d1:4f:e7:8c:3c: 9c:2f:77:0b:e7:b2:d7:80:93:89:8c:a2:f7:13:0f: a8:a4:6e:7d:de:df:31:48:3a:b0:8a:dc:98:1e:de: f6:df:83:4a:50:3e:07:75:c9:67:ea:31:26:05:97: c9:9e:7d:4f:1a:97:58:55:2a:cc:13:27:10:ab:52: 01:41:01:7e:0c:53:df:a0:86:e8:f0:2e:0a:9b:22: 8a:34:48:23:74:72:26:26:98:92:a3:5b:f0:c8:1a: f3:e2:5b:71:7d:6a:91:b9:ae:6e:cf:4b:9e:2f:f7: 48:c3:ee:6e:e4:b8:5b:ec:da:a3:ad:eb:b3:1e:b9: d8:c9:c4:32:58:4b:6c:67:e2:29:ee:48:03:5d:47: 6c:f6:67:45:fc:22:1c:c0:ba:91:fe:bc:34:29:86: 2c:af:cf:04:0b:ea:48:3a:b2:16:ba:b1:3a:04:e4: 31:fd:cb:aa:6c:fa:81:09:13:33:c1:e6:61:ff:c9: 19:8f:17:aa:36:d5:2e:43:ae:4d:71:4e:d1:a5:80: e7:8d:51:aa:96:d0:14:7e:f2:bf:98:b3:9a:8e:03: 8e:d4:a4:40:7f:07:16:fb:12:9f:dd:57:b7:9e:7e: f9:cb:3f:72:c0:83:9e:5d:67:fe:62:0e:70:fb:cb: fe:67
X509v3 Subject Key Identifier	59:8B:1C:77:58:89:7C:6A:B6:1E:F5:80:F2:8C:63:54:E8:99: 1C:33
Signature Algorithm	90:10:be:e1:c7:cb:ad:ce:39:b0:0f:82:bc:c3:75:9f:c5:e9: 94:c0:a8:e7:3b:63:c1:75:9b:9b:58:88:ce:a6:91:08:77:89: 37:3b:f9:df:ba:9d:1d:47:bf:c8:e5:69:c3:56:63:8b:0f:46: 46:3f:d8:00:2a:c2:4e:1f:67:cd:69:43:a5:c7:8d:b2:a9:ed: a8:22:6e:d3:7f:17:17:5d:0f:12:95:55:8f:8d:76:70:97:38: e0:58:62:55:7f:97:c8:7e:29:10:bb:b1:92:f9:10:41:b2:e5: db:7a:c5:5a:2e:17:3e:f4:05:c9:7b:56:90:1d:85:d5:39:0a: 7a:c0:c4:c0:89:bf:ca:81:50:00:17:1b:ca:c9:47:9f:cf:4b: cd:60:e1:dd:68:90:a0:b3:ef:bd:22:92:61:99:86:9b:d1:a0: e8:c3:5e:a4:b7:a9:d0:97:07:21:94:52:35:8d:39:97:d0:79: ad:1a:d6:8c:a0:6b:db:36:f1:85:65:1b:b0:8a:64:c4:ff:3e: 70:be:37:cf:1e:f7:53:dd:2c:1a:4c:b0:a8:95:b0:4c:f7:3a: 38:23:c3:a4:c7:d0:09:e0:89:27:15:2b:b1:08:cb:a3:a2:42: 84:4a:4a:59:a5:91:0f:ff:45:0d:9a:28:89:e9:1b:09:18:fe: da:4e:f6:47:4a:ac:15:44:73:a8:78:02:c7:88:e2:ba:ed:f0: c2:e0:64:03:4c:fc:4c:a1:9a:81:0e:60:87:6b:ce:70:89:8d: b5:4a:53:7f:f6:7e:61:14:7f:a3:62:3e:bc:8c:ac:bf:e2:51: cb:81:d7:85:68:2e:bf:d8:d3:61:9b:43:bf:33:29:69:5d:e3: 6e:1c:2e:01:41:20:a5:b8:3a:d2:1e:f1:2e:b5:79:7a:18:35: 1f:92:98:51:af:1a:8a:36:8b:87:86:8e:30:17:8c:cb:1c:93: d2:2a:08:c5:46:cc:19:e3:6c:8d:55:57:b0:67:23:f3:23:68: 6c:eb:83:0f:06:db:d0:25:7e:94:29:3e:85:0f:93:8d:2c:d1: 00:39:44:70:41:e6:b1:bd:5c:18:2f:7e:77:4d:e3:c7:07:84: ce:74:8b:46:2d:1e:65:ce:54:c8:e4:cf:f7:83:f9:6b:79:7a: a0:3e:12:cf:a4:5d:9d:22:bc:6a:4e:c1:c1:94:97:2a:f1:35: eb:e0:4f:eb:30:b2:e1:d1:d8:76:ae:36:69:76:9c:84:f7:9c: fe:f6:50:3b:9a:7b:d5:02:4d:5b:36:b4:51:f9:33:2d:81:a5: 5f:3a:86:34:88:5b:54:7c:c1:18:a8:d6:bb:7c:b4:04:ff:69: 54:ae:67:18:29:a0:49:40

VII.4.25 Comité départemental de la Guyane

Champ	Valeur
Serial Number	11:20:d5:0f:29:43:03:15:ca:2a:4c:17:b3:72:dc:38:3e:87

Champ	Valeur
Subject	C=FR, O=CDOEC de Guyane, OU=0002 508714565, CN=Ordre des Experts-Comptables - comité Guyane
Modulus	00:b8:16:bb:74:19:c8:0e:7a:34:57:95:31:6c:4b: e6:dc:f3:0c:f8:9c:ba:fc:da:3a:ad:e5:e0:b2:29: c0:74:63:bb:8e:5d:0a:03:b4:48:94:a9:47:4e:3b: a0:4b:57:f0:ea:8e:c9:4d:6e:89:ab:16:ab:4d:fd: 20:84:c4:31:69:e0:1d:2d:07:b4:ab:1a:43:dd:14: f2:88:8f:bd:d7:36:21:ae:d3:a8:0f:06:7e:76:52: 42:a9:51:9a:ef:61:35:84:f9:f1:bd:ed:cc:b1:ce: 18:ba:18:67:0d:1f:99:8d:31:a4:5a:84:2d:e2:49: e7:e2:80:2b:18:50:88:1c:a2:12:4d:05:0d:d0:7a: 7c:5c:a9:3a:5a:97:17:7e:3e:b6:37:87:68:8a:d7: 4f:c0:e8:1d:0a:0a:58:92:9f:9d:2b:c3:38:e4:7d: 7b:f1:99:c9:02:b7:19:28:dd:d8:49:91:2f:30:65: 0d:86:e0:3d:46:af:6e:94:f3:7c:8a:70:94:89:94: 22:49:07:6d:14:5e:bc:9c:ad:52:bd:ef:2f:8a:87: 28:c0:9b:0b:b4:94:c1:5a:9b:13:b0:4d:64:9a:7f: a3:ce:53:fe:4a:c4:0c:8c:1f:07:fa:6b:a4:89:92: 34:37:4b:02:7b:06:33:69:ee:ec:c8:09:f3:77:8f: 8d:13
X509v3 Subject Key Identifier	7C:02:B4:42:8F:DA:50:A1:05:BB:96:85:8D:FF:94:1E:14:B8:2A:72
Signature Algorithm	5d:f5:42:c0:1f:da:ee:4a:72:14:8d:63:9b:ff:47:e8:b2:ec: d0:a7:11:a1:ac:6d:d4:cd:85:37:7a:5c:3c:ca:d7:f8:67:92: fc:86:6b:0e:cd:d0:7a:7c:0e:f6:df:ba:af:f7:72:53:c7:e7: 11:fc:29:1a:4f:62:22:a1:36:f4:6b:99:a5:28:21:98:23:23: fc:83:d3:81:6a:51:26:80:c6:5e:dd:53:4d:c7:0d:d6:8e:c5: b4:c9:d8:16:86:c1:e2:e0:10:05:d2:7c:4b:c9:27:1f:bd:9f: a8:1e:a4:56:7d:2d:78:98:42:61:2e:4f:bd:c9:cb:68:ab:a2: 6f:da:12:2b:80:d8:bc:ac:8a:40:d2:e1:37:c5:ea:12:be:92: 78:dc:57:1f:32:be:12:61:fb:25:c9:d5:c2:a3:5c:e2:fd:68: e5:85:a1:a1:34:cc:a5:3b:fa:d5:b6:40:bf:3f:68:20:42:7f: 9b:29:15:08:53:aa:e1:77:03:6d:84:9e:06:8a:da:01:f6:c7: 72:43:ab:b4:20:36:78:78:2c:86:87:86:f6:ed:6d:c1:81:31: 6f:ac:d9:ce:c1:a2:7f:7b:6b:c0:34:dd:c1:42:56:19:5f:24: aa:00:7f:da:0d:d9:19:f1:e5:34:e8:d0:07:37:68:47:bf:49: 3a:c5:c1:f0:98:db:78:69:1b:09:ce:b8:76:8b:c0:5b:03:6d: 2e:fb:fa:ce:fc:d4:1a:87:0b:06:a4:6c:e9:f7:fd:63:d2:c4: 75:dc:08:b6:9a:8f:5e:b6:5b:44:e9:9d:7b:21:9b:36:d6:76: 84:1e:6f:8a:95:d6:7e:db:60:b3:61:9b:34:91:41:f7:cf:95: e0:96:be:94:ca:97:85:c9:9e:e6:ba:cd:00:f1:fd:40:53:84: 1a:b4:33:90:55:e6:1c:6e:cd:37:82:11:0f:08:f0:29:9e:13: a5:a3:c6:87:34:21:f7:75:cb:d2:71:60:c9:c6:cd:b2:05:c0: 17:68:36:24:32:2f:bb:41:44:91:bf:64:d9:03:a2:f8:7d:ef: 73:37:ae:8a:4e:c1:23:13:e7:63:2f:a1:f1:14:d2:e5:bc:d3: e6:44:28:a5:3a:8e:13:cf:04:98:56:1a:ab:6f:6e:58:bf:c9: 28:ab:2a:e5:fb:c1:ff:aa:b5:10:41:7f:b9:da:09:6b:67:a0: f8:43:57:d3:cb:05:07:19:32:74:5b:fd:7a:f6:3a:90:24:b4: 97:02:b9:f4:de:0c:02:5f:62:3f:ff:37:f4:b7:07:c9:5c:e4: 71:21:a6:c3:37:40:e3:a8:db:a9:4c:40:b5:14:fd:b8:fe:f2: 18:19:aa:aa:77:ca:ad:b6

VIII AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent,

- d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens de l'Ordonnance n° 2005-1516 du 8 décembre 2005 (schéma de qualification des prestataires de services de confiance conformément au Décret du 8 décembre 2005 précité)
- et, d'autre part, ceux que doit réaliser, ou faire réaliser, le PSCE afin de s'assurer que l'ensemble de son ICP est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

La suite du présent chapitre ne concerne donc que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son ICP.

VIII.1 Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son ICP ou suite à toute modification significative au sein d'une composante, le PSCE procède à un contrôle de conformité de cette composante. L'AC procède régulièrement à un contrôle de conformité de l'ensemble de son ICP, une fois par an.

VIII.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante est assigné à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

VIII.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'ICP contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

VIII.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'ICP (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'ICP (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

VIII.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend au PSCE, un avis parmi les suivants : "réussite", "échec", "à confirmer". Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités sont levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

VIII.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

IX AUTRES PROBLEMATIQUES METIERS ET LEGALES

IX.1 Tarifs

IX.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.1.2 Tarifs pour accéder aux certificats

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

L'accès aux LCR et, éventuellement, deltaLCR est en accès libre en lecture.

IX.1.4 Tarifs pour d'autres services

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.1.5 Politique de remboursement

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.2 Responsabilité financière

La responsabilité financière de l'AC pour l'émission de certificats qualifiés est déterminée par la loi (*art 33 de la Loi n° 2004-801 du 6 août 2004 relative à la confiance dans l'économie numérique*). Elle pourra être recherchée en cas de délivrance d'un certificat SEEC à une personne physique non membre de l'Ordre.

IX.3 Confidentialité des données professionnelles

IX.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- la partie non-publique de la DPC de l'AC,
- les clés privées de l'AC, des composantes et des porteurs de certificats,
- les données d'activation associées aux clés privées d'AC et des porteurs,
- tous les secrets de l'ICP,
- les journaux d'événements des composantes de l'ICP,
- les dossiers d'enregistrement des porteurs,
- les causes de révocations, sauf accord explicite du porteur.

IX.3.2 Informations hors du périmètre des informations confidentielles

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre IX.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.

L'AC respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au porteur.

IX.4 Protection des données personnelles

IX.4.1 Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi *Informatique et Libertés*.

IX.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- le dossier d'enregistrement du porteur.

IX.4.3 Informations à caractère non personnel

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.4.4 Responsabilité en termes de protection des données personnelles

Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.4.5 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

IX.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire français.

IX.4.7 Autres circonstances de divulgation d'informations personnelles

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.5 Droits sur la propriété intellectuelle et industrielle

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.6 Interprétations contractuelles et garanties

Sans objet.

IX.7 Limite de garantie

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.8 Limite de responsabilité

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.9 Indemnités

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.10 Durée et fin anticipée de validité de la PC

IX.10.1 Durée de validité

La PC de l'AC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

IX.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la « PC Type » du R.G.S. peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.

IX.10.3 Effets de la fin de validité et clauses restant applicables

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'ICP, l'AC devra :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

IX.12 Amendements à la PC

Les amendements à la PC ne peuvent être apportés que par le PSCE.

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) donnera lieu à une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la présente PC évoluera dès lors qu'un changement majeur intervient dans les exigences de la PC Type applicable à la famille de certificats considérée.

IX.13 Dispositions concernant la résolution de conflits

Le PSCE met en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles il fournit des services électroniques de confiance ou d'autres points qui y sont liés.

IX.14 Juridictions compétentes

Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.15 Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre X ci-dessous.

IX.16 Transfert d'activités

Cf. chapitre V.8.

X ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

X.1 Législation et réglementation

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
Décret n° 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

X.2 Documents techniques

Document
Référentiel Général de Sécurité – Version 1.0
RGS - Fonction de sécurité « Authentification et Signature » - Version 2.3
RGS - Politiques de Certification Types - Variables de Temps - Version 2.3
RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3
Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - Version 1.20
CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+.
CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)
CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP). Ce PP a été certifié EAL4+.
CWA 14169 (2002-04) Secure Signature Creation Devices (SSCD). Ce PP a été certifié EAL4+.
AFNOR AC Z74-400 "Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés" (traduction de : ETSI TS 101 456 V1.4.3 (mai 2007) "Policy Requirements for Certification Authorities issuing qualified certificates".
ETSI TR 102 272 - ASN.1 format for signature policies V1.1.1 (décembre 2003) ETSI TR 102 038 - XML format for signature policies V1.1.1 (avril 2002)
Exigences de sécurité des sites de personnalisation, V1.0 (août 2007) http://www.references.modernisation.gouv.fr/sites/default/files/Exigences_sites_de_perso_V1_0.pdf
RFC3647 - IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003

X.3 Autres documents

[PC_S] *Politique de certification « Signature » pour les A.C. de la profession comptable (AC CROEC),* Version 6.0 du 1er juillet 2011, OID n° 1.2.250.1.165.1.2.x.1.6

XI ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

XI.1 Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les biclés des porteurs, doit répondre aux exigences de sécurité suivantes :

- si les biclés de signature des porteurs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des biclés générées
- si les biclés de signature des porteurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des porteurs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de création de signature du porteur et assurer leur destruction sûre après ce transfert
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie - être capable d'identifier et d'authentifier ses utilisateurs
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées
- créer des enregistrements d'audit pour chaque modification concernant la sécurité
- si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Il est recommandé que le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.

XI.2 Exigences sur la qualification

Le module cryptographique utilisé par l'AC doit être qualifié au niveau renforcé, selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XI.1 ci-dessus. Si le catalogue des produits qualifiés par l'ANSSI ne contient pas de module cryptographique qualifié au niveau renforcé, le PSCE doit obtenir une dérogation de l'ANSSI.

XII ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF D'AUTHENTIFICATION ET DE SIGNATURE

XII.1 Exigences sur les objectifs de sécurité

Le dispositif d'authentification et de création de signature, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa biclé, doit répondre aux exigences de sécurité suivantes :

- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une authentification ou une signature qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer la fonction de signature pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

XII.2 Exigences sur la qualification

Le dispositif de création de signature utilisé par le porteur doit être qualifié au niveau renforcé, selon le processus décrit dans le [RGS], et être conforme aux exigences énoncées en XII.1 ci-dessus.