

Autorité de Certification CA Certificat

POLITIQUE DE CERTIFICATION

Version : 1

Date de publication : 01/07/2010

Référence : CA_C_PC_090401_V3.3_Politique de Certification CA Certificat.doc



Cedicam 2001-2008. Ce document est la propriété du Cedicam. Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité. Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste.

HISTORIQUE

VERSION	DATE LIVRAISON	OBJET (REFERENCE COURRIER D'ORIGINE DE LA MAJ, CHAPITRES MODIFIES, ETC)	REDIGE PAR :	VALIDE PAR :
1.0	04/05/01	Création du document	S. THIRY	D. SAVOYEN
1.1	06/06/01	Suppression des processus de re-génération	S. THIRY	D. SAVOYEN
1.2	26/06/01	Complétion des renseignements manquants	X. ASSOUD	D. SAVOYEN
1.3	24/08/01	Passe de cohérence / Mise à jour / décorrélation entre vie du certificat et notion d'abonnement	X. ASSOUD	D. SAVOYEN
1.4	28/08/01	Prise en compte remarques XDM	X. ASSOUD	D. SAVOYEN
1.5	14/09/01	Prise en compte remarques STI et DS	X. ASSOUD	D. SAVOYEN
1.6	21/09/01	Prise en compte remarques STI et DS	X. ASSOUD	D. SAVOYEN
2.0	24/09/01	Validation	X. ASSOUD	D. SAVOYEN
3.0b1	14/11/02	Mise en conformité avec la PC-Type v3	S. PUJADAS	X. de MONNERON
3.0	27/04/2003	Fin de mise en conformité avec la PC-Type V3 (procédure supplémentaire)	X. de MONNERON	D. SAVOYEN
3.1	30/05/2008	Mise à jour	S GONIDEC	G SIRE
3.2	27/03/2009	Réduction de la durée de vie des certificats	A DUCHAMP	E.POTTIER
3.3	01/07/2010	Augmentation de la durée de vie des Certificats	E.POTTIER	Membres du CAP

RESUME / ÉVOLUTION PAR RAPPORT A LA DERNIERE VERSION

Evolutions principales entre la version 1.0 et la version 2.0 :

- Le vocabulaire, les processus et les procédures ont été mis en cohérence avec les autres documents projet.
- Mise à jour : décorrélation entre vie du certificat et notion d'abonnement, prise en compte de l'offre sur support matériel, correction des erreurs de la v1.0.

Evolutions principales de la version 3.0 par rapport à la version 2.0 :

- Mise à jour des processus, procédures et éléments techniques, conformément à la PC-type version 3 du MINEFI.
- Ajout d'un paragraphe sur les certificats spécifiques délivrés aux Applications utilisant la PKI

pour leurs procédures de recette (3.10).

- Remplacement du terme « Représentant d'Entreprise » par « Gestionnaire des Certificats » pour éviter la confusion avec le représentant légal de l'entreprise.

Evolutions principales de la version 3.1 par rapport à la version 3.0 :

- Changement
 - de la personne physique responsable de la PC
 - de la personne déterminant la conformité de la DPC à la PC
 - du siège social du CEDICAM
- Ajout au §7.2.1 du code de déblocage du support materiel

Evolutions principales de la version 3.1 par rapport à la version 3.0 :


- Changement

MOTS CLEFS

- PKI, Politique de Certification, CA Certificat, Crédit agricole, CEDICAM
- ICP, certificat logiciel, carte à puce, support matériel
- MinEFI, TéléTVA

REFERENCES

TITRE	VERSION	EMETTEUR	DATE	CONTENU
PC-Type	3.0	MinEFI	Novembre 2002	Modèle – cahier des charges

	CA CERTIFICAT	N° page : 4/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

TITRE	VERSION	ÉMETTEUR	DATE	CONTENU
RFC 2527 Politique de certification CA Certificat	2.0	W3C Crédit agricole	Décembre 2001	




	CA CERTIFICAT	N° page : 5/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

TABLE DES MATIERES

1	PREAMBULE	7
2	PRESENTATION GENERALE DE LA POLITIQUE DE CERTIFICATION CA CERTIFICAT	8
2.1	IDENTIFICATION DE LA PC-TELEPROCEDURES - OID	8
2.2	LISTE DES ACRONYMES UTILISES	8
2.3	DEFINITIONS DES TERMES UTILISES DANS LA POLITIQUE DE CERTIFICATION CA CERTIFICAT	9
2.4	TYPE D'APPLICATIONS CONCERNEES PAR LA POLITIQUE DE CERTIFICATION CA CERTIFICAT	16
2.5	TYPES DE CERTIFICATS CONCERNEES PAR LA POLITIQUE DE CERTIFICATION CA CERTIFICAT	16
2.6	SUPPORTS DES CERTIFICATS CA CERTIFICAT	16
2.7	MODIFICATION DE LA POLITIQUE DE CERTIFICATION CA CERTIFICAT	16
2.8	COORDONNEES DES ENTITES RESPONSABLES DE LA PRESENTE POLITIQUE DE CERTIFICATION	17
3	DISPOSITIONS DE PORTEE GENERALE	19
3.1	CONTROLE DE CONFORMITE A LA POLITIQUE DE CERTIFICATION CA CERTIFICAT	19
3.2	RESPECT ET INTERPRETATION DES DISPOSITIONS JURIDIQUES	20
3.3	ROLES ET OBLIGATIONS DE L'ICP ET DE SES COMPOSANTES	21
3.4	OBLIGATIONS DU CLIENT	25
3.5	OBLIGATIONS DE L'ABONNE	26
3.6	LIMITATION DE LA RESPONSABILITE DU CEDICAM EN QUALITE D'AC	27
3.7	TARIFS	27
3.8	PUBLICATION ET DEPOT DE DOCUMENTS	27
3.9	POLITIQUE DE CONFIDENTIALITE DE L'ICP "CA CERTIFICAT"	28
3.10	CERTIFICATS DE RECETTE	29
4	IDENTIFICATION ET AUTHENTIFICATION	31
4.1	ENREGISTREMENT INITIAL DE L'ABONNE	31
4.2	AUTHENTIFICATION D'UNE DEMANDE DE REVOCATION	34
4.3	VERIFICATION PERIODIQUE D'EXISTENCE	34
5	BESOINS OPERATIONNELS	35
5.1	DEMANDE DE CERTIFICAT CA CERTIFICAT	35
5.2	REVOCATION DE CERTIFICAT CA CERTIFICAT	37
5.3	RENOUVELLEMENT DE CERTIFICATS (HORS REVOCATION)	42
5.4	EMISSION DES NOUVEAUX CERTIFICATS APRES REVOCATION	42
5.5	SUSPENSION DE CERTIFICATS	42
5.6	VERIFICATION DE LA VALIDITE DES CERTIFICATS	42
5.7	RENOUVELLEMENT DE CLE D'UNE COMPOSANTE DE L'ICP	43
5.8	REVOCATION D'UNE CLE D'UNE COMPOSANTE DE L'ICP	43
5.9	CAUSES DE REVOCATION D'UN CERTIFICAT D'UNE COMPOSANTE DE L'ICP	43
5.10	JOURNALISATION DES EVENEMENTS	44

	CA CERTIFICAT	N° page : 6/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.11	ARCHIVES	45
5.12	FIN D'ABONNEMENT	46
5.13	CONTROLES DE SECURITE PHYSIQUE	47
5.14	CONTROLES DES PROCEDURES	47
5.15	CONTROLE DU PERSONNEL	48
6	CONTROLES TECHNIQUES DE SECURITE	49
6.1	GENERATION ET INSTALLATION DE BI-CLES	49
6.2	PROTECTION DE LA CLE PRIVEE	50
6.3	AUTRES ASPECTS DE LA GESTION DES BI-CLES	51
6.4	DONNEES D'ACTIVATION DES CLES PRIVEES DES ABONNES	51
6.5	SECURITE DES POSTES DE TRAVAIL DES COMPOSANTES DE L'ICP	51
6.6	CONTROLES TECHNIQUES DU SYSTEME DURANT SON CYCLE DE VIE	52
6.7	CONTROLES DE LA SECURITE RESEAU	52
6.8	CONTROLES DES MODULES CRYPTOGRAPHIQUES	52
7	PROFILS DE CERTIFICATS ET DE LCR	53
7.1	PROFIL DES CERTIFICATS	53
7.2	PROFIL DE LCR	55
8	ADMINISTRATION DES SPECIFICATIONS REFERENTES A L'AC	56
8.1	MODIFICATION DES SPECIFICATIONS	56
8.2	CHANGEMENTS DE COMPOSANTES DE L'AC OU DE L'AE	56
8.3	PROCEDURE D'APPROBATION DE LA POLITIQUE DE CERTIFICATION CA CERTIFICAT	56


	CA CERTIFICAT	N° page : 7/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

1 PREAMBULE

Le CEDICAM développe ses activités de commerce électronique et s'est donc doté d'une Infrastructure à Clé Publique (ICP) destinée à fournir des certificats à ses clients. Cette Infrastructure à Clé Publique (ICP) est gérée pour le groupe CEDICAM par le CEDICAM (CENTRE D'ECHANGES DE DONNEES ET D'INFORMATIONS DU CREDIT AGRICOLE MUTUEL).

Ce document constitue la Politique de Certification de l'Autorité de Certification "CA Certificat", c'est à dire l'ensemble des engagements concernant la délivrance de certificats numériques par cette AC.

L'ambition de cette Autorité de Certification "CA Certificat" est de satisfaire aux exigences de la Loi du 13 Mars 2000 et de son Décret d'application du 31 Mars 2001, afin que les certificats émis soient à terme éligibles à la « qualification ».

	CA CERTIFICAT	N° page : 8/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

2 PRESENTATION GENERALE DE LA POLITIQUE DE CERTIFICATION CA CERTIFICAT

Ce document décrit la **Politique de Certification CA Certificat** inhérente à l'Autorité opérationnelle de Certification ci-après désignée comme AC opérationnelle "CA Certificat" de l'Infrastructure à Clés Publiques du CEDICAM gérée par le CEDICAM.

Une Politique de Certification (PC) est identifiée par un nom unique (OID*). Elle est composée d'un ensemble de règles décrivant les conditions de recevabilité d'un certificat pour des applications ayant des besoins de sécurité communs.

Une PC est définie indépendamment des modalités de mise en œuvre de l'Infrastructure à Clés Publiques (ICP) à laquelle elle s'applique. Elle décrit les exigences auxquelles l'ICP doit se conformer pour l'enregistrement et la validation des demandes de certificats, et pour la gestion des certificats. Les procédures de certification sont rassemblées dans un document appelé Déclaration des Pratiques de Certification (DPC), distinct de la PC, qui décrit comment ces exigences sont atteintes en pratique.

Cette PC est donc associée à la DPC relative à l'AC opérationnelle "CA Certificat". Contrairement à la PC, la consultation de la DPC n'a pas vocation à être publique et doit faire l'objet d'une demande argumentée auprès du CEDICAM (cf. 2.8.2).

La gestion des certificats couvre toutes les opérations relatives à la vie d'un certificat, depuis son émission jusqu'à la fin de vie de ce certificat (péremption, révocation).

Le but de la présente PC est de fournir aux Clients/Abonnés du CEDICAM les informations relatives aux garanties offertes par les **certificats CA Certificat** qu'il émet, ainsi que les conditions d'utilisation de ces certificats.

Enfin, cette PC vise la conformité au document "Procédures et Politiques de Certification de Clés (PC²)" émis par la Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI), à la PC-type version 3.0 du MinEFI ainsi qu'au document RFC 2527 de l'IETF.


2.1 Identification de la PC-TELEPROCEDURES - OID

La présente PC est identifiée par l'OID 1.2.250.1.104.3.1.1.1.1.2.3.2 La Déclaration des Pratiques de Certification correspondante est référencée par l'OID 1.2.250.1.104.3.1.1.2.1.2.3.2

Les PC et DPC correspondantes aux OID ci-dessus sont ci-après désignées sous le nom de "PC" et de "DPC".

2.2 Liste des acronymes utilisés

AC	Autorité de Certification
AE	Autorité d'Enregistrement

	CA CERTIFICAT	N° page : 9/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc


ACE	Autorité Centrale d'Enregistrement
AED	Autorité d'Enregistrement Décentralisée
C	<i>Country</i> (Pays)
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	<i>Common Name</i>
DGI	Direction Générale des Impôts
DN	<i>Distinguished Name</i>
DPC	Déclaration des Pratiques de Certification
DSA	<i>Digital Signature Algorithm</i>
ICP	Infrastructure à Clés Publiques
LDAP	<i>Lightweight Directory Access Protocol</i>
LCR	Liste des Certificats Révoqués
GC	Gestionnaire des Certificats
MD5	<i>Message Digest number 5</i>
MinEFI	Ministère de l'Économie, des Finances et de l'Industrie
O	<i>Organisation</i>
OID	<i>Object Identifier</i>
OU	<i>Organisational Unit</i>
OSC	Opérateur de Service de Certification
PC	Politique de Certification
PC ²	Procédures et Politiques de Certification de Clés
RSA	Rivest Shamir Adelman
S/MIME	<i>Secure Multipurpose Internet Mail Extensions</i>
SHA-1	<i>Secure Hash Algorithm One</i>
SSL	<i>Secure Sockets Layer</i>
TLS	<i>Transport Layer Security</i>

2.3 Définitions des termes utilisés dans la Politique de Certification CA Certificat

Le symbole (*) signifie que le terme est défini dans le présent chapitre. Il est utilisé dans le reste du document lorsqu'il est important de renvoyer à la définition du terme employé.

Application utilisatrice : service applicatif exploitant les certificats émis par l'Autorité de Certification* pour des besoins d'authentification ou de signature de l'Abonné.

Abonné : personne physique qui utilise un certificat CA Certificat au nom du Client. Le Client peut avoir un ou plusieurs Abonnés. L'Abonné peut également être désigné sous le nom de *porteur de certificat*. Dans la phase amont de certification il est un *demandeur* de certificat et dans le contexte du certificat X.509 il est un *sujet*.

	CA CERTIFICAT	N° page : 10/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Assistance téléphonique CA Certificat : la ligne de support téléphonique de l'ICP CA Certificat mise à disposition publique par l'AC et l'ACE.

Autorité Administrative : voir Comité d'Approbation des Politiques.

Autorité Centrale d'Enregistrement : entité responsable de la validation des informations fournies par les Autorités d'Enregistrement Décentralisées (AED). Le rôle d'ACE est tenu par le CEDICAM.

Ses fonctions sont les suivantes :

- Contrôle, validation des **demandes de certificats et de révocations** transmises par les AED,
- Transmission des demandes validées à l'Autorité de Certification pour exécution,
- Journalisation et archivage des demandes.


Autorité de Certification : autorité à laquelle le Client fait confiance pour émettre et gérer des certificats et des LCR*.

Afin de lever l'ambiguïté terminologique concernant l'Autorité de Certification, les conventions suivantes seront prises pour ce document :

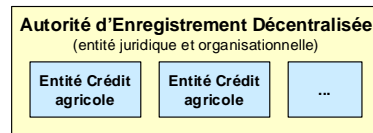
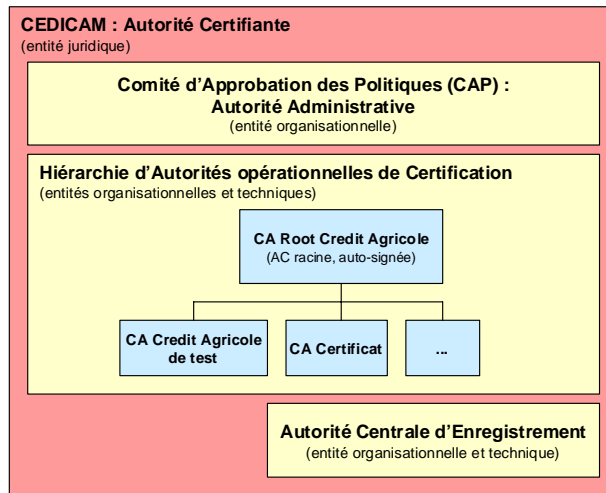
Le terme Autorité Certifiante désigne le concept d'autorité légale émettant des certificats pour une communauté. L'Autorité Certifiante dans le cas de CA Certificat est le GIE CEDICAM ayant son siège social à 83 boulevard des chênes 78280 GUYANCOURT inscrit au RCS de PARIS sous le numéro 723 001 467.

Le terme Autorité opérationnelle de Certification (AC opérationnelle) correspond à l'entité organisationnelle et technique qui reçoit la demande de certificat, constitue le gabarit de certificat et le signe avec sa clé privée. L'Autorité opérationnelle de Certification dans le cas de CA Certificat est dénommée « CA Certificat » et appartient à la hiérarchie de certification (décrite ci-après) dont l'Autorité Certifiante (le CEDICAM) est responsable. Lorsqu'il est question de certificat d'AC, c'est toujours l'AC opérationnelle qui est évoquée.

Le terme d'Autorité de Certification (AC) désigne de manière indifférenciée ces deux concepts.

	CA CERTIFICAT	N° page : 11/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Le modèle de confiance de l'ICP Crédit agricole est le suivant :



Modèle de confiance de l'ICP Crédit Agricole

De même que pour le reste des AC opérationnelles de l'ICP du CEDICAM, l'AC opérationnelle nommée "CA Certificat" est gérée pour le compte du groupe CEDICAM par le CEDICAM.


L'AC assure les fonctions suivantes :

- Mise en application de la Politique de Certification CA Certificat,
- Gestion des certificats,
- Publication des Listes des Certificats Révoqués,
- Journalisation et archivage des évènements et informations relatives au fonctionnement de l'infrastructure.

La fonction d'enregistrement des certificats est remplie par les Autorités d'Enregistrement*.

Autorité d'Enregistrement (AE) : entité responsable de l'identification et de l'authentification des sujets des certificats, mais qui ne signe ni ne délivre des certificats.

L'AE réceptionne et traite les demandes de révocation de certificat.

	CA CERTIFICAT	N° page : 12/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

L'AE archive les dossiers de demande de certificat ou de révocation.

Dans le cas de CA Certificat, les fonctions d'AE sont réparties entre l'Autorité Centrale d'Enregistrement, les Autorités d'Enregistrement Décentralisées, et les Mandataires de Certification* (ou Représentants d'Entreprise*).

Autorités d'Enregistrement Décentralisées : les Autorités d'Enregistrement Décentralisées (AED) correspondent aux entités en relation directe avec les Clients. Dans le contexte de l'ICP CA Certificat, elles correspondent à une décentralisation de la fonction *enregistrement* auprès des distributeurs de l'offre, chargés de sa commercialisation. Le rôle des AED consiste en particulier à enregistrer les demandes de certificats CA Certificat et à vérifier que les demandeurs et les porteurs de certificat sont identifiés, que leur identité est authentique et que les contraintes liées à l'usage d'un certificat sont remplies, tout cela conformément à la présente PC.

Les AED réceptionnent et vérifient également, selon les critères établis dans la présente PC, des demandes de révocation de certificats CA Certificat et les transmettent à l'ACE pour traitement.

Bi-clé : un bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptographie basée sur des algorithmes asymétriques. Dans le cas des certificats CA Certificat, le même bi-clé assure les fonctions :

- de **signature** (la clé privée est utilisée à des fins de signature et la clé publique à des fins de vérification),
- **d'échange de clés** ou de transport de clé (transport des clés secrètes [symétriques] mises en œuvre pour chiffrer ou déchiffrer un message protégé en confidentialité).

Les bi-clés de **chiffrement**, utilisés pour le chiffrement de données (hors clés symétriques) ne sont pas pris en compte par CA Certificat.


Certificats CA Certificat : certificats numériques concernés par la présente Politique de Certification et émis par l'AC opérationnelle "CA Certificat". Ils sont proposés sous forme logicielle ou sur support matériel (carte à puce ou clé cryptographique USB).

Chaîne de confiance (chaîne de certification) : ensemble ordonné des certificats nécessaires pour valider la filiation d'un certificat porteur. Dans le cas d'un certificat signé par l'AC "CA Certificat", la chaîne de confiance comprend le certificat de l'AC "CA Certificat" et celui de l'AC racine "CA Root Credit Agricole".

Clé privée d'échange de clés : c'est la clé privée du bi-clé d'échange de clé* (voir bi-clé).

Client : personne contractante avec l'AED :

- personne morale qui demande un certificat CA Certificat pour chacun de ses Abonnés,

	CA CERTIFICAT	N° page : 13/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- personne physique qui demande un certificat CA Certificat pour chacun de ses Abonnés dans le cadre de son activité professionnelle.

Code de Retrait : mot de passe généré aléatoirement par l'ACE et envoyé à l'Abonné par courrier électronique. Le Code de Retrait est employé par l'Abonné conjointement à son Code Personnel Utilisateur pour s'authentifier lors du retrait de son certificat.

Code Personnel Utilisateur : mot de passe choisi par chaque Abonné et chaque Gestionnaire des Certificats* (ou Représentant d'Entreprise*) et fourni au moment de leur enregistrement. Leur Code Personnel Utilisateur sera utilisé pour les authentifier pour les opérations de retrait et/ou de révocation des certificats.

Comité d'Approbation des Politiques : comité qui est constitué de représentants du CEDICAM, pour créer, contrôler le respect et faire évoluer la documentation des politiques régissant l'ICP du Crédit Agricole. C'est l'Autorité Administrative de l'Autorité Certifiante*.

Common Name (CN) : identité réelle de l'Abonné* titulaire du certificat (exemple CN = Jean Dupont).

Composante de l'ICP : plate-forme jouant un rôle déterminé au sein de l'ICP* dans le cycle de vie du certificat.

Compromission : une clé est dite compromise lorsqu'elle est connue par d'autres personnes que celles habilitées à la mettre en œuvre.


Contrat de Souscription CA Certificat : contrat liant le Client à une AED pour la souscription au service de certification CA Certificat. Il contient l'ensemble des documents nécessaires à l'élaboration des Dossiers Client. La fourniture d'un Contrat de Souscription CA Certificat vierge se fait sur simple demande auprès des différentes AED Crédit Agricole.

Déclaration des Pratiques de Certification (DPC) : énoncé des procédures et pratiques appliquées par une Autorité Certifiante pour émettre et gérer des certificats émis par une AC opérationnelle dont elle est responsable.

Distinguished Name (DN) : nom distinctif X.500 de l'Abonné* pour lequel le certificat est émis.

Données d'activation : données privées associées à un Abonné* permettant de mettre en œuvre sa clé privée. Les données d'activation sont également nommées *PIN code* pour une carte à puce.

Dossier client : ensemble des pièces justificatives (demande et éventuellement Contrat de Souscription y compris) à fournir à l'AED* afin de lui permettre de vérifier les informations demandées par l'ACE pour l'émission d'un certificat CA Certificat, l'enregistrement d'un nouveau Gestionnaire des Certificats* (ou Représentant d'Entreprise*), la modification des données concernant un Abonné ou un Gestionnaire des

	CA CERTIFICAT	N° page : 14/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Certificats, ou enfin pour révoquer le mandat d'un Gestionnaire des Certificats. Ces pièces justificatives sont décrites dans le Contrat de Souscription CA Certificat.

Émission (d'un certificat) : un certificat est émis (ou délivré) lorsqu'il a été généré et est exporté pour être remis à l'Abonné ou publié.

Enregistrement (d'un Abonné) : opération qui consiste pour une Autorité d'Enregistrement* à extraire d'un Dossier Client les informations sur un demandeur de certificat à renseigner dans les champs du certificat, conformément à la Politique de Certification*.

Génération (d'un certificat) : action réalisée par une AC* opérationnelle et qui consiste à signer l'ensemble des champs contenus dans un certificat édité par l'ACE*.

Identifiant d'objet (OID) : identifiant alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Infrastructure à Clé Publique (ICP) : ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique. Dans l'ensemble de ce document, le terme **ICP CA Certificat** ne désigne que la partie de l'ICP du Crédit agricole relative au service de certification CA Certificat.

Journaux d'exploitation ou d'événement : journaux collectant toutes les traces d'exécution des traitements, transactions et programmes produites par un système d'information (dénommés aussi "logs" ou "journaux d'événements").


Liste de Certificats Révoqués (LCR) : liste de numéros de certificats ayant fait l'objet d'une révocation*.

Gestionnaire des Certificats (GC) : aussi appelé Représentant d'Entreprise, personne physique, dûment identifiée, appartenant à l'entreprise et ayant délégation pour assurer au nom du Client la gestion des certificats CA Certificat, en particulier recueillir et valider les pièces du dossier d'enregistrement lors d'un face à face avec le demandeur.

Les prérogatives du Gestionnaire des Certificats lui permettent de demander et/ou de révoquer les certificats CA Certificat des Abonnés du Client. Une seule et même personne peut tenir les rôles d'Abonné et de Gestionnaire des Certificats simultanément. Un Client peut avoir un ou plusieurs Mandataires de Certification.

Module cryptographique : dispositif matériel, du type carte à mémoire, carte PCGCIA ou autre, permettant de protéger les éléments secrets tels que les clés privées ou les Données d'Activation, et de procéder à des calculs cryptographiques mettant en œuvre ces éléments.

Politique de Certification (PC) : ensemble de règles définissant les exigences auxquelles chacun des acteurs impliqués se conforment et qui indiquent le niveau de sécurité commun accordé aux certificats. La Politique de Certification est identifiée par un OID* défini par l'AC*.

	CA CERTIFICAT	N° page : 15/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Porteurs de (certificats) : voir Abonnés*.

Publication (d'un certificat) : opération consistant à mettre un certificat à disposition d'utilisateurs pour leur permettre de vérifier une signature ou de chiffrer des informations (ex : annuaire X.500).

Recréation d'un certificat : opération à l'initiative d'un Gestionnaire des Certificats* (ou de l'Abonné titulaire) faisant suite à la compromission, vol ou perte d'un certificat CA Certificat. Cette opération constitue une demande de révocation de l'ancien certificat et l'émission d'un nouveau certificat contenant les mêmes informations. La re-génération d'un certificat peut également être sollicitée pour renouveler un certificat après sa date de fin de validité. La preuve d'identité de l'Abonné étant assurée par le Code Personnel Utilisateur, il s'affranchit de repasser par la procédure de demande initiale de certificat.

Référencement : engagement d'une personne à accepter une famille de certificats pour une application donnée. Cette opération est généralement accompagnée du contrôle de la conformité de ladite famille de certificats à des exigences préalablement établies.

Re-génération d'un certificat : cf. recréation d'un certificat*.

Renouvellement (d'un certificat) : opération effectuée en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un Abonné. La Re-génération de certificat après révocation n'est pas un renouvellement.

Représentant d'Entreprise : Gestionnaire des Certificats*.


Révocation (d'un certificat) : opération de mise en opposition demandée par l'Abonné, le Gestionnaire des Certificats* (ou Représentant d'Entreprise*), le Client, l'AE ou l'AC ou par toute autre personne autorisée par l'AC, dont le résultat est la suppression de la garantie d'engagement de l'AC* sur un certificat donné, avant la fin de sa période de validité. Par exemple, la compromission d'une clé ou le changement d'informations contenues dans un certificat doivent conduire à la révocation du certificat. L'opération de révocation est considérée comme terminée lorsque le numéro de certificat à révoquer et la date de révocation sont publiés dans la Liste des Certificats Révoqués (LCR*).

Service de Certification CA Certificat : offre de services distribuée par les AED, comprenant en particulier la délivrance et la gestion de certificats CA Certificat.

Signature électronique : Une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil. Une signature électronique est un cryptogramme issu du chiffrement d'un *condensat* de fichier à l'aide d'une clé privée, lequel condensat étant obtenu par application d'une fonction de hachage (algorithme de codage irréversible) sur ledit fichier.

Validation (de certificat) : opération de contrôle du statut d'un certificat ou d'une chaîne de certification*.

Vérification (de signature) : opération de contrôle d'une signature électronique.

	CA CERTIFICAT	N° page : 16/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

2.4 Type d'applications concernées par la Politique de Certification CA Certificat

2.4.1 Liste des applications utilisatrices autorisées

La liste des applications utilisatrices dans le cadre desquelles les certificats numériques délivrés par l'Autorité opérationnelle de Certification "CA Certificat" peuvent être utilisés est publiée sur le site *web* du service CA Certificat : <http://www.ca-certificat.com>.

2.4.2 Liste des applications utilisatrices interdites

L'AED, l'ACE et l'AC déclinent toute responsabilité dans l'usage que ferait un Abonné de son certificat CA Certificat dans le cadre d'une application non mentionnée dans le paragraphe précédent. En particulier, ne sera acceptée aucune plainte, de quelque sorte que ce soit, d'Abonnés ou de Mandataires de Certification (ou Représentants d'Entreprise), liée à des litiges sans rapport avec les applications mentionnées dans le précédent paragraphe.

2.5 Types de certificats concernés par la Politique de Certification CA Certificat

La présente Politique de Certification CA Certificat concerne les **certificats CA Certificat** du Crédit Agricole, émis par l'AC opérationnelle "CA Certificat" et gérés par le CEDICAM agissant en tant qu'Autorité Certifiante.

2.6 Supports des certificats CA Certificat


Deux modes de stockage sont possibles pour les **certificats CA Certificat** :

- La clé privée et le certificat correspondant sont stockés sur un poste de travail (dans ce cas le certificat est appelé « certificat logiciel »),
- La clé privée et le certificat correspondant sont stockés sur support matériel (dans ce cas le certificat est appelé « certificat sur support matériel »), à l'exemple d'une carte à puce ou clé à puce sur port USB. Il est à noter que le certificat sur support matériel carte à puce nécessite pour être utilisé l'installation d'un lecteur de carte à puce (cf. § 5.1.3.4).

2.7 Modification de la Politique de Certification CA Certificat

Cette PC sera revue périodiquement par le Comité d'Approbation des Politiques de l'Autorité Certifiante, notamment pour :

- assurer sa conformité aux normes de sécurité attendues par les applications qui référencent la famille de certificats CA Certificat ;

	CA CERTIFICAT	N° page : 17/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- mettre à jour la liste des applications concernées par la PC ;
- s'adapter aux évolutions technologiques.

La périodicité minimale de révision de cette PC est de un (1) an.

Ce présent paragraphe indiquera les principales modifications de ce document en comparaison à la version antérieure.

Version présente	Date	Principaux points de modification
1.00	03/05/01	Version initiale de la PC de l'AC "CA Certificat"
2.00	24/09/01	Elargissement de l'utilisation des certificats CA Certificat à d'autres applications – Mise en place de l'offre support matériel – ajout du processus de Régénération.
3.00	14/11/02	Modification des modalités d'enregistrement – Renforcement de la sécurité cryptographique – Amélioration de la qualité de service de l'AC.

2.8 Coordonnées des entités responsables de la présente Politique de Certification

2.8.1 Organisme responsable


Le CEDICAM est responsable de cette PC.

GIE CEDICAM, inscrit au RCS de PARIS sous le numéro 723 001 467, ayant son siège social au :

83 BOULEVARD DES CHENES
78280 GUYANCOURT - FRANCE

2.8.2 Personne physique responsable

M. JEAN-MARC DEGEZ
RESPONSABLE DE DEPARTEMENT
BATIMENT PROVENCE
83, BOULEVARD DES CHENES
78280 GUYANCOURT - FRANCE

	CA CERTIFICAT	N° page : 18/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Téléphone : (+33) 1 57 72 80 40

Fax : (+33) 1 57 72 15 80

Mél : support@ca-certificat.com

2.8.3 Personne déterminant la conformité de la DPC à la PC

La conformité de la Déclaration des Pratiques de Certification (DPC-CA Certificat) à la Politique de Certification (Politique de Certification CA Certificat) est déterminée par le Comité d'Approbation des Politiques de l'Autorité Certifiante sous la responsabilité de :

M. JEAN-MARC DEGEZ

RESPONSABLE DE DEPARTEMENT

BATIMENT PROVENCE


83, BOULEVARD DES CHENES

78280 GUYANCOURT - FRANCE

Téléphone : (+33) 1 57 72 80 40

Fax : (+33) 1 57 72 15 80

Mél. : support@ca-certificat.com

	CA CERTIFICAT	N° page : 19/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

3 DISPOSITIONS DE PORTEE GENERALE

3.1 Contrôle de conformité à la Politique de Certification CA Certificat

Le Comité d'Approbation des Politiques de l'Autorité Certifiante a la responsabilité du bon fonctionnement des composantes de l'ICP CA Certificat, conformément aux dispositions énoncées dans le présent document. Il effectuera des contrôles réguliers de conformité et de bon fonctionnement des composantes de cette ICP CA Certificat.

Par ailleurs, le CEDICAM s'engage à effectuer les audits demandés par le MinEFI et éventuellement par les autres applications utilisatrices autorisées, pour lesquels il s'y oblige contractuellement, afin que ceux-ci s'assurent du bon respect des exigences liées aux référencements de la famille de certificat "CA Certificat". Ces audits pourront éventuellement être réalisés aux frais de l'Autorité Certifiante, selon les dispositions du contrat liant la liant à l'application, et pourront concerner toutes les composantes de l'ICP CA Certificat.

3.1.1 Fréquence du contrôle de conformité

Le contrôle de conformité est réalisé en cas de renouvellement d'un bi-clé d'AC, avant toute génération et émission de certificats par cette dernière.

Ce contrôle est à nouveau réalisé au minimum tous les un (1) an.

3.1.2 Indépendance et qualifications du contrôleur

Le contrôleur est désigné par le Comité d'Approbation des Politiques de l'Autorité Certifiante. Dans le cas où le contrôle est effectué à la demande du MinEFI, le contrôleur est choisi selon des critères d'indépendance et d'expertise dans le domaine de la sécurité informatique et, en particulier, des ICP.

Dans les autres cas, le contrôleur désigné pourra éventuellement être une entité d'audit interne au Crédit Agricole experte dans le domaine de la sécurité informatique.


Les non-conformités révélées par ces audits seront publiées aux responsables des applications utilisatrices autorisées, pour lesquelles l'Autorité Certifiante s'y oblige contractuellement.

3.1.3 Périmètre du contrôle de conformité

Le périmètre de l'audit concerne les chapitres 3 à 8 de la présente PC.

3.1.4 Communication des résultats

Les résultats sont communiqués au Comité d'Approbation des Politiques, qui est responsable de leur éventuelle diffusion aux entités concernées.

	CA CERTIFICAT	N° page : 20/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Eu égard au caractère confidentiel de ces informations, la publication des résultats est limitée et strictement contrôlée.

3.1.5 Actions entreprises en cas de non-conformité

En cas de non-conformité, le Comité d'Approbation des Politiques décide de toute action correctrice nécessaire.

En fonction du degré de non-conformité de la DPC à la PC, l'AC peut :

- demander la mise en place d'actions correctrices dont la réalisation sera vérifiée lors du prochain audit ;
- demander la correction des non-conformités selon un calendrier précis à la suite duquel un contrôle de mise en conformité sera effectué ;
- révoquer le certificat de l'AC opérationnelle "CA Certificat".

3.2 Respect et interprétation des dispositions juridiques

3.2.1 Droit applicable

La Loi française est applicable aux dispositions du présent document (y incluant le "Contrat de Souscription CA Certificat"). En cas de traduction, seule la version française du présent document fera foi. En cas de difficulté, les parties se conformeront à la procédure de règlement des litiges prévue dans le "Contrat de Souscription CA Certificat". A défaut de règlement amiable, le litige sera porté devant les juridictions compétentes.


Les textes législatifs et réglementaires applicables à la présente Politique de Certification sont indiqués en Annexe 1.

3.2.2 Séquestre

Une fonction de séquestre des clés privées de chiffrement peut être assurée par une ICP pour permettre le recouvrement de documents chiffrés, notamment à la demande des autorités compétentes. L'ICP CA Certificat ne réalise pas de fonction de séquestre (les clés privées de chiffrement dans le cadre de l'ICP CA Certificat n'étant jamais utilisées pour le chiffrement de documents statiques).

3.2.3 Arbitrage des litiges

Toute contestation de l'Abonné ou du Client relative aux dispositions du présent document et du "Contrat de Souscription CA Certificat" sera soumise, préalablement à toute instance judiciaire, à la procédure décrite à l'article "droit applicable" du "Contrat de Souscription CA Certificat".

	CA CERTIFICAT	N° page : 21/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

3.2.4 Permanence de la Politique de Certification CA Certificat

Le fait que l'un des intervenants (Abonné, AC, ...) n'ait pas exigé l'application d'une clause quelconque du présent document et/ou du "Contrat de Souscription CA Certificat", que ce soit de façon permanente ou temporaire, ne pourra en aucun cas être considéré comme une renonciation aux droits de cette partie découlant de ladite clause dont l'inapplication a été tolérée.

Si l'une quelconque des dispositions du présent document et/ou du "Contrat de Souscription CA Certificat" est non valide, nulle ou sans objet, elle sera réputée non écrite et les autres dispositions conserveront toute leur force et leur portée.

Aucune action, quelle qu'en soient la nature, le fondement ou les modalités, née du présent document et/ou du "Contrat de Souscription CA Certificat", ne peut être intentée par les parties plus de cinq ans après la survenance de son fait générateur.

Les titres des articles du présent document et/ou du "Contrat de Souscription CA Certificat" sont insérés dans le seul but d'en faciliter la référence et ne peuvent être utilisés pour donner une interprétation à ces articles ou en affecter la signification. Aussi, en cas de difficulté d'interprétation entre l'un quelconque des titres et l'une quelconque des clauses constituant le document et/ou le "Contrat de Souscription CA Certificat", les titres seront déclarés comme inexistantes.

3.3 Rôles et obligations de l'ICP et de ses composantes

3.3.1 Rôle de l'Autorité Certifiante

Le rôle de l'AC est de garantir le respect des exigences, émises dans le présent document et dans la DPC, relatives à son activité de certification. Dans le cadre de cette activité, elle sous-traite une partie des opérations aux différentes composantes de l'ICP (AE etc.).


Les fonctions de Certification sont assurées par le CEDICAM (agissant en tant qu'Autorité de Certification).

3.3.2 Rôles de l'AE et du Gestionnaire des Certificats

3.3.2.1 Intervenants pour les fonctions d'enregistrement

Pour les fonctions d'enregistrement, les intervenants sont :

- l'AED (Autorité d'Enregistrement Décentralisée), à qui est confiée la commercialisation (distribution) du service de certification CA Certificat. L'AED collecte et vérifie les Dossiers Client et réalise en particulier l'authentification en face-à-face des Mandataires de Certification (ou Représentants d'Entreprise).
- l'ACE (Autorité Centrale d'Enregistrement) qui valide les enregistrements demandés par les AED.

	CA CERTIFICAT	N° page : 22/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- les Mandataires de Certification (ou GC ou Représentants d'Entreprise), membres de l'entreprise cliente en relation directe avec l'AED, qui réunissent les pièces constitutives des Dossiers Client et réalisent l'authentification en face-à-face des Abonnés.

La relation entre les AED et l'AC est formalisée par une convention de service liant l'AED avec l'AC précisant les droits et obligations des parties.

La relation entre les GC et les AED est formalisée par un contrat liant le Client avec l'AED précisant les droits et obligations des parties et les modes de résolution des litiges.

3.3.2.2 Obligations des AED

Le contrôle effectif de la véracité des informations communiquées par les demandeurs de certificats est réalisé par différentes AED.


Les AED s'engagent à :

- Remettre les dossiers de souscription au service, de demande de nouveaux certificats, de changement dans les informations concernant un Abonné ou un GC (ou Représentant d'Entreprise), et les dossiers d'ajout ou de révocation de mandat d'un GC.
- Garantir que la personne identifiée dans les dossiers d'ajout de GC transmis a prouvé son identité et vérifier l'authenticité des pièces justificatives et l'exactitude des mentions qui établissent l'identité de l'Abonné, du GC et du Client selon les modalités décrites au chapitre 3.
- Mettre en œuvre la procédure d'enregistrement initial et de contrôles inhérents ; cette procédure s'exerce également dans le temps, concernant l'évolution des informations.
- Protéger la confidentialité et l'intégrité des données transmises par les demandeurs.
- Recevoir des demandes formelles de révocation, en vérifier l'origine et l'exactitude, et les transmettre pour traitement à la l'ACE selon les exigences décrites au §4.4
- Maintenir les procédures de Contrôle Interne adéquates, afin de garantir la fiabilité des opérations dont elles ont la charge.
- S'assurer que ses Clients connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés et des certificats.

3.3.2.3 Obligations de l'ACE

L'entité responsable de l'ACE s'engage à :

- Vérifier, à la réception d'un formulaire (notamment de demande ou de révocation de certificat CA Certificat), la validation effective des AED, en comparant les signatures avec celles déposées par les personnes responsables desdites AED.

	CA CERTIFICAT	N° page : 23/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- Etablir le lien entre la clé publique à certifier et l'identité du futur Abonné .
- Fournir l'identifiant de l'Abonné selon la convention de noms de la norme X.500 (cf. §4.1.).
- Contrôler la complétude et la cohérence des informations fournies.
- Vérifier l'origine et l'exactitude d'une demande de révocation de certificat, et mettre en œuvre les moyens permettant de traiter cette demande selon les exigences décrites au § 4.4.
- Maintenir les procédures de Contrôle Interne adéquates, afin de garantir la fiabilité des opérations dont elle a la charge.

3.3.2.4 Obligations du Gestionnaire des Certificats


Le Gestionnaire des Certificats (ou Représentant d'Entreprise) a le devoir de :

- communiquer des informations justes lors de la demande de certificat,
- faire respecter les conditions d'utilisation de la clé privée et du certificat correspondant,
- informer sans délai l'AED ou l'ACE en cas de compromission d'une clé privée, selon les conditions indiquées en 4.4.3,
- révoquer en cas de besoin tout certificat conformément au chapitre 4 (§ 4.4),
- garantir que la personne identifiée dans les dossiers de demande de certificat (nouveaux Abonnés) transmis a prouvé son identité et vérifier l'exactitude des mentions qui établissent l'identité de l'Abonné.

3.3.3 Obligations communes à toutes les composantes de l'ICP CA Certificat

Le CEDICAM est le maître d'œuvre de l'AC opérationnelle "CA Certificat" et à ce titre s'engage à :

- protéger et garantir l'intégrité et la confidentialité des clés privées des composantes de l'ICP CA Certificat ;
- n'utiliser ses clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, dans les conditions fixées par la présente Politique de Certification ;
- respecter et appliquer la DPC CA Certificat ;
- se soumettre aux contrôles de conformité effectués pour le compte du MinEFI, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- respecter les accords ou contrats qui le lient aux différents acteurs ;

	CA CERTIFICAT	N° page : 24/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- documenter ses procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles il s'engage, dans des conditions garantissant qualité et sécurité.

3.3.4 Obligations relatives à la gestion des certificats

L'entité responsable de l'AC "CA Certificat" s'engage à :

- assurer par le certificat le lien entre l'identité d'un Abonné et sa clé publique ;
- tenir à disposition des Abonnés et des applications la notification de révocation du certificat d'une composante de l'ICP CA Certificat ou d'un Abonné,
- garantir et maintenir la cohérence de la DPC avec la PC.

3.3.5 Obligations relatives à la gestion des supports et données d'activation

Les éléments secrets d'un Abonné sont gérés soit dans un fichier chiffré, soit sur un support matériel, et dans les deux cas leur mise en œuvre est conditionnée par l'utilisation d'un mot de passe ou autre Donnée d'Activation.

Le support matériel est expédié « vierge » au Client et est personnalisé électriquement (tirage du bi-clé et stockage du certificat) par l'Abonné lui-même au niveau du poste client.

Les Données d'Activation des secrets de l'Abonné ne sont jamais choisies ou imposées par l'AC.


3.3.6 Obligations relatives à l'identification

Le Gestionnaire des Certificats (ou Représentant d'Entreprise) s'engage à effectuer les vérifications suivantes :

- établir l'identité des Abonnés pour lesquels il demande des certificats ;
- s'assurer que le futur Abonné a pris connaissance des modalités applicables pour l'utilisation du certificat.

L'AED s'engage à effectuer les vérifications suivantes :

- établir l'identité du Client ;
- établir l'identité des GC ;
- établir le droit des GC à représenter le Client.

	CA CERTIFICAT	N° page : 25/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Il est entendu que l'établissement de l'identité des personnes physiques doit être réalisé en présence desdites personnes (mode « face-à-face »), avec présentation de justificatifs officiels d'identité comme indiqué dans le Contrat de Souscription CA Certificat.

De même, les pièces justificatives permettant d'établir l'identité du Client sont indiquées dans le Contrat de Souscription CA Certificat.

3.3.7 Obligations relatives à la publication

L'entité responsable de l'AC "CA Certificat" s'engage à diffuser publiquement la Politique de Certification CA Certificat.

Elle s'engage également à diffuser publiquement la Liste de Certificats Révoqués (LCR) qui sera :

- fiable, c'est-à-dire comportant uniquement des informations contrôlées et à jour ;
- protégée en intégrité ;
- d'un accès contrôlé quant à la mise à jour (accès libre en consultation) ;
- publiée suivant les modalités décrites au § 4.4 de cette PC ;
- disponible 24 heures sur 24 et 7 jours sur 7.

L'AC publie la liste des certificats auxquels la clé racine de l'ICP est subordonnée.

3.3.8 Obligations relatives à la journalisation

Se reporter au paragraphe § 5.10.

3.3.9 Obligations relatives à l'archivage

Se reporter au paragraphe § 5.11.


3.3.10 Obligations relatives au séquestre

Sans objet, l'ICP CA Certificat ne réalisant pas de fonction de séquestre.

3.4 Obligations du Client

Les fonctions de gestion des certificats pour le compte d'un Client sont réalisées par ses Mandataires de Certification* (ou Représentants d'Entreprise*), qui ont délégation pour les assurer.

Le rôle du Gestionnaire des Certificats est, outre sa fonction d'Enregistrement, de demander ou de révoquer les certificats des Abonnés* (ou porteurs de certificats) du Client.

	CA CERTIFICAT	N° page : 26/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Le Client est lié contractuellement avec son AED pour l'émission de certificats aux Abonnés désignés par et sous la responsabilité du Client dûment représenté par ses Mandataires de Certification (ou Représentants d'Entreprise).

Le Client est responsable des obligations mentionnées ci-dessous qu'elles soient exécutées par les GC et/ou les Abonnés du Client.


Le Client doit :

- Désigner, sous sa responsabilité, ses GC et les personnes physiques auxquelles sera délivré un certificat,
- Garantir l'authenticité, le caractère complet et à jour des informations communiquées lors de la demande de certificat ainsi que des documents qui accompagnent ces informations,
- Informer sans délai l'AED de toute modification relative à ces informations et/ou documents,
- Assurer l'information des Abonnés sur les conditions d'utilisation des certificats, de la gestion des clés ou encore de l'équipement et des logiciels permettant de les utiliser,
- Faire assurer l'acceptation du certificat par chaque Abonné ainsi que les vérifications préalables à cette acceptation,
- Faire protéger la clé privée de chaque Abonné par des moyens appropriés à son environnement,
- Faire protéger les Données d'Activation de chaque Abonné par des moyens appropriés à son environnement,
- Faire respecter les conditions d'utilisation de la clé privée et du certificat correspondant par chaque Abonné, notamment l'utilisation dans le strict cadre des applications décrites au § 1.6.1 de cette PC,
- Faire demander la révocation d'un certificat dès lors qu'elle est nécessaire,
- Faire informer sans délai l'AED ou l'ACE en cas de suspicion de compromission ou de compromission de la clé privée d'un de ses Abonnés, selon les conditions indiquées en 4.4.3.

3.5 Obligations de l'Abonné

L'Abonné a l'obligation de :

- communiquer des informations justes lors de la demande de certificat ;
- protéger sa clé privée par des moyens appropriés à l'environnement dans lequel se trouve cette clé ;

	CA CERTIFICAT	N° page : 27/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- protéger ses Données d'Activation ;
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- informer sans délai l'AED ou l'ACE en cas de compromission de sa clé privée, selon les conditions indiquées en 4.4.3.

La relation entre l'Abonné et l'AED est formalisée par un engagement de l'Abonné visant à certifier l'exactitude des renseignements et des documents fournis (cf. Contrat de Souscription CA Certificat).

3.6 Limitation de la responsabilité du CEDICAM en qualité d'AC

Il est expressément entendu que le CEDICAM ne saurait être tenu pour responsable ni d'un dommage résultant d'une faute ou négligence d'un Client et/ou de son(s) Représentant(s) d'Entreprise habilité(s) et/ou de ses Abonnés ni d'un dommage causé par un fait extérieur ou un cas de force majeure, notamment en cas de :

- Utilisation d'un certificat pour une autre application que les Applications définies au chapitre 2.4 ;
- Utilisation d'un certificat pour garantir un autre objet que l'identité de l'Abonné ;
- Utilisation d'un certificat révoqué ;
- Mauvais modes de conservation de la clé privée du certificat de l'Abonné ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Non respect des obligations des autres Intervenants définies aux chapitres 2.2.5 et 2.2.8 ;
- Faits extérieurs à l'émission du certificat tel qu'une défaillance de l'application pour laquelle il peut être utilisé ;
- Cas de force majeure tels que définis par les tribunaux français.

3.7 Tarifs


Cf. "Conditions de tarification du service CA Certificat" en annexe du "Contrat de Souscription CA Certificat".

3.8 Publication et dépôt de documents

3.8.1 Informations publiées

Les informations publiées seront les suivantes :

- la Politique de Certification CA Certificat (PC) ;

	CA CERTIFICAT	N° page : 28/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- les Listes de Certificats Révoqués (LCR).

3.8.2 Fréquence de diffusion

- la Politique de Certification (PC) est mise à jour sur le site de l'offre CA Certificat du groupe CEDICAM <https://www.ca-certificat.com/PC> après chaque modification ;
- les Listes de Certificats Révoqués (LCR) sont actualisées dans un délai de 24 heures.

3.8.3 Contrôle d'accès

Des habilitations spécifiques sont mises en place afin de n'autoriser l'accès en modification à la PC qu'au personnel autorisé.

3.8.4 Dépôt des documents

L'Autorité Certifiante diffuse la Politique de Certification CA Certificat sur le site <https://www.ca-certificat.com/PC> du groupe CEDICAM. Les LCR sont quant à elles publiées aux adresses indiquées dans le champ « Point de distribution de la LCR » du certificat CA Certificat (cf. § 7.1).

3.9 Politique de confidentialité de l'ICP "CA Certificat"

3.9.1 Types d'informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :


- les clés privées des entités propriétaires de certificats ;
- les Données d'Activation pour les Abonnés ;
- les journaux d'événements des composantes de l'AC et de l'AE ;
- tous les Dossiers Client, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les certificats) ;
- les rapports d'audit ;
- la DPC.

3.9.2 Divulgence des causes de révocation/suspension de certificat

Cf. paragraphe 5.2.8.

3.9.3 Remise sur demande du propriétaire

Les informations nominatives recueillies lors de l'enregistrement de l'Abonné de même que celles qui seront recueillies ultérieurement, sont destinées à l'AED et à l'Autorité

	CA CERTIFICAT	N° page : 29/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Certifiante qui, de convention expresse, sont autorisés à les conserver en mémoire informatique, à les utiliser, ainsi qu'à les communiquer aux mêmes fins aux personnes morales du groupe CEDICAM, voire à des tiers ou à des sous-traitants pour des besoins de gestion.

Les droits d'accès et de rectification peuvent être exercés auprès de l'AED ou auprès de :

CEDICAM – CEDICAM (QP)

SERVICE CA CERTIFICAT

83, BOULEVARD DES CHENES

78280 GUYANCOURT - FRANCE

3.9.4 Délivrance aux autorités habilitées

Les procédures de l'AC CA Certificat relatives au traitement de la confidentialité sont conformes à la législation française [L90-1170].

3.9.5 Droits de propriété intellectuelle

Lors de l'exécution des prestations de services définies dans le présent document et/ou le "Contrat de Souscription CA Certificat", il peut être livré des éléments protégés par la législation sur les droits d'auteur.

Ces éléments, ainsi que les droits d'auteur qui y sont attachés, resteront la propriété du détenteur des droits correspondants. Le bénéficiaire de ces services aura le droit de reproduire ces éléments pour son usage interne. Mais il ne pourra, sans l'autorisation préalable du détenteur des droits d'auteur, mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci, en particulier logiciels ou bases de données.


Sous réserve des dispositions du présent article, aucune licence, implicite ou explicite, n'est concédée par le détenteur des droits sur des inventions, brevets ou demandes de brevets lui appartenant et ayant été réalisés hors du présent document et/ou du "Contrat de Souscription CA Certificat".

3.9.6 Protection des données à caractère personnel

Toute collecte de données à caractère personnel par l'AC et l'ensemble de ses composantes est réalisée dans le strict respect des lois et règlements en vigueur, en particulier de la loi n° 78-18 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3.10 Certificats de Recette

Le CEDICAM, en tant qu'entité responsable de l'Autorité Centrale d'Enregistrement, peut émettre des certificats dist « de recette », en nombre restreint, afin de permettre par exemple la validation finale d'un processus de développement d'une application.

	CA CERTIFICAT	N° page : 30/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Ces certificats sont identiques à ceux des Abonnés, à l'exception des caractéristiques suivantes :


- le champ « nom » est libre, mais le champ « prénom » qui constitue le début du CN est systématiquement « XXX TEST ». Exemple de CN résultant : XXX TEST APPLI. Cette syntaxe permet aux applications utilisatrices de filtrer les certificats de recette ou de leur attribuer d'autorité des habilitations spécifiques.

Remarque : le CN des certificats de recette d'avant la version 3.0 de la PC commençaient par ---TEST au lieu de XXX TEST.

- le SIREN de la société est celui de l'Entité demandeuse, responsable légale de l'Application (et non celui de la société dont dépend le porteur du certificat).
- Ces certificats ne sont pas renouvelables.

Il est de la responsabilité des Applications de refuser les certificats présentant ces caractéristiques ou de les accepter sous contrôle (avec des habilitations restreintes, etc.).

Ces certificats sont délivrés uniquement par l'ACE, sous son contrôle et à l'aide de processus qui peuvent différer des processus standards utilisés pour les Abonnés.

	CA CERTIFICAT	N° page : 31/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

4 IDENTIFICATION ET AUTHENTIFICATION

Ce chapitre traite des principes retenus pour identifier et authentifier un Abonné lors de :

- la création initiale du certificat "CA Certificat" dudit Abonné ;
- le renouvellement du certificat "CA Certificat" dudit Abonné ;
- la re-génération du certificat "CA Certificat" dudit Abonné ;
- la révocation du certificat "CA Certificat" dudit Abonné.

4.1 Enregistrement initial de l'Abonné

4.1.1 Conventions de noms

Le nom de l'Abonné figure dans le champ "Objet" ("*Subject*" en anglais) du certificat CA Certificat, sous la rubrique CN ("*Common Name*") au format *printableString* X.501. Cette mention est obligatoire. Il est constitué du prénom usuel et du nom patronymique.

Ce nom est celui de l'Abonné tel qu'il figure dans les documents d'État Civil.


4.1.2 Nécessité d'utilisation de noms explicites

Les informations portées dans le champ "Objet" du certificat CA Certificat sont décrites ci-dessous de manière explicite :

- le nom de l'Abonné (rubrique CN, tel que décrit au § 4.1.1) ;
- l'adresse électronique de l'Abonné ;
- la raison sociale de l'organisation représentée par l'Abonné, tel que figurant au K-Bis ou équivalent ;
- l'identifiant ICD (*International Code Designators*) ISO 6523 de l'organisation représentée par l'Abonné, par exemple le SIREN tel que figurant au K-Bis ou équivalent ;
- le nom de la commune du siège social de l'organisation représentée par l'Abonné, tel que figurant au K-Bis ou équivalent ;
- le nom de pays du siège social de l'organisation représentée par l'Abonné, tel que figurant au K-Bis ou équivalent, et formulé selon la convention internationale de nommage.

4.1.3 Règles d'interprétation des différentes formes de noms

Aucune interprétation particulière n'est à faire des informations portées dans le champ "Objet" des certificats CA Certificat.

	CA CERTIFICAT	N° page : 32/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Ces informations sont établies par l'ACE et reposent essentiellement sur les règles suivantes :

- tous les caractères sont au format printableString, i.e. sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501 ;
- les prénoms et noms composés sont séparés par des tirets " - ".

4.1.4 Unicité des noms

L'unicité d'un certificat est établie au sein de l'ICP "CA Certificat" par l'unicité du numéro de série. L'Autorité Certifiante s'engage également à ce que le champ "Objet" présente aussi un caractère d'unicité, obtenu par la présence conjointe des nom, prénom et adresse électronique de l'Abonné (à l'exception du renouvellement de certificat pendant lequel le champ objet est réutilisé).

4.1.5 Procédure de résolution de litige sur déclaration de nom

L'Autorité Certifiante s'engage quant à l'unicité des noms de ses Abonnés, conformément aux § 4.1.1 et § 4.1.2, et proposera des procédures de résolution amiable des litiges portant sur la revendication d'utilisation d'un nom.

4.1.6 Reconnaissance, authentification et rôle des noms de marques

Sans objet (les certificats CA Certificat ne contiennent pas des noms de marque).

4.1.7 Identification de l'entreprise

Dans le dossier initial de demande de certificat, l'entreprise est identifiée par :


- une pièce portant l'identifiant ISO 6523 de l'organisation représentée par l'Abonné (par exemple pour le SIREN : extrait Kbis, Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou équivalent),
- un exemplaire des statuts de l'entreprise, signé par l'un des représentants légaux (de préférence mentionné sur la pièce justificative de l'identifiant ISO 6523).

4.1.8 Authentification du Gestionnaire des Certificats

Une AED constitue un dossier d'enregistrement pour un Gestionnaire des Certificats (GC) en vue d'utiliser ce dossier comme référence pour les données d'identification de tous les porteurs présentés par le GC.

Le dossier d'enregistrement d'un GC comprend :

- une délégation de pouvoir signée par le chef d'entreprise ou son représentant,
- un engagement signé du GC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles du dossier du demandeur,

	CA CERTIFICAT	N° page : 33/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- un engagement signé du GC à signaler à l'AED son départ de l'entreprise, et le départ des porteurs de l'entreprise,
- un justificatif d'identité officiel du GC, selon les règles de la législation française (carte d'identité nationale, passeport, livret de famille, permis de conduire, etc.).

4.1.9 Authentification de l'Abonné

Les vérifications sont du ressort de l'AED et du GC (ou Représentant d'Entreprise), selon les modalités décrites au § 3.3.6.

4.1.9.1 Authentification lors d'une demande initiale

L'authentification lors d'une demande initiale est décrite au §5.1.

4.1.9.2 Authentification lors du renouvellement de clés (hors révocation)

Les bi-clés sont périodiquement renouvelés afin de minimiser les risques d'attaques cryptographiques. Ainsi, les bi-clés des Abonnés sont à renouveler tous les 2 ans.


Avant l'expiration du certificat, l'Abonné et son(ses) Mandataire(s) de Certification (ou Représentant(s) d'Entreprise) sont informés de la fin de vie du certificat. L'Abonné doit alors se connecter sur le site *web* CA Certificat <http://www.ca-certificat.com> pour retirer son nouveau certificat en s'authentifiant à l'aide de son ancien certificat (HTTP/SSLv3 avec authentification mutuelle).

Après l'expiration du certificat, l'Abonné (ou un GC) peut solliciter une Re-génération* auprès de l'Assistance Téléphonique CA Certificat. L'Abonné viendra alors retirer son nouveau certificat sur le site *web* CA Certificat, comme lors du retrait de son premier certificat, à l'aide des secrets convenus avec l'AC (le Code Personnel Utilisateur tel que défini lors de l'enregistrement et un nouveau Code de Retrait généré par l'AC et envoyé par courrier électronique).

4.1.9.3 Authentification lors de la génération d'un nouveau certificat après révocation

Après une révocation, et si cette révocation avait pour cause la compromission, la perte, le vol ou une erreur de retrait du certificat (aucune des informations contenues dans le certificat n'ont changé et l'Abonné est toujours habilité à utiliser un certificat au nom du Client), l'Abonné (ou un Gestionnaire des Certificats) peut solliciter une Re-génération* auprès de l'Assistance Téléphonique CA Certificat.

Dans tous les cas, l'Abonné viendra retirer son nouveau certificat sur le site *web* CA Certificat, comme lors du retrait de son premier certificat, à l'aide des secrets convenus avec l'AC.

	CA CERTIFICAT	N° page : 34/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

4.2 Authentification d'une demande de révocation

L'authentification d'une demande de révocation est la même pour les modes de révocation par téléphone via l'Assistance téléphonique CA Certificat, et par Internet via le site *web* CA Certificat.

Sont demandés :

- le nom du demandeur,
- le prénom du demandeur,
- le motif de révocation,
- l'adresse électronique de l'Abonné,
- le Code Personnel Utilisateur (choisi par le demandeur lors de la souscription et également utilisé lors du retrait du certificat).

Le représentant légal du Client (ou mandataire social), le Gestionnaire des Certificats (Représentant d'Entreprise) ou l'Abonné peuvent se rendre à l'AED pour demander une révocation, et justifier de leur identité en mode "face à face" avec un justificatif d'identité officiel. Ce mode de révocation peut notamment être utilisé si le GC ou l'Abonné ont perdu leur Code Personnel Utilisateur.

4.3 Vérification périodique d'existence


Un certificat et son bi-clé sont délivrés à un *Abonné* dans le cadre de son activité au sein d'une entreprise. Les moyens utilisés lors de la création du bi-clé et du certificat sont suffisants pour garantir que c'est bien la personne physique auquel ils sont destinés qui les reçoivent.

Par contre, l'utilisation ultérieure du certificat par la personne à laquelle il correspond n'est garantie que par l'engagement de respect de la présente PC, signé par l'Abonné lors de sa demande de certificat.

Aussi, une confirmation régulière par l'entreprise de la présence des Abonnés dans l'entreprise et de leur droit au certificat est nécessaire. Elle permettra de détecter les oublis de révocation (suite à des départs en retraite par exemple) et contribuera au renforcement de la sécurité.

La fréquence du contrôle est fixée au maximum à quatre fois la durée de vie du certificat, soit 4 ans. Elle se fera à travers un bordereau envoyé automatiquement au Gestionnaire de Certificat, que ce dernier remplira, signera et transmettra à son AED.

En cas de non-réponse, des relances seront effectuées. Au bout de 6 mois de non-réponse, le certificat concerné sera révoqué d'office par l'AC.

	CA CERTIFICAT	N° page : 35/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5 BESOINS OPERATIONNELS

5.1 Demande de certificat CA Certificat

La demande de certificat se fait en trois temps :

- étape 1 : Remise du Dossier Client par le ou les Mandataire(s) de Certification (Représentant(s) d'Entreprise) dûment mandaté(s) ;
- étape 2 : Contrôle par l'AED des pièces reçues ; contrôle et validation de la demande par l'ACE ;
- étape 3 : Récupération du certificat par l'Abonné.

La demande de certificat suit une procédure différente selon que le Client a déjà ou non souscrit au service "CA Certificat" :

- futur Client n'ayant pas déjà souscrit au service "CA Certificat"

Le(s) Mandataire(s) de Certification (Représentant(s) d'Entreprise) doit(doivent) remettre en main propre (opération d'authentification en « face-à-face », cf. §3.3.6) à l'AED le dossier complet accompagné de l'ensemble des pièces justificatives.

- Client représenté par un de ses GC et ayant déjà souscrit au service "CA Certificat"

Le GC doit seulement constituer un dossier de demande de certificat (ajout d'Abonné). Le dossier est envoyé à l'AED par courrier.

Un Client peut être directement représenté par son représentant légal sans passer par une tierce personne mandatée (cas des artisans, associations, ...). Dans ce cas, le représentant légal est lui-même GC (et peut éventuellement être Abonné). Le dossier doit être accompagné des mêmes pièces justificatives que dans le cas général.

5.1.1 Origine de la demande


Une demande de souscription au service de certification du CEDICAM doit venir d'un représentant légal ou mandataire social.

Les demandes de certificats CA Certificat pour les Abonnées viennent ensuite des Mandataires de Certification (ou Représentants d'Entreprise) désignés par le Client lors de la souscription.

5.1.2 Informations à fournir

Les informations à fournir sont celles transmises dans les Dossiers Clients.

5.1.3 Dossiers Clients

	CA CERTIFICAT	N° page : 36/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.1.3.1 Demande de souscription

La demande de souscription au service de certification CA Certificat prend la forme d'un contrat (« Contrat de Souscription CA Certificat ») liant le Client à l'AED. Ce contrat contient notamment dans ses annexes les fiches nécessaires pour demander des certificats pour des Abonnés, désigner des Mandataires de Certification (ou Représentants d'Entreprise) et louer des lecteurs de carte à puce. Les pièces justificatives à fournir sont indiquées dans le Contrat de Souscription CA Certificat.

5.1.3.2 Demande de certificat CA Certificat

Les demandes de certificats (logiciel ou sur support matériel) pour les Abonnés prennent la forme d'une fiche fournie en annexe du Contrat de Souscription CA Certificat (« Fiche Client n°3 : Abonné »).

Une demande de certificat peut être réalisée au moment d'une souscription au service ou ultérieurement par le biais d'un autre Dossier Client.

Le dépôt d'une demande de certificat ne constitue pas une obligation pour l'AED ou l'Autorité Certifiante d'émettre le certificat demandé.

5.1.3.3 Demande d'ajout ou de révocation de mandat de Gestionnaire des Certificats

Les demandes d'ajout ou de révocation de mandat de Gestionnaire des Certificats (ou Représentant d'Entreprise) prennent la forme d'une fiche fournie en annexe du Contrat de Souscription CA Certificat (« Fiche Client n°2 : Représentant d'Entreprise »).

Une telle demande peut être réalisée au moment d'une souscription au service ou ultérieurement par le biais d'un autre Dossier Client.

5.1.3.4 Demande de location de lecteur de carte à puce


Les demandes de location de lecteur de carte à puce sont réalisées indépendamment de la demande de certificat sur carte à puce. Elles prennent la forme d'une fiche fournie en annexe du Contrat de Souscription CA Certificat (« Fiche Client n°5 : demande de Kit lecteur CA Certificat »).

Une telle demande peut être réalisée au moment d'une souscription au service ou ultérieurement par le biais d'un autre Dossier Client. La mise à disposition de ces lecteurs constitue une prise de location par le Client auprès de l'AED.

5.1.4 Preuve de possession de la clé privée / Format de signature

L'AC opérationnelle "CA Certificat" exige des Abonnés, au moment de la requête de certificat, la preuve de possession de la clé privée, associée à la clé publique à certifier.

La mise en œuvre de ces exigences est décrite dans la DPC.

	CA CERTIFICAT	N° page : 37/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.1.5 Acceptation d'un certificat CA Certificat

L'Autorité de Certification est automatiquement informée du retrait de chaque certificat par l'Abonné correspondant. L'Abonné est tenu d'avertir l'AED de toute inexactitude ou défection d'un certificat dans les sept jours ouvrés consécutifs au retrait du certificat, afin que celui-ci soit révoqué et qu'un autre certificat puisse lui être fourni. L'Abonné est réputé avoir accepté son certificat lorsque ce délai est dépassé, ou lorsqu'il a utilisé son certificat dans le cadre d'une application décrite au § 2.4.1 de cette PC, ou lorsqu'il a utilisé son certificat dans le cadre du service de vérification du certificat offert sur le site *web* <http://www.ca-certificat.com> à l'issue du processus de retrait.

En outre, l'acceptation d'un certificat vaut acceptation de la PC en référence (OID unique stocké dans le certificat).

5.1.6 Génération et émission d'un certificat CA Certificat

Le certificat est généré en ligne puis téléchargé par l'Abonné à partir du site *web* CA Certificat (<http://www.ca-certificat.com>) via son navigateur. Le certificat sera stocké soit sur le disque dur du poste de travail de l'Abonné soit sur le support matériel qui lui a été fourni, selon l'option choisie. Il incombe à l'Abonné de respecter la procédure de retrait indiquée pour ne pas risquer de télécharger son certificat sur son disque dur tandis qu'il avait choisi l'option support matériel.

5.1.7 Archivage des dossiers

Le CEDICAM en tant qu'entité responsable de l'Autorité Centrale d'Enregistrement s'engage à archiver les Dossiers Client.

Ces dossiers sont conservés pendant 10 ans à partir de la date de fin d'abonnement (date de la révocation du certificat pour ce motif spécifique) et / ou à partir de la date de résiliation du Contrat de Souscription CA Certificat.

Durant cette période d'archivage, les dossiers sont consultables sur demande justifiée par les autorités habilitées ou par le représentant légal du Client / l'Abonné / le Gestionnaire des Certificats (Représentant d'Entreprise) concerné.

5.2 Révocation de certificat CA Certificat


Un certificat CA Certificat est dans l'un des trois états suivants : valide, expiré ou révoqué.

5.2.1 Causes possibles de révocation

Lorsque l'une des circonstances ci-dessous se réalise, le certificat concerné doit être révoqué, et le numéro de série est alors placé dans la Liste de Certificats Révoqués (LCR).

5.2.1.1 Révocation d'un certificat d'une composante de l'ICP CA Certificat

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

	CA CERTIFICAT	N° page : 38/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc


- compromission possible, probable ou certaine de la clé privée de l'AC ou de l'ACE ;
- non-conformité de la DPC par rapport à la PC ;
- cessation d'activité de l'Autorité Certifiante ;
- décision de l'Autorité Certifiante de mettre fin à son activité d'AC ou d'ACE, ou de migrer celle-ci sur une autre solution technique incompatible avec la première.

5.2.1.2 Révocation d'un certificat d'Abonné

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

- la clé privée de l'Abonné est suspectée de compromission, est compromise, est perdue ou est volée (y compris perte ou vol du support matériel) ;
- les Données d'Activation conditionnant l'utilisation de la clé privée ont été perdues, ou bien l'utilisation de la clé privée sur support matériel a été bloquée suite à la saisie consécutive d'un nombre déterminé de codes PIN erronés ;
- le non respect des règles d'utilisation du certificat ;
- les informations de l'Abonné figurant dans son certificat ne sont pas ou plus exactes, ceci avant l'expiration normale du certificat ;
- le départ, la mutation à un autre poste ou le décès de l'Abonné, ainsi que la cessation d'activité du Client ;
- l'Abonné ou l'un des Mandataires de Certification (ou Représentants d'Entreprise) en fait la demande (fin d'abonnement) ;
- la résiliation du Contrat de Souscription CA Certificat ;
- le défaut de paiement des sommes dues au titre du Contrat de Souscription CA Certificat ;
- les informations figurant dans les Dossiers Clients ne sont pas ou plus exactes ;
- le changement de numéro de SIREN ou de la dénomination sociale du Client (par exemple en cas de transfert du Contrat de Souscription CA Certificat par apport universel de patrimoine) ;
- le certificat de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats signés par la clé privée correspondante).

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a eu connaissance, le certificat concerné doit être révoqué et le numéro de série placé dans la Liste de Certificats Révoqués (LCR).

	CA CERTIFICAT	N° page : 39/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.2.2 Origines d'une demande de révocation d'un certificat d'Abonné

La révocation d'un certificat d'Abonné peut émaner de :

- l'Abonné au nom duquel le certificat a été émis ;
- l'un des GC (ou Représentants d'Entreprise) ;
- le représentant légal (ou mandataire social) du Client (même s'il ne s'est pas désigné Gestionnaire des Certificats [ou Représentant d'Entreprise]) ;
- l'AC émettrice du certificat ;
- l'ACE ayant autorisé l'émission du certificat ;
- l'AED avec laquelle le Client a établi le "Contrat de Souscription CA Certificat".

5.2.3 Informations à fournir

Cf. paragraphe 4.2.

5.2.4 Procédure de demande de révocation d'un certificat d'Abonné


Une révocation peut être demandée :

- En ligne par l'Abonné (via le site *web* CA Certificat <http://www.ca-certificat.com> accessible 24h/24 7j/7),
- Par téléphone^(*) par l'Abonné ou un Gestionnaire des Certificats (ou Représentant d'Entreprise) (via l'Assistance téléphonique CA Certificat),
- Auprès de l'AED (durant ses heures d'ouverture) par l'Abonné, un Gestionnaire des Certificats, ou le représentant légal du Client (ou mandataire social).

() Aux heures ouvrées, le demandeur est en ligne avec le Support ; aux heures non ouvrées, la demande est prise en charge par un répondeur vocal (enregistrement de la demande).*

Les informations demandées pour une révocation sont indiquées au § 3.2.4 du présent document.

Les procédures de révocation sont détaillées dans la DPC.

	CA CERTIFICAT	N° page : 40/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.2.5 Traitement d'une demande de révocation d'un certificat d'Abonné

A la réception d'une demande de révocation, en provenance de l'un des Mandataires de Certification (ou Représentants d'Entreprise), de l'Abonné, de l'AC ou de l'AED, l'authenticité du demandeur est vérifiée par l'ACE via le Code Personnel Utilisateur renseigné par le demandeur (code correct ou incorrect). Dans le cas où l'Abonné (ou le Représentant d'Entreprise) ne peut pas fournir son Code Personnel Utilisateur, ou si le représentant légal du Client souhaite solliciter une révocation, l'authentification est réalisée dans les locaux de l'AED en mode "face à face" avec un justificatif d'identité officiel. L'AED transmet alors la demande à l'ACE qui vérifie l'habilitation du demandeur à révoquer le certificat.

Si la demande est recevable, l'AC révoque le certificat en faisant introduire le numéro de série du certificat et la date de révocation du certificat dans la Liste des Certificats Révoqués. Si la demande n'est pas recevable, l'AC en informe l'AED afin de reprendre contact avec le demandeur.

L'Abonné, les GC et l'AED sont informés par l'AC de la prise en compte de la demande de révocation via récépissé émanant de l'ACE sous forme d'un courrier électronique.

L'opération est enregistrée dans les journaux d'événements de l'AC.


5.2.6 Procédure de traitement de la révocation d'une composante de l'ICP

Lorsque la décision est prise de révoquer l'une des AC opérationnelles appartenant à la chaîne de confiance d'un certificat d'Abonné (soit l'AC "CA Certificat", soit l'AC racine), les actions suivantes sont réalisées :

- tous les certificats d'Abonnés en cours de validité délivrés par cette AC sont révoqués et inclus dans la LCR,
- les responsables des applications utilisatrices autorisées, les Mandataires de Certification (ou Représentants d'Entreprise) et les Abonnés sont notifiés de la fin de la confiance,
- une demande de révocation pour le certificat de l'AC est transmise à l'AC racine à laquelle l'AC "CA Certificat" est subordonnée.

Lorsque la décision est prise de révoquer l'un des certificats de l'ACE et que le motif de cette révocation est la compromission (avérée ou supposée) de la clé privée correspondante, les actions suivantes sont réalisées :

- tous les certificats d'Abonnés en cours de validité, délivrés depuis la date de compromission (assortie d'une période de sûreté) sur demande de l'ACE, sont révoqués et inclus dans la LCR,

	CA CERTIFICAT	N° page : 41/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

- les GC et les Abonnés concernés sont notifiés de la raison de la révocation de leur certificat,
- une demande de révocation pour le certificat de l'ACE est transmise à l'AC qui l'a émis.

S'il y a lieu, l'émission de certificats « de remplacement » pour les Abonnés sera assurée dans les meilleurs délais.

5.2.7 Délai de traitement d'une révocation

5.2.7.1 Certificat d'une des composantes de l'ICP CA Certificat

En cas de compromission du certificat d'une des composantes de l'ICP CA Certificat (comme décrit au § 4.4.1.1), les Abonnés, les Mandataires de Certification (ou Représentants d'Entreprise) et les responsables des applications utilisatrices autorisées sont prévenus de cette compromission selon les indications du § 4.4.5 au plus tard dans les trois (3) jours ouvrés.

5.2.7.2 Certificat d'Abonné

La demande de révocation et la vérification des droits du demandeur à révoquer le certificat se fait :

- immédiatement si la demande a été réalisée sur le site *web* CA Certificat,
- pendant les heures ouvrées sinon,

et la LCR en ligne est alimentée et rafraîchie toutes les 12 heures. Le délai de publication de la révocation d'un certificat n'excède donc jamais 24 heures ouvrées.

5.2.8 Publication des causes de révocation d'un certificat d'Abonné


Cf. paragraphe 3.9.2.

5.2.9 Besoins spécifiques en cas de révocation pour compromission de clé

Aucune procédure de révocation particulière n'est mise en place si la cause de révocation est la compromission de la clé privée de l'Abonné. La demande de révocation suit le processus défini au § 4.4.4.

5.2.10 Suspension de certificats

Le service de suspension n'est pas proposé dans le cadre de l'ICP CA Certificat.

	CA CERTIFICAT	N° page : 42/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.3 Renouvellement de certificats (hors révocation)

Les bi-clés doivent être périodiquement renouvelés afin de minimiser les attaques cryptographiques. Ainsi, les bi-clés des porteurs seront renouvelés à chaque renouvellement de certificat, et au minimum tous les trois ans.

Afin de faciliter l'exploitation, un nouveau certificat peut être obtenu alors que le certificat courant est encore valide. La demande de renouvellement de clé est alors signée par la clé privée courante du porteur.

5.4 Emission des nouveaux certificats après révocation

Après une révocation, l'attribution et la certification de nouvelles clés suivent la procédure d'enregistrement initial.

Il appartient au porteur de formuler une nouvelle demande de certificat.

5.5 Suspension de certificats

L'Autorité de Certification opérationnelle "CA Certificat" ne permet pas la suspension des certificats.

5.6 Vérification de la validité des certificats

Les applications utilisatrices d'un certificat autorisées doivent vérifier et valider préalablement à son utilisation, le statut du certificat et de sa chaîne de certification, c'est-à-dire vérifier également la signature garantissant l'origine et l'intégrité de la LCR.

5.6.1 Intégrité de la LCR

L'AC signe la LCR disponible, pour garantir son intégrité et attester de son origine.

5.6.2 Contrôle en ligne du statut de révocation de certificat

Il est possible pour un Abonné de vérifier en ligne si son propre certificat CA Certificat est révoqué.


Il est de la responsabilité du porteur de certificat de contrôler la validité (statut de révocation) d'un certificat avant toute utilisation.

L'ICP CA Certificat n'offre pas de service de validation en ligne de type OCSP (*Online Certificate Status Protocol*) aux applications.

5.6.3 Formes de publication des LCR

Les LCR sont consultables aux adresses indiquées dans le champ "Point de distribution de la LCR" du certificat CA Certificat.

Les LCR sont au format LCR version 2 de X.509 version 3.

	CA CERTIFICAT	N° page : 43/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

L'accès aux Listes de Certificats Révoqués est possible via l'annuaire LDAP de l'AC ou via le serveur Web de l'AC en HTTP.

5.7 Renouvellement de clé d'une composante de l'ICP

La période de validité de la clé de l'AC racine est de 20 ans.

La période de validité de la clé de l'AC "CA Certificat" est de 10 ans.

Une AC opérationnelle ne peut pas émettre de certificat dont la date de fin de validité serait postérieure à la date d'expiration du bi-clé de l'AC.

Par conséquent, la période de validité de la clé de l'AC "CA Certificat" doit être supérieure à celle des certificats des Abonnés. L'AC "CA Certificat" doit donc disposer d'un nouveau bi-clé deux ans avant l'expiration de son certificat.

L'Autorité Certifiante se réserve la possibilité de renouveler les clés des AC opérationnelles dont elle est responsable avant leur limite de validité. La décision d'un tel renouvellement anticipé peut être prise en fonction de divers critères (notamment en cas d'évolution soudaine de l'état de l'art cryptographique obligeant à l'emploi de clés de longueur supérieure) et relève du Comité d'Approbaton des Politiques.

L'AC opérationnelle concernée par un tel renouvellement disposera alors de deux certificats correspondant à deux bi-clés, jusqu'à expiration du premier certificat. En ce qui concerne l'AC "CA Certificat", cette période est de 2 ans, et les certificats d'Abonné émis au cours de cette période seront signés par la clé privée du nouveau bi-clé de l'AC.

5.8 Révocation d'une clé d'une composante de l'ICP


5.9 Causes de révocation d'un certificat d'une composante de l'ICP

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

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante,
- décision de changement de composante de l'ICP suite à la détection d'une non-conformité des procédures appliquées par la composante avec celles annoncées dans la DPC,
- cessation d'activité de la composante.

5.9.1 Révocation d'un certificat d'une composante de l'ICP

Les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'ICP sont précisées dans la DPC.

	CA CERTIFICAT	N° page : 44/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.9.2 Révocation du certificat de signature de l'AC

En cas de révocation du certificat de signature de l'AC, l'Autorité Certifiante révoque l'ensemble des certificats des porteurs en cours de validité.

L'ICP indique à tous les Abonnés que leur certificat est révoqué.

L'Autorité Certifiante prévient tous les responsables des applications utilisatrices autorisées (paragraphe 2.4.1), par lettre recommandée avec accusé de réception que le certificat de signature de l'AC a été révoqué.

5.9.3 Délai de traitement

La révocation d'un certificat d'AE ou d'une composante de l'ICP est effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

La révocation du certificat de signature est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.


5.10 Journalisation des événements

La journalisation des événements concerne tous les événements ayant trait à la sécurité des systèmes informatiques utilisés.

Elle permet de garantir l'auditabilité, la traçabilité, l'imputabilité ainsi que de s'assurer que la séparation des fonctions est effective. Ce système permet également de collecter des preuves et de détecter des anomalies. La journalisation des événements est protégée, sauvegardée, intègre et fait l'objet de règles strictes d'exploitation.

Les actions de journalisation sont décrites précisément dans les manuels internes de l'entité responsable de l'ACE et de l'AC opérationnelle et abordent notamment les thèmes suivants :

- événements enregistrés par l'ACE ;
- événements enregistrés par l'AC opérationnelle ;
- processus de journalisation des événements ;
- conservation des journaux d'événements ;
- protection des journaux d'événements ;
- duplication des sauvegardes des journaux d'événements ;
- collecte des journaux d'événements (interne ou externe) ;
- imputabilité ;
- anomalies et audit.

	CA CERTIFICAT	N° page : 45/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Ces éléments sont également décrits dans la DPC.

5.11 Archives

L'archivage est réalisé par l'ACE et l'AC dans le but d'assurer la continuité de service, l'auditabilité et la non-répudiation des opérations.

Les mesures nécessaires sont mises en place par l'ACE et l'AC afin que ces archives soient disponibles, ré-exploitable, protégées en intégrité et qu'elles fassent l'objet de règles strictes d'exploitation et de protection contre la destruction.

L'AC décrit précisément dans ses procédures internes, et notamment la DPC, les points suivants :

- types de données à archiver ;
- période de rétention des archives ;

Dont notamment :


- ▶ Les PC et DPC successives sont conservées pendant toute la durée du service de l'AC.
- ▶ Les certificats, récépissés, notifications et justificatifs d'identité officiels sont conservés 10 ans à partir de la date de fin d'abonnement (date de la révocation du certificat pour ce motif spécifique) et/ou à partir de la date de résiliation du Contrat de Souscription CA Certificat.
- ▶ Les LCR sont conservées 10 ans.
- protection des archives ;
- duplication des archives ;
- horodatage des enregistrements ;
- collecte des archives (interne ou externe) ;
- récupération et vérification des archives.

5.11.1 Cessation ou transfert d'activité d'une composante de l'ICP CA Certificat

5.11.2 Cas des AED

En cas de transfert d'activité d'une AED, cette dernière prévient tous ses Clients, par un moyen à sa discrétion avec un préavis de trois mois.

En cas de cessation d'activité d'une AED, cette dernière prévient tous ses Clients, par un moyen à sa discrétion avec un préavis de trois mois, en lui proposant éventuellement une solution de remplacement.

	CA CERTIFICAT	N° page : 46/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.11.3 Cas de l'Autorité Certifiante

En cas de cessation ou de transfert d'activité de l'Autorité Certifiante,

- l'Autorité Certifiante prévient tous les responsables des applications utilisatrices autorisées, par lettre recommandée avec accusé de réception trois mois avant la date effective de cessation ou de transfert de l'activité,
- l'AED prévient tous ses Clients, par un moyen à sa discrétion avec un préavis de trois mois.

Au terme des trois mois de préavis, si l'Autorité Certifiante est en cessation d'activité, les certificats des AC opérationnelles seront révoqués, ainsi que tous les certificats émis.

Les archives (de l'AC ou de l'ACE) sont prises en charge par la société reprenant l'activité dans le cas d'un transfert d'activité, ou, dans le cas de la cessation d'activité, reprise par une société d'archivage spécialisée, fiable et reconnue par les responsables des applications utilisatrices autorisées. Les entités précitées sont avisées des coordonnées de ces sociétés.

5.11.4 Cas des AC opérationnelles

Si les fonctions de fourniture de certificats pour l'AC sont transférées à une autre entité (transfert de la maîtrise d'œuvre des AC opérationnelles), l'Autorité Certifiante préviendra les responsables des applications utilisatrices autorisées (cf. § 8.2) qui pourront alors vérifier si cette entité a un niveau d'assurance compatible avec leur Référencement. En outre, les dispositions techniques prises pour un tel transfert seront du ressort du Comité d'Approbation des Politiques.


Si décision est prise de mettre un terme à la vie d'une AC opérationnelle, la clé privée de cette dernière qui lui a servi à signer les certificats précédemment émis est détruite, et l'Autorité Certifiante conserve ses obligations d'archivage définies au § 4.7, et s'oblige à :

- communiquer avec un préavis de trois mois son intention de cesser l'activité de l'AC opérationnelle considérée ;
- mettre en œuvre tous les moyens dont elle dispose pour informer ses partenaires de ses intentions ;
- révoquer le certificat de l'AC opérationnelle considérée ;
- révoquer tous les certificats valides qu'elle a signés.

5.12 Fin d'abonnement

Un Gestionnaire des Certificats (ou l'Abonné concerné) peut demander la fin d'un abonnement en révoquant le certificat d'un Abonné et en invoquant le motif adéquat. Aucune Re-génération* ne sera alors possible, et l'abonnement ne sera plus facturé.

La résiliation du Contrat de Souscription CA Certificat entraîne la révocation de tous les certificats d'Abonnés du Client et met fin à leur abonnement.

	CA CERTIFICAT	N° page : 47/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

Contrôle de sécurité physique, contrôle des procédures, contrôle du personnel

Les différents contrôles décrits ici visent, par une gestion des risques adéquate, à assurer un niveau de confiance fort dans le fonctionnement de l'ACE et de l'AC.

5.13 Contrôles de sécurité physique


Des contrôles de sécurité physique sont mis en place par l'ACE et l'AC et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

- situation géographique ;
- contrôle d'accès physique ;
- énergie et air conditionné ;
- exposition aux liquides ;
- sécurité incendie ;
- conservation des médias ;
- destruction des supports ;
- sauvegarde hors site.

5.14 Contrôles des procédures

Des contrôles des procédures sont mis en place par l'ACE et l'AC et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :


- rôles de confiance ;
- nombre de personnes nécessaires à l'exécution de tâches sensibles ;
- identification et authentification des rôles.

	CA CERTIFICAT	N° page : 48/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

5.15 Contrôle du personnel

Des contrôles effectués sur le personnel sont mis en place par l'ACE et l'AC et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

- passé professionnel, qualifications, expérience, et exigences d'habilitations ;
- procédures de contrôle du passé professionnel ;
- exigences de formation ;
- fréquence des formations ;
- gestion des métiers ;
- sanctions pour des actions non-autorisées ;
- contrôle des personnels contractants ;
- documentation fournie au personnel.

	CA CERTIFICAT	N° page : 49/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

6 CONTROLES TECHNIQUES DE SECURITE

6.1 Génération et installation de bi-clés

6.1.1 Génération d'un bi-clé d'Abonné

Dans la procédure de génération de clés pour les certificats CA Certificat, l'Abonné génère lui-même son bi-clé soit de manière logicielle via son navigateur Web, soit sur son support matériel. Il appartient à l'Abonné de se conformer à la procédure correspondant à l'option qu'il a choisie (certificat logiciel ou sur support matériel) pour retirer correctement son certificat.

Le bi-clé généré assure les fonctions :

- de signature (la clé privée est utilisée à des fins de signature et la clé publique à des fins de vérification),
- d'échange de clé (transport des clés secrètes [symétriques] mises en œuvre pour chiffrer ou déchiffrer un message protégé en confidentialité).

6.1.2 Transmission de la clé publique (de l'Abonné) à l'émetteur de certificat

La clé publique est transmise en PKCS#10, au travers d'une session SSL, permettant d'authentifier l'Abonné.

6.1.3 Fourniture d'un certificat d'AC

Le certificat de l'AC est fourni par un moyen protégé en intégrité de bout en bout : il est mis à disposition sur le site *web* de CA Certificat, sécurisé par SSL.

6.1.4 Tailles des clés des Abonnés


Les clés utilisées sont des clés RSA 1024 bits et seront mises à niveau au fur et à mesure de l'évolution de la technique et/ou de la législation.

6.1.5 Paramètres de génération des clés

Les paramètres des clés doivent respecter les normes internationales.

6.1.6 Contrôle de qualité des paramètres des clés de l'AC

La qualité des paramètres des clés doit être effectuée dans le respect des normes internationales.

	CA CERTIFICAT	N° page : 50/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

6.1.7 Mode de génération des clés des composantes de l'ICP CA Certificat

Les procédures détaillées dans la DPC correspondante à la présente PC décrivent la génération des bi-clés des composantes de l'ICP CA Certificat.

La taille de la clé de l'AC opérationnelle "CA Certificat" est de 1024 bits. L'AC racine dispose d'une clé RSA de 2048 bits.

6.1.8 Usage de la clé publique des Abonnés

Les usages possibles de la clé publique des Abonnés sont restreints aux utilisations dans le cadre des applications utilisatrices autorisées en 2.4.1. En particulier, le bi-clé de l'Abonné est utilisé pour la signature et l'échange de clés.

6.2 Protection de la clé privée

6.2.1 Dispositifs de gestion des éléments secrets de l'Abonné

Si l'option choisie est le certificat logiciel, le bi-clé de l'Abonné est stocké par le navigateur sur le disque dur de son poste de travail. L'Abonné doit protéger l'accès à sa clé privée par un mot de passe (ce mot de passe est usuellement défini au moment de la génération des clés).

Dans le cas où l'Abonné dispose d'un support matériel, un code PIN (pendant du mot de passe) est nécessaire pour utiliser la clé privée stockée dans ce support. La saisie d'un nombre déterminé de codes PIN erronés consécutifs provoque le blocage du support matériel.

Néanmoins, le support matériel peut être débloqué par la saisie d'un code de déblocage. Ce code peut être obtenu par un appel au service client après authentification de l'abonné.


Toutefois, La saisie d'un nombre déterminé de codes de déblocage erronés entraîne le blocage du support matériel de manière définitive.

L'Abonné doit dans ce cas révoquer son certificat et solliciter sa recréation.

Il est de la responsabilité de l'Abonné de protéger par mot de passe (« Données d'Activation ») les clés privées de ses bi-clés. Ces Données d'Activation doivent être considérées par l'Abonné comme confidentielles.

6.2.2 Contrôle de la clé privée de signature de l'AC par plusieurs personnes

Un système de secrets partagés (où n exploitants parmi m doivent s'authentifier pour mettre en œuvre les clés privées de signature de l'AC) est mis en place.

	CA CERTIFICAT	N° page : 51/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

6.2.3 Récupération de la clé privée de confidentialité* de l'Abonné

L'ICP "CA Certificat" n'offre pas de service de sauvegarde / séquestre / recouvrement de clé.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques des Abonnés

Les certificats des Abonnés, contenant la clé publique, sont archivés pendant 10 ans après leur fin de validité (expiration ou révocation).

6.3.2 Durée de vie des certificats

La durée de vie des certificats CA Certificat fournis par l'AC "CA Certificat" est de deux ans.

6.4 Données d'Activation des clés privées des Abonnés

6.4.1 Génération et utilisation des Données d'Activation

Les Abonnés gèrent eux-mêmes la protection de leurs clés privées et, à ce titre, génèrent et utilisent de manière autonome, personnelle et sous leur seule responsabilité leurs Données d'Activation.


Dans le cas du support matériel, la saisie de trois Codes PIN erronés consécutifs provoque le blocage du support qui ne peut alors plus être utilisé : l'Abonné doit dans ce cas révoquer son certificat et solliciter sa Re-génération.

6.4.2 Protection des Données d'Activation

L'Abonné est responsable de l'intégrité et de la confidentialité des Données d'Activation liées à sa clé privée.

6.5 Sécurité des postes de travail des composantes de l'ICP

La question de la sécurité des postes de travail des composantes de l'ICP est traitée dans la DPC.

	CA CERTIFICAT	N° page : 52/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

6.6 Contrôles techniques du système durant son cycle de vie

6.6.1 Contrôles des développements des systèmes

L'autorité Certifiante s'engage à ce que les programmes et systèmes de l'ICP CA Certificat aient été développés et implémentés dans le strict respect de l'analyse de risque préalable et de la politique de sécurité qui en découle.

6.6.2 Contrôles de la gestion de la sécurité


L'Autorité Certifiante s'engage à ce que toute évolution des systèmes soit enregistrée sur le livre d'activité du centre de production.

6.7 Contrôles de la sécurité réseau

L'Autorité Certifiante s'engage à ce que les réseaux utilisés dans le cadre de l'ICP CA Certificat fassent l'objet de règles de sécurité informatique correspondant à l'état de l'art en la matière, définies dans la DPC.

6.8 Contrôles des modules cryptographiques


L'Autorité Certifiante s'engage à ce que les modules cryptographiques utilisés dans le cadre de l'ICP CA Certificat soient évalués selon les critères FIPS 140-1 au niveau 2.

	CA CERTIFICAT	N° page : 53/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc


7 PROFILS DE CERTIFICATS ET DE LCR

7.1 Profil des certificats

Champ	Valeur	Détail valeur	Explications
Version	Version 3	2	Version du certificat X.509
Numéro de série	5116 75D5 5D11 8A90 DCBC 0E65 250D B3EF		Le numéro de série unique du certificat attribué par le module cryptographique
Algorithme de signature	md5WithRSAEncryption	1.2.840.113549.1.1.4	Identifiant de l'algorithme de signature de l'AC
Emetteur	CN = nom de l'AC OU = nom de l'Infrastructure O = nom de l'organisation	CN = CA Certificat OU = Infrastructure PKI O = Credit Agricole	Le nom de l'AC émettrice est le Distinguished Name (X.500) de l'AC signant les certificats
Valide à partir du	26 avril 2001 02:00:00	010426020000Z	Dates et heures d'activation et d'expiration du certificat
Valide jusqu'au	27 avril 2003 02:00:00	020427020000Z	
Objet	E = pdurand@societe.fr CN = Pierre DURAND OU = 0002 123456789 O = RAISON SOCIALE L = VILLE SIEGE SOCIAL C = PAYS SIEGE SOCIAL	 Code 2 caractères (ex : FR)	Nom distinctif de l'entité identifiée Un des champs OU doit contenir l'identification ISO 6523 de l'entité, constituée des 4 chiffres de l'ICD (celui du SIREN étant 0002), suivi d'un espace, suivi de l'identifiant proprement dit (par exemple, le numéro de SIREN).
Informations sur la clé publique de l'objet.	RSA(1024 Bits)	3081 8902 8181 00B8 0736 0E69 16B3 38B1 A968 23BD CD1C 346B F5F7 0417 1154 168B A836 9A38 09F2 EFF5 881E 8D4F BE34 6E06 E15A EC10 8519 6D23 12B3 24AE EF5C BF74 6F54 2574 E2DE 6EEE 4CAF 709D 3CBE A273 E3E5 C862 0E7A 0FB3 8A62 0638 44CF 81D1 46B3 69A4 9700 A23C ABD5 32D6 C98C 7095 ECB7 2AD2 4010 76F9 EFAA F9A5 A889 DC4B 9BD3 6759 665D 7B02 0301 0001	Identifiant de l'algorithme d'usage de la clé publique contenue dans le certificat, et valeur de la clé publique

	CA CERTIFICAT	N° page : 54/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc


Contrainte de base	Subject Type=End Entity Path Length Constraint=None	CA = False	
Point de distribution de la LCR	[1]CRL Distribution Point Distribution Point Name: Full Name:	URL = http://crl.certificat.com/CreditAgricoleCACertificat/LatestCRL URL = ldap://ldap.certificat.com/ou=InfrastructurePKI,o=CreditAgricole?certificaterevocationlist?sub?objectclass=certificationAuthority	Point de distribution des CRL. Deux points (un en http et un en LDAP)
Informations sur la politique	[1]PolicyInformation: PolicyIdentifier = 1.2.250.1.104.3.1.1.1.1.2.3.2 [1,1]Policy Qualifier Info: Policy Qualifier Id = 1.3.6.1.5.5.7.2.1 Qualifier = 161C 6874 7470 733A 2F2F 7777 772E 6365 7274 706C 7573 2E63 6F6D 2F52 5041		Identifiant de la Politique de Certification Cet identifiant varie au fil des versions de la PC sur la partie dédiée au CEDICAM (il correspond à un document, la version étant fixée pour identifier sa révision).
Identifiant de la clé de l'émetteur (non-critique)	AuthorityKeyIdentifier: KeyIdentifier [0] = ...	(Valeur hexadécimale calculée automatiquement)	Paragraphe 4.2.1.1 de la RFC 3280 pour la description de cette extension. Paragraphe 4.2.1.2 de la RFC 3280 pour le détail du remplissage.
Utilisation de la clé (non-critique)	digitalSignature, keyEncipherment		
Identifiant de la clé de l'objet (non-critique)	SubjectKeyIdentifier: KeyIdentifier [0] = ...	(Valeur hexadécimale calculée automatiquement)	Paragraphe 4.2.1.2 de la RFC 3280 pour la description de cette extension et le détail du remplissage.
Netscape CertType	03 02 07 80		
2.16.840.1.113733.6.1.9	01 01 FF		

	CA CERTIFICAT	N° page : 55/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

7.2 Profil de LCR

Les LCR de l'AC opérationnelle "CA Certificat" contiennent les champs suivants :

- **version** : la version de la LCR, soit la version 2 (valeur 1) ;
- **signature** : l'identifiant de l'algorithme de signature de l'AC, soit MD5-RSA (1.2.840.113549.1.1.4) ;
- **issuer** : le nom de l'AC opérationnelle émettrice qui signe les certificats, soit l'AC "CA Certificat" ;
- **thisUpdate** : date de génération de la LCR ;
- **nextUpdate** : prochaine date à laquelle cette LCR sera mise à jour ;
- **revokedCertificates** : liste des numéros de série des certificats révoqués, contenant les champs suivants :
 - **userCertificate** : numéro de série du certificat révoqué ;
 - **revocationDate** : date à laquelle un certificat donné a été révoqué.
- **crlExtensions** : liste des extensions de la LCR :
 - **authorityKeyIdentifier** : identifiant de la clé publique de l'AC opérationnelle émettrice qui a signé la LCR ; seul le champ **keyIdentifier** est rempli ;
 - **CRLNumber** : numéro de série de la LCR ;

	CA CERTIFICAT	N° page : 56/56
	POLITIQUE DE CERTIFICATION CA CERTIFICAT	Ref : CA_C_PC_080401_V3.3_Politique de Certification CA Certificat.doc

8 ADMINISTRATION DES SPECIFICATIONS REFERENTES A L'AC

8.1 Modification des spécifications

En cas de projet de modification des spécifications, les cas suivants sont envisageables pour l'AC "CA Certificat" :

- des changements typographiques ne donnant pas lieu à notification et à modification de l'OID de la PC/DPC ou de l'URL ;
- des changements sur le niveau de qualité et de sécurité des fonctions de l'AC et de l'AE (ACE et AED) vis-à-vis des certificats CA Certificat, sans pour autant perdre la conformité de ces derniers avec la PC, et moyennant une période de notification d'un mois avant le début des changements et ne donnant pas lieu à modification de l'OID de la PC/DPC ou de l'URL ;
- des changements entraînant la perte de la conformité des certificats CA Certificat avec la PC et impliquant la modification de l'OID de la PC/DPC et de l'URL de téléchargement.

Les modifications définitives sont soumises aux responsables des applications utilisatrices autorisées avant d'être publiées.

Les modifications sont publiées sur le site Web CA Certificat le jour où l'on en donne notification. Par ailleurs, l'ACE avertit les Clients des modifications par courrier électronique.

8.2 Changements de composantes de l'AC ou de l'AE

En cas de changement intervenant dans la composition de l'AE (ACE et AED) ou de l'AC, le CEDICAM prévient les responsables des applications utilisatrices autorisées :

- Au plus tard un mois avant le début de l'opération si elle a un impact sur le niveau de qualité et de sécurité des fonctions de l'AE (ACE et AED) et de l'AC vis-à-vis des certificats référencés ;
- Au plus tard un mois après la fin de l'opération s'il n'y a pas d'impact.

8.3 Procédure d'approbation de la Politique de Certification CA Certificat

Le Comité d'Approbation des politiques est responsable de la Politique de Certification CA Certificat : il ordonne et approuve ses mises à jour. Les modalités du contrôle de conformité à la Politique de Certification CA Certificat sont précisées au § 2.7.