Politique de Certification

Dématérialisation des contrats et actes de gestion du Groupe BPCE

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 155 742 320 €.

Siège social : 50 avenue Pierre Mendes France

75201 Paris Cedex 13.

RCS n° 493 455 042.

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

Le Groupe BPCE, pour ses réseaux Caisse d'Epargne, Banque Populaire et Filiales, met en œuvre pour ses Clients un service de dématérialisation des contrats et des actes de gestion intégrant un processus de signature électronique. Ce service de signature peut avoir lieu à distance ou en face à face dans une agence du réseau. Dans le cadre de ce processus :

- Les Clients peuvent signer des contrats et des actes de gestion à l'aide des bi-clés associées des certificats générés à la volée et valables le temps de la transaction de signature électronique.

- Les Etablissements signent et horodatent les contrats et des actes de gestion en leur nom à l'aide de bi-clés associées à des certificats de type cachet serveur.

Ces certificats sont gérés par l'Infrastructure de Gestion de Clés du Groupe BPCE. Il s'agit de l' « AC SIGNATURE CAISSE D EPARGNE » pour le réseau Caisse d'Epargne et de l'« AC SIGNATURE BANQUE POPULAIRE » pour le réseau Banque Populaire et Filiales qui s'appuient sur le référentiel ETSI 102042 pour le niveau Lightweight Certificate Policy (LCP). Ces deux AC sont opérées par le Groupe BPCE.

Dans ce cadre, les réseaux Caisse d'Epargne et Banque Populaire utilisent chacun des Autorités de Certification (AC) dédiées, internes au Groupe BPCE, pour émettre les certificats.

Ces AC sont inclues dans la hiérarchie d'Adobe de la manière suivante :

- Les AC sont toutes signées par l'AC intermédiaire d'OpenTrust appelée « KEYNECTIS CDS CA » ;

- L'AC « KEYNECTIS CDS CA » est certifiée par l'AC racine « Adobe Root CA » d'Adobe.

Les certificats délivrés par les AC permettent de signer des documents au format PDF. A la relecture des documents au travers d'outils tels que les logiciels de la gamme ADOBE ou visionneuse, les utilisateurs peuvent vérifier la validité de la signature.

Le présent document constitue la Politique de Certification (PC).Il a pour objet de décrire la gestion des certificats et leurs cycles de vie.

La présente PC est élaborée conformément :

- Au RFC 3647 : « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF) ;
- Au document : « Electronic Signatures and Infrastructures (ESI), Policy requirements for certification authorities issuing public key certificates », ETSI TS 102 042 v 2.4.1 ;
- Au document : « X.509 V.3 Certificate Profile for, Certificates Issued to Natural Persons », ETSI TS 102 280 V1.1.1 (2004-03).

1.2 Identification du document

La présente PC appelée : « Dématérialisation des contrats et actes de gestion du Groupe BPCE» est la propriété du Groupe BPCE. La PC contient plusieurs Object Identifier (OID).

Les numéros d'OID de ce document répondent aux principes de nommage suivants :

- iso(1)
- org(3)
- dod(6)
- internet(1)
- private(4)
- enterprise(1)
- bpce (40559)
- Service informatique (1)
- Programme de confiance numérique (0)
- Politiques de Certification (1)
- Politique de Certification UCG lot 2c (21)
    - UCG-lot2c-CE-Client(101), UCG-lot2c-BP-Client(111), UCG-lot2c- Entite-cachet serveur signature personne morale (121), UCG-lot2c-Entite-Horodatage(131), UCG-lot2c- Entite-cachet serveur signature application 141
- Environnement :
    - Production (1)
    - Qualification développement (2)
- Version (1)

Politique de certification	OID
BPCE UCG-lot2c-CE-Client	1.3.6.1.4.1.40559.1.0.1.21.101.1.1
BPCE UCG-lot2c-BP-Client	1.3.6.1.4.1.40559.1.0.1.21.111.1.1
BPCE UCG-lot2c- Entite-cachet serveur signature personne morale	1.3.6.1.4.1.40559.1.0.1.21.121.1.1
BPCE UCG-lot2c- Entite-horodatage	1.3.6.1.4.1.40559.1.0.1.21.131.1.1
BPCE UCG-lot2c- Entite-cachet serveur signature application	1.3.6.1.4.1.40559.1.0.1.21.141.1.1

Des éléments plus explicites comme le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins le seul identifiant de la version applicable de la PC est l'OID.

1.3 Entités intervenant dans l'Infrastructure de Gestion des Clés

Pour délivrer les certificats, l'AC s'appuie sur les services suivants :

- Service de génération de bi-clé d'AC : ce service génère les bi-clés et les demandes de signature de certificats (CSR) associées durant une cérémonie des clés.
- Service d'enregistrement : ce service collecte et vérifie les informations et identifie le porteur puis transmet la demande de certificats à l'AC.
- Service de gestion des bi-clés : ce service permet de générer les bi-clés des Porteurs dans des ressources cryptographiques (matériel certifié).
- Service de gestion des données d'activation: Ce service permet de générer et d'utiliser les données d'activation associées aux bi-clés. Service de génération de certificat : ce service génère les certificats électroniques à partir des informations transmises par l'Autorité d'Enregistrement (AE) ;
- Service de remise au porteur : ce service remet au porteur au minimum son certificat.
- Service de révocation de certificats: ce service traite les demandes de révocation des certificats des porteurs et détermine les actions à mener, dont la génération des Liste de Certificats Révoqués (LCR).
- Service de Publication : ce service met à disposition des Utilisateurs de Certificat (UC) les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales d'utilisation, politique de certification publiée par l'AC et certificat d'AC), ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations (LCR, avis d'information, …) ;
- Service de journalisation et d'audit : ce service permet de collecter l'ensemble des données utilisées et /ou générées dans le cadre de la mise en œuvre des services d'Infrastructure de Gestion des Clés afin d'obtenir des traces d'audit consultables. Ce service est mis en œuvre par l'ensemble des composantes techniques de l'Infrastructure de Gestion des Clés.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus dans la délivrance des certificats par l'AC aux porteurs. La Déclaration des Pratiques de Certification (notée DPC) donnera les détails des pratiques de l'Infrastructure de Gestion des Clés dans cette même perspective.

1.3.1 Autorité de Gestion des Politiques (AP)

La Direction de la Sécurité des Systèmes d'Information (DSSI-G) sous la responsabilité du RSSI-Groupe constitue l'Autorité de Gestion des politiques (AP).

En tant qu'Autorité, l'AP a pour responsabilité de:

- Définir l'organisation des composantes de l'infrastructure de gestion de clés du Groupe BPCE.
- Définir les normes de constitution des numéros d'identifiant d'objet (OID) associés à l'Infrastructure de Gestion des Clés.
- Autoriser la création et les évolutions d'AC.
- Définir et faire approuver auprès de la Direction Juridique, la Direction Conformité et Sécurité Groupe et la Direction Informatique et Technologie Groupe (DIT-G), les Politiques de Certifications
- Faire approuver auprès de la Direction Juridique, la Direction Conformité et Sécurité Groupe et la Direction Informatique et Technologie Groupe (DIT-G), les Déclarations des Pratiques de Certification associées.
- Définir les règles de nommage unique des AC et les règles de nommages des Porteurs.
- Auditer périodiquement les composantes de l'Infrastructure de Gestion des Clés et leur organisation.
- Valider les demandes de révocation d'AC et, le cas échéant, demander la révocation d'une AC.
- Arbitrer les litiges relatifs aux services d'Infrastructure de Gestion de Clés et à l'usage des certificats.
- Contrôler de la mise en œuvre de l'ensemble des points cités ci-dessus.
- Contrôler la validité et l'intégrité des informations publiées (liste des certificats d'AC, Liste des AC Révoquées, Liste des Certificats Révoqués et Politiques de Certifications).

L'AP agît conformément à la présente PC et à la DPC associée.

1.3.2 Autorité de Certification (AC)

L'AC définit les Déclarations des Pratiques de Certification et les procédures associées pour son domaine de responsabilité.

L'AC génère des certificats et révoque des certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. L'AC met en œuvre les services de ; génération de bi-clé d'AC, de génération de certificats, de révocation de certificats et de journalisation et d'audit.

Le Groupe BPCE s'appuie sur ses capacités d'Opérateur Technique (OT) afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création des certificats et à la gestion de leur cycle de vie.

L'AC agit conformément à la présente PC et à la DPC associée. Dans la présente PC, l'AC est identifiée par son Common Name (CN).

L'Autorité de Certification est le Groupe BPCE. Elle est représentée par le Directeur de la Sécurité des Systèmes d'informations Groupe.

1.3.3 Autorité d'Enregistrement (AE)

L'AE définit les Déclarations des Pratiques de Certification et les procédures associées pour son domaine de responsabilité.

L'AE est utilisée pour la mise en œuvre des services d'enregistrement, de gestion des bi-clés, de gestion des données d'activation, de remise au porteur, de révocation de certificats et de journalisation et d'audit. L'AE est chargée d'authentifier et d'identifier les porteurs.

L'AE est mise en œuvre par :

- Les établissements du Groupe BPCE pour les Clients.
- L'OT pour les Cachets serveurs.

La présente PC n'utilisera que le vocabulaire AE sans distinction du type de Porteur.

Dans tous les cas, l'AE agit conformément à la PC et à la DPC associée.

1.3.4 Service de Publication (SP)

Le SP est en charge de la publication des informations (Se reporter au § 2).

Le SP agit conformément à la PC et à la DPC associée.

1.3.5 Opérateur Technique (OT)

L'OT définit les Déclarations des Pratiques de Certification et les procédures associées pour son domaine de responsabilité.

L'OT assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification, conformément à la présente PC et à la DPC. L'OT est techniquement dépositaire des clés privées et des moyens informatiques de l'AC, de l'AE et du SP. Sa responsabilité se limite au respect des procédures, référencées dans la DPC, définies afin de répondre aux exigences de la présente PC. La DPC précise quelles sont les entités qui sont OT pour les composantes et les opérations de l'Infrastructure de Gestion de Clés.

L'OT agit conformément à la PC et à la DPC associée.

1.3.6 Porteurs de certificats

1.3.6.1 Client

Le Porteur de certificat est une personne physique, agissant pour son compte ou représentant une personne morale, cliente du Groupe BPCE et souhaitant signer électroniquement un contrat ou un acte de gestion, Il obtient dans ce cadre un certificat, dont les informations d'identification sont regroupées dans le champ "Objet" du « DN » du certificat (se reporter au § 3.1 ci-dessous).

Le Client active sa clé privée conformément au protocole d'activation de la clé et à la Politique de signature appliquée par l'AE. En ce cas, le Porteur est soit une personne physique qui agît en son nom propre (un particulier) soit une personne physique agissant dans un cadre professionnel pour son compte ou en tant que représentant d'une personne morale. Le contenu du DN sera différent suivant le type de Client.

1.3.6.2 Cachet serveur

Dans le cas du certificat Cachet serveur le Porteur est un système informatique et un Contact Technique en a la charge.

1.3.7 Autres participants

1.3.7.1 Utilisateurs de certificats (UC)

L'utilisateur de certificat est une personne ou un système informatique qui valide la signature électronique d'un document signé par le porteur et par l'Etablissement et horodaté par le Groupe BPCE.

1.3.7.2 Contact Technique (CT)

Un Contact Technique est une personne nommée par le Groupe BPCE et autorisée à :
- Générer les bi-clés dont les clés publiques seront associées à un certificat « cachet serveur » ;
- Remplir les formulaires de demande de certificat « cachet serveur » ;
- Retirer les certificats « cachet serveur » ;
- Procéder le cas échéant aux demandes de révocation des certificats « cachet serveur ».

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Certificat de l'AC

Le certificat de l'AC sert à authentifier les certificats porteurs et les LCR.

La clé privée associée au certificat d'AC sert pour :

- La signature de certificat Porteur;
- La signature de LCR ;
- La signature de CSR (format Pkcs#10).

1.4.1.2 Certificat Client

La clé privée associée au certificat sert pour :

- La signature de document au nom du Client ;
- La signature de CSR (format Pkcs#10).

1.4.1.3 Certificat cachet serveur : signature personne morale

La clé privée associé au certificat sert pour :

- La signature de document au nom de l'Etablissement ;
- La signature de CSR (format Pkcs#10).

1.4.1.4 Certificat cachet serveur : signature application

La clé privée associé au certificat sert pour :

- La signature de document au nom du Coffre-Fort d'Archivage à valeur probante du Groupe BPCE ;
- La signature de CSR (format Pkcs#10).

1.4.1.5 Certificat cachet serveur : horodatage

La clé privée associé au certificat sert pour :

- L'horodatage de document au nom du Groupe BPCE ;
- La signature de CSR (format Pkcs#10).

1.4.2 Domaines d'utilisation interdits

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues au § **Erreur ! Source du renvoi introuvable.** ci-dessus ne sont pas autorisées. En pratique, cela signifie que l'AC ne peut être en aucun cas tenue pour responsable d'une utilisation des certificats qu'elle émet autre que celles prévues dans la présente PC.

En cas de violation de cette obligation par le Porteur, le Groupe BPCE ne pourra voir sa responsabilité engagée vis-à-vis de quiconque.

Les actions résultant de l'utilisation du certificat ne peuvent être considérées comme ayant une valeur probante au sens de la directive européenne 1999/93/CE et des articles 1316 et suivants du Code civil.

Les certificats ne peuvent être utilisés que conformément aux lois applicables en vigueur, en particulier seulement dans les limites autorisées par les lois sur l'importation et l'exportation et les lois, décrets, arrêtés et directives propres à la signature électronique.

Cette PC décrit la gestion du cycle de vie des certificats de signature et de leurs supports. Elle n'a pas vocation de remplacer une politique de signature qui décrit la gestion du cycle de vie des signatures établies à l'aide des certificats délivrés par l'AC. Dans le cas de la présente PC, c'est le Groupe BPCE qui élabore la politique de signature associée aux certificats gérés par la présente PC.

L'usage des certificats, pour les Clients, est rappelé dans les Conditions Générales d'Utilisation, qui lui sont soumises durant le processus de signature de son contrat. Le Porteur approuve ces Conditions Générales d'Utilisation sans quoi le processus de signature de son contrat ne peut pas aboutir.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

La présente PC est sous la responsabilité de l'AP.

1.5.2 Point de contact

Les demandes d'informations ou questions concernant l'Autorité de Certification sont adressées à :

- Groupe BPCE
- Directeur de la Sécurité des Systèmes d'informations Groupe
- 50 Avenue Pierre Mendes France

- 75201 Paris Cedex 13
- rssi-pssi-icg@bpce.fr

Ce point de contact est disponible et à jour sur le site du SP (voir le paragraphe 2.2).

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

L'AP détermine la conformité de la DPC à la présente PC.

1.5.4 Procédure d'approbation de la conformité de la DPC

L'AP possède ses propres méthodes pour approuver le présent document. L'AP procède à des analyses/contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour l'AC d'émettre des certificats. L'AP approuve les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet et détermine en fonction des résultats la conformité de la DPC.

1.6 Définitions et Acronymes

1.6.1 Définitions

Audit : Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures. [ISO/IEC POSIX Security].

Critères Communs : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu [ISO/IEC 15408]. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettre en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC ou AE est générée, sa clé privée transférée éventuellement sauvegardée, et/ou sa clé publique certifiée.

Certificat : clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

Certificat d'AC : certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8; ITU-T X.509]. **Certificat auto signé :** certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification : (ou chaîne de confiance, ou chaîne de certification) chaîne constituée de multiples certificats nécessaires pour valider un certificat.

Clé privée : clé de la bi-clé de chiffrement asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique : clé de la bi-clé de chiffrement asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1].

Compromission : violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

Confidentialité : La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

Déclaration des Pratiques de Certification (DPC) : une déclaration des pratiques qu'une entité (agissant en tant qu'Autorité de Certification) utilise pour approuver ou rejeter des demandes de certificat (émission, gestion, renouvellement et révocation de certificats). [RFC 3647].

Demande de certificat : message transmis par l'AE à l'AC pour obtenir l'émission d'un certificat d'AC.

Disponibilité : La propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Données d'activation : Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent (bi-clés) et qui sont protégées (par ex. un PIN, une phrase secrète, code OTP, …).

Etablissement : Membre du réseau Banque Populaire ou du réseau Caisse d'Epargne

Fonction de hachage : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux trois propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie ;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1] ;
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Infrastructure de Gestion de Clés: c'est l'infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués ainsi que la base dans laquelle les certificats et les LCR sont publiés. [2nd DIS ISO/IEC 11770-3 (08/1997)].

Intégrité : fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Interopérabilité : implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles; et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Modules cryptographiques : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.

Période de validité d'un certificat : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

PKCS #10 : (Public-Key Cryptography Standard #10) mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (en anglais: Certificate Signing Request: CSR).

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'Infrastructure de Gestion de Clés après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Point de distribution de LCR *:* entrée de répertoire ou une autre source de diffusion des LCR; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification (PC) : ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

Politique de sécurité : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Porteur de secret : personnes qui détient une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Qualificateur de politique : Des informations concernant la politique qui accompagnent un identifiant de politique de certification (OID) dans un certificat X.509. [RFC 3647]

RSA : algorithme de cryptographique à clé publique inventé par Rivest, Shamir, et Adelman.

Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC de la chaine de délivrance et la vérification de la signature électronique de l'ensemble des AC contenue dans le chemin de certification.

1.6.2 Acronymes

- AC : Autorité de Certification ;
- AE : Autorité d'Enregistrement ;

- AP : Autorité de Gestion des Politiques ;
- CC : Critères Communs ;
- CSR : Certificate Signing Request ;
- DN : Distinguished Name ;
- DPC : Déclaration des pratiques de certification ;
- EAL : Evaluation assurance level, norme ISO 15408 (Critères Communs) pour la certification des produits de sécurité ;
- HTTP : Hypertext Transport Protocol ;
- Infrastructure de Gestion de Clés : Infrastructure de Gestion de Clés ;
- IP : Internet Protocol ;
- ISO : International Organization for Standardization ;
- LCP : Lightweight Certificate Policy ;
- LCR : liste de certificats révoqués ;
- LDAP : Lightweight Directory Access Protocol ;
- OCSP : Online Certificate Status Protocol ;
- OID : Object Identifier ;
- PC : Politique de Certification ;
- PKCS : Public-Key Cryptography Standard ;
- RFC : Request for comment ;
- RSA : Rivest, Shamir, Adleman ;
- SHA : Secure Hash Algorithm (norme fédérale américaine) ;
- SP : Service de Publication ;
- UC : Utilisateur de certificat ;
- URL : Uniform Resource Locator.

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

2.1 Entités chargées de la mise à disposition des informations

Le SP est en charge de la publication des données identifiées au § 2.2 ci-dessous.

L'AP valide les données qui sont publiées comme la PC et les certificats d'AC.

2.2 Informations devant être publiées

L'AC, via le SP, rend disponibles les informations suivantes :

- La PC de l'AC :
  - AC « AC SIGNATURE CAISSE D EPARGNE U<XX>-<YY> » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_signature_ce.html
  - AC AC SIGNATURE BANQUE POPULAIRE U<XX>-<YY> : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_signature_bp.html
  - AC « AC CACHET SERVEUR CAISSE D EPARGNE » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_cachet_ce.html
  - AC « AC CACHET SERVEUR BANQUE POPULAIRE » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_cachet_bp.html

- Le certificat de l'AC :
  - AC AC SIGNATURE BANQUE POPULAIRE U01-01 : http://www.dossiers-securite.bpce.fr/AC/ucg_lot2/ac_signature_bp_u01-01.cer
  - AC AC SIGNATURE BANQUE POPULAIRE U01-02 : http://www.dossiers-securite.bpce.fr/AC/ucg_lot2/ac_signature_bp_u01-02.cer
  - AC « AC SIGNATURE CAISSE D EPARGNE U01-01 » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_signature_ce_u01-01.cer
  - AC « AC SIGNATURE CAISSE D EPARGNE U01-02 » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_signature_ce_u01-02.cer
  - AC AC SIGNATURE BANQUE POPULAIRE U02-01 : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_signature_bp_u02-01.cer
  - AC AC SIGNATURE BANQUE POPULAIRE U02-02 : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_signature_bp_u02-02.cer

- AC « AC SIGNATURE CAISSE D EPARGNE U02-01 » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_signature_ce_u02-01.cer
- AC « AC SIGNATURE CAISSE D EPARGNE U02-02 » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_signature_ce_u02-02.cer
- AC « AC CACHET SERVEUR CAISSE D EPARGNE » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_cachet_ce.cer
- AC « AC CACHET SERVEUR BANQUE POPULAIRE » : http://www.dossiers-securite.bpce.fr/docs/pc-ucg/ac_cachet_bp.cer

- Les certificats de la chaîne de confiance à laquelle l'AC est rattachée à savoir : le certificat racine de l'ACR d'Adobe « Adobe Root CA » et le certificat de l'AC « KEYNECTIS CDS CA » : https://www.opentrust.com/PC/ ;
- Le formulaire de demande de certificat est assimilé au contrat à signer. Le contrat ou l'acte de gestion à signer est fourni par l'AE soit en agence soit dans le portail de l'AE ;
- Le formulaire et/ou les modalités de révocation d'un certificat : sur demande auprès de l'AE soit en agence soit dans le portail de l'AE ;
- Les conditions générales d'utilisation : sur demande auprès de l'AE en agence et mises à disposition sur le Portail de l'AE et ce conformément à la politique de signature applicable par l'AE;
- La liste des certificats révoqués (LCR) :
  - AC CACHET SERVEUR CAISSE D EPARGNE
    - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-cachet-ce-ss1-ucg1_v1.crl
  - AC CACHET SERVEUR BANQUE POPULAIRE
    - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-cachet-bp-ss1-ucg1_v1.crl
  - AC SIGNATURE BANQUE POPULAIRE U01-01 :
    - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-signature-bp-ss1-ucg1_v1.crl
  - AC SIGNATURE BANQUE POPULAIRE U01-02 :
    - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-signature-bp-ss1-ucg2_v1.crl
  - AC SIGNATURE CAISSE D EPARGNE U01-01 :
    - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-signature-ce-ss1-ucg3_v1.crl

- AC SIGNATURE CAISSE D EPARGNE U01-02 :
  - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-signature-ce-ss1-ucg4_v1.crl
- AC SIGNATURE BANQUE POPULAIRE U02-01 :
  - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-signature-bp-ts1-ucg1_v1.crl
- AC SIGNATURE BANQUE POPULAIRE U02-02 :
  - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-signature-bp-ts1-ucg2_v1.crl
- « AC SIGNATURE CAISSE D EPARGNE U02-01 »
  - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-signature-ce-ts1-ucg3_v1.crl
- « AC SIGNATURE CAISSE D EPARGNE U02-02 »
  - http://www.dossiers-securite.bpce.fr/crl-ucg/ac-signature-ce-ts1-ucg4_v1.crl
- Émise par l'AC : « Adobe Root CA » : http://crl.adobe.com/cds.crl
- Émise par l'AC : « KEYNECTIS CDS CA » : http://trustcenter-crl.certificat2.com/Internal/KEYNECTIS_CDS_CA.crl

La DPC n'est pas publiée mais consultable auprès de l'AP sur demande justifiée et autorisée par l'AP.

L'UC accède aux informations qui lui sont nécessaires et qui lui incombent au regard de la vérification d'un certificat par la publication de la présente PC et des chapitres suivants : 1.4, 4.5.2, 5.5, 9, 9.6, 9.7, and 9.8.Délais et fréquences de publication

La PC de l'AC et le certificat de l'AC sont disponibles 24h/24 et 7j/7 et mis à jour selon les besoins. Ces éléments sont publiés avant toute génération d'un certificat final correspondant.

La LCR est disponible 24h/24 et 7j/7 et mise à jour toutes les 24 heures. Il est prévu de publier une LCR après chaque révocation.

2.3 Contrôle d'accès aux informations publiées

Le SP s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées. L'AC s'assure que toute information conservée dans une base documentaire de son Infrastructure de Gestion de Clés et dont la diffusion publique ou la modification n'est pas prévue, est protégée.

L'ensemble des informations publiques et publiées (Se reporter au § 2.2) est libre d'accès en lecture et téléchargement sur Internet.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat X.509, le fournisseur (Issuer) et le porteur (subject) sont identifiés par un Distinguished Name (DN).

Les attributs du DN sont encodés en « printableString » ou en « UTF8String » à l'exception des attributs emailAddress qui sont en « IA5String ».

3.1.1.1 Certificat AC : Caisse d'Epargne : pour signer les certificats « cachet serveur »

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	CN = KEYNECTIS CDS CA OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR
Subject	CN = AC CACHET SERVEUR CAISSE D EPARGNE OU = 0002 493455042 O = BPCE C = FR

3.1.1.2 Certificat AC : Banque Populaire : pour signer les certificats « cachet serveur »

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	CN = KEYNECTIS CDS CA OU = KEYNECTIS for Adobe

	O = KEYNECTIS C = FR
Subject	CN = AC CACHET SERVEUR BANQUE POPULAIRE OU = 0002 493455042 O = BPCE C = FR

3.1.1.3 Certificat AC : Caisse d'Epargne : pour signer les certificats « Client »

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	CN = KEYNECTIS CDS CA OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR
Subject	CN = AC SIGNATURE CAISSE D EPARGNE U<XX>-<YY> OU = 0002 493455042 O = BPCE C = FR

Les valeurs <XX> et <YY> sont des chiffres de la forme « 01 », « 02 », …

3.1.1.4 Certificat AC : Banque Populaire : pour signer les certificats Client

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	CN = KEYNECTIS CDS CA OU = KEYNECTIS for Adobe

	O = KEYNECTIS C = FR
Subject	CN = AC SIGNATURE BANQUE POPULAIRE U<XX>-<YY> OU = 0002 493455042 O = BPCE C = FR

Les valeurs <XX> et <YY> sont des chiffres de la forme « 01 », « 02 », …

3.1.1.5 Certificat « cachet serveur » Caisse d'Epargne

L'identité du porteur dans le certificat est la suivante :

Champ de base	Valeur
Issuer	Identité de l'AC du réseau (se reporter au § 3.1.1.1 et 3.1.1.2 ci-dessus) pour lequel le cachet serveur est émis.
Subject	C = FR OU = 0002 Numéro de SIREN de l'Etablissement O = Nom de l'Etablissement CN = nom commercial de l'Etablissement

3.1.1.6 Certificat « cachet serveur » : signature application

L'identité du porteur dans le certificat est la suivante :

Champ de base	Valeur
Issuer	Identité de l'AC du réseau (se reporter au § 3.1.1.1 et 3.1.1.2 ci-dessus) pour lequel le cachet serveur est émis.
Subject	C = FR OU = 0002 493455042 O = BPCE CN = <Nom applicatif du coffre-fort d'archivage à valeur probante>-ee-id (où

	« ee » est utilisé pour indiquer l'enseigne (BP ou CE) et « id » est utilisé pour l'unicité du certificat)

3.1.1.7 Certificat « Horodatage »

L'identité du porteur dans le certificat est la suivante :

Champ de base	Valeur
Issuer	Identité de l'AC du réseau (se reporter au § 3.1.1.1 et 3.1.1.2 ci-dessus) pour lequel le cachet serveur est émis.
Subject	CN = HORODATAGE-ee (où « ee » est utilisé pour indiquer l'enseigne (BP ou CE)) OU = 0002 493455042 O = BPCE C = FR

3.1.1.8 Certificat « cachet serveur » Banque Populaire

L'identité du porteur dans le certificat est la suivante :

Champ de base	Valeur
Issuer	Identité de l'AC du réseau (se reporter au § 3.1.1.1 et 3.1.1.2 ci-dessus) pour lequel le cachet serveur est émis.
Subject	C = FR OU = 0002 Numéro de SIREN de l'Etablissement O = Nom de l'Etablissement CN = nom commercial de l'Etablissement

3.1.1.9 Certificat Client

L'identité du porteur dans le certificat est la suivante :

Champ de base	Valeur

Issuer	Identité de l'AC du réseau (se reporter au § 3.1.1.1 et 3.1.1.2 ci-dessus) dont l'AE dépend et auprès de laquelle le Porteur est enregistrée.
Subject	<u>Pour les Clients Professionnels</u> C = contient le pays où est basé le siège social de l'organisation d'appartenance du Client O = contient le libellé de l'organisation d'appartenance du Client. OU = Identifiant du Client ou de la Session de Signature du Client OU = Identification de l'entité légale (Pour les Clients de droit français : ICD = 0002 suivi du n° SIREN ou du n° SIRET) CN = contient le nom suivi du prénom du Client, tels qu'inscrits dans le référentiel d'identification des Clients. <u>Pour les Client Particuliers</u> C = FR O = BPCE OU = Identifiant du Client ou de la Session de Signature du Client CN = contient le nom suivi du prénom du Client, tels qu'inscrits dans le référentiel d'identification des Clients.

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 Certificat AC

L'identité utilisée pour les certificats d'AC permet d'identifier le Groupe BPCE et le réseau de l'AE.

3.1.2.2 Certificat Client

Dans tous les cas, l'identité du porteur (Se reporter au § 3.1.1 ci-dessus) est construite à partir des nom et prénom de son état civil tel que porté sur le document officiel d'identité présenté lors de son enregistrement.

Lorsque le certificat est pour un porteur au sein d'une Entreprise ou d'une Administration, alors l'identité de l'Entreprise ou de l'Administration est aussi contenue dans le certificat.

3.1.2.3 Certificat cachet serveur

Les noms choisis pour désigner les cachets serveurs dans les certificats sont explicites.

L'identification de l'Etablissement auquel le serveur est rattaché est obligatoire.

3.1.3 Pseudonymisation des porteurs

3.1.3.1 Certificat AC

L'identité utilisée pour les certificats d'AC n'est ni un pseudonyme ni un nom anonyme (Cf. § **Erreur ! Source du renvoi introuvable.**).

3.1.3.2 Certificat Client

L'identité utilisée pour les certificats de porteurs n'est ni un pseudonyme ni un nom anonyme (Se reporter au § 3.1.1 ci-dessus).

3.1.3.3 Certificat cachet serveur

S'agissant de certificats entités, les notions d'anonymisation ou de pseudonymisation sont sans objet.

3.1.4 Règles d'interprétation des différentes formes de noms

Les UC peuvent se servir de l'identité incluse dans les certificats (Se reporter au 3.1.1) afin d'authentifier les Clients, le Groupe BPCE, ainsi que le réseau de l'AE et les Établissements.

3.1.5 Unicité des noms

3.1.5.1 Certificat AC

Les identités des certificats (Cf. § 3.1.1) sont uniques au sein du domaine de certification de l'AC « KEYNECTIS CDS CA ». L'AP assure cette unicité au moyen de son processus d'enregistrement.

En cas de différend au sujet de l'utilisation d'un nom pour un certificat, l'AP a la responsabilité de résoudre le différend en question.

3.1.5.2 Certificat Client

Les identités portées par l'AC dans les certificats (Se reporter au § 3.1.1) sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, une identité attribuée à un porteur (Se reporter au 3.1.1) de certificat ne peut être attribué à un autre porteur.

L'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC. Ce numéro est propre au certificat et non pas au Porteur. Il ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un porteur donné.

L'AE assure cette unicité au moyen de son processus d'enregistrement et de la valeur unique du DN attribué à un porteur (se reporter au § 3.1.1).

En cas de différend au sujet de l'utilisation d'un nom pour un certificat, l'AP a la responsabilité de résoudre le différend en question.

Les certificats des Porteurs de l'« AC Infrastructure de Gestion de Clés CE Client » ou de l'« AC Infrastructure de Gestion de Clés BP Client » pour le profil Signature sont identifiés de manière unique par le DN du certificat. Le DN contient le prénom, le nom et l'identifiant du client.

3.1.5.3 Certificat cachet serveur

Les identités portées par l'AC dans les certificats (Se reporter au § 3.1.1) sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, une identité attribuée à un porteur (Se reporter au 3.1.1) de certificat ne peut être attribué à un autre porteur.

L'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC. Ce numéro est propre au certificat et non pas au Porteur. Il ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un porteur donné.

L'AE assure cette unicité au moyen de son processus d'enregistrement et de la valeur unique du DN attribué à un porteur (se reporter au § 3.1.1).

En cas de différend au sujet de l'utilisation d'un nom pour un certificat, l'AP a la responsabilité de résoudre le différend en question.

L'AE s'assure qu'une identité de Cachet serveur ne peut être attribuée qu'à un unique Etablissement (pour les certificats de signature de personne morale) ou Groupe BPCE (pour les certificats d'Horodatage).

3.1.6 Identification, authentification et rôle des marques déposées

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'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par le Porteur de type « Client » des marques déposées, des marques notoires et des signes distinctifs.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

3.2.1.1 Certificat AC

La preuve de la possession de la clé privée par les composantes de l'Infrastructure de Gestion de Clés et par l'AC est réalisée par les procédures de génération (Cf. § **Erreur !**

Source du renvoi introuvable.) de la bi-clé privée correspondant à la clé publique à certifier, l'audit réalisé par l'AP sur l'AC à certifier et le mode de transmission de la clé publique (Cf. § 6.1.3) de l'AC « KEYNECTIS CDS CA » qui signe les AC.

3.2.1.2 Certificat client et certificat cachet serveur

La preuve de la possession de la clé privée par le porteur est réalisée par les procédures de génération de la clé privée (se reporter au § 6.1.1 ci-dessous) correspondant à la clé publique à certifier et par le mode de transmission de la clé publique (se reporter au § 6.1.3 ci-dessous).

3.2.2 Validation de l'identité d'un organisme

3.2.2.1 Certificat AC

L'authentification est réalisée sous la responsabilité de l'AP qui communique les données d'identification de l'organisme à inclure dans l'identité des AC (Cf. § 3.1.1) à l'OT au préalable de toute cérémonie des clés.

L'AP vérifie le nom de l'organisme pendant le processus d'authentification, ainsi que son numéro SIREN ou des informations issues d'instances étatiques qui enregistrent les sociétés pour les organismes étrangers.

Les vérifications sont effectuées en consultant les bases de données officielles de noms d'entité.

3.2.2.2 Certificat « Client » : Professionnel

L'AE qui procède à la vérification s'assure que l'entité légale existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande Porteur aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité du Client comprennent au minimum le numéro SIREN et le nom de l'entité légale.

Dans tous les cas, la vérification de l'appartenance d'un Porteur à l'organisation dont il se réclame est effectuée.

3.2.2.3 Certificat « Client » : Particulier

Sans objet.

3.2.2.4 Certificat « Cachet serveur »

Les cachets serveurs sont émis au nom du Groupe BPCE.

3.2.3 Validation de l'identité d'un individu

3.2.3.1 Certificat d'AC

Les Porteurs de secrets et les rôles de confiance de l'AC sont authentifiés et identifiés lors d'un face à face avec des personnes représentant l'AP et l'OT pendant la phase de mise en place de l'AC et la cérémonie des clés. L'identification et l'authentification s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.2 Certificat « client » : identifié en agence

L'identification et l'authentification du porteur par l'AE s'effectue sur la base d'une pièce d'identité officielle (carte nationale d'identité, passeport, …) conservée par l'AE dans le Référentiel d'Informations des Clients ou présentée à l'AE puis conservée dans le Référentiel d'Informations des Clients.

L'AE est responsable de mettre à jour le Référentiel d'Informations des Clients.

Le Client est identifié et authentifié lors d'un face à face avec l'AE.

3.2.3.3 Certificat « Client » : identifié en ligne

L'identification et l'authentification du Client s'effectue sur la base d'une pièce d'identité officielle (carte nationale d'identité, passeport, …) et des informations contenues dans le dossier Client (se reporter au § 4.1) transmis à l'AE par le Client. Ce dossier Client permet d'alimenter le Référentiel d'Informations des Clients.

Le Client s'identifie et s'authentifie ensuite sur le portail de l'AE via le protocole d'authentification choisi par l'AE parmi ceux proposés par le Groupe BPCE. L'AE authentifie le Client à partir des informations saisies dans le dossier de demande de certificat (Cf. § 4.1.2).

L'AE a la responsabilité de la distribution sécurisée des moyens et/ou des données d'authentification que le Client doit utiliser. L'AE est responsable de la mise à jour et de la vérification périodique que le moyen utilisé par le Client est toujours le sien (numéro de téléphone par exemple).

3.2.3.4 Certificat « Cachet serveur »

L'identification et l'authentification du CT est effectuée par l'AE à partir des informations contenues dans le dossier de demande de certificat (Cf. § 4.1.2) et du référentiel de l'AE sur les CT habilités du Groupe BPCE.

3.2.4 Informations non vérifiées

Les informations non vérifiées ne sont pas introduites dans les certificats.

3.2.5 Validation de l'autorité du demandeur

La validation de l'autorité d'un porteur correspond à la validation de l'appartenance à une organisation (se reporter au § 3.2.2 ci-dessus).

3.2.6 Certification croisée d'AC

Un porteur qui obtient un certificat émis par l'AC a la garantie d'être authentifiable dans le domaine de confiance CDS d'Adobe.

3.3 Identification et validation d'une nouvelle demande de bi-clé

3.3.1 Identification et validation pour une nouvelle demande

3.3.1.1 Certificat AC

Le renouvellement de certificat d'AC s'apparente en situation normale à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (Cf. § 3.2). Dans tous les cas, la procédure d'authentification est conforme à la procédure initiale (Cf. § 3.2).

3.3.1.2 Certificat « Client » : identifié en agence

Le Client est identifié et authentifié lors d'un face à face avec l'AE.

Si le Client a été authentifié une première fois en agence, il peut par la suite s'identifier et s'authentifier sur le portail de l'AE (Cf. § 3.3.1.3).

Remarque : un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante.

3.3.1.3 Certificat « Client » : identifié en ligne

Le Client s'identifie et s'authentifie ensuite sur le portail de l'AE via le protocole d'authentification choisi par l'AE parmi ceux proposés par le Groupe BPCE.

Remarque : un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante.

3.3.1.4 Certificat Cachet serveur

Lors d'une nouvelle demande, l'AE s'assure au minimum que les informations du CT contenues dans le dossier d'enregistrement initial sont toujours valides et que le porteur est toujours autorisé à avoir un certificat.

Remarque : un nouveau certificat ne peut pas être fourni sans renouvellement de la bi-clé correspondante.

3.3.2 Identification et validation pour une nouvelle demande après révocation

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2).

3.4 Identification et validation d'une demande de révocation

3.4.1.1 Certificat AC

Les demandes de révocation sont authentifiées par l'AP. La procédure de vérification est identique à celle utilisée pour l'enregistrement initial (Cf. § 3.2).

3.4.1.2 Certificat « Client »

Sans objet.

3.4.1.3 Certificat : « cachet serveur »

Les demandes de révocation sont authentifiées par l'AE suivant les procédures définies par le réseau de l'AE.

4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

L'objet du chapitre 4.1, 4.2 et 4.3 est de décrire le processus de demande d'un premier certificat. La gestion des certificats suivants sont décrits dans les chapitres 4.6, 4.7 et 4.8.

4.1.1 Origine d'une demande de certificat

4.1.1.1 Certificat AC

Une demande de certificat d'AC est effectuée par l'AP.

4.1.1.2 Certificat « Client »

Un certificat peut être demandé par un porteur sous la responsabilité de l'AE. La demande de certificat est assimilée à une demande de signature de contrat ou d'acte de gestion. Elle est effectuée conformément à la politique de signature mise en œuvre par l'AE.

4.1.1.3 Certificat « cachet serveur »

Un certificat peut être demandé par un CT.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

4.1.2.1 Certificat AC

Les ACs sont enregistrées auprès de l'AP.

Une demande de création d'AC contient l'identifiant de l'AC « KEYNECTIS CDS CA » qui signe son certificat.

Dans tous les cas une demande de certificat est assimilée au document de nommage signé par l'AP et transmis à OpenTrust.

4.1.2.2 Certificat « Client »

Les informations qui servent à construire la demande de certificat sont les suivantes :

- Nom et prénom du Client tel que portés sur la pièce d'identité en cours de validité lors de l'entrée en relation et tel qu'enregistrés par l'AE.
- La présentation de la pièce d'identité officielle du Client en agence.
- La transmission de la copie de deux pièces d'identité officielles du Client en cas d'entrée en relation à distance

- L'information permettant de contacter et d'authentifier le Porteur (adresse de courrier électronique, et/ou numéro de téléphone, …) en fonction de la politique de signature qui est appliquée par l'AE.

- Pour les professionnels, les informations d'identification de l'entreprise du porteur.

4.1.2.3 Certificat « cachet serveur »

Les informations suivantes figurent dans la demande de certificat « cachet serveur » :

- Le nom et prénom du CT.

- Les Informations permettant à l'AE de contacter le CT et d'authentifier le CT (numéro de téléphone, courriel, …).

- La CSR pour la clé publique à certifier.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

4.2.1.1 Certificat AC

L'AP est responsable d'identifier, authentifier et traiter la demande de certificat d'AC.

4.2.1.2 Certificat « Client »

La demande est authentifiée (se reporter aux § 3.2.2 et le 3.2.5) et validée par l'AE.

L'AE identifie et authentifie le Porteur (Cf. § 3.2.2 et le 3.2.5).

L'AE s'assure que le porteur a pris connaissance des conditions générales d'utilisation.

L'AE conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement.

4.2.1.3 Certificat : « cachet serveur »

La demande est authentifiée (se reporter aux § 3.2.2 et le 3.2.5) et validée par l'AE.

L'AE identifie et authentifie le CT (Cf. § 3.2.2 et le 3.2.5).

L'AE s'assure que le CT a pris connaissance des conditions générales d'utilisation.

L'AE conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement.

4.2.2 Acceptation ou rejet de la demande

4.2.2.1 Certificat AC

L'AP autorise ou rejette la création d'un certificat AC. En cas d'acceptation, l'AP transmet cette demande à l'OT et à OpenTrust afin de procéder à la cérémonie des clés et à la création du certificat d'AC en fonction de la demande.

4.2.2.2 Certificat « Client »

En cas d'approbation de la demande, l'AE transmet la demande à l'AC dans le cadre de cinématique de signature décrite dans la politique de signature.

En cas de rejet de la demande, l'AE en informe le porteur (en fonction de l'origine de la demande) en justifiant le rejet.

4.2.2.3 Certificat : « cachet serveur »

En cas d'approbation de la demande, l'AE (service de demande de certificat) transmet la demande à l'AC (service de génération de certificat).

En cas de rejet de la demande, l'AE en informe le CT (en fonction de l'origine de la demande) en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

4.2.3.1 Certificat AC

La durée du traitement d'une demande de certificat par l'AP est définit dans la DPC.

4.2.3.2 Certificat « Client »

La durée du traitement est liée au processus de signature électronique et est immédiate suite à acceptation de la demande de signature.

4.2.3.3 Certificat « cachet serveur »

La demande de certificat est traitée dès la réception de la demande par l'AE dans les meilleurs délais.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

4.3.1.1 Certificat AC

Les ACs sont générées pendant une cérémonie des clés (se reporter au § 6.1) dans les locaux de l'OT.

Dans ce cas, le certificat d'AC est signé au cours d'une cérémonie de certification par l'AC choisie dans les locaux d'OpenTrust (qui est OT pour la cérémonie des clés). La cérémonie des clés de l'AC et la cérémonie de certification par l'AC d'OpenTrust ne sont pas obligatoirement effectuées le même jour. Dans tous les cas, la cérémonie des clés nécessite l'activation des clés d'AC sous multiples contrôles (cf. 6.1.1 et 6.2.8).

L'AP vérifie le contenu du document de nommage des AC, en termes de complétude et d'exactitude des informations présentes. Ce document est utilisé comme base de réalisation de la cérémonie de clés de création des AC.

À la fin de la cérémonie des clés, les clés privées de l'AC n'existent que sous forme de sauvegarde (Cf. § 6.2.9) et sont transférées dans la ressource cryptographique (HSM) de production (Cf. 6.2.6).

4.3.1.2 Certificat « Client »

Le Porteur déclenche la génération de sa bi-clé dans le Portail de l'AE suivant la cinématique d'activation choisie par l'AE et décrite dans la politique de signature (se reporter au § 6.1.1 ci-dessous).

L'AE transmet la demande technique de certificat, qui contient la CSR, à l'AC.

L'AC authentifie l'AE.

L'AC signe le certificat.

L'opération de signature est effectuée sur le contrat ou l'acte de gestion à signer conformément à la cinématique de signature décrite dans la politique de signature.

Les communications, entre les différentes composantes de l'AC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

4.3.1.3 Certificat : « cachet serveur «

L'AC (service de génération de certificat) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC signe le certificat.

L'AC transmet le certificat à l'AE.

L'AE transmet le certificat au CT.

Les communications, entre les différentes composantes de l'AC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

4.3.2 Notification par l'AC de la délivrance du certificat au porteur

4.3.2.1 Certificat AC

La notification est effectuée à la fin de la cérémonie des clés de l'AC. Les certificats d'AC sont remis à l'AP.

4.3.2.2 Certificat « Client »

Il n'y a pas de notifications particulières de la délivrance du certificat. Le certificat est éphémère et utilisé immédiatement dans les opérations de signature électronique.

Le certificat est intégré au document électronique matérialisant le contrat ou l'acte de gestion signé du Porteur.

4.3.2.3 Certificat : « cachet serveur »

La remise du certificat au CT s'effectue par l'AE par courrier électronique au CT.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

4.4.1.1 Certificat AC

L'AP vérifie que le certificat d'AC généré contient les informations décrites dans le document de nommage signé. Dès que l'AP confirme l'adéquation entre le certificat généré et le document de nommage, alors l'AP accepte le certificat émis et le témoin de l'AP signe une acceptation officielle du certificat émis.

4.4.1.2 Certificat « Client »

Le Client peut récupérer le contrat ou l'acte de gestion signé et ensuite vérifier le contenu du certificat (notamment les informations qui composent son identité cf. 3.1.1). Si le Client n'informe pas l'AE d'une anomalie dans le certificat, alors le certificat est considéré comme accepté.

4.4.1.3 Certificat : « cachet serveur »

A réception, le CT vérifie les informations du certificat. En cas d'anomalie il le signale à l'AE qui révoque le certificat. Si l'AE ne reçoit pas d'alerte de la part du CT, le certificat est considéré comme accepté.

4.4.2 Publication du certificat

4.4.2.1 Certificat AC

Les certificats d'AC sont publiés par le SP. L'AP est dépositaire officiel de l'ensemble des certificats d'ACs et des ARLs. L'AP est responsable de la diffusion des certificats et des ARLs en plus des moyens fournis par le SP.

4.4.2.2 Certificat Porteur : « Client »

Les certificats ne sont pas publiés après leur délivrance.

4.4.2.3 Certificat : « cachet serveur »

Ils ne sont pas publiés.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

4.4.3.1 Certificat AC

En cas de besoin, l'AP est responsable des communications de certificat d'AC aux entités externes.

4.4.3.2 Certificat Porteur

Sans objet.

4.5 Usage de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation des bi-clés et des certificats est définie au § 1.4 ci-dessus. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (se reporter au § **Erreur ! Source du renvoi introuvable.**). La clé privée du porteur ne peut être utilisée que pour une opération de signature de contrat ou d'acte de gestion comme indiqué au § 1.4 en fonction du type de certificat.

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

L'utilisation des certificats par les UC est décrites dans les paragraphes 1.4 et 3.1.4 ci-dessus.

4.6 Renouvellement d'un certificat

Cette section concerne le processus de renouvellement du certificat, sans que les clés publiques ou toute autre information incluse dans les certificats soient modifiées. Seule la période de validité et le numéro de série changent.

Ce type d'opération n'est pas autorisé au titre de la présente PC.

Il est interdit de prolonger ainsi les bi-clés d'AC. Par défaut, il n'existe pas de prolongation des clés d'AC. Ce cas peut être autorisé si les conditions opérationnelles des applications utilisatrices le requièrent et qu'il n'existe pas d'autre solution. En ce cas, l'AP pourra accepter ce type de renouvellement uniquement si les recommandations en matière cryptographique (portant sur les algorithmes de signature et les algorithmes de calcul d'empreinte) le permettent et que ce renouvellement n'engendre pas un risque pour les applications utilisatrices.

Au plus, un seul renouvellement de certificat sans changement de bi-clé d'AC est autorisé.

Dans tous les cas, pour le changement de certificat d'AC, la procédure à suivre est identique à la procédure initiale de certification décrite aux § 3.2 et § 4.1, § 4.2 et § 4.3 ci-dessus.

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Cette section concerne la génération d'un nouveau certificat avec changement de la clé publique associée.

Le changement de la clé publique d'un certificat implique la création d'un nouveau certificat.

4.7.1 Certificat AC

Dans ce cas la procédure à appliquer pour renouveler un certificat porteur est identique à celles décrites pour la délivrance du premier certificat porteur (se reporter au § 3.3, § **Erreur ! Source du renvoi introuvable.**, § 4.2 et § 4.3 ci-dessus).

4.7.2 Certificat : « Client »

Dans ce cas la procédure à appliquer pour renouveler un certificat porteur s'appuie sur les informations déjà remises et demandées lors des phases décrites aux § 3.2 et § 4.1.

La demande est authentifiée (se reporter aux § 3.3) et validée par l'AE.

L'AE identifie et authentifie le Porteur (Cf. § 3.3).

L'AE conserve dans ses journaux l'ensemble des mises à jour des pièces qui composent le dossier d'enregistrement.

En cas d'approbation de la demande, l'AE transmet la demande à l'AC dans le cadre de cinématique de signature décrite dans la politique de signature.

En cas de rejet de la demande, l'AE en informe le porteur (en fonction de l'origine de la demande) en justifiant le rejet.

L'AC génère ensuite le certificat (Cf. § 4.3) et le Porteur l'accepte ensuite (Cf. § 4.4.1).

4.7.3 Certificat: « Cachet serveur »

Dans ce cas la procédure à appliquer pour renouveler un certificat est identique à celles décrites pour la délivrance du premier certificat (se reporter au § 3.3, § **Erreur ! Source du renvoi introuvable.**, § 4.2 et § 4.3 ci-dessus).

4.8 Modification du certificat

Cette section concerne la génération d'un nouveau certificat avec conservation de la même clé. Cette opération est rendue possible uniquement si la clé publique réutilisée dans le certificat est toujours conforme aux recommandations de sécurité cryptographique applicables en matière de longueur de la clé.

Ce type d'opération n'est pas autorisé au titre de la présente PC pour les certificats Porteurs.

Il est interdit de prolonger ainsi les bi-clés d'AC. Par défaut, il n'existe pas de prolongation des clés d'AC. Ce cas peut être autorisé si les conditions opérationnelles des applications utilisatrices le requièrent et qu'il n'existe pas d'autre solution. En ce cas, l'AP pourra accepter ce type de renouvellement uniquement si les recommandations en matière cryptographique (portant sur les algorithmes de signature et les algorithmes de calcul d'empreinte) le permettent et que ce renouvellement n'engendre pas un risque pour les applications utilisatrices.

Au plus, un seul renouvellement de certificat sans changement de bi-clé d'AC est autorisé.

Dans tous les cas, pour le changement de certificat d'AC, la procédure à suivre est identique à la procédure initiale de certification décrite aux § 3.2 et § 4.1, § 4.2 et § 4.3 ci-dessus.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat AC

Les causes de révocations sont les suivantes :

- Cessation d'activité de l'AC « KEYNECTIS CDS CA »qui a servi à signer les AC.
- Fin du programme Adobe Certified Document Services (CDS)
- Compromission de clé privée de l'AC « KEYNECTIS CDS CA » qui a servi à signer les AC.
- Compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'AC (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés).
- Non-respect de la politique de certification et de la déclaration des pratiques de certification de l'AC « KEYNECTIS CDS CA » qui a servi à signer les AC.
- Non-respect de la politique de certification et de la déclaration des pratiques de certification de l'AC.
- Changement d'informations dans le certificat.
- Obsolescence de la cryptographie au regard des exigences internationales en la matière.

4.9.1.2 Certificat : « Client »

Sans objet.

4.9.1.3 Certificat « Cachet Serveur »

Un certificat est révoqué quand l'association de la clé publique et de l'identité qu'il certifie n'est plus considérée comme valide. Les motifs qui invalident cette association sont :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat.
- Le CT n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent.
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement.
- La cessation d'activité du service référencé dans le cachet serveur ou de l'entité légale référencé dans le cachet serveur ou la compromission du serveur qui héberge la clé privée du cachet serveur.
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé.
- La révocation de l'AC.
- La fin de vie de l'AC.
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

Quand l'une de ces occurrences se produit, le certificat en question est révoqué.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat AC

L'AP est à l'origine de la demande de révocation des certificats d'AC.

OpenTrust peut être à l'origine de la demande de révocation des certificats en fonction des résultats d'audit réalisés sur l'AC.

4.9.2.2 Certificat « Client »

Sans objet.

4.9.2.3 Certificat « Cachet Serveur »

Le CT, son responsable, l'AE ou l'AC peuvent faire une demande de révocation dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat.
- Le CT n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent.
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement.
- La cessation d'activité du service référencé dans le cachet serveur ou de l'entité légale référencé dans le cachet serveur ou la compromission du serveur qui héberge la clé privée du cachet serveur.
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé.
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes (uniquement l'AC).
- La révocation de l'AC (uniquement l'AC).
- La fin de vie de l'AC (uniquement l'AC).

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat AC

L'AP est responsable de gérer la mise en œuvre de la demande de la révocation.

La procédure de révocation d'une AC est écrite dans la PC d'OpenTrust qui est utilisée pour gérer les certificats d'AC (se reporter à https://www.opentrust.com/PC/).

4.9.3.2 Certificat « Client »

Sans objet.

4.9.3.3 Certificat « cachet serveur »

Une demande de révocation contient les informations suivantes :

- L'identité du porteur du certificat utilisée dans le certificat (nom, prénom, ...) ;

- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série du certificat,...).

La demande de révocation est conservée par l'AE dans ses journaux.

La demande de révocation est authentifiée conformément au § 3.4.

L'AE transmet la demande de révocation à l'AC.

L'AC authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC révoque le certificat du porteur en incluant le numéro de série du certificat dans la prochaine LCR qui sera émise par l'AC.

Le demandeur de la révocation est informé de la révocation effective. De plus, si le porteur du certificat n'est pas le demandeur, le porteur est également informé de la révocation effective du certificat.

Dans le cas d'un porteur au sein d'une Entreprise ou d'une Administration, l'organisation d'appartenance (se reporter § 3.2.2) est informée de la révocation des certificats des porteurs qui lui sont rattachés.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

4.9.4.1 Certificat AC

Il n'y a pas de période de grâce dans le cas d'une révocation d'une AC. L'AP demande la révocation d'un certificat dès lors qu'elle en identifie une cause de révocation comme définie au § **Erreur ! Source du renvoi introuvable.**.

4.9.4.2 Certificat « cachet serveur »

Dès que le demandeur a connaissance qu'une des causes possibles de révocation de son ressort, est effective, il formule sa demande de révocation sans délai.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Certificat AC

Le service de demande de révocation est disponible tous les jours H24 et 7J7. Une demande de révocation est traitée dans les meilleurs délais, et au maximum sous 24 heures par l'AP.

En cas d'indisponibilité du système, du service, ou d'autres éléments, qui échappe au contrôle de l'AP, ce dernier fait de son mieux pour que l'indisponibilité de ce service puisse permettre à l'AP de demander une révocation de certificat d'AC au plus vite auprès d'OpenTrust.

4.9.5.2 Certificat « Client »

Sans objet

4.9.5.3 Certificat « Cachet Serveur »

Une demande de révocation, authentifié et dûment établie par l'AE, émise par le CT est traitée dans un délai inférieur à 24 heures.

4.9.6 Exigences de vérification de révocation pour les utilisateurs de certificats

Il appartient aux UC de vérifier l'état de validité d'un certificat d'AC à l'aide de l'ensemble des ARLs émises par OpenTrust.

Il appartient aux UC de vérifier l'état de validité d'un certificat Porteur à l'aide de l'ensemble des LCR émises par l'AC.

4.9.7 Fréquences d'établissement des LCR

La LCR émise par l'AC est émise toutes les 24 Heures. Elles sont également générées après chaque révocation et publiées sous un délai de 3 heures.

4.9.8 Délai maximum de publication d'une LCR

Le délai maximum de publication d'une LCR suite à sa génération est de 3 heures.

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

Sans objet.

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

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

Pour les certificats d'AC la révocation suite à une compromission de sa clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC (Cf. § 2.2) et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.). En cas de révocation de l'AC, l'ensemble des certificats porteurs sont révoqués.

Les conditions générales d'utilisation du certificat mentionnent clairement qu'en cas de compromission de la clé privée du porteur ou de connaissance de la compromission de la

clé privée de l'AC ayant émis son certificat, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.13 Causes possibles d'une suspension

Sans objet.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

Sans objet.

4.10.2 Disponibilité de la fonction

Sans objet.

4.11 Fin de la relation entre le porteur et l'AC

Sans objet.

4.12 Séquestre de clé et recouvrement

Les bi-clés et les certificats des porteurs et d'AC émis conformément à la PC ne font pas l'objet de séquestre ni de recouvrement.

5 MESURES DE SÉCURITÉ NON TECHNIQUES

5.1 Mesures de sécurité physiques

5.1.1 Situation géographique et construction des sites

La construction des sites respecte les règlements et normes en vigueur.

La localisation géographique des sites ne présente pas de risque concernant les tremblements de terre, les explosions ou les inondations.

Le site d'exploitation est protégé par des systèmes de détection d'intrusion, de caméra, de gardiennage permettant la protection contre les accès non autorisés aux équipements.

Les équipements de l'OT doivent toujours être protégés contre tout accès non autorisé. Les exigences relatives aux équipements sont les suivantes :

- S'assurer qu'aucun accès non autorisé au matériel ne soit autorisé.
- S'assurer que tous les supports amovibles et documents papier contenant des informations sensibles en texte brut sont stockés de manière sûre.
- S'assurer de l'existence d'une surveillance permanente via vidéo et gardiennage pour protéger les locaux contre les risques d'intrusions.
- S'assurer que les ressources cryptographiques et les composantes de l'AC sont accessibles uniquement sous double contrôle.
- Assurer qu'un journal des accès est entretenu et inspecté régulièrement.
- Fournir plusieurs niveaux de renforcement pour la sécurité périmétrique des accès physique.
- Assurer que seules les personnes physiques autorisées ont accès aux composantes de l'Infrastructure de Gestion de Clés.
- Assurer la désactivation des modules cryptographiques avant leur stockage.
- Assurer que les données d'activation utilisées pour accéder aux modules cryptographiques sont placées dans des coffres.
- Assurer que les données d'activation sont soit mémorisées soit enregistrées et stockées de manière compatible avec la sécurité offerte par le module cryptographique.
- Assurer que les données d'activation non nécessaire au fonctionnement quotidien de la ressource cryptographique « en ligne » ne sont pas stockées avec le module cryptographique associé.

Une personne ou un groupe de personnes doit être explicitement chargé d'effectuer ces contrôles.

5.1.2 Accès physique

L'accès physique aux fonctions sensibles de l'infrastructure est strictement limité aux seules personnes nominativement autorisées.

L'accès physique aux composantes supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants.

La traçabilité des accès est assurée.

Des mesures de détection d'intrusion physique sont mises en œuvre, notamment via l'utilisation de caméras.

Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (DPC, documents d'applications).

5.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre par l'opérateur de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne portent pas atteinte aux engagements pris par l'OT en matière de disponibilité pour l'ensemble des fonctions sensibles de son infrastructure.

5.1.4 Vulnérabilité aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre pour parer les risques résiduels (rupture de canalisation par exemple).

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie permettent de respecter les engagements pris par l'OT en matière de disponibilité, et de pérennité de l'archivage pour l'ensemble des fonctions sensibles de son infrastructure.

5.1.6 Conservation des supports

Les moyens de conservation des supports permettent de respecter les engagements pris par l'OT en matière de restitution et de pérennité de l'archivage.

5.1.7 Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction, ou peuvent être réutilisés dans un contexte opérationnel identique à un même niveau de sensibilité.

5.1.8 Sauvegardes hors site

Afin de permettre une reprise après incident conforme aux engagements pris par l'AP, l'OP met en place 2 sites redondés permettant dans cette forme de garantir

l'externalisation des données. L'archivage des fichiers de preuve (Se reporter au document « Politique de Gestion des Preuves BPCE SA ») de l'AE à valeur légale est hébergé chez un OT externe choisi par l'AP.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance sont classés de la manière suivante :

- Les personnels d'exploitation, dont la responsabilité est le maintien des systèmes qui supportent l'Infrastructure de Gestion de Clés en conditions opérationnelles de fonctionnement.
- Les personnels d'administration, dont la responsabilité est l'administration fonctionnelle des composantes de l'Infrastructure de Gestion de Clés.
- Les personnels de « sécurité », dont la responsabilité est de définir et de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de l'Infrastructure de Gestion de Clés.
- Auditeur : tiers désigné par l'AP pour effectuer l'audit de l'ensemble des mesures techniques, physiques, fonctionnelles et organisationnelles permettant de mesurer la conformité de l'Infrastructure de Gestion de Clés par rapport aux PC et DPC. Il est choisi selon des critères d'indépendance et d'expertise dans le domaine de la sécurité informatique et, en particulier, des Infrastructure de Gestion de Clés.
- Détenteur de données d'activation (ou détenteur de secret) : personne désignée par l'AP pour détenir une donnée d'activation de la clé privée d'une AC conformément aux règles de sécurité définies dans la PC, la DPC et des pratiques associées pour l'AC concernée. Cette personne peut posséder plusieurs éléments secrets provenant de plusieurs AC dès lors qu'il ne possède pas plus d'un élément par AC.
- Témoin : personne nommée par l'AP pour attester que l'intégralité des opérations effectuées lors de la cérémonie des clés ont été effectivement réalisées conformément aux documents présentés et approuvés au préalable assurant ainsi l'intégrité des opérations effectuées.

5.2.2 Nombre de personnes requises par tâches

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre (se reporter au § **Erreur ! Source du renvoi introuvable.**).

5.2.3 Identification et authentification pour chaque rôle

L'OT fait vérifier l'identité et les autorisations de tout membre de son personnel amené à mettre en œuvre les services de l'Infrastructure de Gestion de Clés avant de lui attribuer un rôle et les droits correspondants. L'attribution des accès et des rôles techniques donne lieu systématiquement à un enregistrement. Les accès sont nominatifs et permettent ainsi d'imputer les actions à une personne.

Les contrôles sont décrits dans la DPC et sont conformes à la politique de sécurité de l'OT. Chaque attribution d'un rôle à un membre du personnel de l'Infrastructure de Gestion de Clés lui est notifiée par écrit ou équivalent.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous encadrant le cumul soient respectées :

- Les rôles Sécurité et Auditeur ne peuvent pas être cumulés avec administration et exploitation.

- Le rôle Témoin peut être cumulé avec seulement Auditeur et détenteur de secret.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de l'Infrastructure de Gestion de Clés est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant dans les procédures de certification de l'Infrastructure de Gestion de Clés est informée de ses responsabilités relatives aux services de l'Infrastructure de Gestion de Clés et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

L'Infrastructure de Gestion de Clés met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Le choix des personnes pour exercer un rôle de confiance ne doit pas créer une situation de conflits d'intérêts susceptible de porter préjudice à l'impartialité de ces dernières.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

5.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité, correspondants à la composante au sein de laquelle il opère.

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

En fonction de la nature des évolutions apportées, le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Dès qu'une personne change de rôle de confiance, ses comptes dans l'Infrastructure de Gestion de Clés sont réinitialisés afin de ne pas porter atteinte à la sécurité du non cumul des rôles décrit au paragraphe 5.2.

5.3.6 Sanctions en cas d'actions non autorisées

Les procédures internes de l'OT précisent ou font référence aux sanctions prévues en cas d'actions non autorisées. Elles sont communiquées au personnel avant la prise de fonction.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les exigences sont identiques au § **Erreur ! Source du renvoi introuvable.**.

5.3.8 Documentation fournie au personnel

Le personnel a accès à la documentation concernant les procédures et les systèmes techniques qui le concernent dans le cadre de ses fonctions. Notamment il a accès à la politique de sécurité correspondante.

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier et/ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'événements à enregistrer

L'Infrastructure de Gestion de Clés journalise les évènements concernant les systèmes liés aux fonctions qu'elles mettent en œuvre dans le cadre de l'Infrastructure de Gestion de Clés :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.).
- Démarrage et arrêt des systèmes informatiques et des applications.

- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation.
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes.

D'autres évènements sont également recueillis. Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- Les accès physiques aux zones sensibles.
- Les actions de maintenance et de changements de la configuration des systèmes.
- Les changements apportés au personnel ayant des rôles de confiance.
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Utilisateurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'Infrastructure de Gestion de Clés, des évènements spécifiques aux différentes fonctions de l'GC sont également journalisés :

- Réception d'une demande de certificat (initiale et renouvellement).
- Validation / rejet d'une demande de certificat.
- Evènements liés aux clés de signature des Porteurs (Client) et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction,...).
- Génération des certificats de porteurs.
- Transmission des certificats aux porteurs et selon les cas, acceptations / rejets par les Porteurs.
- Publication et mise à jour des informations liées à l'AC.
- Génération d'information de statut d'un certificat (porteur).

Chaque enregistrement d'un évènement dans un journal contient les champs suivants :

- Type de l'évènement.
- Nom de l'exécutant ou référence du système déclenchant l'évènement.
- Date et heure de l'évènement.
- Résultat de l'évènement (échec ou réussite).

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

Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés:

- Destinataire de l'opération.
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande.
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes).
- Cause de l'évènement.
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

5.4.2 Fréquence de traitement des journaux d'événements

Les opérations de journalisation sont effectuées au cours du processus considéré. En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'évènements sont conservés sur site pendant au moins 1 an.

Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 15 jours (recouvrement possible entre la période de conservation sur site et la période d'archivage). L'auditeur a la responsabilité des données d'audit qu'il consulte ou génère lors de toutes les phases de son travail (collecte, diffusion et archivage).

5.4.4 Procédures de sauvegarde des journaux d'événements

L'OT met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC.

5.4.5 Système de collecte des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non). Le système de datation des évènements respecte les exigences du § **Erreur ! Source du renvoi introuvable.**. Les journaux sont conservés y compris une fois mis sur le site de secours.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

Les journaux ne sont accessibles que par les personnes autorisées.

5.4.6 Evaluation des vulnérabilités

L'AC et l'AE sont en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont analysés suite à la détection d'une anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

5.5 Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'Infrastructure de Gestion de Clés.

5.5.1 Type de données à archiver

Les données archivées au niveau de chaque composante, sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques.
- La politique de certification.
- La déclaration des pratiques de certification.
- Les certificats tels qu'émis ou publiés.
- Les justificatifs d'identité des porteurs et, le cas échéant, les justificatifs d'existence juridique de leur entité de rattachement (pour les entreprises et les administrations).
- Les fichiers de preuves de l'AE (Se reporter au document « Politique de Gestion des Preuves BPCE SA »).
- Les dossiers complets de demandes de certificats.
- Les journaux d'évènements des différentes entités de l'Infrastructure de Gestion de Clés.

5.5.2 Période de conservation des archives

Les données archivées sont conservées au minimum 10 ans.

5.5.3 Protection des archives

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

- Seront protégées en intégrité.
- seront accessibles aux seules personnes autorisées.
- pourront être consultées et exploitées.

5.5.4 Exigences d'horodatage des données

Si un service d'horodatage est utilisé pour dater les enregistrements, il répond aux exigences formulées à l'article 6.8.

5.5.5 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (Se reporter au 5.5.3).

5.5.6 Procédures de récupération et de vérification des archives

Les sauvegardes électroniques archivées sont récupérables dans les meilleurs délais.

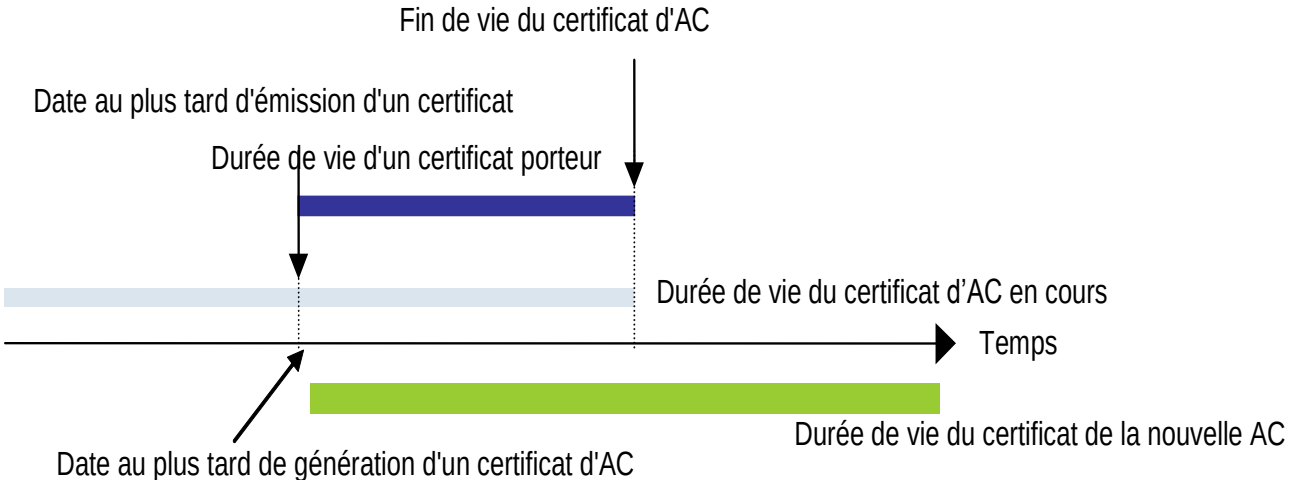
5.6 Changement de clé d'AC

5.6.1 Certificat d'AC

La durée de vie d'un certificat d'AC est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationales ou internationales compétentes en la matière. La DPC précise les standards utilisés.

Une AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats de porteurs. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats porteurs émis à l'aide de cette bi-clé.



Par ailleurs, l'AC change sa bi-clé et le certificat correspondant quand la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

5.6.2 Certificat de Porteur

5.6.2.1 Certificat « Client »

La durée de validité d'un certificat est de 10 minutes maximum.

5.6.2.2 Certificat « Cachet serveur »

La durée de validité d'un certificat est de 3 ans maximum.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

L'AC a établi un plan de continuité de service. Il est composé des différentes étapes à exécuter dans l'éventualité de la corruption ou de la perte des ressources système, des logiciels et / ou des données et qui pourraient perturber ou compromettre le bon déroulement des services d'AC.

Le plan de continuité de l'AC fait partie du périmètre audité, selon le paragraphe 8 ci-dessous.

Les personnels de l'AC dans un rôle de confiance sont spécialement entraînés à réagir selon les procédures définies dans le plan de reprise d'activité qui concernent les activités les plus sensibles.

Dans le cas où l'AC détecte une tentative de piratage ou une autre forme de compromission, elle mène une analyse afin de déterminer la nature des conséquences et leur niveau. L'AC informe les CT et éventuellement révoque les certificats « cachet serveur ».

L'AC prévient directement et sans délai OpenTrust.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Si le matériel de l'AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Si la clé de signature de l'AC est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- L'AP, après enquête sur l'évènement décide de révoquer le certificat de l'AC.
- les CT sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué.
- L'AP décide ou non de générer une nouvelle bi-clé d'AC et un nouveau certificat d'AC.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le plan de reprise d'activité après sinistre traite de la continuité d'activité telle qu'elle est décrite au § 5.7.1. Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

5.8 Fin de vie d'Infrastructure de Gestion de Clés

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

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

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

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

5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'Infrastructure de Gestion de Clés

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

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

Des précisions quant aux engagements suivants sont ainsi annoncées par l'AC dans sa PC :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire.
- L'AC communique à OpenTrust, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC devra communiquer à OpenTrust, selon les différentes composantes de l'Infrastructure de Gestion de Clés concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.
- L'AC tient informé OpenTrust de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2 Cessation d'activité affectant l'AC

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

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC.

L'AC procède aux actions suivantes :
- La notification des entités affectées,
- Le transfert de ses obligations à d'autres parties,
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :
- S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats,
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante,
- Révoque son certificat,
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité,
- Informe (par exemple par récépissé) tous les porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Bi-clés d'AC

Suite à l'accord de l'AP pour la génération d'un certificat d'AC, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle (se reporter au § 6.2.11 ci-dessous).

Les cérémonies de clés se déroulent sous le contrôle d'au moins trois personnes dans des rôles de confiance (maître de cérémonie et témoins) et sont impartiaux. Elle se déroule dans les locaux de l'OT choisi par l'AP.

Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. La cérémonie des clés se déroule sous vidéo ou en présence d'un auditeur externe.

Suite à leur génération, les parts de secrets (données d'activation) sont remises à des détenteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par le Groupe BPCE. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secret d'une même AC à un moment donné sauf si ça ne remet pas en cause la sécurité définit pour les clés d'AC. Chaque part de secret est mise en œuvre par son porteur.

6.1.1.2 Bi-clés Client

Les bi-clés du Porteur sont générées par l'AE dans une ressource cryptographique (HSM) (se reporter au § 6.2.11 ci-dessous) de manière à ne pas porter atteinte à la confidentialité et l'intégrité des bi-clés. La génération est consécutive aux différentes cinématiques d'activation choisies par les AE et décrites dans la politique de signature.

6.1.1.3 Bi-clés Cachet serveur

La génération des bi-clés est effectuée par le CT ou sous contrôle du CT, dans une ressource cryptographique (HSM) (se reporter au § 6.2.11 ci-dessous) de manière à ne pas porter atteinte à la confidentialité et l'intégrité des bi-clés. Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération de bi-clé en toute sécurité.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

6.1.3.1 Clé publique Client

La clé publique est transmise à l'AC lors de la génération de la bi-clé, sous un format PKCS#10, et lors d'une connexion sécurisée de manière à garantir l'intégrité et la confidentialité de la communication et l'authentification entre l'AC et l'AE.

6.1.3.2 Clé publique Cachet serveur

La clé publique est transmise à l'AE par le CT, lors de la demande de certificat, au format PKCS#10 et la transmission est authentifiée par l'AE.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

L'ensemble des certificats de la chaîne de confiance de l'AC est contenu dans le contrat ou l'acte de gestion signé.

L'ensemble des certificats de la chaîne de confiance de l'AC est remis au CT par l'AE.

L'ensemble des certificats d'AC est publié par le SP.

Le certificat de l'AC OpenTrust dont dépend l'AC est contenu dans les logiciels d'Adobe.

6.1.5 Taille des clés

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats porteurs et AC sont ou ne sont pas modifiés.

L'utilisation de l'algorithme RSA avec la fonction de hachage SHA-256 est utilisée pour l'AC. La taille de la bi-clé de l'AC est d'au moins 2048 bits.

La longueur des clés des certificats porteurs est de 2048 bits pour l'algorithme RSA avec la fonction de hachage SHA-256.

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

6.1.6.1 Bi-clés AC

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles évaluées certifiées critère commun EAL 4+ ou FIPS 140-2 level 3.

6.1.6.2 Bi-clés Clients et Cachet serveur

Les équipements utilisés pour la génération des bi-clés sont des ressources cryptographiques matérielles évaluées certifiées critère commun EAL 4+ ou FIPS 140-2 level 3.

6.1.7 Objectifs d'usage des bi-clés

6.1.7.1 Bi-clés AC

L'utilisation du champ "key usage" (Utilisation de la clé) dans le certificat AC est la suivante :

- Key CertSign (Certificate Signature) (Signature de certificat)
- Key CRL Sign (CRL Signature) (Liste de révocation de certificat).

L'utilisation du champ "Extented key usage" (Utilisation de la clé avancée) est la suivante :

- Documents Acrobat Authentiques.

6.1.7.2 Bi-clés Client

L'utilisation du champ "key usage" (Utilisation de la clé) est la suivante :

- Digital Signature (Signature de document)
- Non Repudiation (Signature de transaction)

L'utilisation du champ "Extented key usage" (Utilisation de la clé avancée) est la suivante :

- Documents Acrobat Authentiques

6.1.7.3 Bi-clés Cachet serveur : signature personne morale

L'utilisation du champ "key usage" (Utilisation de la clé) dans le certificat Porteur est la suivante :

- Digital signature (Signature de document)
- Non Repudiation (Signature de transaction).

L'utilisation du champ "Extented key usage" (Utilisation de la clé avancée) est la suivante :

- Documents Acrobat Authentiques

6.1.7.4 Bi-clés Cachet serveur : signature application

L'utilisation du champ "key usage" (Utilisation de la clé) dans le certificat Porteur est la suivante :

- Digital signature.

6.1.7.5 Bi-clés Cachet serveur : horodatage

L'utilisation du champ "key usage" (Utilisation de la clé) dans le certificat Porteur est la suivante :

- Digital signature.

L'utilisation du champ "Extented key usage" (Utilisation de la clé avancée) est la suivante :

- Timestamping (Tampon temporel).

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Bi-clés AC

La ressource cryptographique matérielle pour les bi-clés utilise des algorithmes conformes aux standards en vigueur ou respectant les spécifications de la normalisation lorsqu'ils sont normalisés.

6.2.1.2 Bi-clés Clients et Cachet serveur

La ressource cryptographique matérielle pour les bi-clés utilise des algorithmes conformes aux standards en vigueur ou respectant les spécifications de la normalisation lorsqu'ils sont normalisés.

6.2.2 Contrôle de la clé privée par plusieurs personnes

6.2.2.1 Clé privée d'AC

Le contrôle de la clé privée d'une d'AC est réalisé par au moins 2 personnes, désignées par le Groupe BPCE, détenant des données d'activation. Les détenteurs de données d'activation participant à l'activation de la clé privée d'AC font l'objet d'une authentification forte.

L'AC est activée dans une ressource cryptographique matérielle identique à celle utilisée pour la génération de la bi-clé. Ainsi elle peut être utilisée uniquement par les seuls rôles de confiance et seuls processus autorisés qui peuvent émettre des certificats Porteurs et des CRL, sans diminuer la sécurité apportée aux bi-clés.

6.2.2.2 Bi-clés Client

Après authentification réussie du client, la bi-clé Clients est générée dans un HSM, personnalisé par des rôles de confiance de l'OT sous multi-contrôle. L'authentification est mise en œuvre suivant la cinématique d'activation choisie par l'AE et décrite dans la politique de signature.

6.2.2.3 Bi-clés Cachet serveur

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé cachet serveur en toute sécurité.

Le contrôle de la clé privée d'un cachet serveur est réalisé par au moins 2 personnes, désignées par l'OT, détenant des données d'activation. Les détenteurs de données d'activation participant à l'activation de la clé privée du cachet serveur font l'objet d'une authentification forte.

Le cachet serveur est activé dans une ressource cryptographique matérielle identique à celle utilisée pour la génération de la bi-clé. Elle peut être utilisée uniquement par les seuls rôles de confiance et seuls processus autorisés pour émettre des signatures électroniques ou des contremarques de temps, sans diminuer la sécurité apportée aux bi-clés.

6.2.3 Séquestre de clé privée

Les clés privées ne font pas l'objet de séquestre.

6.2.4 Copie de secours de clé privée

6.2.4.1 Bi-clés AC

Les bi-clés d'AC sont sauvegardées à des fins de disponibilité sous le contrôle de plusieurs personnes (détenteurs de données d'activation) afin de respecter les conditions initiales de contrôle de la clé privée. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles identiques à celles utilisées pour générer les bi-clés d'AC et stockées dans les locaux de l'OT.

Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'Infrastructure de Gestion de Clés (se reporter au § **Erreur ! Source du renvoi introuvable.**). Les sauvegardes de clés privées d'AC sont stockées sous forme de fichiers chiffrés qui permettent de garantir un même niveau de sécurité (multi-contrôle comme décrit au § **Erreur ! Source du renvoi introuvable.**) que celle utilisée pour la génération ou sous forme de fichier chiffré.

6.2.4.2 Bi-clés : Client

Il n'y a pas de copie de secours des clés privées des Clients.

6.2.4.3 Bi-clés : Cachet serveur

Le CT peut décider de faire des copies de secours des clés privées pour des raisons de disponibilités.

En ce cas, les bi-clés sont sauvegardées à des fins de disponibilité sous le contrôle de plusieurs personnes (détenteurs de données d'activation) afin de respecter les conditions initiales de contrôle de la clé privée. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles identiques à celles utilisées pour générer les bi-clés et stockées dans les locaux de l'OT.

Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'Infrastructure de Gestion de Clés (se reporter au § **Erreur ! Source du renvoi introuvable.**). Les sauvegardes de clés privées des cachets serveurs sont stockées sous forme de fichiers chiffrés qui permettent de garantir un même niveau de sécurité (multi-contrôle comme décrit au § **Erreur ! Source du renvoi introuvable.**) de même niveau de sécurité que celle utilisée pour la génération ou sous forme de fichier chiffré.

6.2.5 Archivage de la clé privée

Les clés privées ne sont pas archivées.

6.2.6 Transfert de la clé privée vers/depuis le module cryptographique

6.2.6.1 Bi-clés AC

Les clés d'ACs sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'AC sont chiffrées au moyen de l'algorithme de chiffrement. Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

Les ressources cryptographiques des ACs sont déployées en ligne uniquement afin de signer des certificats de porteurs et les CRLs après avoir authentifié la demande de signature.

Lorsque les clés privées d'AC sont déployées « en ligne », alors la ressource cryptographique dans laquelle ces clés sont présentes est obligatoirement matérielle. Cette ressource cryptographique peut être mutualisée entre plusieurs AC de même niveau de confiance et conforme à la présente PC.

6.2.6.2 Bi-clés Client

Sans objet.

6.2.6.3 Bi-clés Cachet serveur

Le CT est responsable de définir et de faire respecter les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité afin de ne pas porter atteinte à leur confidentialité.

Les clés sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées sont chiffrées au moyen de l'algorithme de chiffrement. Une clé privée chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

Les ressources cryptographiques sont déployées en ligne uniquement afin de signer et d'horodater des contrats ou des actes de gestion après avoir authentifié la demande de signature.

Lorsque les clés privées sont déployées « en ligne », alors la ressource cryptographique dans laquelle ces clés sont présentes est obligatoirement matérielle. Cette ressource cryptographique peut être mutualisée entre plusieurs cachets serveurs de même niveau de confiance et conforme à la présente PC.

6.2.7 Stockage de la clé privée dans un module cryptographique

6.2.7.1 Bi-clés AC

Les clés privées d'AC sont stockées dans des ressources cryptographiques matérielles et protégées avec le même niveau de sécurité que lors de leur génération (se reporter au § **Erreur ! Source du renvoi introuvable.**).

6.2.7.2 Bi-clés cachet serveur

Les clés privées des Porteurs sont stockées dans des ressources cryptographiques matérielles et protégées avec le même niveau de sécurité que lors de leur génération (se reporter au § **Erreur ! Source du renvoi introuvable.**).

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Bi-clés AC

Lorsqu'elle est activée dans une ressource cryptographique matérielle dite « hors ligne », la clé privée n'est activée que par les détenteurs de données d'activation.

Les clés privées d'AC ne peuvent être activées qu'avec des rôles de confiance (minimum 2).

Lorsqu'elle est activée dans une ressource cryptographique matérielle dite « en ligne », la clé privée de l'AC ne peut être activée que par les processus autorisés de génération de certificat Porteur et de LCR.

6.2.8.2 Bi-clés Client

Les bi-clés des Porteurs sont activées dans un HSM après authentification réussie du Porteur mise en œuvre suivant la cinématique d'activation choisie par l'AE et décrite dans la politique de signature.

6.2.8.3 Bi-clés Cachet serveur

Le CT est responsable de définir et de faire respecter les moyens et procédures permettant d'activer les clés en toute sécurité afin de ne pas porter atteinte à leur confidentialité et à la sécurité du service applicatif qui les utilise.

Les clés privées ne peuvent être activées des rôles de confiance de détenteur de données d'activation

Lorsqu'elle est activée dans une ressource cryptographique matérielle dite « en ligne », la clé privée du cachet serveur ne peut être activée que par les processus autorisés de génération de signature et de contremarque de temps.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Bi-clés AC

Les clés privées sont utilisées par le processus autorisé lorsqu'elles sont « en lignes ». Après la décision de fin d'utilisation d'une clé privée d'AC dans une ressource cryptographique matérielle « en lignes », les clés sont supprimées. Les sauvegardes sont aussi détruites.

Lorsqu'elles sont utilisées dans des ressources cryptographiques « hors ligne », les clés sont supprimées dans la ressource cryptographique et la ressource cryptographique matérielle est ensuite désactivée.

6.2.9.2 Bi-clés Client

Les clés privées peuvent être utilisées uniquement pour signer un contrat ou un acte de gestion. Elles sont détruites immédiatement après la fin du processus de signature

comme décrit dans la cinématique d'activation choisie par l'AE et décrite dans la politique de signature.

6.2.9.3 Bi-clés Cachet serveur

Le CT est responsable de définir et de faire respecter les moyens et procédures permettant de désactiver les clés en toute sécurité afin de ne pas porter atteinte à leur confidentialité et à la sécurité du service applicatif qui les utilise.

Les clés privées sont utilisées par le processus autorisé lorsqu'elles sont « en lignes ». Après la décision de fin d'utilisation d'une clé privée de cachet serveur dans une ressource cryptographique matérielle « en lignes », les clés sont supprimées. Les sauvegardes sont aussi détruites.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Bi-clés AC

Les clés privées d'AC sont détruites quand les certificats auxquels elles correspondent sont expirés ou révoqués ou quand elles ne sont plus utilisées dans la ressource cryptographique matérielle « hors ligne » (pour ce cas les sauvegardes ne sont pas détruites).

La destruction d'une clé privée comprend la destruction des copies de sauvegarde et l'effacement de cette clé dans la ressource cryptographique qui la contient de manière à ce qu'aucune information ne puisse être utilisée pour la recouvrer.

Une clé d'AC qui est dans une ressource cryptographique « hors ligne » ou « en ligne » est détruite en utilisant les fonctions de la ressource cryptographique prévue à cet effet. Les sauvegardes de la clé sont aussi détruites avec des logiciels prévus à cet effet pour réaliser des effacements sécurisés et les supports des sauvegardes, lorsqu'ils sont dédiés à une sauvegarde, sont aussi détruits. Ces opérations sont réalisées sous le contrôle de plusieurs rôles de confiance lors de cérémonies.

Les personnes ayant un rôle de confiance pour l'AC détruite sont libérées de leur rôle si l'AC n'est pas renouvelé et que leur rôle n'est pas utilisé par d'autres ressources cryptographiques. Les supports associés détenus par les détenteurs d'éléments d'initialisation et les détenteurs de données d'activation sont détruits ou effacés, si ils ne sont pas utilisés pour d'autres AC, de manière à ce qu'aucune information ne puisse être récupérée.

6.2.10.2 Bi-clés Client

Les clés privées sont détruites à la fin du processus de signature comme décrit dans la cinématique d'activation choisie par l'AE et décrite dans la politique de signature. L'AE utilise les fonctions du HSM afin de détruire en toute sécurité les clés des Porteurs sans laisser de trace qui permettrait de les reconstituer.

6.2.10.3 Bi-clés Cachet serveur

Le CT est responsable de définir et de faire respecter les moyens et procédures permettant de détruire les clés en toute sécurité afin de ne pas porter atteinte à leur confidentialité et à la sécurité du service applicatif qui les utilise.

Les clés privées sont détruites quand les certificats auxquels elles correspondent sont expirés ou révoqués.

La destruction d'une clé privée comprend la destruction des copies de sauvegarde et l'effacement de cette clé dans la ressource cryptographique qui la contient de manière à ce qu'aucune information ne puisse être utilisée pour la recouvrer.

Les sauvegardes de la clé sont aussi détruites avec des logiciels prévus à cet effet pour réaliser des effacements sécurisés et les supports des sauvegardes, lorsqu'ils sont dédiés à une sauvegarde, sont aussi détruits. Ces opérations sont réalisées sous le contrôle de plusieurs rôles de confiance.

Les personnes ayant un rôle de confiance pour le HSM utilisé par les cachets serveurs sont libérées de leur rôle si le HSM n'est pas réutilisé pour d'autres cachets serveurs et que leur rôle n'est pas utilisé par d'autres ressources cryptographiques au titre de cette PC. Les supports associés détenus par les détenteurs d'éléments d'initialisation et les détenteurs de données d'activation sont détruits ou effacés, s'ils ne sont pas utilisés pour d'autres besoins, de manière à ce qu'aucune information ne puisse être récupérée.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs d'authentification et de signature

Se reporter au § 6.2.1.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (se reporter au § 5.5.2 ci-dessus).

6.3.2 Durée de vie des bi-clés et des certificats

6.3.2.1 Bi-clé et certificat d'AC

La durée de vie des bi-clés et des certificats d'AC est limitée à la fin de vie de l'AC Opentrust qui a émis le certificat d'AC.

L'AC veillera à n'émettre des certificats que si leur date de fin de validité est antérieure à la date de fin de validité du certificat de l'AC.

6.3.2.2 Bi-clé et certificat cachet serveur

Les bi-clés et certificats cachet serveur couverts par la présente Politique de Certification ont une durée de vie de 3 ans maximum.

6.3.2.3 Bi-clé et certificat client

Les bi-clés et certificats Client couverts par la présente Politique de Certification ont une durée de vie de 10 minutes.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 AC

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (Se reporter au § 6.1.1.1). Les données d'activation sont générées automatiquement selon un schéma de type M of N. Dans tous les cas les données d'activation sont remises à leurs porteurs après génération pendant la cérémonie des clés. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.1.2 Client

Le type de données d'activation qu'utilise le client est décrit dans la politique de signature. Les données d'activation sont soit enregistrées par l'AE soit générées par l'AE et distribuées de manière sécurisée au Client de façon à avoir l'assurance que seul le Client pourra signer un contrat ou un acte de gestion à l'aide de la donnée d'activation. La politique de signature indique si une donnée d'activation est utilisée ou pas. Une donnée d'activation est obligatoire pour les Porteurs qui signent des contrats ou des actes de gestion à distance en passant par le Portail d' AE.

6.4.1.3 Cachet serveur

Le CT est responsable de définir et de faire respecter les moyens et procédures permettant de générer et d'utiliser les données d'activation utilisées pour les clés en toute sécurité afin de ne pas porter atteinte à leur confidentialité et à la sécurité du service applicatif qui les utilise.

Les données d'activation des clés privées sont générées suivant une procédure définie par le CT et approuvée par l'AP (se reporter au § 6.1.1.3). Les données d'activation sont générées de façon à mettre en œuvre un contrôle multiple qui requiert plusieurs personnes pour l'activation des clés privées cachets serveurs hébergées dans le HSM. Les détenteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.2 Protection des données d'activation

6.4.2.1 AC

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de données d'activation sont responsables de leur gestion et de leur protection. Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'une même AC à un même instant sauf si cela ne remet pas en cause la sécurité définie pour la protection des clés privées. Les données d'activation d'une AC sont continuellement tracées par l'AP.

6.4.2.2 Client

Le Client est responsable de la protection de sa donnée d'activation.

6.4.2.3 Cachet serveur

Le CT est responsable de définir et de faire respecter les moyens et procédures permettant de protéger les données d'activation utilisées pour les clés en toute sécurité

afin de ne pas porter atteinte à leur confidentialité et à la sécurité du service applicatif qui les utilise.

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de données d'activation sont responsables de leur gestion et de leur protection. Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'une même HSM à un même instant sauf si cela ne remet pas en cause la sécurité définie pour la protection des clés privées. Les données d'activation d'une AC sont continuellement tracées par l'AP.

6.4.3 Autres aspects liés aux données d'activation

6.4.3.1 AC

Les données d'activation ne sont en aucun cas transmissibles sauf dans le cadre de la transmission éventuelle du rôle de détenteur de données d'activation à une autre personne, échange effectué sous le contrôle de l'AP.

Une vigilance est apportée au respect de cette exigence en particulier dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance.

6.4.3.2 Client

En cas de compromission de sa donnée d'activation, le Client alerte l'AE.

6.4.3.3 Cachet serveur

Le CT est responsable de définir et de faire respecter les moyens et procédures permettant de générer et d'utiliser les données d'activation utilisées pour les clés en toute sécurité afin de ne pas porter atteinte à leur confidentialité et à la sécurité du service applicatif qui les utilise.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une Infrastructure de Gestion de Clés comprend les fonctions suivantes :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs).
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles).
- 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 et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels.
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès.

- Fonctions d'audits (non-répudiation et nature des actions effectuées).

Quand un composant d'Infrastructure de Gestion de Clés est hébergé sur une plateforme évaluée au regard d'exigences d'assurance de sécurité, il est utilisé dans sa version certifiée. Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié. Les composants d'Infrastructure de Gestion de Clés sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC.

6.5.2 Niveau de qualification des systèmes informatiques

Les composants d'Infrastructure de Gestion de Clés utilisés pour supporter les services d'AC et qui sont hébergés par l'OT ont été conçus en suivant les recommandations du document du PP CIMCPP (Certificate Issuing and Management Components Family of Protection Profiles Version 1.0) pour l'AC et l'AE.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées aux développements des systèmes

Le contrôle des développements des systèmes s'effectue comme suit :

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré.
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce.
- Tous les matériels et logiciels sont expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation.
- Les matériels et logiciels sont dédiés aux activités d'Infrastructure de Gestion de Clés. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'Infrastructure de Gestion de Clés.
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'Infrastructure de Gestion de Clés. Seules les applications nécessaires à l'exécution des activités Infrastructure de Gestion de Clés sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite.
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

6.6.2 Mesures liées à la gestion de la sécurité

La configuration du système d'Infrastructure de Gestion de Clés, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AP. Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'Infrastructure de Gestion de Clés. Une méthode de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'Infrastructure de Gestion de Clés. Lors de son premier chargement, on vérifie que le logiciel de l'Infrastructure de Gestion de Clés est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

En ce qui concerne les logiciels et matériels évalués, l'Infrastructure de Gestion de Clés poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

6.7 Mesures de sécurité réseau

L'AC est en ligne accessible par des postes informatiques sous contrôle et uniquement d'un réseau interne à l'OT. L'AC n'est pas hébergé sur le même réseau que l'AE et le SP. Le principe de défense en profondeur est appliqué.

Les composantes accessibles de l'Infrastructure de Gestion de Clés sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu.

Les autres composantes de l'Infrastructure de Gestion de Clés comme l'AE et le SP utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion provenant d'Internet.

Dans tous les cas, les mesures comprennent l'utilisation de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système Infrastructure de Gestion de Clés est hébergé refuse tout service, hormis ceux qui sont nécessaires au système Infrastructure de Gestion de Clés, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

Le réseau est protégé contre toute intrusion d'une personne ou d'un système non autorisée et assurer la confidentialité et l'intégrité des données qui y transitent.

L'interconnexion de l'Infrastructure de Gestion de Clés à des applications ou des utilisateurs ne remet pas en cause les règles de sécurité réseau prévues par l'AP.

6.8 Horodatage / Système de datation

L'AC utilise une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (NTP). Le temps fourni par ce serveur de temps est utilisé pour établir l'heure :

- Du début de validité d'un certificat du Porteur,
- De la révocation d'un certificat de Porteur,

- De l'affichage de mises à jour de LCR.

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profil de Certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2"). Les champs des certificats porteurs et AC sont définis par le RFC 5280.

7.1.1 Extensions de Certificats

7.1.1.1 Certificat AC

Les informations contenues dans le certificat d'AC sont données au § 11 ci-dessous.

7.1.1.1.1 Certificat Porteur

Les informations contenues dans le certificat Porteur sont données au § 11 ci-dessous.

7.1.2 Identifiant d'algorithmes

L'identifiant d'algorithme utilisé est Sha-2WithRSAEncryption: 1.2.840.113549.1.1.11.

7.1.3 Formes de noms

Les formes de noms respectent les exigences du § 3.1.1 pour l'identité des porteurs et de l'AC qui est portée dans les certificats émis par l'AC.

7.1.4 Identifiant d'objet (OID) de la Politique de Certification

Les certificats émis par l'AC contiennent l'OID de la PC qui est donné au § 1.2 ainsi qu'un autre OID (afin d'indiquer que l'AC est dans le programme Adobe CDS) comme indiqué par le § 11 ci-dessous.

Les certificats de l'AC contiennent l'OID « any policy » ainsi qu'un autre OID (afin d'indiquer que l'AC est dans le programme Adobe CDS) comme indiqué par le § 11 ci-dessous.

7.1.5 Extensions propres à l'usage de la Politique

Sans objet.

7.1.6 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies"

Pas d'exigence formulée.

7.2 Profil de LCR

7.2.1 LCR et champs d'extensions des LCR

Le paragraphe 11 ci-dessous donne les détail de la CRL.

7.3 Profil OCSP

Sans objet.

8 AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

8.1 Fréquence et / ou circonstances des audits

L'Infrastructure de Gestion de Clés fait l'objet d'audit périodique de conformité au moins une fois par an, pour permettre à l'AP d'autoriser l'Infrastructure de Gestion de Clés d'émettre ou non (selon le résultat des audits) des certificats porteurs au titre de la présente PC.

La reconnaissance du respect par l'AC des exigences de la présente PC est effectuée dans le cadre du schéma de certification des AC externes élaborés par OpenTrust (ce chapitre ne décrit pas la démarche d'audit conduit par OpenTrust car elle décrite dans la PC ACR d'OpenTrust). Cependant, l'AP conduit également des audits des composantes de l'Infrastructure de Gestion de Clés afin d'en déterminer leur conformité au regard de la présente PC.

A ce titre, des audits appelés « audit interne » quand ils sont réalisés par l'AP et « audit externe » quand ils sont réalisés par un auditeur externe sont réalisés de manière régulière. De même, les AE sont informées que dans le cadre du schéma d'audit utilisé pour auditer l'Infrastructure de Gestion de Clés dans son ensemble, l'auditeur OpenTrust se réserve le droit de réaliser des audits de l'AE. La réalisation de ces audits (dit audit externe) est conduite par l'AP quand elle le souhaite.

8.2 Identités / qualifications des évaluateurs

Les auditeurs démontrent leurs compétences dans le domaine des audits de conformité et doivent être familiers avec les exigences de la PC. L'AP apporte une attention particulière quant à l'audit de conformité, notamment vis-à-vis de ses exigences en matière d'audit. L'AP effectue elle-même le choix des auditeurs.

8.3 Relation entre évaluateurs et entités évaluées

Les auditeurs en charge de l'audit de conformité sont soit une entreprise privée indépendante du Groupe BPCE, soit une entité du Groupe BPCE suffisamment indépendante afin d'effectuer une évaluation juste et indépendante.

L'AP détermine si un auditeur remplit cette condition.

8.4 Sujets couverts par les évaluations

L'objectif de l'audit de conformité est de vérifier qu'une composante de l'Infrastructure de Gestion de Clés opère ses services en conformité avec la présente PC et sa DPC. Le sujet et le périmètre de l'évaluation seront préalablement définis dans un protocole d'audit validé par l'AP.

8.5 Actions prises suite aux conclusions des évaluations

À l'issue de ses vérifications, l'auditeur rend à l'AP, un avis parmi les suivants : « réussite », « échec », « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'auditeur émet

des recommandations à l'AP qui peuvent être :

  - la cessation (temporaire ou définitive) d'activité,
  - l'invalidation de tout ou partie des données déjà établies,
  - le choix de la mesure à appliquer est effectué par l'Autorité et respecte ses politiques de sécurité interne.

- En cas de résultat « à confirmer », l'AP remet à la composante un avis précisant sous quel délai les non-conformités sont levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.

- En cas de réussite, l'Autorité confirme à la composante contrôlée la conformité aux exigences de la Politique visée.

8.6 Communication des résultats

Un Rapport de Contrôle de Conformité, incluant le cas échéant la mention des mesures correctives déjà prises ou en cours par la composante, est remis à l'AP comme prévu au § 8.1 ci-dessus. Ce rapport cite les versions des PC et DPC utilisées pour cette évaluation.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Non applicable.

9.1.2 Tarifs pour accéder aux certificats

Non applicable.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Le service de publication de l'AC (qui contient la LCR pour le certificat de l'AC) est accessible gratuitement sur Internet (cf chapitre 2.2).

9.1.4 Tarifs pour d'autres services

Non applicable.

9.1.5 Politique de remboursement

Non applicable.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Le Groupe BPCE assume en fonds propres le règlement des litiges éventuels liés à la délivrance de certificats électroniques.

9.2.2 Autres ressources

L'AC dispose de ressources financières suffisantes à son bon fonctionnement et à l'accomplissement de sa mission.

9.2.3 Couverture et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité utilisatrice du fait d'un manquement par l'Infrastructure de Gestion de Clés à ses obligations, l'AC pourra être amenée à dédommager l'entité utilisatrice dans la limite de sa responsabilité définie dans les conditions générales d'utilisation.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- La DPC,

- Les clés privées de l'AC, des composantes et des porteurs (Client) de certificats,
- Les données d'activation associées aux clés privées d'AC et des porteurs (Client),
- Toutes les données d'activation (secrets) de l'Infrastructure de Gestion de Clés,
- Les journaux d'évènements des composantes de l'Infrastructure de Gestion de Clés,
- L'affectation des rôles de confiance
- Le dossier de demande de certificat pour les certificats cachet et horodatage,
- Les causes de révocations, sauf accord explicite du porteur,
- La PSSI du Groupe BPCE.

Par ailleurs, l'AP garantit que seuls ses personnels dans des rôles de confiance autorisés, les auditeurs, ou d'autres personnes ayant des besoins avérés et vérifiés par l'AP, ont accès et peuvent utiliser ces informations confidentielles.

9.3.2 Informations hors du périmètre des informations confidentielles

Les données figurant dans le certificat ne sont pas considérées comme confidentielles.

9.3.3 Responsabilité en termes de protection des informations confidentielles

L'AP a mis en place et respecte des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme confidentielles au sens du paragraphe 9.3.1 ci-dessus.

A cet égard, l'Infrastructure de Gestion de Clés respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, il est précisé qu'elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales.

L'AP permet également l'accès aux informations contenues dans les dossiers d'enregistrement au porteur.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

La collecte et l'usage de données personnelles par l'Infrastructure de Gestion de Clés dans le cadre du traitement des demandes de certificats sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi CNIL.

9.4.2 Informations à caractère personnel

L'AC considère que les informations suivantes sont des informations à caractère personnel :

- Données d'identification du porteur,
- Identité du porteur,
- Demande (renseignée) d'émission de certificat,
- Fichier de preuve de l'AE,
- Demande (renseignée) de révocation de certificat.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

L'AP a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles au sens de l'article 9.4.1 ci-dessus dans le cadre de la délivrance et la gestion d'un certificat de porteur.

A cet égard, l'Infrastructure de Gestion de Clés respecte la législation et la réglementation en vigueur sur le territoire français, en particulier, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés révisée 2006.

En application de l'article 34 de la loi Informatique et Libertés du 6 janvier 1978, les porteurs disposent d'un droit d'accès, de modification, de rectification et de suppression des données qui les concernent comme convenu et décrit dans la demande de certificat et les CGU associés. Pour l'exercer, les porteurs s'adressent à :

- Groupe BPCE
- Directeur de la Sécurité des Systèmes d'informations Groupe
- 50 Avenue Pierre Mendes France
- 75201 Paris Cedex 13
- rssi-pssi-icg@bpce.fr

Les infractions aux dispositions de la loi Informatique et Libertés du 6 janvier 1978 sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

Les données personnelles du Porteur sont recueillies aux seules fins de permettre :

- l'identification et l'authentification par l'AE,
- la réalisation des vérifications nécessaires à la délivrance d'un certificat et le cas échéant à sa révocation,
- la construction de l'identité personnelle du Porteur portée dans le certificat (Cf. § 3.1.1)
- l'apport des preuves nécessaires à la gestion du certificat du porteur.

9.4.5 Notification et consentement d'utilisation de données personnelles

Aucune des données à caractère personnel communiquées par un porteur ne peut être utilisée par l'Infrastructure de Gestion de Clés, pour une utilisation autre que celle définie

dans le cadre de la PC, sans consentement express et préalable de la part du porteur. Le consentement du porteur pour l'utilisation desdites données dans le cadre de la PC est considéré comme obtenu lors de la soumission de la demande de certificat et du fait de l'acceptation par le porteur du certificat émis par l'AC. Le consentement doit être express.

Le droit de rectification ne porte que sur ces informations portées dans les certificats générés par l'AC. Le Client est informé de son droit de faire rectifier les informations le concernant dans la seule période d'acceptation du certificat. La rectification consiste en ce cas à détecter une erreur dans le certificat ou dans le dossier d'enregistrement concernant les données personnelles et donc à demander un nouveau certificat. En ce cas, les anciens certificats sont révoqués et le dossier d'enregistrement est mis à jour.

Une fois que les CGU sont acceptées par le Porteur, il est considéré que le Porteur accepte dans son intégralité que ses données personnelles soient conservées par l'Infrastructure de Gestion de Clés. Le Client peut par contre demander à ce que ses données soient modifiées mais les anciennes données ne peuvent pas être supprimées car elles servent de preuve dans le processus de gestion des certificats.

9.4.6 Condition de divulgation d'informations personnelles aux autorités judiciaires ou administratives

L'Infrastructure de Gestion de Clés agit conformément aux réglementations européenne et française et dispose de procédures sécurisées pour permettre l'accès des autorités judiciaires sur décision judiciaire ou autre autorisation légale aux données à caractère personnel.

9.4.7 Autres circonstances de divulgation d'informations personnelles

L'AC obtient l'accord du porteur via les CGU, de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8 à condition que le transfert n'altère pas les droits juridiques et techniques du Porteur définis par la présente PC.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'AC sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, …) est sanctionnée par le Code de la propriété intellectuelle et le Code pénal.

L'AC détient tous les droits de propriété intellectuelle : elle est propriétaire de la PC de la DPC associée et des certificats émis par l'AC.

Le porteur détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les certificats porteurs émis par l'AC et dont il est propriétaire.

9.6 Interprétations contractuelles et garanties

Les composantes de l'Infrastructure de Gestion de Clés, les Clients et la communauté d'utilisateurs de certificats sont responsables pour tous dommages occasionnés en suite

d'un manquement de leurs obligations respectives telles que définies aux termes de la PC.

9.6.1 Obligations communes

Les différentes composantes de l'Infrastructure de Gestion de Clés:

- Assurent l'intégrité et la confidentialité des clés privées dont elles sont dépositaires, ainsi que des données d'activation desdites clés privées, le cas échéant,
- Utilisent les clés publiques et privées dont elles sont dépositaires qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés,
- Mettent en œuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent,
- Documentent leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de l'Infrastructure de Gestion de Clés,
- Respectent et appliquent les termes de la présente PC qu'elles reconnaissent,
- Acceptent le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées,
- Respectent les conventions qui les lient aux autres entités composantes de l'Infrastructure de Gestion de Clés.

9.6.2 Obligations et garanties de l'AP

L'AP :

- Elabore et valide la PC et la DPC associée,
- Maintien et fait évoluer la présente PC et la DPC associée,
- Assure le suivi et le contrôle de l'Infrastructure de Gestion de Clés par le biais d'audit,
- Autorise la génération et la révocation des certificats d'AC,
- Autorise les composantes de l'Infrastructure de Gestion de Clés pour la mise en œuvre des services de l'Infrastructure de Gestion de Clés.

9.6.3 Obligations et garanties de l'AC

L'AC :

- Protège les clés privées et leurs données d'activation en intégrité et confidentialité,
- N'utilise ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC,
- Respecte et applique les dispositions de la partie de la DPC qui les concerne (cette partie de la DPC est transmise à la composante concernée),
- Accepte que l'équipe de contrôle effectue les audits et lui communique toutes les informations utiles, conformément aux intentions de l'AP de contrôler et vérifier la conformité avec la PC,
- Documente ses procédures internes de fonctionnement afin de compléter la DPC générale,

- Met en œuvre les moyens techniques et emploie les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC,
- Assure la protection des données personnelles des Porteurs.

9.6.4 Obligation et garanties de l'OT

L'OT:

- Protège les clés privées et leurs données d'activation en intégrité et confidentialité,
- N'utilise ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles elles ont été générées et avec les moyens appropriés, comme spécifié dans la DPC,
- Respecte et applique les dispositions de la partie de la DPC qui les concerne (cette partie de la DPC est transmise à la composante concernée),
- Accepte que l'équipe de contrôle effectue les audits et lui communique toutes les informations utiles, conformément aux intentions de l'AG-Infrastructure de Gestion de Clés de contrôler et vérifier la conformité avec la PC,
- Documente ses procédures internes de fonctionnement afin de compléter la DPC générale,
- Met en œuvre les moyens techniques et emploie les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC.

9.6.5 Obligations et garanties de l'AE

L'AE:

- vérifie les données du Porteur et met à jour le dossier d'enregistrement du Porteur,
- Authentifie la demande de certificat,
- Authentifie la demande de révocation,
- Transmet la demande de certificat,
- Authentifie la demande de révocation,
- Accepte que l'équipe de contrôle effectue les audits et lui communique toutes les informations utiles, conformément aux intentions de l'AP de contrôler et vérifier la conformité avec la PC,
- Respecte la PC et la DPC,
- Assure la protection des données personnelles des Porteurs,
- Met en œuvre les moyens techniques et emploie les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC.

9.6.6 Obligations et garanties du client

Le client:

- Protège en confidentialité et intégrité les informations confidentielles qu'il détient (donnée d'activation),
- Se conforme à toutes les exigences de la PC et de la DPC associée,
- Garantit que les informations qu'il fournit à l'AE sont complètes et correctes,

- Prend toutes les mesures raisonnables pour éviter l'utilisation non autorisée de sa donnée d'activation et du moyen de réception et/ou d'élaboration de la donnée d'activation et en protéger la confidentialité et l'usage,
- Avise immédiatement l'AE en cas de besoin de révocation de son certificat.

9.6.7 Obligations et garanties du SP

Le SP:

- Publie les LCR,
- Publie les certificats d'AC,
- Publie la PC,
- Garantit les taux de disponibilités des informations publiées,
- Protège les accès au SP.

9.6.8 Obligations et garanties des autres participants

9.6.8.1 Obligations et garanties de l'UC

L'UC :

- Contrôle l'état de validité des certificats Porteurs à l'aide des CRLs publiées,
- Vérifie que les certificats Porteurs sont signés par une AC,
- Si un certificat est révoqué, alors vérifie la validité du certificat pour un document signé en fonction de la date contenue dans la CRL (par exemple une signature peut être produite avec un certificat valide alors que le certificat sera ensuite révoqué lors d'un renouvellement),
- Contrôle l'état de validité des certificats d'AC à l'aide des CRLs publiée par l'AC d'OpenTrust,
- Vérifie que les certificats d'AC sont signés par une AC valide.

9.6.8.2 Obligations et garanties du CT

Le CT :

- Met en œuvre les procédures afin de protéger en confidentialité et intégrité les informations confidentielles qu'il détient (clé privée et donnée d'activation),
- Se conforme à toutes les exigences de la PC et de la DPC associée,
- Garantit que les informations qu'il fournit à l'AE sont complètes et correctes.
- Transmet la clé publique à l'AE,
- Prend toutes les mesures et procédures raisonnables pour éviter l'utilisation non autorisée de sa clé privée et en protéger la confidentialité,
- Avise immédiatement l'AE en cas de besoin de révocation de son certificat.
-

9.7 Champ de garantie

L'AC garantit au travers de ses services d'Infrastructure de Gestion de Clés :

- L'identification et l'authentification des porteurs avec les certificats générés par l'AC.
- La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Ces garanties sont exclusives de toute autre garantie de l'AC.

L'émission de Certificats, conformément à la PC, ne fait pas de l'une des composantes de l'Infrastructure de Gestion de Clés, un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du porteur ou de toutes autres parties concernées.

En conséquence de quoi, les porteurs et les utilisateurs de Certificat sont des personnes juridiquement et financièrement indépendantes de l'AC et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'AC ou l'une des composantes de l'Infrastructure de Gestion de Clés, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'AC ou de l'une des composantes de l'Infrastructure de Gestion de Clés. Les services de certification ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association qui imposerait une responsabilité basée sur les actions ou les carences de l'autre.

Le fait que le nom d'une organisation soit dans un certificat et utilisé à des fins de signature électronique ne constitue pas en soi un mandat spécial ou général de cette organisation en faveur du porteur.

9.8 Limite de responsabilité

L'AC est responsable des exigences et des principes édictés dans la présente PC, ainsi que de tout dommage causé à un porteur ou une application / utilisateur de certificat en suite d'un manquement aux procédures définies dans la PC et la DPC associée.

L'AC décline toute responsabilité à l'égard de l'usage des certificats émis par elle ou des bi-clés publiques/privées associées dans des conditions et à des fins autres que celles prévues dans la PC ainsi que dans tout autre document contractuel applicable associé.

L'AC décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

L'AC ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, les conflits sociaux, la défaillance des installations ou des réseaux de télécommunications externes.

L'AC n'est en aucun cas responsable des préjudices indirects subis par les entités utilisatrices, celles-ci n'étant pas pré-qualifiées par les présentes.

En cas de prononcé d'une quelconque responsabilité de l'AC, les dommages, intérêts et indemnités à sa charge toutes causes confondues, et quel que soit le fondement de sa responsabilité, sont limités par certificat à la somme prévue au titre de limite de responsabilité dans les conditions générales d'utilisation applicables audit certificat.

9.9 Indemnités

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'AC vis-à-vis d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge seront déterminés conformément aux process en vigueur dans les établissements.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La PC devient effective une fois approuvée par l'AP. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

Selon l'importance des modifications apportées à la PC, l'AP décidera soit de faire procéder à un audit de la PC/DPC des AC concernées, soit de donner instruction à l'AC de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé.

9.10.3 Effets de la fin de validité et clauses restant applicables

La fin de validité de la PC entraîne la cessation de toutes les obligations et responsabilités de l'AC pour les certificats émis conformément à la PC.

9.11 Amendements à la PC

9.11.1 Procédures d'amendements

L'AP révise sa PC et sa DPC au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion de l'AP. Les corrections de fautes d'orthographe ou de frappe qui ne modifient pas le sens de la PC sont autorisées sans avoir à être notifiées.

9.11.2 Mécanisme et période d'information sur les amendements

L'AP donne un préavis d'1 mois au moins aux composantes de l'Infrastructure de Gestion de Clés de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification. Ce délai ne vaut que pour des modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de profil de certificat, …) et non sur la forme de la PC et de la DPC.

9.11.3 Circonstances selon lesquelles l'OID est changé

Si l'AP estime qu'une modification de la PC modifie le niveau de confiance assuré par les exigences de la PC ou par le contenu de la DPC, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (OID).

9.12 Dispositions concernant la résolution de conflits

En cas de contestation ou de litige, les parties décident de soumettre cette difficulté à une procédure amiable, préalablement à toute procédure devant un tribunal conformément aux CGU et accord passé avec le Porteur.

L'AP s'assure que tous les accords qu'elle conclut prévoient des procédures adéquates pour le règlement des différends.

Lorsque le différend porte sur une identité de porteur, il est du ressort de l'AE de gérer et de résoudre le litige. L'AP s'assure que l'AE l'a décrit et prévu dans ses procédures de gestion bancaire.

9.13 Juridictions compétentes

Les dispositions de la politique de certification sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive aux tribunaux compétents de Paris, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire.

9.14 Conformité aux législations et réglementations

La PC est sujette aux lois, règles, règlements, ordonnances, décrets et ordres nationaux, d'état, locaux et étrangers concernant les, mais non limités aux, restrictions à l'importation et à l'exportation de logiciels ou de matériels cryptographiques ou encore d'informations techniques.

Les textes législatifs et réglementaires applicables à la PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.15 Disposition diverses

9.15.1 Accord global

Le cas échéant, la DPC précisera les exigences spécifiques.

9.15.2 Transfert d'activités

Seule l'AP a le droit d'affecter et de déléguer la PC à une partie de son choix.

9.15.3 Conséquence d'une clause non valide

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La Politique de Certification continue à s'appliquer en l'absence de la disposition inapplicable et ce tout en respectant l'intention de ladite Politique de Certification.

Les intitulés portés en tête de chaque Article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

9.15.4 Application et renonciation

Les exigences définies dans la PC/DPC sont appliquées selon les dispositions de la PC et de la DPC associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

9.15.5 Force majeure

L'AC ne saurait être tenue pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs aux porteurs.

9.16 Autres dispositions

Sans objet.

10 RÉFÉRENCES

Les documents référencés sont les suivants :

- [CNIL] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
- [DIRSIG] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
- [SIGN] : Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

11 PROFIL DE CERTIFICAT ET CRL

11.1 Certificat CA

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	CN = KEYNECTIS CDS CA OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR		
NotBefore	YYYY/MM/DD 00:00 Z (Key Ceremony Date)		
NotAfter	2018/10/11 07:00 Z (Date of end of life of Issuer CA)		
Subject	**Att.**	**Attribute value**	**Directory String1**
	C	FR	PrintableString
	O	BPCE	UTF8String
	OU	0002 493455042	UTF8String
	CN	Se reporter au paragraphe 3.1.1 ci-dessus.	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		9f 22 78 d7 71 1b de 33 b0 7f c9 20 7a a9 a8 e0 4e 62 e3 fb Defined by Software (SHA1 160bits of the subject public key)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Extended Key Usage	**FALSE**	
Documents Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSE**	
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		
policyIdentifier		2.5.29.32.0
policyQualifier-cps		Se reporter au paragraphe 2.2 ci-dessus pour mettre l'URL de publication de la PC en fonction de l'AC.

[1] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality	Value
policyQualifier-unotice		
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
CRL Distribution Points	**FALSE**	
distributionPoint		http://trustcenter-crl.certificat2.com/Internal/KEYNECTIS_CDS_CA.crl

11.2Certificat « Client »

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	Se reporter au paragraphe 3.1.1 ci-dessus en fonction de l'AC qui émet le certificat d'AC.		
NotBefore	YYYY/MM/DD 00:00 Z (date de génération du certificat)		
NotAfter	YYYY/MM/DD 00:00 Z (date de génération du certificat plus 10 minutes)		
Subject	**Att.**	**Attribute value**	**Directory String2**
	C	Se reporter au paragraphe 3.1.1	PrintableString
	O	Se reporter au paragraphe 3.1.1	UTF8String
	OU	Se reporter au paragraphe 3.1.1	UTF8String
	CN	Se reporter au paragraphe 3.1.1	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
DigitalSignature		Set
NonRepudiation		Set
Extended Key Usage	**FALSE**	
Documents Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSE**	
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/

[2] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality	Value
policyQualifier-unotice		OID pour un certificat émis par une AC signature CE : 1.3.6.1.4.1.40559.1.0.1.21.101.1.1 OID pour un certificat émis par une AC signature BP : 1.3.6.1.4.1.40559.1.0.1.21.111.1.1
policyIdentifier		
policyQualifier-cps		Se reporter au paragraphe 2.2 ci-dessus pour mettre l'URL de publication de la PC en fonction de l'AC.
policyQualifier-unotice		
CRL Distribution Points	**FALSE**	
distributionPoint		Se reporter au paragraphe 2.2 ci-dessus.

11.3Certificat « Cachet serveur » : signature personne morale

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	Se reporter au paragraphe 3.1.1 ci-dessus en fonction de l'AC qui émet le certificat d'AC.		
NotBefore	YYYY/MM/DD 00:00 Z (date de génération du certificat)		
NotAfter	YYYY/MM/DD 00:00 Z (date de génération du certificat plus 3 années maximum)		
Subject	**Att.**	**Attribute value**	**Directory String3**
	C	Se reporter au paragraphe 3.1.1	PrintableString
	O	Se reporter au paragraphe 3.1.1	UTF8String
	OU	Se reporter au paragraphe 3.1.1	UTF8String
	CN	Se reporter au paragraphe 3.1.1	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
digitalSignature		Set
NonRepudiation		Set
Extended Key Usage	**FALSE**	

[3] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality	Value
Documents Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSE**	
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		
policyIdentifier		1.3.6.1.4.1.40559.1.0.1.21.121.1.1
policyQualifier-cps		Se reporter au paragraphe 2.2 ci-dessus pour mettre l'URL de publication de la PC en fonction de l'AC.
policyQualifier-unotice		
CRL Distribution Points	**FALSE**	
distributionPoint		Se reporter au paragraphe 2.2 ci-dessus pour mettre l'URL de publication de la LCR en fonction de l'AC.

11.4Certificat « authentification serveur » : signature application

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	Se reporter au paragraphe 3.1.1 ci-dessus en fonction de l'AC qui émet le certificat d'AC.		
NotBefore	YYYY/MM/DD 00:00 Z (date de génération du certificat)		
NotAfter	YYYY/MM/DD 00:00 Z (date de génération du certificat plus 3 années maximum)		
Subject	**Att.**	**Attribute value**	**Directory String4**
	C	Se reporter au paragraphe 3.1.1	PrintableString
	O	Se reporter au paragraphe 3.1.1	UTF8String
	OU	Se reporter au paragraphe 3.1.1	UTF8String
	CN	Se reporter au paragraphe 3.1.1	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
digitalSignature		Set

[4] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality	Value
Certificate Policies	**FALSE**	
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		
policyIdentifier		1.3.6.1.4.1.40559.1.0.1.21.141.1.1
policyQualifier-cps		Se reporter au paragraphe 2.2 ci-dessus pour mettre l'URL de publication de la PC en fonction de l'AC.
policyQualifier-unotice		
CRL Distribution Points	**FALSE**	
distributionPoint		Se reporter au paragraphe 2.2 ci-dessus pour mettre l'URL de publication de la LCR en fonction de l'AC.

11.5Certificat Horodatage

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	Se reporter au paragraphe 3.1.1 ci-dessus en fonction de l'AC qui émet le certificat d'AC.		
NotBefore	YYYY/MM/DD 00:00 Z (date de génération du certificat)		
NotAfter	YYYY/MM/DD 00:00 Z (date de génération du certificat plus 3 années maximum)		
Subject	**Att.**	**Attribute value**	**Directory String5**
	C	Se reporter au paragraphe 3.1.1	PrintableString
	O	Se reporter au paragraphe 3.1.1	UTF8String
	OU	Se reporter au paragraphe 3.1.1	UTF8String
	CN	Se reporter au paragraphe 3.1.1	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
digitalSignatue		Set
Extended Key Usage	**FALSE**	

[5] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality	Value
timeStamping		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		
policyIdentifier		1.3.6.1.4.1.40559.1.0.1.21.131.1.1
policyQualifier-cps		Se reporter au paragraphe 2.2 ci-dessus pour mettre l'URL de publication de la PC en fonction de l'AC.
policyQualifier-unotice		
CRL Distribution Points	**FALSE**	
distributionPoint		Se reporter au paragraphe 2.2 ci-dessus pour mettre l'URL de publication de la LCR en fonction de l'AC.

11.6CRL

Fields	Value
Version	V2
Issuer DN	Se reporter au paragraphe 3.1.1 ci-dessus en fonction de l'AC qui émet le certificat d'AC.
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (date d'émission de la CRL)
NextUpdate	YYYY/MM/DD HH:MM:SS Z (1 semaine de plus que la date d'émission de la CRL)
Signature (algorithm & OID)	SHA256WithRSAEncryption (1.2.840.113549.1.1.11)

CRL Extension	Include	Critical (True/False)	Value
CRLNumber	Yes	False	Entier croissant monotone et jamais répété.
AKI	Yes	False	Identique à l'AKI de l'AC émettrice.

CRL Entry Extension	Include	Critical (True/False)	Value
Revocation Reason	Optional	False	Reason code according to the RFC5280 Limited to: unspecified (0)