Politique et pratiques de certification

Cachet Serveur & Horodatage

V. 1.3

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 180 478 270€.

Siège social : 50 avenue Pierre Mendes France

75201 Paris Cedex 13.

RCS n° 493 455 042.

Version du document	1.3	Nombre de pages	46
Statut du document	☐ Projet	☒ Version finale	

Historique du document		
Date	Version	Commentaire
10/01/2021	1.0	Version Initiale
06/02/2021	1.1	Ajout précisions sur OCSP
20/05/2021	1.2	Ajout dispositions liées à la fin de vie de l'AC
15/06/2022	1.3	Ajout de précisions sur modes de révocation

SOMMAIRE

1 INTRODUCTION 4
1.1 PRESENTATION GENERALE 4
1.2 IDENTIFICATION DU DOCUMENT 4
1.3 ENTITES INTERVENANT DANS L'INFRASTRUCTURE DE GESTION DES CLES 5
1.4 USAGE DES CERTIFICATS 8
1.5 GESTION DE LA PC/DPC 8
1.6 DEFINITIONS ET ACRONYMES 9

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES 10

3 IDENTIFICATION ET AUTHENTIFICATION 11
3.1 NOMMAGE 11
3.2 VALIDATION INITIALE DE L'IDENTITE 13
3.3 IDENTIFICATION ET VALIDATION D'UNE NOUVELLE DEMANDE DE BI-CLE 14
3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION 14

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 15
4.1 DEMANDE DE CERTIFICAT 15
4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT 15
4.3 DELIVRANCE DU CERTIFICAT 16
4.4 ACCEPTATION DU CERTIFICAT 17
4.5 USAGE DE LA BI-CLE ET DU CERTIFICAT 17
4.6 RENOUVELLEMENT D'UN CERTIFICAT 18
4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE 18
4.8 MODIFICATION DU CERTIFICAT 18
4.9 REVOCATION ET SUSPENSION DES CERTIFICATS 18
4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS 22
4.11 FIN DE LA RELATION ENTRE LE PORTEUR DE CERTIFICAT ET L'AC 22
4.12 SEQUESTRE DE CLE ET RECOUVREMENT 23

5 MESURES DE SECURITE NON TECHNIQUES 24

6 MESURES DE SECURITE TECHNIQUES 25
6.1 GENERATION ET INSTALLATION DE BI-CLES 25
6.2 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES 26
6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES 29
6.4 DONNEES D'ACTIVATION 30
6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES 30
6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE 31
6.7 MESURES DE SECURITE RESEAU 31
6.8 HORODATAGE / SYSTEME DE DATATION 31

7 PROFIL DE CERTIFICATS 32

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 33

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES 34
9.1 TARIFS 34
9.2 RESPONSABILITE FINANCIERE 34
9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES 35
9.4 PROTECTION DES DONNEES PERSONNELLES 36
9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE 37
9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES 38
9.7 CHAMP DE GARANTIE 40

9.8 LIMITE DE RESPONSABILITE 41
9.9 INDEMNITES 42
9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC/DPC 42
9.11 AMENDEMENTS A LA PC/DPC 42
9.12 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS 43
9.13 JURIDICTIONS COMPETENTES 43
9.14 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS 43
9.15 DISPOSITION DIVERSES 43
9.16 AUTRES DISPOSITIONS 44
10 REFERENCES 45
10.1 DOCUMENTS NORMATIFS 45
10.2 POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION 46
10.3 MESURES COMMUNES 46
10.4 PROFILS DE CERTIFICATS ET CRL 46

1 INTRODUCTION

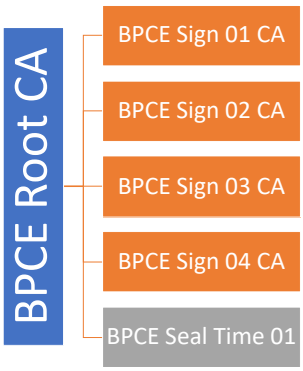
1.1 Présentation générale

Le Groupe BPCE, pour ses réseaux Caisse d'Épargne, Banque Populaire et Filiales, met en œuvre pour ses clients un service de signature électronique de documents et met en œuvre les règles applicables à l'établissement et à la conservation des dossiers de preuve. Le service de signature peut, quant à lui, avoir lieu à distance ou en face à face dans une agence du réseau.

Ce service de Signature Électronique utilise des certificats gérés par l'Infrastructure de Gestion de Clés (IGC) du Groupe BPCE. Il s'agit de l'AC *BPCE AC Cachets*. Cette AC est opérée par le Groupe BPCE et s'appuie sur la norme *ETSI EN 319-411-1*, au niveau *Normalized certificate Policy* (NCP+).

Les certificats délivrés par les AC permettent de signer des documents au format PDF. À 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. Ces AC font partie du programme AATL *(Adobe Approved Trust List)*.

La hiérarchie d'AC est la suivante :



Le présent document constitue la politique et les pratiques de certification (PC/DPC). Il a pour objet de décrire la gestion des certificats et leurs cycles de vie.

La présente PC/DPC est élaborée en conformité avec les documents suivants :

- RFC 3647, *X.509 Public Key Infrastructure certificate Policy certification Practise Statement Framework* de l'*Internet Engineering Task Force* (IETF) ;
- *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service providers issuing certificates ; Part 1: General requirements* (ETSI EN 319411-1, V1.2.2).
- *Certificate profile for certificates issued to legal persons* (ETSI EN 319412-3)

1.2 Identification du document

La présente PC/DPC est la propriété du Groupe BPCE. La PC/DPC contient plusieurs *Object Identifier* (OID).

Le numéro d'OID de la présente P.C. est : 1.3.6.1.4.1.40559.1.0.1.31.201.1.1

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 BPCE eIDAS (31)
- Horodatage (211), Cachet serveur(210)
- Environnement :
  - Production (1)
  - Qualification développement (2)
- Version (1)

Politique de certification	OID
Cachet Serveur	*1.3.6.1.4.1.40559.1.0.1.31.210.1.1*
Horodatage	*1.3.6.1.4.1.40559.1.0.1.31.211.1.1*

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

1.3 Entrée en vigueur

Le présent document est publié au plus tard le 22/11/2022.

Le présent document entre en vigueur le 23/11/2022.

1.4 Entités intervenant dans l'Infrastructure de Gestion des Clés

Pour délivrer les certificats, l'AC s'appuie sur les fonctionnalités suivantes :

- Génération de bi-clé d'AC : génère les bi-clés et les demandes de signature de certificats (CSR) associées durant une cérémonie des clés ;
- Enregistrement : collecte et vérifie les informations et identifie le Client puis transmet la demande de certificats à l'AC ;
- Gestion des bi-clés : génère les bi-clés des Clients dans des ressources cryptographiques (matériel certifié) ;
- Gestion des données d'activation : génère et utilise les données d'activation associées aux bi-clés ;

- Génération de certificat : génère les certificats électroniques à partir des informations transmises par l'Autorité d'Enregistrement (AE) ;
- Révocation de certificats : traite les demandes de révocation des certificats des Clients et détermine les actions à mener, dont la génération des Liste de certificats Révoqués (LCR) ;
- Publication : 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, …) ;
- Journalisation et audit : collecte l'ensemble des données utilisées et 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.

La présente PC/DPC définit les exigences de sécurité et les pratiques des services décrits ci-dessus dans la délivrance des certificats par l'AC.

1.4.1 Autorité de Gestion des Politiques (AP)

L'AP agit conformément à la présente PC/DPC.

Le [CESSIG] est l'Autorité de Gestion des Politiques (AP).

1.4.2 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 les capacités de l'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/DPC. Dans la présente PC/DPC, 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.

1.4.3 Autorité d'Enregistrement (AE)

L'AE agit conformément à la présente PC/DPC ; elle est chargée d'authentifier et d'identifier les contacts techniques (1.4.7.2) et les porteurs de certificats (1.4.6).

L'AE technique est mise en œuvre par l'OT (1.4.5).

L'AE est : DIS-IAM-PKI.

1.4.4 Service de Publication (SP)

Le SP est en charge de la publication des informations.

Le SP agit conformément à la présente PC/DPC.

1.4.5 Opérateur Technique (OT)

L'OT assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification, conformément à la présente PC/DPC. L'OT est techniquement dépositaire des clés privées et des moyens informatiques de l'AC, de l'AE et du SP.

L'OT agit conformément à la présente PC/DPC.

L'OT est : DIS-IAM-PKI.

1.4.6 Porteurs de certificats

1.3.6.1.4.1.40559.1.0.1.31.210.1.1	Dans le cas du certificat « Cachet Serveur », le porteur est établissement du groupe BPCE, et un Contact Technique (1.4.7.2) en a la charge.
1.3.6.1.4.1.40559.1.0.1.31.211.1.1	Dans le cas du certificat « Horodatage », le client est une unité d'horodatage de l'AH du groupe BPCE et un Contact Technique (1.4.7.2) en a la charge.

1.4.7 Autres participants

1.4.7.1 Utilisateurs de certificats (UC)

L'utilisateur de certificat est une personne ou un système informatique qui valide la signature électronique d'un document scellé (par l'Établissement) ou horodaté (par le Groupe BPCE).

1.4.7.2 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 ;
- Remplir les formulaires de demande de certificat ;
- Retirer les certificats ;
- Procéder, le cas échéant, aux demandes de révocation des certificats.

1.4.7.3 Autorité d'Horodatage (AH)

L'Autorité d'Horodatage (AH) est l'AH de BPCE, dont la Politique d'horodatage a pour OID : 1.3.6.1.4.1.40559.1.0.4.4.0.1.2.

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

1.5.1.1 Certificat de l'AC

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

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

- Certificats ;
- LCR ;
- CSR (format PKCS#10).

1.5.1.2 Certificat cachet serveur : Cachet Serveur

La clé privée associé au certificat sert pour la signature de :

- Documents au nom de l'Établissement ;
- CSR (format PKCS#10).

1.5.1.3 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).

1.5.2 Domaines d'utilisation interdits

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues au § 1.4 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/DPC.

1.6 Gestion de la PC/DPC

1.6.1 Entité gérant la PC/DPC

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

1.6.2 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.

1.6.3 Entité déterminant la conformité d'une DPC avec cette PC/DPC

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

1.6.4 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.

1.7 Définitions et Acronymes

Cf. [MCOM].

2 RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES

Cf. [MCOM].

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 Client (*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 d'AC

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

Champ de base	Valeur
Issuer	CN=`BPCE Root CA` OU=`0002 493455042` OI=`NTRFR-493455042` O=`BPCE` C=`FR`
Subject	

3.1.1.2 Certificat Cachet Serveur

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

Champ de base	Valeur
Issuer	Identité de l'AC du réseau (*cf.* § 3.1.1.1) pour lequel le cachet serveur est émis
Subject	C = `FR` O = `BPCE` OU = `0002` ⟨Numéro de SIREN de l'établissement⟩ OI = `NTRFR-`⟨Numéro de SIREN de l'établissement⟩ SerialNumber = ⟨Numéro de série aléatoire⟩ CN = ⟨Nom commercial de l'établissement⟩

3.1.1.3 Certificat Horodatage

L'identité de l'unité d'horodatage dans le certificat est la suivante :

Champ de base	Valeur
Issuer	Identité de l'AC du réseau (*cf.* § 3.1.1.1)
Subject	C = `FR` O = `BPCE` OU = `0002 493455042` OI = `NTRFR-493455042` SerialNumber = ⟨Numéro de série aléatoire⟩ CN = identifiant de l'UH⟩

3.1.2 Nécessité d'utilisation de noms explicites

Les noms utilisés dans les certificats sont explicites.

3.1.2.1 Certificat de test

Les certificats de test sont identifiables par la présence du mot « TEST » dans le DN.

3.1.3 Pseudonymisation

Sans objet.

3.1.4 Règles d'interprétation des différentes formes de noms

L'identité incluse dans les certificats permet d'identifier le Groupe BPCE, les établissements et les unités d'horodatage.

3.1.5 Unicité des noms

3.1.5.1 Certificat AC

L'AP assure l'unicité des noms d'AC au sein de son domaine de certification via son processus d'enregistrement.

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

3.1.5.2 Certificat Cachet Serveur

Les identités portées par l'AC dans les certificats 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 client ne peut être attribué à un autre client.

L'AE assure cette unicité au moyen de son processus d'enregistrement et de la valeur unique du DN attribué à un client, qui contient le numéro SIREN/SIRET du client.

3.1.5.3 Certificat Horodatage

Le champ *CN* du *DN* contient la valeur ⟨id⟩, qui est utilisée par l'AC pour assurer l'unicité du certificat.

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.

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 (IGC) et par l'AC est réalisée par les procédures de génération de la bi-clé privée correspondant à la clé publique à certifier et l'audit réalisé par l'AP sur l'AC à certifier.

3.2.1.2 Certificat Cachet Serveur et Horodatage

La preuve de la possession de la clé privée par le client est réalisée par les procédures de génération de la clé privée correspondant à la clé publique à certifier et par le mode de transmission de la clé publique (signature de CSR, format PKCS#10).

3.2.2 Validation de l'identité d'une personne morale

3.2.2.1 Certificat AC

L'authentification est réalisée sous la responsabilité de l'AP qui communique les données d'identification de l'établissement ou filiale à inclure dans l'identité des AC à l'OT, préalablement à la cérémonie des clés.

3.2.2.2 Certificat Cachet Serveur et Horodatage

Les cachets serveurs sont émis au nom des établissements du Groupe BPCE.

L'AE transmet au RSSI Groupe les demandes pour validation. Celui-ci vérifie le nom de l'établissement ou filiale, ainsi que son numéro SIREN ou des informations issues d'instances étatiques qui enregistrent les sociétés pour les établissements ou filiales étrangers.

Pour les certificats d'horodatage, l'AC vérifie auprès de l'Autorité d'Horodatage le nom devant apparaître dans le certificat.

3.2.3 Validation de l'identité d'une personne physique

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 Cachet Serveur et Horodatage

L'identification et l'authentification du contact technique (CT) est effectuée par l'AE en face à face.

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 CT correspond à la validation de l'appartenance à une organisation : Le CT appartient forcément à l'ICG (DPM-PCL-STR-ICG).

3.2.6 Certification croisée d'AC

Sans objet.

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

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

3.4 Identification et validation d'une demande de révocation

3.4.1 Certificat AC

Les demandes de révocation sont authentifiées par l'AP.

3.4.2 Certificat Cachet Serveur

Les demandes de révocation sont authentifiées par l'AE grâce au code de révocation généré aléatoirement par l'AC et transmis lors de la création du certificat.

Les demandes sont traitées soit en face-à-face avec le CT, soit via un e-mail provenant de l'adresse de messagerie interne utilisée pour déposer la demande initiale de certificat.

3.4.3 Certificat Horodatage

Les demandes de révocation sont authentifiées par l'AE, soit en face-à-face avec le CT, soit sur la base de l'adresse de messagerie interne utilisée pour déposer la demande initiale de certificat.

4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

Les sections 4.1, 4.2, 4.3 décrivent le processus de demande d'un premier certificat. La gestion des certificats suivants est décrite dans les sections 4.7 et 4.8.

4.1.1 Origine d'une demande de certificat

4.1.1.1 Certificat d'AC

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

4.1.1.2 Certificat Cachet Serveur et Horodatage

Un certificat peut être demandé par un CT. Le CT appartient à l'ICG : DPM-PCL-STR-ICG.

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

4.1.2.1 Certificat AC

Les AC sont enregistrées auprès de l'AP.

4.1.2.2 Certificat Cachet Serveur et Horodatage

Les informations suivantes figurent dans la demande de certificat Cachet Serveur :

- Le nom et prénom du CT ;
- Une pièce d'identité en cours de validité ;
- Les informations permettant à l'AE de contacter le CT et d'authentifier le CT (numéro de téléphone, courriel…) ;
- Pour les certificats d'Horodatage : Une copie du P.-V. de la cérémonie des clés ;
- 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 Cachet Serveur et Horodatage

La demande est authentifiée et validée par l'AE.

1. L'AE identifie et authentifie le CT en face-à-face.
2. L'AE s'assure que le CT a pris connaissance des conditions générales d'utilisation.

3. L'AE conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement.
4. L'AE transmet au RSSI Groupe les demandes pour validation (cf. 3.2.2.2).

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 afin de procéder à la cérémonie des clés et à la création du certificat d'AC.

4.2.2.2 Certificat Cachet Serveur et Horodatage

En cas d'approbation de la demande, l'AE 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 de trois mois calendaires.

4.2.3.2 Certificat Cachet Serveur et Horodatage

La demande de certificat est traitée par l'AE dans un délai de deux semaines calendaires.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

4.3.1.1 Certificat AC

Les AC sont générées pendant une cérémonie des clés dans les locaux de l'OT.

4.3.1.2 Certificat Cachet Serveur et Horodatage

1. L'AC (service de génération de certificat) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.
2. L'AC génère le certificat.
3. Le CT notifié par courriel de la mise à disposition du certificat sur l'outil Venafi.

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 client

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 : « cachet serveur »

Le CT est notifié par courrier électronique.

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 prévues. L'AP accepte le certificat émis et le témoin de l'AP signe une acceptation officielle du certificat émis.

4.4.1.2 Certificat Cachet Serveur et Horodatage

À réception, le CT vérifie les informations du certificat et l'accepte ou le refuse par retour de courriel. Si le CT n'informe pas l'AED d'une anomalie dans le certificat dans les 24 heures, alors 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'AC et des ARL. L'AP est responsable de la diffusion des certificats et des ARL en plus des moyens fournis par le SP.

4.4.2.2 Certificat Cachet Serveur et Horodatage

Les certificats ne sont pas publiés par l'AC après leur délivrance. Le CT, ou le service dont il dépend, peut publier le certificat remis s'il le souhaite (ex. : certificat d'unité d'horodatage publié sur le site du service d'horodatage).

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

Pas d'exigence.

4.5 Usage de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat

L'usage d'une bi-clé et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés. Voir aussi 1.5.

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

L'utilisateur du certificat est libre d'utiliser la clé publique et le certificat comme bon lui semble.

4.6 Renouvellement d'un certificat

Le renouvellement des certificats Cachet Serveur et Horodatage n'est pas autorisé au titre de la présente PC/DPC.

Le renouvellement des clés d'AC 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.

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

La procédure est identique à celle décrite pour la délivrance initiale.

4.8 Modification du certificat

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

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 :

- 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 ;
- Changement d'informations dans le certificat ;
- Obsolescence de la cryptographie au regard des exigences internationales en la matière.

4.9.1.2 Certificat Cachet Serveur et Horodatage

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/DPC 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.

4.9.2.2 Certificat Cachet Serveur et Horodatage

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/DPC 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.

4.9.3.2 Certificat Cachet Serveur et Horodatage

Une demande de révocation contient les informations suivantes :

- L'identité du Client 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 (numéro de série du certificat...).

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

La demande de révocation est authentifiée via la vérification de l'adresse de messagerie interne utilisée pour déposer la demande. Optionnellement, le CT peut se présenter en face-à-face auprès de l'AE ; il est alors authentifié dans les mêmes conditions que pour une demande initiale de certificat.

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 client 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 CT du certificat n'est pas le demandeur, le CT est également informé de la révocation effective du certificat.

4.9.4 Délai accordé au Client 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.

4.9.4.2 Certificat Cachet Serveur et Horodatage

Dès que le CT 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.

4.9.5.2 Certificat « Cachet Serveur »

Une demande de révocation, authentifiée 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 à l'aide de l'ensemble des LCR et LAR 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.

4.9.8 Délai maximum de publication d'une LCR

Le délai maximum de publication d'une LCR suite à sa génération est de 60 minutes.

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

La fonction d'information sur l'état des certificats est disponible 24h/24 et 7j/7, avec un taux de 99,9% et une durée d'indisponibilité maximale de quatre (4) heures.

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

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

4.9.11 Autres moyens disponibles d'information sur les révocations

Les CRL et les certificats d'AC sont aussi disponibles sur le site de publication l'AC (https://www.dossiers-securite.bpce.fr/).

4.9.12 Exigences spécifiques en cas de 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 et

éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.). En cas de révocation de l'AC, l'ensemble des certificats clients sont révoqués.

Les conditions générales d'utilisation du certificat mentionnent clairement qu'en cas de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le client 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.

4.10Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC diffuse l'information sur l'état des certificats via la publication d'une CRL (4.9.7). Les caractéristiques de la dernière LCR/LAR sont décrites dans le plan de fin de vie de l'AC.

Aucun service OCSP n'est fourni par les AC.

4.10.2 Disponibilité de la fonction

Voir 4.9.9.

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

En cas de fin de relation (fusion, acquisition, etc.) entre l'établissement identifié dans le certificat et l'AC (Groupe BPCE), le certificat est révoqué.

BPCE dispose d'un plan de fin de vie détaillant les responsabilités et les actions à mener en cas de cessation d'activité de l'AC. Ce plan décrit la procédure de fin de vie : révocation des certificats en cours de validité, destruction des clés privées, maintien de la publication des informations, conservation des éléments de preuve, information des tiers (Clients, organisme d'audit).

BPCE s'engage à prévenir tous ses clients et les porteurs de certificats (excepté les porteurs de certificats éphémères) par courriel et par un message sur son site Internet au minimum au moins 3 mois avant la date effective de cessation d'activité de l'AC (sauf cas d'incident de sécurité).

Avant de mettre fin à ses services, BPCE met fin à l'autorisation de tous les sous-traitants d'agir pour son compte dans l'exercice de toute fonction liée au processus d'émission de certificats.

4.12Séquestre de clé et recouvrement

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

5 MESURES DE SÉCURITÉ NON TECHNIQUES

Voir [MCOM].

6 MESURES DE SÉCURITÉ 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.

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 client 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 client.

6.1.1.2 Bi-clés Client

Les bi-clés du client sont générées par l'AE dans une ressource cryptographique (HSM) 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 et Horodatage

La génération des bi-clés est effectuée par le CT ou sous contrôle du CT, dans une ressource cryptographique (HSM) 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

La clé publique du Cachet Serveur ou d'Horodatage 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 publié sur Internet.

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 clients 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 4096 bits.

La longueur des clés des certificats clients est de 2048 bits (algorithme RSA) pour les clés dont la durée de vie ne dépasse pas 2025, et de 3072 bits au-delà.

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

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

6.1.7 Objectifs d'usage des bi-clés

Voir 1.5.1 ; pour les *key usage* (Utilisation de la clé), voir [PROFILS].

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

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 deux 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 clients et des CRL, sans diminuer la sécurité apportée aux bi-clés.

6.2.2.2 Cachet Serveur et Horodatage

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. 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) que celle utilisée pour la génération ou sous forme de fichier chiffré.

6.2.4.2 Cachet Serveur et Horodatage

Le CT peut faire des copies de secours des clés privées.

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'AC 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.

6.2.6.2 Bi-clés Cachet Serveur et Horodatage

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.

6.2.7 Stockage de la clé privée dans un module cryptographique

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.

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 client et de LCR.

6.2.8.2 Bi-clés Cachet Serveur et Horodatage

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.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Bi-clés AC

Le cas échéant, l'AC définit les procédures permettant de désactivation des clés.

6.2.9.2 Bi-clés Cachet Serveur et Horodatage

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.

6.2.10 Méthode de destruction des clés privées

La destruction des clés privées suit la procédure déterminée par le fournisseur du matériel cryptographique.

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.

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

Aucune exigence de qualification.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées via l'archivage des certificats.

6.3.2 Durée de vie des bi-clés et des certificats

6.3.2.1 Bi-clé et 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-clés 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-clés Horodatage

Les bi-clés et certificats d'horodatage couverts par la présente Politique de certification ont une durée de vie de 4 ans maximum.

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. Les données d'activation sont générées automatiquement selon un schéma de Shamir. Dans tous les cas les données d'activation sont remises à leurs clients après génération pendant la cérémonie des clés. Les clients de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.1.2 Bi-clés Cachet Serveur et Horodatage

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. 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 données d'activation d'une AC sont continuellement tracées par l'AP.

6.4.2.2 Bi-clés Cachet Serveur et Horodatage

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.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

Voir [MCOM].

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

Voir [MCOM].

6.7 Mesures de sécurité réseau

Voir [MCOM].

6.8 Horodatage / Système de datation

Voir [MCOM].

7 PROFIL DE CERTIFICATS

Voir [PROFILS].

8 AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

Voir [MCOM].

9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

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.

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 :

- Certaines parties de la DPC,
- les clés privées de l'AC, des composantes et des Clients (Client) de certificats,
- les données d'activation associées aux clés privées d'AC et des Clients (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 Client,
- 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.

À 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 clients à des tiers dans le cadre de procédures légales.

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

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.

9.4.2 Informations à caractère personnel

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

- Données d'identification du CT
- Identité du CT
- Demande (remplie) d'émission de certificat,
- Fichier de preuve de l'AE,
- Demande (remplie) 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 dans le cadre de la délivrance et la gestion d'un certificat de client.

À 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 modifiée relative à l'informatique, aux fichiers et aux libertés.

En application de l'article 34 de la loi Informatique et Libertés du 6 janvier 1978, les clients 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 clients 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 client 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 Client portée dans le certificat
- l'apport des preuves nécessaires à la gestion du certificat du Client.

9.4.5 Notification et consentement d'utilisation de données personnelles

Aucune des données à caractère personnel communiquées par un client ne peut être utilisée par l'Infrastructure de Gestion de Clés, pour une utilisation autre que celle définie dans le cadre de la PC/DPC, sans consentement express et préalable de la part du client. Le consentement du client pour l'utilisation desdites données dans le cadre de la PC/DPC est considéré comme obtenu lors de la soumission de la demande de certificat et du fait de l'acceptation par le client 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 client, il est considéré que le client 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 client via les CGU, de transférer ses données à caractère personnel dans le cas d'un transfert d'activité à condition que le transfert n'altère pas les droits juridiques et techniques du client définis par la présente PC/DPC.

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/DPC et des certificats émis par l'AC.

Le client détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les certificats clients 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/DPC.

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/DPC 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 :

- élabore et valide la PC/DPC,
- maintien et fait évoluer la présente PC/DPC,
- 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/DPC,
- 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 clients.

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/DPC,
- 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 client et met à jour le dossier d'enregistrement du client,
- 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/DPC,
- respecte la PC/DPC et la DPC,
- assure la protection des données personnelles des clients,

- 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 SP

Le SP:

- publie les LCR,
- publie les certificats d'AC,
- publie la PC/DPC,
- garantit les taux de disponibilités des informations publiées,
- protège les accès au SP.

9.6.7 Obligations et garanties des autres participants

9.6.7.1 Obligations et garanties de l'UC

L'UC :

- contrôle l'état de validité des certificats à l'aide des CRL publiées,
- vérifie que les certificats 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 CRL publiée par l'AC
- vérifie que les certificats d'AC sont signés par une AC valide.

9.6.7.2 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/DPC,
- 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 Clients avec les certificats générés par l'AC.
- la gestion des certificats correspondants et des informations de validité des certificats selon la présente PC/DPC.

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

L'émission de certificats, conformément à la PC/DPC, 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 client ou de toutes autres parties concernées.

En conséquence de quoi, les clients 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 client.

9.8 Limite de responsabilité

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

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/DPC 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 processus en vigueur dans les établissements.

9.10 Durée et fin anticipée de validité de la PC/DPC

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

Selon l'importance des modifications apportées à la PC/DPC, 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/DPC entraîne la cessation de toutes les obligations et responsabilités de l'AC pour les certificats émis conformément à la PC/DPC.

9.11 Amendements à la PC/DPC

9.11.1 Procédures d'amendements

L'AP révise sa PC/DPC 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/DPC 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/DPC et de la DPC.

9.11.3 Circonstances selon lesquelles l'OID est changé

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

9.12Dispositions concernant la résolution de conflits

Le service juridique BPCE traitera des différends relatifs aux certificats entre entités du Groupe.

9.13Juridictions 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.

9.14Conformité aux législations et réglementations

La PC/DPC 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/DPC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.15Disposition 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/DPC 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/DPC 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 clients.

9.16Autres 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 n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

[EIDAS] Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE.

http://www.europa.eu

[GDPR] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

10.1 Documents normatifs

[ANSSI_HOR] Services d'horodatage électronique qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.1 du 3 janvier 2017

[ANSSI_PSCO] Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.2 du 5 juillet 2017

[ETSI_TSP] ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf

[ETSI_QTST] ETSI EN 319421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

http://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf

[RFC_3161] Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)

https://www.ietf.org/rfc/rfc3161.txt

[RFC_5816] ESSCertIDv2 Update for RFC 3161
https://www.ietf.org/rfc/rfc5816.txt

[SOGIS-CRYPTO] SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms – Version 1.0 – May 2016.
http://sogis.org

10.2Politique de Sécurité du Système d'Information

[PSSI] *Politique de Sécurité de l'Infrastructure de Gestion des Clefs du Groupe*, PSIGC-G_2020_V1.0-FR_BPCE

10.3Mesures communes

[MCOM] *Mesures communes*, publié à l'adresse www.dossiers-securite.bpce.fr

10.4Profils de certificats et CRL

[PROFILS] *Description des profils de certificats et des CRL*, publié à l'adresse www.dossiers-securite.bpce.fr