Autorité de Certification Certigreffe Classe 3Plus v2

POLITIQUE DE CERTIFICATION

Date : 29/06/2006
Version :2.0
OID : 1.2.250.1.106.1.1

Version	Date	Rédigée par	Validée par
1.9.1	03/05/2004	François Renou	Jean-Marc Bahans Jacques Doucède
2.0	29/06/2006	Daniel Mampionona	Dominique Marolleau

Sommaire :

1 PREAMBULE

Une Politique de Certification (PC) est un ensemble de règles identifié par un nom, qui indique les conditions d'applicabilité d'un certificat pour une communauté donnée, ou pour des applications ayant des besoins de sécurité communs.

La PC est définie indépendamment des détails concernant l'environnement de mise en oeuvre de l'infrastructure à clé publique (ICP) à laquelle elle s'applique. La PC établit ce à quoi il faut se conformer lors de la gestion des certificats concernés.

La gestion d'un certificat comprend toutes les phases du cycle de vie d'un certificat, de la demande d'attribution d'un certificat à la fin de vie de ce certificat (péremption, révocation).

Cette PC vise la conformité au document «Procédures et Politiques de Certification de Clés (PC^2)» émis par la Commission Interministérielle pour la Sécurité des Systèmes d'information (CISSI) et la Politique de Certification-type du MINEFI. Compte tenu de la nature des informations échangées entre les déclarants et les services du MINEFI le niveau de conformité recherché est le niveau moyen pour ce qui concerne la mise en oeuvre de la signature numérique.

2 PRESENTATION GENERALE DE LA PC

La Politique de Certification définie dans le présent document est destinée à être utilisée pour les services de certification notamment pour les greffiers des tribunaux de commerce et les entreprises. A cette fin elle s'appuie notamment sur les directives professionnelles définies en matière de signature électronique par le Conseil National des Greffiers des Tribunaux de Commerce (CNG). La Politique de Certification couvre la gestion et l'utilisation des clés et des certificats servant aux fonctions de non-répudiation, d'authentification et d'intégrité. Par exemple, les certificats délivrés en vertu de la présente politique pourraient servir à vérifier l'identité du signataire d'un bilan envoyé aux Greffes des Tribunaux de Commerce, ou d'une télé-déclaration de TVA au MINEFI.

La délivrance d'un certificat en vertu de la présente politique ne signifie pas que le client ou le Porteur soit autorisé de quelque façon que ce soit à faire des transactions commerciales, ou autres, au nom de l'organisation qui exploite l'AC.

L'AC sera assujettie aux lois et règlements en vigueur sur le territoire de la République française, ainsi qu'aux normes européennes en vigueur et aux conventions internationales ratifiées par la France, et qui touchent à l'application, l'élaboration, l'interprétation et la validité des politiques de certification mentionnées dans le présent document.

La présente Politique de Certification s'applique aux certificats de type entreprise.

Cette politique a été conçue pour être utilisée dans certaines situations, et indique par conséquence les rôles et responsabilités spécifiques de l'AC qui délivre ce type de certificat, et ceux des autorités d'enregistrement qui doivent effectuer les tâches qui leur sont assignées par l'AC. Les Porteurs et les Utilisateurs de certificat (ces termes sont définis au §2.2) ont également des obligations spécifiques qui sont définies dans cette politique.

INFOGREFFE décline toute responsabilité concernant l'utilisation de ces certificats pour tout usage autre que ceux permis par la présente PC.

Tout litige concernant la gestion des clés ou des certificats, en vertu de cette politique , doit être réglé par les parties concernées au moyen d'une procédure appropriée comme la négociation, la médiation ou l'arbitrage.

Les Utilisateurs de ce document doivent consulter l'AC émettrice afin d'obtenir plus de détails sur la mise en œuvre de cette politique si cela est nécessaire. L'applicabilité de ces certificats dépendra de leurs utilisations envisagées.

Les certificats pourront être émis en vertu de cette politique après authentification de l'identité du Porteur. L'identification se fera de la manière décrite dans cette politique.

Aucun renseignement personnel recueilli par une AC ne peut être divulgué sans le consentement du Porteur, à moins que la loi ne le prescrive.

Cette PC met en œuvre des certificats de classe 3+ tels que définis ci-après. Selon cette politique sont émis des clés privées et des certificats de clés publiques de classe 3+ utilisés pour l'identification des individus désirant accéder à des données ou à des systèmes d'informations, et pour s'assurer de l'identité du signataire d'un document.

Les certificats sont délivrés dans une procédure incluant un face-à-face avec une AE.

Pour permettre le service de non-répudiation à l'émission dans de bonnes conditions, INFOGREFFE impose l'utilisation de modules cryptographiques de type carte à puce (la clé secrète reste dans la carte).

Les certificats d'Autorité d'Enregistrement dédiés aux greffiers seront validés par une AE supplémentaire réservée à ce seul usage.

Les certificats de classe 3+ comportent un niveau d'assurance garantie, précisé par contrat et accessible à la partie utilisatrice. Lors de l'enregistrement initial, l'identité des détenteurs potentiels de certificats doit être vérifiée par l'AE. L'AE garantit le lien qui existe entre le détenteur du certificat et une paire de clés.

Les demandes de certificats feront l'objet d'une vérification d'identité en face-à-face du Porteur ou du mandataire de certification.

Ce service d'INFOGREFFE est mis en oeuvre sous la forme d'une Autorité de Certification nommée « AC Certigreffe Classe 3Plus v2».

2.1 Liste des acronymes utilisés

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AP	Autorité de Politique
C	Country (Pays)
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
DDS	Dossier de Souscription
DGI	Direction Générale des Impôts
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification, ou EPC
DSA	Digital Signature Algorithm
EAR	Entité d'Audit et de Référencement
EPC	Enoncé des Pratiques de Certification, ou DPC
ICP	Infrastructure à Clés Publiques
LDAP	Light Directory Access Protocol
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
MD5	Message Digest n°5
MINEFI	Ministère de l'Économie, des Finances et de l'Industrie
O	Organisation
OID	Object Identifier
OU	Organisation Unit
PC	Politique de Certification
PC²	Procédures et Politiques de Certification de Clés
RSA	Rivest Shamir Adelman
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standard
PKIX	Public Key Infrastructure X.509
S/MIME	Secure/Multipurpose Internet Mail Extensions

SHA-1	Secure Hash Algorithm One
SSL	Secure Sockets Layer
TLS	Transport Layer Security

2.2 Définitions des termes utilisés dans la PC

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

Abonné : voir Porteur

Applications utilisatrices (de Certificats) : applications nécessitant la mise en œuvre des Certificats délivrés par l'AC*. Dans le cas de l'AC Certigreffe Classe 3Plus v2, ce terme désigne notamment l'application TéléTVA du MINEFI.

Autorité de Certification (AC) : autorité à laquelle les Porteurs* font confiance pour émettre et gérer des clés, des Certificats et des LCR*. Ce terme désigne l'entité responsable des Certificats signés en son nom. L'AC est le maître d'ouvrage de l'ICP*. Elle assure les fonctions suivantes :

- mise en application de la PC* ;
- gestion des Certificats* ;
- gestion des supports et de leur code PIN* ;
- publication des Listes de Certificats Révoqués (LCR*) ;
- journalisation et archivage des événements et informations relatives au fonctionnement de l'ICP*.

Autorité d'Enregistrement (AE) : entité qui vérifie que les demandeurs ou les Porteurs de Certificat sont identifiés, que l'identité présentée est valide et cohérente, que les contraintes liées à l'usage d'un certificat sont remplies, tout cela conformément à la Politique de Certification. L'AE a également pour tâche :

- de réceptionner les demandes de révocation de certificats et de les traiter ;
- d'archiver les dossiers de demande de certificats ou de révocation ;
- l'AE peut être constituée d'une seule unité ou d'unités distinctes, toutes appartenant à la Profession des Greffiers des Tribunaux de Commerce. Elles se sont toutes engagées à répondre aux exigences de la PC* Certigreffe Classe 3Plus v2 en matière d'enregistrement des Porteurs.

Autorité de Politique (AP) : entité chargée d'établir les besoins et les exigences en termes de sécurité dans l'ensemble du processus de certification et d'utilisation des certificats (par exemple le MINEFI). Elle établit des lignes directrices, qui peuvent prendre la forme d'un canevas de Politique de Certification. Elle peut demander un audit de l'AC.

Bi-clé : 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. Le bi-clé peut être utilisé à des fins de signature, ou d'échange de clé ou de transport de clé.

Chaîne de confiance : ensemble des Certificats nécessaires pour valider la filiation d'un Certificat Porteur. Dans une architecture plate ("*flat*"), la chaîne se compose du Certificat de l'AC et de celui

du Porteur. Dans le cadre de cette PC, l'AC Certigreffe Classe 3Plus v2, dispose d'un certificat de signature émis par l'AC Racine appelée CertEurope Root CA.

Code PIN : code adressé par courrier postal au Porteur* après avoir été généré automatiquement et aléatoirement par l'AC*. Il permet de mettre en œuvre le Certificat du Porteur. Le Porteur* assume en toutes circonstances le caractère secret du Code PIN* , aussi l'utilisation de celui-ci fera présumer de manière irréfragable que le Porteur* est bien l'initiateur de l'action opérée (non-répudiation) .

Code de révocation d'un Certificat : code adressé par courrier postal au Porteur* après avoir été généré automatiquement par l'AC* et permettant d'authentifier la demande de révocation du Certificat.

Common Name (CN) : identité réelle ou pseudonyme du Porteur* (exemple CN = Jean Dupont).

Communauté : ensemble de personnes liées entre elles soit par des contrats (exemples : une entreprise et ses fournisseurs, des employés d'une entreprise..) soit par leur qualité (membres d'un ordre….

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

Déclaration des Pratiques de Certification (DPC) : énoncé des procédures et pratiques appliquées par l'AC* pour émettre et gérer des Certificats en respectant les engagement pris dans sa Politique de Certification

Demandeur (de certificats) : personne physique ou morale souhaitant obtenir les services de l'AC.

Distinguished Name (DN) : nom distinctif X.500 pour lequel le Certificat est émis.

Dossier de Souscription (DDS) : ensemble des pièces justificatives à fournir à l'AE* afin de lui permettre de vérifier les informations demandées par l'AC* pour l'émission d'un Certificat. Ces pièces justificatives sont décrites dans la présente PC*.

Émission (d'un Certificat) : fait d'exporter un Certificat à l'extérieur d'une AC* (pour une remise à un Porteur*, ou une demande de publication).

Enregistrement (d'un Porteur) : opération qui consiste pour une Autorité d'Enregistrement* ou un Mandataire de Certification à constituer le profil* d'un demandeur de Certificat à partir de son Dossier de Souscription*, conformément à la Politique de Certification*.

Entité d'Audit et de Référencement (EAR) : organisme qui, sous la responsabilité du MINEFI, est chargé du référencement des Certificats recevables pour la signature de télé-déclarations vers le MINEFI et de l'audit en vue de la vérification du respect des procédures édictées par le MINEFI.

Entreprise : personne morale qui souscrit le contrat avec Certigreffe Classe 3Plus v2 afin que les personnes qu'elle a autorisées puissent être Porteurs* de Certificats.

Génération (d'un Certificat) : action réalisée par une AC* et qui consiste à signer un ensemble de champs (dont la clé publique et le DN du Porteur*) après en avoir vérifié l'origine.

Hébergeur : composante de l'ICP hébergeant la plate-forme matérielle permettant de générer et émettre des Certificats et des Listes de Certificats Révoqués*.

Identificateur d'objet (OID) : identificateur 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.

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*.

Mandataire de Certification : personne physique, dûment identifiée, appartenant à l'Entreprise*, et habilitée par l'AE* pour recueillir et valider les pièces du dossier d'enregistrement lors d'un face à face avec le demandeur*. Le Représentant légal* ou le chef d'Entreprise peuvent également revêtir cette qualité, soit d'emblée, soit lorsqu'au cours du contrat d'abonnement conclu avec l'AC Certigreffe Classe 3Plus v2 ils sont amenés à donner des instructions concernant un Certificat, en lieu et place du Mandataire de Certification habituellement désigné.

Module cryptographique : dispositif matériel, du type module cryptographique ou token muni de microprocesseur, permettant d'une part de générer et protéger les éléments secrets tels que les clés privées ou les codes PIN*, et d'autre part de procéder à des calculs cryptographiques mettant en œuvre ces éléments.

Opérateur de Service de Certification (OSC) : composante de l'ICP disposant d'une plate-forme lui permettant de générer et émettre des certificats pour le compte d'Autorités de Certification.

Politique de Certification (PC) : ensemble de règles, définissant les exigences auxquelles l'AC* se conforme dans la mise en place de prestations adaptées à certains types d'applications. La Politique de Certification doit être identifiée par un OID* défini par l'AC*.

Porteur (de Certificats) : personne physique à qui est délivré un Certificat. Dans la phase amont de certification, il est un "demandeur" de Certificat, et dans le contexte du Certificat X.509V3, il est un "Subject".

Profil (d'un demandeur de Certificat) : informations qui permettent de renseigner les champs du Certificat.

Publication (d'un Certificat) : opération consistant à mettre un Certificat à disposition d'Utilisateurs* pour leur permettre de vérifier une signature (ex : annuaire X.500).

Référencement : opération consistant à contrôler la conformité d'une famille de Certificats afin que ceux-ci soient acceptés par le MINEFI dans le cadre des télé-déclarations. Si le résultat de cette opération est positif, cette famille de Certificats est inscrite dans la liste des certificats référencés tenue par le MINEFI.

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 Porteur*. La re-génération de Certificat après révocation* n'est pas un renouvellement.

Représentant légal : personne physique qui, de par la loi, a qualité pour représenter une entreprise lorsque cette entreprise est une personne morale.

Révocation (d'un Certificat) : opération demandée par le Porteur*, l'AE*, l'AC* ou par toute autre personne autorisée 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*).

Utilisateurs (de certificats) : toute entité (Utilisateur humain, organisme ou entité des technologies de l'information) ayant à utiliser des certificats de clé publique à des fins de vérification de signature. Un Utilisateur de certificat ne détient pas forcément de certificat propre. Par exemple, les services du MINEFI gestionnaires des télé-procédures sont des Utilisateurs des certificats Certigreffe pour vérifier les signatures des télé-déclarants. Dans la suite du document, le terme tiers Utilisateur est également utilisé pour désigner un Utilisateur de certificat.

Validation (de Certificat) : opération de contrôle du statut d'un Certificat ou d'une Chaîne de confiance*.

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

2.3 Type d'applications concernées par la PC

L'Autorité de Certification Certigreffe Classe 3Plus v2 distribue des Certificats qui peuvent être utilisés dans le cadre :

- des télé-procédures administratives du MINEFI comme la déclaration de TVA (Télé-TVA) et la déclaration d'Échanges de Biens (Télé-DEB) ;
- d'applications mises en œuvre par INFOGREFFE;
- d'autres applications ayant signé un accord avec l'AC Certigreffe Classe 3Plus v2 ;
- d'échange de documents signés entre diverses parties.

Cette utilisation implique en particulier l'acceptation par les gestionnaires de l'application ou les utilisateurs de l'intégralité des chapitres contenus dans cette PC.

Si le Certificat est éligible à d'autres télé-procédures, et si l'AC Certigreffe Classe 3Plus v2 accepte que les Certificats soient effectivement utilisés dans le cadre de ces nouvelles applications éventuelles, cette PC sera revue pour que le présent paragraphe les mentionne de façon explicite.

2.4 Type de certificats délivrés par l'AC Certigreffe Classe 3Plus v2

Les certificats délivrés par l'AC Certigreffe Classe 3Plus v2 présentent la particularité de n'être délivrés que suite à un face-à-face entre l'AE et le futur porteur du certificat. Ils ont pour support un module cryptographique (ou autre dispositif cryptographique matériel), dans laquelle le bi-clé est directement généré et stocké.

Ces certificats bien que personnels et nominatifs sont uniquement des certificats « Entreprise » : le Porteur ne peut les utiliser qu'en tant que préposé d'une entreprise concernée par le certificat.

2.5 Modification de la PC

Cette PC sera revue périodiquement notamment pour :

- assurer sa conformité aux normes de sécurité attendues par le MINEFI et l'EAR ;
- 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 deux ans. Les modifications sont réalisées conformément au paragraphe 8 de ce présent document.

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

Version	Date	Principaux points de modification
1.0	01/06/2002	Création de la PC de l'AC Certigreffe Classe 3Plus
1.3.1	05/09/2002	Modification de la PC pour mise en accord avec la PC-type v2
1.9.1	03/05/2004	Modification de la PC pour mise en accord avec la PC-type v3
2.0	29/06/2006	Modification de la PC pour mise en accord avec le standard ETSI TS 101 456

2.6 Identification de la PC - OID

La présente PC est identifiée par l'OID 1.2.250.1.106.1.1. La Déclaration des Pratiques de Certification correspondante est référencée par l'OID 1.2.250.1.105.1.2.

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

2.7 Coordonnées des entités responsables de la présente PC

2.7.1 Organisme responsable

Le GIE INFOGREFFE est responsable de cette PC.

INFOGREFFE

4 Place Félix Eboué

75583 Paris CEDEX 12

FRANCE

2.7.2 Personnes physiques responsables

M. Dominique Marolleau

INFOGREFFE

4 place Félix Eboué

75583 Paris CEDEX 12

2.7.3 Personne déterminant la conformité de la DPC à la PC

INFOGREFFE détermine la conformité de la DPC à la PC soit directement, soit par l'intermédiaire d'experts indépendants spécialisés dans le domaine des Infrastructures à Clé Publique.

3 DISPOSITIONS DE PORTEE GENERALE

3.1 Contrôle de conformité à la PC

3.1.1 Objet des contrôles de conformité

L'Autorité de Certification Certigreffe Classe 3Plus v2 a la responsabilité du bon fonctionnement des composantes de l'ICP, conformément aux dispositions énoncées dans le présent document. L'AC effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement des composantes de cette ICP.

Par ailleurs, l'AC Certigreffe Classe 3Plus v2 souhaite obtenir le référencement par le MINEFI de sa famille de Certificats, afin que ceux-ci soient éligibles aux applications mentionnées parmi les applications concernées (voir § 2.3). Dans ce cadre, l'AC accepte les audits demandés par le MINEFI concernant toutes les composantes de l'ICP, afin que celui-ci s'assure du bon respect de ses exigences.

Enfin l'AC Certigreffe Classe 3Plus v2 accepte les audits demandés par le Conseil National des Greffiers.

3.1.2 Indépendance et qualifications du contrôleur

Le contrôleur est désigné par l'AC ou par le MINEFI dans le cadre du référencement de celui-ci. Le contrôleur est choisi selon des critères d'indépendance et d'expertise dans le domaine de la sécurité informatique et, en particulier, des ICP.

Concernant les audits pour le référencement MINEFI, ceux-ci sont réalisés par l'EAR du MINEFI.

3.1.3 Fréquence du contrôle de conformité

Un contrôle est réalisé au moins une fois par an à la demande de l'AC.

Le contrôle de conformité est réalisé en cas de renouvellement d'un bi-clés d'AC, avant toute nouvelle émission et signature de Certificats par cette dernière.

Les contrôles réalisés à la demande du MINEFI sont renouvelés tous les 2 ans..

3.1.4 Périmètre du contrôle de conformité

Le contrôle de conformité porte sur les points suivants

- dispositions générales (cf. chapitre 3) ;
- identification et authentification (cf. chapitre 4) ;
- besoins opérationnels. (cf. chapitre 5) ;
- contrôles de sécurité physique, contrôle des procédures, contrôle du personnel.(cf. chapitre 6) ;
- contrôles techniques de sécurité . (cf. chapitre 7) ;
- profil des certificats et LCR. (cf. chapitre 8) ;
- spécifications d'administration. (cf. chapitre 9) ;

3.1.5 Communication des résultats

Les résultats du contrôle de conformité sont communiqués par le contrôleur au demandeur (par exemple INFOGREFFE, le Conseil National des Greffiers ou le MINEFI).

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

3.1.6 Actions entreprises en cas de non-conformité

En cas de non-conformité, l'AC Certigreffe Classe 3Plus v2 décide de toute action correctrice nécessaire.

En fonction du degré de non-conformité de la DPC à la PC, l'AC Certigreffe Classe 3Plus v2 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 ;
- demander la révocation de son Certificat à l'AC racine CertEurope Root CA.

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 l'ensemble des documents relatifs à l'abonnement au service de certification de l'AC Certigreffe Classe 3Plus v2). 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 aux Conditions Générales du Service de Certification Certigreffe Classe 3Plus v2.

Si une disposition de la présente PC s'avérait inapplicable ou incompatible avec une loi ou un règlement en vigueur, elle sera considérée comme nulle, mais cette nullité n'affectera en aucune manière la validité des autres dispositions de la présente PC.

La liste des textes spécifiques à l'activité de prestataire de services de certification est en Annexe 1 du présent document.

3.2.2 Séquestre

Sans objet, la présente PC ne concernant que des certificats de signature.

3.2.3 Arbitrage des litiges

En cas de litige relatif à l'émission d'un certificat dans le cadre de la présente PC, l'intervenant concerné adressera une notification à INFOGREFFE. INFOGREFFE et l'Intervenant concerné rechercheront une résolution amiable au litige dans un délai de quinze jours.

En l'absence de solution amiable dans un délai précité, les litiges seront soumis à une procédure d'expertise amiable auprès d'un expert agréé auprès de la cour d'appel de Paris dont la durée sera fixée par l'expert saisi.

L'expert amiable doit tenter de concilier les intervenants dans un délai de deux (2) mois à compter de sa saisie. Il propose un rapport en vue de concilier chacun des intervenants. Ce rapport a un caractère confidentiel et ne peut servir que dans le cadre de la procédure d'expertise amiable. Cette procédure doit être soldée :

- soit par la production d'un accord transactionnel et confidentiel, en cas de conciliation, co-signé par les intervenants,
- soit par un procès verbal de non-conciliation co-signé par les intervenants.

En cas de litige qui ne trouverait pas de solution acceptable par les Intervenants concernés dans les conditions définies aux deux alinéas précédents, les parties à ce contrat conviennent que le litige sera soumis au Tribunal de Commerce de Paris.

Si une disposition de la présente PC s'avérait inapplicable ou incompatible avec une disposition impérative d'une loi ou d'un règlement en vigueur, elle sera considérée comme nulle, mais cette nullité n'affectera en aucune manière la validité des autres dispositions de la présente PC.

3.3 Obligations

3.3.1 Obligations de l'AC

L'AC Certigreffe Classe 3Plus v2 garantit le respect des exigences définies dans la présente PC ainsi que dans la DPC associée. Quels que soient les recours à des entités extérieures pour la mise en œuvre de son activité de certification, l'AC garantit le respect de ces exigences par chacune de ces entités.

3.3.2 Obligations de l'AE

Lorsque l'AE Certigreffe Classe 3Plus v2 est saisie d'une demande de Certificat, elle doit :

- vérifier avec un soin raisonnable l'apparence de conformité et la cohérence des pièces justificatives ainsi que l'exactitude des mentions qui établissent l'identité du Porteur* et de l'Entreprise* selon les procédures décrites au chapitre 4 de cette PC ;
- déclencher la génération du bi-clé du Porteur sur un module cryptographique vierge.
- transmettre la demande de certificat à l'AC Certigreffe Classe 3Plus v2 ;
- transmettre les supports physiques des certificats aux demandeurs ;
- Archiver les pièces du dossier.

Note : L'AE ne peut pas utiliser le certificat du Porteur car le module cryptographique support du certificat est personnalisé devant le demandeur et lui est remise immédiatement.

Lorsque l'AE Certigreffe Classe 3Plus v2 est saisie d'une demande de révocation de Certificat, elle s'engage à :

- vérifier avec un soin raisonnable l'apparence de conformité et la cohérence de l'origine de la demande,
- mettre en œuvre les moyens permettant de traiter la demande de révocation selon les exigences décrites au § 4.4.

L'AE Certigreffe Classe 3Plus v2 doit archiver les dossiers de souscription des porteurs (et éléments de confirmation d'acceptation) et de demandes de révocation suivant les modalités décrites au chapitre 4 de cette PC.

3.3.3 Obligations communes à toutes les composantes de l'ICP

Les composantes de l'ICP s'engagent à :

- protéger et garantir l'intégrité et la confidentialité de leurs clés privées ;
- n'utiliser leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification ;

- respecter et appliquer la PC et DPC associée au moins pour les parties leur incombant;
- se soumettre aux contrôles de conformité effectués par INFOGREFFE ou par l'EAR du MINEFI, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- respecter les accords ou contrats qui les lient entre elles ainsi qu'aux Entreprises et Porteurs de Certificats ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

Les membres du personnel de l'ICP, et les opérateurs mandatés, à qui sont assignés des rôles relatifs à l'ICP doivent être personnellement responsables de leurs actes. L'expression « personnellement responsable » signifie que l'on puisse imputer une action à une personne.

3.3.4 Obligations relatives à la gestion des Certificats

L'AC Certigreffe Classe 3Plus v2 s'engage à :

- pouvoir démontrer aux applications utilisatrices de ses certificats, qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, ceci implique entre particulier de pouvoir justifier de l'identité de tout porteur de certificat ;
- tenir à disposition des Porteurs et des Utilisateurs, la liste des certificats ayant fait l'objet d'une révocation; cette liste est publiée sous la forme d'une LCR conformément au chapitre 3.3.7 ;
- garantir la cohérence entre la PC et la DPC associée ;
- prendre toutes les mesures raisonnables pour s'assurer que ses Porteurs connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des Certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'ICP. La relation entre un Porteur et l'AC Certigreffe Classe 3Plus v2 est formalisée par un document intitulé "Conditions Générales des Certificats Certigreffe Classe 3Plus" précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

3.3.5 Obligations relatives à la gestion des supports, des codes PIN et des codes de révocation

L'AC Certigreffe Classe 3Plus v2 s'engage à :

- transmettre en toute confidentialité les codes PIN aux Porteurs par un moyen sécurisé différent de celui utilisé pour la remise du certificat (qui est délivré en mains propres par l'AE sur un module cryptographique) ;
- supprimer toute trace des codes PIN sur ses systèmes après transmission au Porteur ;
- assurer la confidentialité des codes de révocation* ;
- assurer le caractère aléatoire des codes PIN générés.

3.3.6 Obligations relatives à l'identification

L'identification du Porteur est assurée par l'AE éventuellement assistée du MC.

L'identification du Porteur consiste en la vérification de son identité ainsi que celle de l'entreprise en se basant sur les pièces justificatives présentées, comme précisé au chapitre 3.3.2

3.3.7 Obligations relatives à la publication

L'AC Certigreffe Classe 3Plus v2 s'engage à diffuser publiquement :

- la Politique de Certification Certigreffe Classe 3Plus v2 en cours de validité ;
- la Liste de Certificats Révoqués (LCR) ;
- le certificat de l'AC à laquelle elle est subordonnée (i.e. le certificat de l'AC Certeurope ROOT CA) ;
- La liste des AC avec lesquelles elle est en certification croisée ainsi que les empreintes de leurs certificats.

L'accès à ces informations ne fait l'objet d'aucune facturation.

L'AC Certigreffe Classe 3Plus v2 n'étant en certification croisée avec aucune autre AC, la publication de la liste des AC avec lesquelles elle est en certification croisée est sans objet.

L'AC Certigreffe Classe 3Plus v2 s'engage à ce que la LCR soit :

- 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 (mais accès libre en consultation) ;
- publiée suivant les modalités décrites au chapitre 5.2 de cette PC ;
- disponible 24 heures sur 24 et 7 jours sur 7.

La prise en compte de la demande est immédiate, en cas de succès de l'authentification du demandeur (par l'AE) la requête (création ou révocation) est exécutée immédiatement. Ceci signifie en particulier que, pour une demande licite, la génération du certificat est immédiate ainsi que la publication de la LCR.

3.3.8 Obligations relatives à la journalisation

L'AC Certigreffe Classe 3Plus v2 enregistre tout événement relatif à son activité de certification. Ces enregistrements concernent :

- L'accès physiques aux machines de la plateforme ;
- L'accès logique aux systèmes ;
- L'accès aux applications ;
- Les opérations effectuées sur ces applications.

Certains de ces journaux font l'objet de renseignements manuels, certains sont entièrement automatisés; tous concourent à assurer l'imputabilité de toute action sur la plate-forme de certification.

3.3.9 Obligations relatives à l'archivage

L'AC Certigreffe Classe 3Plus v2 s'engage à archiver non seulement les journaux d'événement tels que décrits au chapitre 3.3.8, mais également tous les dossiers des demandeurs (pièces justificatives…).

Bien entendu ces archives sont disponibles en cas de nécessité (litige ou autre).

3.3.10 Obligations relatives au séquestre

L'AC Certigreffe Classe 3Plus v2 ne réalise pas de fonction de séquestre.

3.3.11 Obligations du Mandataire de Certification.

Le MC* est une personne en relation directe avec l'AE pour le compte des Porteurs de l'entreprise à laquelle il appartient. Il assure les fonctions d'identification des demandeurs pour le compte de l'AE. Il est dûment authentifié par une AE habilitée et lié contractuellement avec l'AC Certigreffe Classe 3Plus v2.

Les engagements du MC à l'égard de l'AC sont précisés dans un contrat dans lequel le MC s'engage en particulier à effectuer correctement et de façon indépendante les contrôles d'identité du demandeur.

Le MC s'engage à :

- vérifier avec un soin raisonnable l'apparence de conformité et la cohérence des pièces justificatives et l'exactitude des mentions qui établissent l'identité du Porteur* de l'Entreprise selon les procédures décrites au chapitre 3 ;
- vérifier avec un soin raisonnable l'origine et l'exactitude d'une demande de révocation de certificat, et mettre en œuvre les moyens permettant de traiter la demande de révocation selon les exigences décrites au §4.4 ;
- effectuer correctement et de façon indépendante les contrôles du dossier du demandeur ;
- n'accepter que les demandes de certificats d'entreprise pour des porteurs mandatés par l'entreprise à laquelle ils appartiennent ;
- à signaler par écrit à l'AE son départ de l'entreprise.
- protéger la confidentialité des codes de révocation d'urgence qui lui seront transmis par les Porteurs.
- ne pas tenter d'utiliser le module cryptographique d'un Porteur.

La relation entre le MC et l'AC Certigreffe Classe 3Plus v2 est formalisée par un engagement contractuel du MC.

Note : Ces engagements ne changent en rien ceux de l'AE.

3.4 Obligations du Porteur

Le Porteur a l'obligation de :

- communiquer des informations exactes lors de la demande de certificat ;
- informer l'AE ou l'AC Certigreffe Classe 3Plus v2 en cas de modifications de ces informations ;

- protéger sa clé privée par des moyens appropriés à l'environnement dans lequel se trouve cette clé, contre la perte, la divulgation, la compromission, la modification ou l'usage non autorisé ;
- définir son code de révocation. Ce code doit impérativement être défini dès réception du code PIN par le Porteur afin de permettre à celui-ci de demander une révocation d'urgence de son certificat. La procédure à suivre pour la définition est indiquée dans le courrier accompagnant le code PIN. Dans le cas où le Porteur ne définirait pas ce code de révocation, la révocation d'urgence ne sera pas possible.
- protéger son code PIN et son code de révocation d'urgence ;
- transmettre son code de révocation d'urgence à son MC lorsque celui-ci existe.
- respecter les conditions d'utilisation de sa clé privée et du Certificat correspondant ;
- informer sans délai son MC, l'AE ou l'AC Certigreffe Classe 3Plus v2 en cas de compromission ou de soupçon de compromission de sa clé privée.

La relation entre le Porteur et l'AC Certigreffe Classe 3Plus v2 est formalisée par un engagement contractuel du Porteur.

3.5 Obligations des applications utilisatrices et des utilisateurs de Certificats

Les applications utilisatrices et utilisateurs de Certificats doivent :

- respecter l'usage pour lequel un Certificat a été émis en particulier lorsque cet usage a été déclaré critique ;
- vérifier la signature numérique de l'AC Certigreffe Classe 3Plus v2 émettrice du Certificat ainsi que celle de l'AC Certeurope Root CA ;
- contrôler la validité des Certificats (date de validité et statut de révocation) des Porteurs mais aussi des AC Certigreffe Classe 3Plus v2 et Certeurope Root CA.

3.6 Responsabilités

La responsabilité de l'un quelconque des intervenants dans la certification d'une transaction et toute opération qui s'y rattache (AC, prestataire de l'AC, client, Abonné, Utilisateur de certificat, …) ne pourra être mise en jeu que si cet intervenant a commis une faute ou une négligence, ou s'il est responsable en vertu d'une clause contractuelle qui lui est applicable.

Le contrat à établir entre l'AC et chaque intervenant définira les limites d'utilisation des certificats émis par l'AC dans le cadre de celui-ci.

D'une façon générale toutes les obligations de l'AC découlant de la présente PC sont des obligations de moyens. En outre, l'AC ne pourra pas être tenue pour responsable d'un fait dommageable qui lui serait imputable si ce fait a été causé par un événement quelconque hors du contrôle raisonnable de l'AC.

3.6.1 Responsabilité de l'AC

L'AC Certigreffe Classe 3Plus v2 s'engage à respecter la conformité de son dispositif de gestion des Certificats et de ses procédures avec les exigences décrites dans cette PC.

L'AC Certigreffe Classe 3Plus v2 est responsable de toute conséquence dommageable résultant du non-respect du présent document par elle-même ou l'une de ses composantes.

L'AC Certigreffe Classe 3Plus v2 est responsable en cas de négligence ou de faute intentionnelle des préjudices causés à une personne physique ou morale, y compris le MINEFI qui s'est fiée raisonnablement aux certificats Certigreffe.

Le détail des engagements pris envers les Porteurs et les Entreprises est détaillé dans les Conditions Générales du contrat d'abonnement et dans les Conditions Générales des Certificats Certigreffe.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes.

3.6.2 Responsabilité de l'AE

Seule l'AC Certigreffe Classe 3Plus v2 peut mettre en cause la responsabilité de l'AE, ce qui exclut explicitement tout engagement de l'AE envers les Entreprises clientes, les Porteurs et les utilisateurs finaux.

3.7 Politique de confidentialité de l'AC

3.7.1 Types d'informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

- les clés privées associées aux Certificats ;
- les Codes PIN pour les Porteurs ;
- les données d'identification ou autres informations personnelles du Porteur contenues dans son certificat, sauf :
    - si le Porteur a donné explicitement son consentement préalablement à la publication du Certificat ;
    - si leur publication a été demandée sur décision judiciaire ou administrative ;
- les causes de révocations des Certificats ;
- les journaux d'événements des composantes de l'ICP Certigreffe Classe 3Plus v2 ;
- le dossier de demande de certificat du Porteur, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les Certificats) ;
- les rapports d'audit ;
- la DPC.

Ces données ne seront utilisées et ne feront l'objet de communication extérieure que pour les seules nécessités de la gestion des opérations effectuées en exécution de la DPC associée à la présente PC, pour répondre aux exigences légales ou pour l'exécution de travaux ou de prestations de services confiés à des prestataires.

Les personnes sur lesquelles portent ces informations nominatives auront le droit d'en obtenir communication, auprès de l'AE, et d'en exiger le cas échéant, la rectification comme précisé dans la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3.7.2 Divulgation des causes de révocation

La cause de la révocation n'est pas publiée dans la LCR.

3.7.3 Remise sur demande du propriétaire

L'AC Certigreffe Classe 3Plus v2 ne dispose pas d'information que le Porteur ne possède (en particulier la clé privée et le code PIN), en conséquence Certeurope ne remettra aucune donnée sur demande du propriétaire hormis bien entendu les informations protégées par la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3.7.4 Délivrance aux autorités habilitées

L'activité de l'AC Certigreffe Classe 3Plus v2 s'exerce dans le cadre de la législation française, aussi sur requête d'une autorité habilitée, l'AC Certigreffe Classe 3Plus v2 peut être amenée à fournir certaines informations confidentielles selon la loi L90-1170.

3.7.5 Droits de propriété intellectuelle

Lors de l'exécution des prestations de services définies dans le présent document et/ou de tout autre document contractuel relatif au Service de Certification Certigreffe Classe 3Plus v2, 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 de tout autre document contractuel relatif au Service de Certification Certigreffe Classe 3Plus v2.

Tous les droits de propriété intellectuelle détenus par l'AC sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non respect. Par exemple, conformément à la loi n°98-536 du 1er juillet 1998 (Journal officiel du 2 juillet, p.10075) et à la directive européenne 96/6/CE du 11 mars 1996, les bases de données réalisées par l'AC sont protégées. Le texte de la loi peut être consulté sur le site suivant : http://www.legifrance.gouv.fr.

En vertu des articles 323-1 à 323-7 du Code pénal, applicables lorsque une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc.

Les peines encourues varient de 1 à 3 ans d'emprisonnement et d'une amende allant de 100.000 à 15.000.000 francs pour les personnes morales.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctifs, droits d'auteur (par exemple : logiciels, pages WEB, bases de données, textes originaux, etc.) est sanctionnée par les articles L 716-1 et suivants du Code de la propriété intellectuelle.

4 IDENTIFICATION ET AUTHENTIFICATION

4.1 Enregistrement initial d'un Porteur

4.1.1 Conventions de noms

Les Certificats émis par l'AC Certigreffe Classe 3Plus v2 contiennent dans le champ "*Subject*", le nom distinctif X501 (DN) du Porteur du Certificat au format *printableString*. Cette mention est obligatoire. En cas d'homonymie, un champ supplémentaire sera utilisé afin de différencier les 2 homonymes.

4.1.2 Nécessité d'utilisation de noms explicites

Les informations portées dans le champ "Subject" du Certificat **Certigreffe** sont décrites ci-dessous de manière explicite selon les différents champs X509:

- dans le champ Country : les caractères FR ;
- dans le champ Organization le numéro SIREN de l'Entreprise, tel que figurant au Registre du Commerce et des Sociétés ou dans l'avis SIRENE ; ce numéro sera précédé de la chaîne de caractères « 0002 » ;
- dans le premier champ Organizational Unit la raison sociale de l'Entreprise, telle que figurant au Registre du Commerce et des Sociétés, ou dans l'avis SIRENE ;
- dans le champ Common Name le prénom et le nom du Porteur ;
- dans le champ Email l'adresse email du porteur.

Tout autre champ (Title, Locality…) est purement informatif et n'a donné lieu à aucune vérification avancée.

4.1.3 Règles d'interprétation des différentes formes de noms

Aucune interprétation particulière n'est à faire sur les informations portées dans le champ "Subject" des Certificats.

Ces informations sont établies par l'AE 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 par l'unicité de son numéro de série.

L'unicité du DN est elle-même garantie par l'unicité des informations permettant de construire ce dernier. Il s'agit du numéro SIREN pour différencier deux Entreprises, du nom et du prénom du Porteur de son adresse de messagerie.

4.1.5 Procédure de résolution de litige sur déclaration de nom

L'AC s'engage quant à l'unicité des noms de ses Porteurs, conformément au chapitre 4.1.4. Elle proposera des procédures de résolution amiable des litiges portant sur la revendication d'utilisation d'un nom, portant sur la demande d'informations complémentaires qui devront être consignées dans

le dossier d'enregistrement. Ces informations sont les prénoms de l'état civil ainsi que la date et lieu de naissance du demandeur.

4.1.6 Reconnaissance, authentification et rôle des noms de marques

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L.711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n°92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

L'AE limite ses vérifications concernant le droit d'utiliser un nom à la vérification des informations contenues dans les pièces d'identité, les mandats éventuels, le Registre du Commerce et des Sociétés ou l'avis SIRENE.

INFOGREFFE dégage toute responsabilité en cas d'utilisation illicite par les clients et Porteurs des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.

4.1.7 Authentification du MC

La distribution des certificats par l'AE nécessite impérativement un face-à-face. Ce face-à-face peut se faire entre un MC et l'AE auquel cas l'AE vérifie la production :

- d'un original d'une pièce d'identité officielle du mandataire de sécurité comportant sa photo et sa signature et en prend copie ;
- du mandat signé par le représentant légal de l'entreprise désignant le MC à qui le certificat doit être délivré ;
- d'un engagement signé par le MC, l'engageant à effectuer correctement les contrôles des dossiers des demandeurs ;
- du Dossier De Souscription (DDS).

4.1.8 Authentification du demandeur

La distribution des certificats par l'AE nécessite impérativement un face-à-face. Ce face-à-face peut se faire directement entre le demandeur et l'AE auquel cas l'AE vérifie un original d'une pièce d'identité officielle du demandeur comportant sa photo et sa signature et en prend une copie.

4.1.8.1 Contenu du dossier déposé par le demandeur

Les informations suivantes doivent au moins figurer dans le DDS :

- une demande écrite, sur papier à entête portant le numéro SIREN de l'entreprise, signée par le représentant légal, un modèle est proposé sur le site www.infogreffe.fr ;
- une photocopie d'un justificatif d'identité du représentant légal muni d'une photo (permis de conduire, carte d'identité nationale, passeport) ;
- une déclaration du Porteur, portant l'acceptation des engagements du Porteur et désignant éventuellement le MC pour le représenter auprès de l'AE et se faire remettre le certificat ;
- une pièce portant le numéro d'identification de l'entreprise si le future Porteur ne fait pas partie d'une société immatriculée au Registre des Commerces et de Sociétés (par exemple avis SIRENE) ;

- une adresse postale professionnelle du Porteur ;
- un justificatif d'identité (du demandeur) muni d'une photo (permis de conduire, carte d'identité nationale, passeport) ainsi qu'une copie de ce justificatif ;
- le nom d'Abonné à utiliser dans le certificat ;
- l'adresse de courrier électronique du demandeur.

4.1.8.2 Contenu du dossier déposé par un MC

En sus des données décrites au chapitre 4.1.8.1, et conformément au chapitre 4.1.7 le DDS doit contenir :

- un justificatif d'identité du MC muni d'une photo (permis de conduire, carte d'identité nationale, passeport) du Porteur ainsi qu'une copie de ce justificatif ;
- Un mandat signé par le représentant légal de l'entreprise désignant le MC comme tel ;
- Un engagement signé par le MC, l'engageant à effectuer correctement les contrôles des dossiers des demandeurs.

4.2 Authentification d'une demande de révocation

La procédure suivie pour authentifier une demande de révocation varie selon le mode de révocation:

- Selon la même procédure que pour l'enregistrement initial ;
- Par l'échange d'informations secrètes (code de révocation d'urgence) entre le demandeur de la révocation (Porteur ou MC) et l'Autorité d'Enregistrement. Le code de révocation d'urgence est défini par le Porteur et n'est connu que de lui-même et de son MC si celui-ci existe.

4.3 Renouvellement de clés (hors révocation)

L'Autorité de Certification Certigreffe Classe 3Plus v2 ne permet pas le renouvellement de ses Certificats.

4.4 Régénération de clés après révocation

Le Porteur suit le processus normal de demande de certificat décrit au § 4.1, si celle-ci intervient après une révocation.

5 BESOINS OPERATIONNELS

5.1 Demande de Certificat

5.1.1 Origine de la demande

Une demande de certificat Certigreffe Classe 3Plus v2 doit venir du représentant légal de l'Entreprise ou du Porteur dans le cas d'artisans, de professionnels libéraux…

5.1.2 Informations à fournir

Les informations à fournir sont celles transmises dans le DDS (voir chapitre 4.1.8.1)

5.1.3 Procédure de demande

La demande de certificat se fait en quatre étapes :

- étape 1 : Face à face entre l'AE et le demandeur (ou le MC représentant le demandeur). Vérification de l'identité du demandeur ou du MC. Vérification et copie du DDS, chaque copie étant signée par l'AE et le demandeur (ou le MC) et accompagnée de la mention « conforme à l'original »;
- étape 2 : Emission du module cryptographique du porteur (contenant son certificat et son bi-clé) par l'AE ;
- étape 3 : Remise du module cryptographique en mains propres au Porteur ou au MC le représentant par l'AE ;
- étape 4 : Envoi par courrier postal du code PIN (et le cas échéant du code de révocation) au Porteur.

Note : Les étapes 1 et 2 peuvent éventuellement être inversées : l'AE génère le bi-clé et le certificat sur simple envoi d'information de la part du demandeur, ce n'est qu'à la remise en mains propres qu'elle effectue les vérifications d'identité.

5.1.4 Preuve de possession de la clé privée.

Afin d'assurer le Porteur qu'aucune copie de sa clé privée n'a été conservée, la clé privée du Porteur est générée par le module cryptographique.

5.1.5 Acceptation du Certificat

L'AC doit obtenir confirmation de l'acceptation du Certificat par le Porteur.

5.1.6 Dossier de Souscription (DDS)

5.1.6.1 Dossier déposé auprès d'une AE

Le dossier doit comprendre au moins l'équivalent des pièces suivantes :

- Si le futur Porteur appartient à une entreprise, un mandat signé par un représentant de l'Entreprise désignant la personne physique à qui le certificat doit être délivré. Ce mandat doit être signé pour acceptation par la personne physique bénéficiaire ;
- Si le futur Porteur n'appartient pas à une Entreprise inscrite au Registre du Commerce et des Sociétés, une pièce portant l'identification officielle de l'Entreprise retenue dans le certificat (généralement cette identification sera le numéro SIREN de l'Entreprise et la pièce un Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements) ;

- un justificatif d'identité du futur Porteur entendus comme tels par la législation française (carte d'identité nationale, passeport, livret de famille, permis de conduire, etc…).

Lorsque le Demandeur est représenté par un MC, celui-ci doit de plus présenter un mandat du futur porteur le désignant comme MC.

5.1.6.2 Dossier du MC d'une entreprise

Le MC n'a pour l'AC Certigreffe Classe 3Plus v2 qu'un rôle de porteur de DDS et de modules cryptographiques, son dossier ne sert pas à compléter ou bâtir les dossiers des Porteurs, en conséquence son dossier doit comprendre les mêmes pièces que celles pour un Porteur.

5.1.7 Archivage des dossiers

Chaque Dossier de Souscription est archivé par l'AE conformément à la législation en vigueur, pendant cinq ans à partir de la date de clôture du dossier de souscription (fin d'abonnement).

Durant cette période d'archivage, le Dossier de Souscription est consultable sur demande justifiée par les autorités habilitées, par le Porteur et le représentant légal de l'Entreprise avant destruction des dites archives.

5.1.8 Opérations à effectuer

L'AE ou le MC s'engagent à effectuer les vérifications suivantes :

- établir l'identité (réelle) du futur Porteur ;
- s'assurer grâce à la chaîne des mandats que le futur Porteur appartient bien à l'Entreprise ;
- s'assurer que le futur Porteur a pris connaissance des modalités applicables pour l'utilisation du Certificat ;
- s'assurer qu'il n'existe pas d'homonyme déjà porteur de certificat dans l'Entreprise.

L'AE s'engage à effectuer les opérations suivantes :

- attribuer un module cryptographique au demandeur, et faire générer par ce module le bi-clé du Porteur ;
- saisir les informations nominatives qui se trouveront dans le certificat ;
- signer la demande de certificat qui est envoyée au serveur de l'AC Certigreffe Classe 3Plus v2 ;
- installer le certificat signé reçu de l'AC Certigreffe Classe 3Plus v2 dans le module ;
- remettre le module cryptographique contenant la clé privée et le certificat au demandeur (Porteur ou MC) ;
- archiver le dossier (DDS) conformément à la procédure d'archivage.

Le MC s'engage à remettre le module cryptographique à son porteur.

*5.1.9 Emission et distribution d'un **Certificat***

A l'issue de la procédure d'enregistrement, le Certificat est transmis par l'AC Certigreffe Classe 3Plus v2 au module cryptographique du Porteur où il est sauvegardé.

L'émission d'un certificat par l'AC Certigreffe Classe 3Plus v2 indique que celle-ci a définitivement et complètement approuvé la demande de certificat selon les procédures décrites dans la DPC. Le

certificat est considéré comme valable dès le moment où le demandeur accepte le module cryptographique, support du certificat.

5.1.9.1 Acceptation d'un Certificat

Lors du face à face avec l'AE Certigreffe Classe 3Plus v2 ou le MC de l'Entreprise, le demandeur :

- valide les informations constituant la demande de certificat.

Lorsque son certificat lui est remis, le Porteur :

- signe l'acceptation du certificat et des obligations qui le lient à l'AC Certigreffe Classe 3Plus v2.

5.2 Révocation de Certificat

Un Certificat Certigreffe Classe 3Plus v2 ne peut être que dans l'un des trois états suivants : valide, expiré ou révoqué.

Les cas de figures suivants peuvent être à l'origine de la révocation d'un Certificat Porteur, et notamment :

- les informations du Porteur figurant dans son Certificat ne sont pas ou plus exactes, ceci avant l'expiration normale du Certificat ;
- les informations figurant dans le Dossier de Souscription ne sont plus exactes ou s'avèrent frauduleuses ;
- le Porteur n'a pas respecté des règles d'utilisation du Certificat ;
- la clé privée du Porteur est suspectée de compromission, est compromise ou perdue ;
- la résiliation ou le non-paiement du contrat d'abonnement ;
- le Porteur, le MC le représentant légal de l'Entreprise en fait la demande ;
- le départ, la mutation à un autre poste ou le décès du Porteur, ainsi que la cessation d'activité de son Entreprise.

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

Note **: cas de la révocation de la clé de l'AC.** Lorsque le certificat de l'AC Certigreffe Classe 3Plus v2 est révoqué, l'ensemble des certificats Porteurs a déjà été révoqué comme détaillé au chapitre 5.8.3.

5.2.1 Origine d'une demande de révocation d'un Certificat Porteur

La révocation d'un Certificat Porteur peut émaner :

- du Porteur au nom duquel le Certificat a été émis ;
- du représentant légal de l'Entreprise ;
- du Mandataire de Certification ;
- de l'AC Certigreffe Classe 3Plus v2 émettrice du Certificat ou de l'AE.

5.2.2 Informations à fournir

La demande de révocation doit comporter au minimum

- le nom du demandeur de la révocation ;
- l'identité du Porteur ;
- le DN du Porteur ou tout autre information (par exemple le code de révocation d'urgence) permettant d'identifier de façon certaine le certificat devant être révoqué.

5.2.3 Procédure de demande de révocation d'un Certificat Porteur

Les demandes de révocation par les Porteurs, les MC et les représentants légaux d'entreprises peuvent être réalisées auprès de l'AE en face-à-face (pendant ses heures d'ouverture), par l'envoi d'une demande sous forme électronique signée à l'aide d'un Certificat émis par l'AC, ou encore par téléphone (pour les Porteurs et MC en possession du code de révocation du certificat concerné).

Les procédures de révocation sont détaillées dans la DPC.

A la réception d'une demande de révocation, l'authenticité du demandeur est vérifiée. Cette vérification est réalisée par l'AE lors d'un face à face, par téléphone ou par échange de documents signés électroniquement. Si la demande est recevable, l'AE demande la révocation du Certificat en demandant à l'AC d'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'AE en informe le demandeur.

Le Porteur est notifié de la publication de la révocation.

L'opération est enregistrée dans les journaux d'événements de l'AC Certigreffe Classe 3Plus v2.

5.2.4 Délai de traitement d'une révocation

Le délai de publication de la révocation d'un Certificat n'excède jamais 24 heures ouvrées à partir de la réception de la demande de révocation.

5.2.5 Publication des motifs de révocation d'un Certificat.

Les motifs de révocation d'un Certificat Porteur sont demandés lors de la révocation (cf. contrat entre le Porteur et l'AC Certigreffe Classe 3Plus v2).

Ces motifs ne sont pas publiés dans les LCR de l'AC Certigreffe Classe 3Plus v2. La société INFOGREFFE se réserve le droit de fournir les motifs de révocation sur demande d'une autorité habilitée.

5.2.6 Besoins spécifiques en cas de révocation pour compromission de clé

Aucune procédure spécifique n'est mise en place si la cause de révocation est la compromission de la clé privée de Porteur.

5.2.7 Suspension de Certificats

Le service de suspension n'est pas proposé dans le cadre de cette PC.

5.3 Renouvellement d'un Certificat

La durée de vie d'un certificat est de trois ans et l'Autorité de Certification Certigreffe Classe 3Plus v2 ne permet pas le renouvellement de ses Certificats.

Le porteur est prévenu par courrier un mois avant la date de fin de validité de son certificat.

5.4 Emission des nouveaux certificats après révocation

Après une révocation, la génération d'un Certificat pour un Porteur suit la même procédure que pour l'enregistrement initial.

5.5 Suspension de certificats

L'AC Certigreffe Classe 3Plus v2 ne gère pas la suspension des certificats

5.6 Vérification de la validité des certificats

5.6.1 Contrôle en ligne du statut de révocation de Certificat

Il est possible de vérifier en ligne si un Certificat émis par l'AC Certigreffe Classe 3Plus v2 est révoqué.

Il est de la responsabilité des applications utilisatrices des Certificats et des utilisateurs de contrôler la validité d'un Certificat avant toute utilisation.

5.6.2 Formes de publication des LCR

L'accès à la Liste de Certificats Révoqués est possible via un annuaire LDAP V2 ainsi que via un serveur HTTP.

Les LCR sont au format dénommé "LCR V2".

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

5.7.1 Clé de signature de l'AC

La clé privée de l'AC est valide jusqu'au 23/05/2014 à compter du 14/04/2006.

La durée de vie des certificats Porteur étant de 3 ans, le renouvellement de cette clé devra intervenir au plus tard trois (3) ans avant la fin de sa validité. L'AC se réserve la possibilité de la renouveler avant sa limite de validité. La décision de son renouvellement pourra être prise plus tôt en fonction de divers critères (évolution de la technique cryptographique, allongement de la longueur, …).

Le nouveau bi-clé généré servira à signer les nouveaux Certificats Porteurs émis ainsi que la LCR.

Le certificat précédent restera utilisable pour la validation de certificats émis avant le renouvellement.

5.7.2 Clé de signature des autres composantes de l'ICP

L'AC Certigreffe Classe 3Plus v2 renouvellera les bi-clés des autres composantes de l'ICP 3 mois avant leur expiration.

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

Afin d'assurer la continuité et la sécurité de ses activités, l'AC Certigreffe Classe 3Plus v2 se doit également de gérer de façon spécifique les clés et certificats des diverses composantes de l'AC.

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

Dans les circonstances suivantes, l'AC pourra révoquer la clé d'une composante de l'ICP :

- Cessation d'activité de la composante ;
- Non conformité des procédures appliquées par la composante ;
- Compromission ou suspicion de compromission perte ou vol de la clé privée de la composante.

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

La procédure de révocation d'un certificat d'une composante de l'ICP est définie dans la DPC et est à nouveau précisée dans le contrat liant l'AE à l'AC Certigreffe Classe 3Plus v2.

5.8.3 Révocation du certificat de signature de l'AC

Cette révocation doit avoir lieu en trois étapes :

5.8.3.1 Etape 1 : Alerte administrative

Elle doit tout d'abord prévenir l'ensemble des applications utilisatrices de ces certificats de l'imminence de la révocation de son certificat et des certificats Porteurs. Ceci s'adresse en particulier au MINEFI.

Elle doit enfin signaler l'imminence de la révocation de son certificat à toute entité lui ayant attribué une quelconque accréditation, qualification,……

5.8.3.2 Etape 2 : Révocation des certificats Porteurs

L'AC doit révoquer l'ensemble des certificats qu'elle aura générés et en avertir les Porteur.

5.8.3.3 Etape 3 : Révocation du certificat de l'AC

L'AC Certigreffe Classe 3Plus v2 doit faire une demande de révocation de son certificat à l'AC Certeurope Root CA.

- L'AC Certeurope Root CA doit révoquer le certificat de signature de l'AC Certigreffe Classe 3Plus v2 et mettre à jour sa LCR.

5.8.4 Délai de traitement

La révocation des certificats des composantes de l'ICP doit avoir lieu dans les plus brefs délais.

5.9 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 la DPC et abordent notamment les thèmes suivants :

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

5.9.1 Information enregistrées

Ces enregistrements d'événements devront contenir au minimum les champs suivants, s'ils sont pertinents :

- type d'opération ;
- destinataire de l'opération ;
- nom du demandeur de l'opération ;
- nom de l'exécutant ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- date et heure de l'opération ;
- cause de l'évènement
- résultat de l'événement (échec ou réussite).

5.9.2 Imputabilité

L'objectif principal de la journalisation est de permettre d'imputer toute action à son auteur que ce soit une personne physique ou un système.

5.9.3 Evènements enregistrés par l'AE

L'AE doit consigner au moins les évènements suivants :

- demandes de certificats ;
- demandes de révocation ;
- sollicitation et accusés de réception de l'AC.

5.9.4 Evènements enregistrés par l'AC

Les évènements suivants seront enregistrés par l'AC, ce sont essentiellement des évènements générés par des systèmes informatiques :

- tous les événements ayant trait à la sécurité des systèmes informatiques impliqués dans l'ICP ;
- demandes de certificats ;
- demandes de révocation ;
- démarrage et arrêt des systèmes informatiques ;
- démarrage et arrêt des applications ;
- opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou modifier les privilèges système d'exploitants privilégiés ;
- génération des clés de ses composantes ;
- la génération et la révocation de certificats ;
- changements des caractéristiques de l'AC et (ou) de ses composantes ;

- la publication de la LCR;
- événements relatifs aux supports cryptographiques (génération des données d'activation à enregistrer).

5.9.5 Evènements divers

D'autres évènements non issus de systèmes informatiques mais essentiels pour la sécurité de l'AC, doivent être enregistrés, ce sont en particulier :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration du système ;
- les changements apportés au personnel ;
- les actions de destruction : des supports contenant des clés, des données d'activation ou des renseignements personnels sur les Porteurs.

5.9.6 Processus de journalisation

Le processus de journalisation doit être effectué en tâche de fond et permettre un enregistrement en temps réel des opérations effectuées. Le processus de journalisation doit être conçu de façon à être incontournable.

En cas de saisie manuelle l'écriture doit se faire dans le même jour ouvré que l'événement.

5.9.7 Protection d'un journal d'événements

L'écriture dans les journaux d'événements doit être conditionnée par des contrôles de droits d'accès. Les enregistrements et l'horloge des composantes de l'ICP doivent être protégés contre les tentatives non autorisées de modification et de destruction.

5.9.8 Copies de sauvegarde des journaux d'évènements

Aucune exigence n'est stipulée.

5.9.9 Système de collecte des journaux (interne ou externe)

L'enregistrement des événements doit commencer au démarrage des systèmes concernés par les événements à enregistrer et se terminer à l'arrêt de ces systèmes.

5.9.10 Anomalies et audit

Les composantes de l'AC responsables de la fonction de journalisation doivent être en mesure de détecter toute tentative de violation de l'intégrité du système de gestion des certificats, y compris les équipements physiques, l'environnement d'exploitation et le personnel.

Les journaux d'événements journaliers doivent être contrôlés pour identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être revus avec une fréquence hebdomadaire. Cette révision donnera lieu à un résumé dans lequel les éléments importants sont analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

La DPC doit documenter les mesures à prendre à la suite de ces analyses.

5.10 Archives

L'archivage est réalisé par l'AE 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'AE et l'AC afin que ces archives soient disponibles, exploitables, 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 dans la DPC, les points suivants :

5.10.1 Types de données à archiver

Doivent être archivées au minimum, les données suivantes

- les logiciels et les fichiers de configuration des équipements informatiques de l'ICP ;
- la PC et la DPC ;
- les agréments contractuels ou les conventions avec d'autres AC ;
- les journaux d'événements ;
- les certificats tels qu'émis ;
- les LCR telles qu'émises ou publiées ;
- les notifications de révocation ;
- le DDS du Porteur ou du MC.

5.10.2 Protection des archives

Les archives doivent être protégées durant leur conservation, cette protection concerne :

- leur intégrité ;
- leur confidentialité ;
- leur lisibilité.

Les moyens mis en œuvre pour atteindre ce triple objectif seront décrits dans la DPC

5.10.3 Période de rétention des archives

5.10.3.1 Certificats et LCR

Les certificats de clés de signature, ainsi que les LCR produites par l'AC doivent être archivés pendant au moins cinq ans après l'expiration des clés.

Les moyens mis en œuvre pour atteindre cet objectif seront décrits dans la DPC

5.10.3.2 Dossier de demande de certificat

Tout dossier de demande de certificat doit être archivé pendant la durée d'opposabilité des documents, c'est-à-dire cinq (5) ans après l'expiration des clés.

Les moyens mis en œuvre pour atteindre cet objectif seront décrits dans la DPC

5.10.3.3 Journaux d'évènements

Les journaux de l'AC seront conservés 8 ans après leur génération. Bien entendu le triple objectif de confidentialité, intégrité, lisibilité est maintenu durant leur conservation.

Les moyens mis en œuvre pour atteindre cet objectif seront décrits dans la DPC

5.10.3.4 Autres journaux

Aucune exigence n'est stipulée.

5.10.4 Duplication des archives

Aucune exigence n'est stipulée.

5.10.5 Horodatage des enregistrements

Les enregistrements des certificats et des LCR sont horodatés conformément à la politique de sécurité de l'AC en matière d'horodatage des évènements.

5.10.6 Procédure de collecte des archives

Aucune exigence n'est stipulée.

5.10.7 Procédure de récupération des archives

Une composante de l'ICP ne peut récupérer et consulter que ses propres archives.

Le processus de récupération doit faire l'objet d'une procédure et figurer dans la DPC.

Une archive doit être récupérée sous un délai inférieur à 2 jours ouvrés.

Les procédures sont décrites dans la DPC

5.11 Cessation d'activité de l'AC

5.11.1 Cessation définitive

En cas de cessation définitive d'activité, l'AC Certigreffe Classe 3Plus v2 procède comme indiqué au 5.8.3. L'AC Certigreffe Classe 3Plus v2 respectera un délai de 3 mois entre les étapes 1 et 2.

5.11.2 Transfert d'activité

Si l'AC décide de transférer son activité de certification, elle doit tout d'abord en informer les applications utilisatrices (parmi lesquelles le MINEFI) et les Porteurs dans un délai de 4 mois avant le transfert effectif d'activité.

Elle doit également informer les applications utilisatrices et les utilisateurs des modifications liées à ce transfert d'activité.

Les archives de l'AC devront être reprises en charge par la société reprenant l'activité.

6 CONTROLE DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES, CONTROLE 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'AC Certigreffe Classe 3Plus v2.

6.1.1 Situation géographique

Aucune exigence n'est stipulée.

6.1.2 Accès physique

Les zones hébergeant les systèmes informatiques de l'AC Certigreffe Classe 3Plus v2 sont physiquement protégées contre un accès extérieur non autorisé.

La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

6.1.3 Energie et air conditionné

Les installations électriques et de conditionnement d'air sont suffisantes pour le bon fonctionnement des systèmes informatiques de l'AC Certigreffe Classe 3Plus v2

6.1.4 Exposition aux liquides

Les systèmes informatiques de l'AC Certigreffe Classe 3Plus v2 ne sont pas situé en zone inondable, ni du fait d'intempéries, ni du fait de tuyauteries défaillantes.

6.1.5 Sécurité incendie

Les locaux d'hébergement des systèmes informatiques de l'AC Certigreffe Classe 3Plus v2 sont protégés contre les incendies (détection et extinction automatiques). La distribution des machines permet par ailleurs d'assurer une disponibilité maximale aux services.

6.1.6 Site de secours

Afin d'assurer l'accès aux services de certification/révocation même en cas de désastre sur le site de production des mesures doivent être prises. Ces mesures doivent permettre la reprise des activités de l'AC Certigreffe Classe 3Plus v2 dans les plus brefs délais.

Deux échelons de reprise d'activité peuvent être envisagés :

- L'accès à la LCR ;
- L'accès à l'ensemble des services (état nominal).

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

6.1.7 Conservation des médias

Les médias contenant des données sauvegardées ou archivées doivent être conservés avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

6.1.8 Destruction des supports

La destruction des supports sera assurée avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

6.1.9 Sauvegarde hors site

L'organisation des sauvegardes des informations sera adaptée de façon à assurer une reprise après désastre la plus rapide possible, en particulier pour les services impliqués dans la révocation de certificats.

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

6.2 Contrôles des procédures

Des contrôles des procédures sont mis en place par l'AC Certigreffe Classe 3Plus v2 et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

6.2.1 Rôles de confiance

L'AC Certigreffe Classe 3Plus v2 s'appuie sur du personnel réparti en 5 catégories (rôles)

- ingénieur système : mise en place et maintenance des systèmes ;
- administrateur sécurité gestion de la sécurité des systèmes ;
- opérateur : exploitation basique du système ;
- responsable sécurité : Application de la politique de sécurité ;
- responsable qualité : assurance de la qualité des services rendus par l'AC Certigreffe Classe 3Plus v2.

Les attributions nominatives de chaque rôle sont décrites dans la DPC.

6.2.2 Nombre de personnes nécessaires à l'exécution de tâches sensibles

Selon la tâche à effectuer une ou plusieurs personnes devront être présentes lors de l'exécution de la tâche.

La DPC précisera pour chacune des tâches liées à la gestion des certificats le nombre et le rôle de personnes nécessaires.

6.2.3 Identification et authentification des rôles

Chaque composante de l'AC doit vérifier l'identité et les autorisations de son personnel devant intervenir, avant :

- que son nom soit ajouté aux listes des personnes ayant accès physiquement aux systèmes informatiques de l'AC.
- qu'un compte lui soit ouvert dans les systèmes informatiques de l'AC Certigreffe Classe 3Plus v2.

6.3 Contrôle du personnel

6.3.1 Passé professionnel, qualifications, expérience, et exigences d'habilitations

L'AC Certigreffe Classe 3Plus v2 vérifie le passé professionnel de la personne et son adéquation aux exigences de la gestion de l'AC Certigreffe Classe 3Plus v2

L'AC Certigreffe Classe 3Plus v2 informera toute personne intervenant dans la Gestion de l'AC Certigreffe Classe 3Plus v2 de ses responsabilités relatives aux services de l'AC ainsi que des procédures liées à la sécurité.

L'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC:

- sont nommés à leur poste par écrit ;
- sont tenus par contrat ou par la loi de respecter les obligations, notamment de confidentialité, du poste qu'ils occupent ;
- n'ont pas de tâches ou d'intérêts susceptibles d'entrer en conflit avec les obligations qui leur incombent à l'égard de l'AC.

6.3.2 Procédures de contrôle du passé professionnel

Aucune exigence n'est stipulée.

6.3.3 Exigences de formation

L'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches touchant la gestion de l'AC ont reçu une formation adaptée concernant les principes de fonctionnement et des mécanismes de sécurité de l'AC, et sont familiarisés aux règles de sécurité en vigueur.

6.3.4 Fréquence des formations

Aucune exigence n'est stipulée.

6.3.5 Gestion des métiers

Aucune exigence n'est stipulée.

6.3.6 Sanctions pour des actions non-autorisées

Sur faute avérée ou soupçonnée d'un membre de l'AC dans l'accomplissement de ses tâches, l'AC doit lui interdire l'accès aux systèmes et, le cas échéant, prendre toutes sanctions disciplinaires adéquates.

6.3.7 Contrôle des personnels contractants

Aucune exigence n'est stipulée.

6.3.8 Documentation fournie au personnel.

L'AC doit s'assurer que son personnel dispose de l'accès à toute loi, ou tout contrat qui s'applique aux postes occupés.

Les documents dont doit disposer le personnel sont notamment les suivants :

- la PC supportée par la composante à laquelle il appartient ;
- la DPC propre au domaine de certification ;
- les procédures internes de fonctionnement ;
- les documents constructeurs des matériels et logiciels utilisés.

7 CONTROLES TECHNIQUES DE SECURITE

7.1 Génération et installation de bi-clés

7.1.1 Génération d'un bi-clé de Porteur

Les clés issues de l'AC Certigreffe Classe 3Plus v2 ont comme seuls usages au sens X509 du terme :

- La signature électronique ;
- La non répudiation.

Dans la procédure de génération de clés pour les Certificats Certigreffe, l'AE fait générer le bi-clé par le module cryptographique du Porteur. La clé privée n'est donc jamais accessible par l'AC ni par l'AE.

Le code d'activation du module est transmis part l'AC au porteur, l'AE n'a donc jamais connaissance de ce code

Le Porteur est réputé assumer l'entière responsabilité de toutes les signatures exécutées avec sa clé privée.

7.1.2 Transmission de la clé publique de signature (du Porteur) à l'AC

La clé publique du porteur est transmise à l'AC avec les informations nominatives que le certificat comportera via un protocole d'échange qui en assure l'intégrité. La DPC précise les modalités de cette transmission.

7.1.3 Fourniture d'un Certificat d'AC

La clé publique de l'AC est téléchargeable sur le site Internet de l'AC.

L'empreinte du Certificat de la clé publique de l'AC permet d'en établir l'authenticité.

La DPC précise les modalités de l'accès au certificat de l'AC.

7.1.4 Tailles des clés

Les clés RSA des Porteurs utilisées ont une taille de 2048 bits et seront mises à niveau au fur et à mesure de l'évolution de la technique et/ou de la législation.

La taille de la clé RSA de l'AC Certigreffe Classe 3Plus v2 est de 2048 bits.

L'AC CertEurope Root CA dispose d'une clé RSA de 2048 bits.

7.1.5 Paramètres de génération des clés

Les modules cryptographiques des Porteurs utilisent des paramètres standard ou normalisés pour garantir l'aspect aléatoire de la génération des bi-clés.

7.1.6 Contrôle de la qualité des paramètres des clés

Les modules cryptographiques des Porteurs vérifient la qualité des bi-clés qu'elles génèrent.

7.1.7 Usage de la clé publique des Porteurs

Les biclés délivrés par l'AC Certigreffe Classe 3Plus v2 ne sont utilisables que pour la signature et la non-répudiation.

Ces usages sont précisés dans le champ keyUsage des certificats **Certigreffe**

7.1.8 Mode de génération du biclé de l'AC

Le bi-clé de l'AC (pour la signature de certificats et de CRLs) est généré et protégé par un module cryptographique matériel.

Ce module doit répondre aux critères FIPS 140-1 niveau 4 ou équivalent.

La génération ou le renouvellement du bi-clé de l'AC par ce module nécessite la présence d'au moins 2 personnes.

7.2 Protection de la clé privée

7.2.1 Dispositifs de gestion des éléments secrets du Porteur

Le bi-clé du Porteur est généré par et stocké sur son module cryptographique. Un code d'activation (code PIN fourni au porteur par l'AC Certigreffe Classe 3Plus v2) protège l'accès à la clé privée. Le Porteur est responsable de la confidentialité du code PIN lié à sa clé privée.

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

Le contrôle des clés privées de l'AC Certigreffe Classe 3Plus v2 (pour la signature de certificats et de CRL) nécessite la présence de plusieurs personnes.

7.2.3 Récupération de clé privée de confidentialité du Porteur.*

L'AC Certigreffe Classe 3Plus v2 n'offre pas de service de recouvrement de clé.

7.3 Autres aspects de la gestion des bi-clés

7.3.1 Archivage des clés publiques des Porteurs

Les Certificats des Porteurs, contenant la clé publique, sont archivés pendant 5 ans après leur expiration conformément au chapitre 5.10.3.1..

7.3.2 Durée de vie des Certificats

La durée de vie des Certificats fournis dans le cadre de Certigreffe Classe 3Plus v2 est de 3 ans non renouvelables.

7.4 Code PIN des Porteurs

7.4.1 Génération et utilisation des codes PIN

Les modules cryptographiques sont fournis aux Porteurs protégées par un code PIN. Le code PIN est défini par l'AC de façon à le rendre imprévisible.

Une fois envoyé ce code est détruit et ne sera pas récupérable.

7.4.2 Protection des codes PIN

Il est de la responsabilité du Porteur de protéger les clés privées de ses bi-clés. Le code PIN doit être considéré par le Porteur comme confidentiel.

L'AC ne conserve pas les codes PINs des Porteurs au delà de leur envoi par courrier

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

Les postes de travail des composantes de l'ICP nécessitent un niveau de sécurité optimal, ce niveau est défini dans la DPC et permet de satisfaire les besoins suivants

- identification et authentification des utilisateurs du poste

- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'Utilisateur),
- protection contre les virus informatiques,
- protection du réseau (confidentialité, intégrité…)
- imputabilité

Le niveau minimal d'assurance recherché doit au moins répondre à ces objectifs de sécurité. Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires, à prendre en compte dans la recherche du niveau minimal d'assurance offert par les postes de travail.

7.6 Contrôles techniques du système durant son cycle de vie

7.6.1 Contrôles des développements des systèmes

Les applications de l'AC ont été implémentées dans le strict respect de l'analyse de risque préalable et de la politique de sécurité qui en découle.

L'implémentation de l'AC et de la plate-forme qui l'héberge est documentée.

Toute modification de l'AC et de la plate-forme qui l'héberge est documentée

7.6.2 Contrôles de la gestion de la sécurité.

Toute évolution des systèmes est enregistrée sur le livre d'activité de l'AC et fait l'objet d'un rapport.

7.7 Contrôles de la sécurité réseau

L'AC est implantée sur une réseau protégée par au moins deux niveaux de passerelles de type « coupe-feu ». Ces passerelles sont configurées de façon à n'accepter que les flux strictement nécessaires.

7.8 Contrôles des modules cryptographiques

Les modules cryptographiques utilisés par l'AC sont évalués selon les critères FIPS 140-1 au niveau 4.

8 PROFILS DE CERTIFICATS ET DE LCR

8.1 Profil des Certificats

Les Certificats de l'AC Certigreffe Classe 3Plus v2 contiennent les champs primaires et les extensions suivantes :

Champ	Valeur	Détail valeur	Explicat
Version	V3	2	Version Certificat X.
Numéro de série	1506 38D4 36F3 K231 C692 B849 E3F7 B943		Le numéro unique Certificat par le cryptographi
Algorithme de signature	Sha1RSA = 1.3.14.3.2.29		Identifiant l'algorithme signature de
Emetteur	/C=FR /O=Infogreffe /CN=AC Certigreffe Classe 3Plus v2		Le nom d émettrice Distinguishe Name (X.5 l'AC signa Certificats
Valide à partir du	Date de début = x (au plus tôt 14 avril 2006 00:00:00)		Dates et d'activation d'expiration Certificat
Valide jusqu'au	Valide jusqu'au x+ 3 ans (au plus tard 23 mai 2014 00:00:00)		
Objet	E = emartin@societe.fr CN = ERIC MARTIN OU = Société AAA O = 0002 124562390 C = FR		Nom distin l'entité identi
Clé publique	RSA(2048 Bits)	7C28 8902 8181 3963 8424 B08C CD71 9110 7E44 2B2E 8014 35F0 49CE B4D2 8CA9 3516 5FC7 9EB8 9A89 637C 20C4 DB30 97AF ECB3 37F2 A000 00E8 E350 BA90 2B20 EEE5 9D5B 4A87 E0D5 895A B6A4 05A6 B2C4 2715 555F 3081 0A68 95AD 00CF 6071 4C00 8431 7693 7EC0 20F9 8C31 EC2A 8585 9054 3478 4DD1 366B 9024 67B7 E8C8 C812 6EE9 E35B 5D04 700D 6699 2702 0301 0001	Identifiant l'algorithme d'usage de publique c dans le Ce et valeur de publique
Contrainte de base	Subject Type=End Entity Path Length Constraint=None		
Point de distribution de la LCR	CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://lcr1.certigreffe.fr/CN=AC Certigreffe Classe 3Plus v2, O=Infogreffe, C=FR?CertificateRevocationList URL=ldap://lcr2.certigreffe.fr:/CN=AC Certigreffe Classe 3Plus v2, O=Infogreffe, C=FR?CertificateRevocationList URL=http://www.certigreffe.fr/reference/certigreffe_v2.crl		

Certificate Policies	Certificate Policy: PolicyIdentifier=1.2.250.1.106.1.1 Policy Qualifier Info: Policy Qualifier Id= Qualifier=	OBJECT IDENTIFIER ' OBJECT IDENTIFIER cps http://www.certigreffe.fr/reference/pc_v2.pdf	Identifiant Politique Certification
Algorithme d'empreinte numérique	Sha1 = 1.3.14.3.2.29		
Empreinte numérique	07F2 AC3F 4E3A 30D5 277C 2A1A 6AD2 6BA4 F019 E130	8C 62 E9 57 0B 94 DF EB 73 14 AE 15 0F A9 36 2B 22 84 81 28 0F 25 06 FF 1C D3 10 EC A5 BC 43 1C AB 02 1D CD 7E 9E D7 B9 A0 DA 13 59 22 26 DF 72 EB 6D B3 AA 4E 2C B0 B3 1B 38 A4 E5 C4 3A 4C 15 2F E2 B2 AD 1C 9D 8F 5A FE D6 05 BC 6D 2E 81 D4 67 96 3D 74 BB F1 3F 37 7C 27 75 8C 9A 9A 9D 56 63 F1 BD 1E 76 89 09 ED 71 AA E1 F0 65 E1 A5 C8 0E DC AE 50 E1 C6 0D BF 76 6F A8 EC D0 D7 55 B9	Champ caractérisant Certificat d ayant sign Certificat

8.2 Profil de LCR

8.2.1 Champs des LCR

Les LCR de l'AC Certigreffe Classe 3Plus v2 contiennent les champs suivants :

- Version : la version de la LCR. Dans le cadre de la présente AC, il s'agit de la version 2;
- Signature : l'identifiant de l'algorithme de signature de l'AC soit Sha1-RSA ;
- Issuer : le nom de l'AC émettrice qui signe les Certificats soit l'AC Certigreffe Classe 3Plus v2 ;
- 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 ;
- UserCertificate : numéro de série de Certificat révoqué ;
- RevocationDate : date à laquelle un Certificat donné à été révoqué.
- crlExtensions : liste des extensions de la LCR.

8.2.2 Extensions des LCR

Les LCR de l'AC Certigreffe Classe 3Plus v2 comportent deux extensions :

- authorityKeyIdentifier : cette extension non critique identifie la clé publique à utiliser pour vérifier la validité de la LCR. Cet identifiant a la même valeur que le champ SubjectKeyIdentifier des certificats émis par l'AC Certigreffe Classe 3Plus v2 ;
- CRLNumber : cette extension non critique contient le numéro de série de la LCR.

9 ADMINISTRATION DES SPECIFICATIONS REFERENTES A L'AC

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente Politique de Certification.

9.1 Procédures de modification de la PC

Le responsable de l'AC doit signaler aux Porteurs et aux applications utilisatrices (dont le MINEFI) toute modification de la présente politique sans préavis.

9.1.1 Causes de modification

Cette PC devra être revue en raison de projets de modifications suivants :

- les certificats référencés ;
- la composition de l'AC ;
- à chaque modification des documents de référence de l'AP (ex : PC-Type du MINEFI) ainsi que chaque année pour assurer sa conformité aux normes de sécurité et à l'évolution des mises en œuvre du marché.

9.1.2 Délai de préavis

Le responsable de l'AC doit donner un préavis de trente (30) jours aux Porteurs et aux applications utilisatrices avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, a un impact majeur sur eux.

Le responsable de l'AC doit donner un préavis de quinze (15) jours aux Porteurs et aux applications utilisatrices avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact mineur sur eux.

Le responsable de l'AC doit donner un préavis aux Porteurs et aux applications utilisatrices dans les sept (7) jours d'un changement de la présente politique qui résulte d'une situation hors du contrôle du responsable de la politique, si ce changement ait un impact sur eux.

En cas de changement intervenant dans la composition de l'AC ou de la présente Politique de Certification, l'AC doit prévenir le MINEFI :

- 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'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.

9.2 Procédures de publication et de notification

La PC est disponible depuis la source suivante : http://www.certigreffe.fr/reference/pc_v2.pdf

9.3 Procédures d'approbation de la PC

L'approbation de la PC de l'AC est réalisée par l'AP qui notamment vérifie son adéquation aux documents de référence de l'AP, suivant une procédure de revue documentée.

La décision du Porteur de ne pas demander la révocation de son certificat suite à la notification d'un changement proposé constitue l'acceptation du changement.

10 ANEXE 1 – TEXTES LEGISLATIVES ET REGLEMENTAIRES

- Directive européenne 95/46/EC relative à la protection des données personnelles
- Directive européenne (1999/93/EC) relative à la signature électronique été adoptée le 13/12/1999
- Directive CE n°2000-31 du 8 juin 2000 sur le Commerce Electronique
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Loi Dutreil ; loi n° 2003-721 du 1 er Août 2003 sur l'Initiative Economique (article 4)
- Décret n° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.
- Décret n°99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie dispensées de toute formalité préalable.
- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
- Décret n°2052-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte pour les produits et les systèmes des technologies de l'Information.
- Arrêté définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fournitures d'un moyen ou d'une prestation de cryptographie, no PRMX9802730A du 13 mars 1998
- Arrêté définissant le modèle de notification préalable par le fournisseur des identités des intermédiaires utilisés pour la fourniture des moyens ou prestations de cryptographie soumis à autorisation, no PRMX9802732A du 13 mars 1998.
- Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptographie.
- Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.