Politique et pratiques de certification

Signature client

V. 1.3

BPCE : Société anonyme à directoire et conseil de surveillance,
au capital de 180 478 270€.
Siège social : 7, promenade Germaine Sablon 75013 PARIS
RCS n° 493 455 042.

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

Version du document	1.3	Nombre de pages	47
Statut du document	☐Projet	☒Version finale	

Historique du document		
Date	Version	Commentaire
10/01/2021	1.0	Version Initiale
17/02/2021	1.1	- Ajout mention sur date d'application et de publication
19/05/2022	1.2	- Ajout disponibilité service de publication - Précision sur l'OCSP(non-utilisé)
12/05/2022	1.3	- Modification des valeurs de champs des certificats clients - Changement OID PC
29/09/2022	1.3	- Modification des valeurs de champs des certificats clients professionnels
19/12/2022	1.3	- Mise à jour Mentions Légales

SOMMAIRE

1 INTRODUCTION

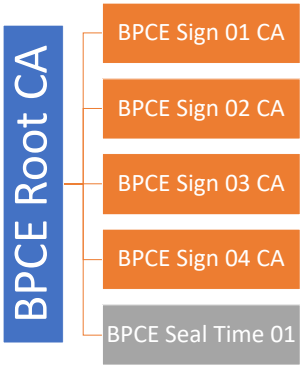
1.1 Présentation générale

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 d'AC opérées par le Groupe BPCE et certifiées selon l'*ETSI EN 319-411-1*, au niveau *Normalized Certificate Policy* (NCP/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 Practice 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 319 411-1, V1.2.2);
- *Certificate profile for certificates issued to natural persons* (ETSI EN 319 412-2)

1.2 Identification du document

La présente PC/DPC est la propriété du Groupe BPCE. La PC/DPC contient plusieurs *Object Identifier* (OID), chaque OID correspondant à un profil client particulier.

Le numéro d'OID de la présente P.C. est : 1.3.6.1.4.1.40559.1.0.1.31.101.1.2

Les numéros d'OID de ce document suivent les 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)
- Profil PRD-SI01-01-01(111), Profil PRD-SI02-01-01(112), Profil PRD-SI03-01-01(113), Profil PRD-SI04-01-01(114), Profil PRD-SI05-01-01(115), Profil PRD-SI06-01-01(116), Profil PRD-SI07-01-01(117), Profil PRD-SI08-01-01(118), Profil PRD-SI09-01-01(119), Profil PRD-SI10-01-01(120)
- Environnement :
  - Production (1)
  - Qualification développement (2)
- Version (1)

Les différentes déclinaisons de la politique de certification *Signature client* sont identifiées par les OID suivants :

Niveau	**Enregistrement**		**Population**	**OID**
NCP	AGENCE	Face à Face en agence avec vérification de carte d'identité	Particulier	1.3.6.1.4.1.40559.1.0.1.31.111.1.1
NCP	AGENCE	Face à Face en agence avec vérification de carte d'identité	Professionnels	1.3.6.1.4.1.40559.1.0.1.31.112.1.1
NCP	AGENCE	OTP CAP ou sur SMS ou SECUR'PASS	Particulier	1.3.6.1.4.1.40559.1.0.1.31.113.1.1
NCP	AGENCE	OTP CAP ou sur SMS ou SECUR'PASS	Professionnels	1.3.6.1.4.1.40559.1.0.1.31.114.1.1
NCP+	AGENCE	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc…)	Particulier	1.3.6.1.4.1.40559.1.0.1.31.115.1.1
NCP+	AGENCE	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc…)	Professionnels	1.3.6.1.4.1.40559.1.0.1.31.116.1.1
NCP	INTERNET	OTP CAP ou sur SMS ou SECUR'PASS	Particulier	1.3.6.1.4.1.40559.1.0.1.31.117.1.1
NCP	INTERNET	OTP CAP ou sur SMS ou SECUR'PASS	Professionnels	1.3.6.1.4.1.40559.1.0.1.31.118.1.1

Niveau	Enregistrement		Population	OID
NCP+	INTERNET	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc…)	Particulier	1.3.6.1.4.1.40559.1.0.1.31.119.1.1
NCP+	INTERNET	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc…)	Professionnels	1.3.6.1.4.1.40559.1.0.1.31.120.1.1

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 07/02/2023.

Le présent document entre en vigueur le 08/02/2023.

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 /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. Cette fonctionnalité est mise

en œuvre par l'ensemble des composantes techniques de l'Infrastructure de Gestion des Clés.

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

Les entités intervenant dans l'IGC sont décrites dans [MCOM] (section 2.2, « Définitions »). Le tableau ci-dessous résume ces différentes entités.

Autorité de Gestion des Politiques (AP)	CESSIG
Autorité de Certification (AC)	Groupe BPCE
Autorité d'Enregistrement (AE)	BPCE-IT
Autorité d'Enregistrement Déléguée (AED)	Établissement, filiale ou réseau distributeur
Service de Publication (SP)	BPCE-IT
Opérateur Technique (OT)	BPCE-IT
Opérateur Fonctionnel (OF)[1]	BPCE SI
Porteurs de certificats/Souscripteur[2]	Client
Utilisateurs de certificats (UC)	Personne ou système informatique qui déclenche la création de la signature d'un document électronique

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 Certificat Client;
- la signature de LCR ;
- la signature de CSR (format PKCS#10).

1.5.1.2 Certificat Client

La clé privée associée au Certificat sert pour :

- la signature de document au nom du Client ;

[1] L'opérateur fonctionnel n'est pas un rôle de confiance de l'IGC mais du service de signature électronique qui utilise l'IGC.

[2] Le client est *subscriber* et *subject* au sens de l'ETSI.

- 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.

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

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/DPC décrit la gestion du cycle de vie des certificats de signature et de leurs supports. Elle n'a pas vocation à remplacer la *Politique de Signature et de Gestion des Preuves* (PSGP) qui décrit la gestion du cycle de vie des signatures établies à l'aide des certificats délivrés par l'AC et des dossiers de preuve. Dans le cas de la présente PC/DPC, c'est le Groupe BPCE qui élabore la PSGP associée aux certificats gérés par la présente PC/DPC.

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 document. Le client approuve ces *Conditions Générales d'Utilisation*, sans quoi le processus de signature de son document ne peut pas aboutir.

1.6 Gestion de la PC/DPC

Voir [MCOM].

1.7 Définitions et Acronymes

Voir [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 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	CN=`BPCE Sign 01 CA`, `BPCE Sign 02 CA`, `BPCE Sign 03 CA`, ou `BPCE Sign 04 CA` OU=`0002 493455042` OI=`NTRFR-493455042` O=`BPCE` C=`FR`

Remarque : Il existe quatre certificats d'AC différents.

3.1.1.2 Certificat Client professionnel

L'identité du client « personne morale » et du porteur « personne physique » qui le représente est la suivante dans le certificat :

Champ de base	Valeur
Issuer	Identité de l'AC (*cf. 3.1.2.1*)
Subject	C = ⟨code pays du client (1)⟩ O = ⟨libellé de l'organisation personne morale (2)⟩ OU = ⟨Identification de l'entité légale cliente (3)⟩ OI = ⟨Identification eIDAS de l'entité légale cliente (4)⟩ *serialNumber* = ⟨identifiant de transaction (5)⟩ *GN* = ⟨nom du porteur personne physique, représentant le client personne morale (6)⟩ *SN* = ⟨prénom du porteur personne physique, représentant le client personne morale (6)⟩ *CN* = ⟨nom et prénom du porteur personne physique, représentant le client personne morale (6)⟩

(1) « FR » par défaut ou tel qu'inscrit dans le référentiel d'identification des clients provenant des SI bancaires

(2) « O » tel qu'inscrit dans le référentiel d'identification des clients, provenant des SI bancaires

(3) Pour les clients de droit français : numéro d'identification national (exemple SIREN, RNA). Pour les clients de droit non-français : identifiant provenant d'un registre national

(4) Pour les clients de droit français : « NTRFR » suivi d'un tiret et du numéro d'identification national. Pour les clients de droit non-français : « NTR<code pays> » suivi d'un tiret et de l'identifiant provenant d'un registre national.

(5) Identifiant de transaction + ordre chronologique de signature + horodatage

(6) tels qu'inscrits dans le référentiel d'identification des clients, provenant des SI bancaires

Les clients professionnels correspondent aux OID suivantes :

1.3.6.1.4.1.40559.1.0.1.31.112.1.1
1.3.6.1.4.1.40559.1.0.1.31.114.1.1
1.3.6.1.4.1.40559.1.0.1.31.116.1.1
1.3.6.1.4.1.40559.1.0.1.31.118.1.1
1.3.6.1.4.1.40559.1.0.1.31.120.1.1

3.1.1.3 Certificat Client particulier

L'identité du client porteur « personne physique » est la suivante dans le certificat :

Champ de base	Valeur
Issuer	Identité de l'AC (*cf. 3.1.2.1*)
Subject	C = FR(1) *serialNumber* = ⟨identifiant de transaction(2)⟩ *GN* = ⟨nom du porteur (3)⟩ *SN* = ⟨prénom du porteur (3)⟩ *CN* = ⟨nom et prénom du porteur (3)⟩

(1) « FR » par défaut ou tel qu'inscrit dans le référentiel d'identification des clients provenant des SI bancaires

(2) Identifiant de transaction + ordre chronologique de signature + horodatage balise

(3) Tels qu'inscrits dans le référentiel d'identification des clients provenant des SI bancaires

Les clients particuliers correspondent aux OID suivantes :

1.3.6.1.4.1.40559.1.0.1.31.111.1.1
1.3.6.1.4.1.40559.1.0.1.31.113.1.1
1.3.6.1.4.1.40559.1.0.1.31.115.1.1
1.3.6.1.4.1.40559.1.0.1.31.117.1.1
1.3.6.1.4.1.40559.1.0.1.31.119.1.1

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.

3.1.2.2 Certificat Client

L'identité du client est construite à partir des nom et prénom de son état civil tel que présent dans le référentiel client de l'AED. Cet état civil est celui porté sur son document officiel d'identité présenté lors de l'entrée en relation bancaire du client.

3.1.2.3 Certificat de test

Les certificats de test sont identifiables par la présence du mot « TEST » dans le CN, en complément du prénom et du nom.

3.1.3 Pseudonymisation des Clients

L'identité utilisée pour les certificats (AC et Clients) n'est ni un pseudonyme, ni anonyme.

3.1.4 Règles d'interprétation des différentes formes de noms

L'identité incluse dans les certificats permet d'authentifier les clients et le Groupe BPCE.

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 Client

Les identités portées par l'AC dans les certificats sont uniques au sein de son domaine de certification. Durant toute la durée de vie de l'AC, une identité attribuée à un client de certificat ne peut être attribué à un autre client.

L'AED assure cette unicité au moyen de son processus d'enregistrement et de la valeur unique du DN attribué à un client (attribut *serialNumber notamment*). En particulier, les différents réseaux du Groupe (Caisse d'Épargne et Banques populaires) utilisent une nomenclature différente pour cet attribut, afin d'éviter toute possibilité de collision.

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 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 (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 Client

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.

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

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

Note : les certificats d'AC sont rattachés à la personne morale « BPCE ».

3.2.2.2 Certificat Client (professionnel)

Note : cette vérification ne concerne que les Clients professionnels.

La vérification de l'appartenance d'un client professionnel, personne physique, à l'organisation dont il se réclame est systématiquement effectuée.

L'AED 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 client aux informations recueillies dans les bases de données officielles de référence.

Les informations vérifiées comprennent au minimum le numéro SIREN et le nom de l'entité légale.

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 la vérification d'identité sont réalisées sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport…).

3.2.3.2 Certificat Client : identification en agence

Le Client est identifié lors d'un face à face avec l'AED lors de l'entrée en relation et tout long de la relation client, conformément aux exigences bancaires réglementaires.

L'identification et la vérification d'identité du client par l'AED sont réalisées sur la base de la présentation d'une pièce d'identité officielle, en cours de validité (carte nationale d'identité, passeport…), dont une trace est conservée par l'AED dans le dossier réglementaire du client.

Le dossier réglementaire du client est mis à jour par l'AED.

3.2.3.3 Certificat Client : identification en ligne

Le client peut s'identifier et s'authentifier sur le portail de l'AE via le protocole d'authentification choisi par l'AED parmi ceux proposés par le Groupe BPCE (voir [PSGP]). Les moyens d'Authentification proposés sont décrits dans la [PSGP] :

- *L'Authentification non rejouable par SMS basée sur le numéro de téléphone mobile ayant été vérifié de manière sécurisée,*
- *L'Authentification non rejouable par CAP, le lecteur CAP ayant été remis au client lors d'un rendez-vous en Face-à-face ou par envoi postal,*
- *L'Authentification par Certificat matériel émis par une autorité de certification acceptée par le Groupe BPCE et conforme aux exigences RGS** ou eIDAS niveau Qualifié*
- *L'Authentification basée sur deux facteurs d'authentification (exemple Sécur'pass) : l'enrôlement d'un téléphone mobile et la détention de ce matériel lors de la Signature pour la saisie d'un mot de passe.*

L'AED distribue de façon sécurisée les moyens et données d'authentification que le client utilise : Dans tous les cas, le moyen d'authentification est remis après la vérification d'identité en face-à-face en agence soit de façon équivalente, comme le prévoit l'Article R. 561-5-2 du *Code monétaire et financier*.

Le moyen d'authentification utilisé par le Client se retrouve dans son certificat, via l'OID de la politique :

1.3.6.1.4.1.40559.1.0.1.31.111.1.1	AGENCE	Face à Face en agence (avec vérification carte d'identité)	Particulier (NCP)
1.3.6.1.4.1.40559.1.0.1.31.112.1.1	AGENCE	Face à Face en agence (avec vérification carte d'identité)	Professionnels (NCP)
1.3.6.1.4.1.40559.1.0.1.31.113.1.1	AGENCE	OTP CAP ou sur SMS ou SECUR'PASS	Particulier (NCP)
1.3.6.1.4.1.40559.1.0.1.31.114.1.1	AGENCE	OTP CAP ou sur SMS ou SECUR'PASS	Professionnels (NCP)
1.3.6.1.4.1.40559.1.0.1.31.115.1.1	AGENCE	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc…)	Particulier (NCP+)
1.3.6.1.4.1.40559.1.0.1.31.116.1.1	AGENCE	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc…)	Professionnels (NCP+)
1.3.6.1.4.1.40559.1.0.1.31.117.1.1	INTERNET	OTP CAP ou sur SMS ou SECUR'PASS	Particulier (NCP)

1.3.6.1.4.1.40559.1.0.1.31.118.1.1	INTERNET	OTP CAP ou sur SMS ou SECUR'PASS	Professionnels (NCP)
1.3.6.1.4.1.40559.1.0.1.31.119.1.1	INTERNET	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc…)	Particulier (NCP+)
1.3.6.1.4.1.40559.1.0.1.31.120.1.1	INTERNET	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc…)	Professionnels (NCP+)

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 client correspond à la validation de l'appartenance à l'organisation dont il se réclame.

3.2.6 Certification croisée d'AC

Il n'y a pas de certification croisée dans la hiérarchie d'AC.

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. Dans tous les cas, la procédure d'authentification est conforme à la procédure initiale.

3.3.1.2 Certificat Client : identification en agence

La procédure d'authentification est conforme à la procédure initiale : voir 3.2.3.2.

3.3.1.3 Certificat Client : identification en ligne

L'AED distribue de façon sécurisée les moyens et données d'authentification que le client utilise (voir [PSGP] et, pour rappel, 3.2.3.3). L'AED vérifie périodiquement que le moyen utilisé par le client est toujours le sien (numéro de téléphone, par exemple).

Remarque : un nouveau certificat ne peut pas être fourni au client 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 (§ 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 Client

En cas de demande de révocation du certificat par le Client, celui-ci doit fournir une copie d'une pièce d'identité en cours de validité.

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 4.6, 4.7 et 4.7.1.

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 Client

Un certificat peut être demandé par un client en relation avec l'AED. 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'AED.

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 Client

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

- Nom et prénom du client tels que portés sur la pièce d'identité en cours de validité lors de l'entrée en relation, et tels qu'enregistrés par l'AED ;
- La présentation de la pièce d'identité officielle du client en agence ;
- L'information permettant de contacter et d'authentifier le client (adresse de courrier électronique ou numéro de téléphone…), en fonction de la politique de signature qui est appliquée par l'AED ;
- Pour les professionnels, les informations d'identification de l'entreprise du client.

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 et validée par l'AED.

L'AED s'assure que le client a pris connaissance des conditions générales d'utilisation.

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

4.2.2.2 Certificat Client

En cas d'approbation de la demande, l'AED 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'AED en informe le client (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, d'au plus, six mois.

4.2.3.2 Certificat « Client »

La durée du traitement est inférieure à une minute après l'acceptation de la demande.

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 Client

Le client déclenche la génération de sa bi-clé sur le portail de l'AE suivant la cinématique d'activation choisie par l'AED et décrite dans la politique de signature (voir [PSGP] et, pour rappel, 3.2.3.3).

1. L'AED transmet la demande technique de certificat, qui contient la CSR, à l'ICG.
2. L'AC authentifie l'ICG (techniquement).
3. L'AC signe le certificat.

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 Client

Une fois le certificat généré, le DN du certificat est présenté au client avant signature.

Le certificat est intégré au document électronique signé par le client si celui-ci accepte de signer.

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 Client

Le DN du certificat est présenté au client avant signature, qui peut accepter ou refuser le certificat.

S'il le refuse, le processus de signature est abandonné et le certificat expire.

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 LAR. L'AP est responsable de la diffusion des certificats et des LAR en plus des moyens fournis par le SP.

4.4.2.2 Certificat Client

Les certificats ne sont pas publiés après leur délivrance.

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 Client

L'AC ne notifie aucune autre entité.

4.5 Usage de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du Certificat par le Client

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. La clé privée du client ne peut être utilisée que pour une opération de signature de document.

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

Aucune exigence.

4.6 Renouvellement d'un certificat

Le renouvellement des certificats clients 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

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

Pour un certificat d'AC, le processus est identique à celui utilisé pour une demande initiale. Le reste de cette section concerne donc le cas des certificats Client.

4.7.1 Demande de certificat Client

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 4.6, 4.7 et 4.7.1.

4.7.1.1 Origine d'une demande de certificat

Idem. 4.1.1.2.

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

La demande de bi-clé et de certificat se déroule dans le cadre d'un processus de signature piloté par l'AED.

4.7.2 Traitement d'une demande de certificat

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

L'AED s'assure que le client a pris connaissance des conditions générales d'utilisation.

Le client s'authentifie sur le portail de l'AED. Pour déclencher sa signature, il s'authentifie auprès de l'AED en utilisant les moyens qui ont été mis à disposition dans le cadre de la demande initiale.

4.7.2.2 Acceptation ou rejet de la demande

Idem. 4.2.2.2.

4.7.2.3 Durée d'établissement du certificat

Idem. 4.2.3.2.

4.7.3 Délivrance du certificat

Idem. 4.3.

4.7.4 Acceptation du certificat

Idem. 4.4.

4.8 Modification du certificat

Cette section concerne la génération d'un nouveau certificat avec conservation de la même clé.

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

Ce cas peut être autorisé pour les certificats d'AC 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.

Dans tous les cas, pour le changement de certificat d'AC, la procédure à suivre est identique à la procédure initiale de certification.

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 Client

Il peut exister plusieurs causes de révocation de certificat Client :

- Les informations figurant dans le certificat ne sont plus correctes ;
- La cessation de la relation entre le client et l'AED ;
- Le client n'a pas respecté les modalités applicables d'utilisation du certificat ;
- La clé privée du client est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- L'AC demande explicitement la révocation du certificat ;
- Cessation d'activité de l'AC.

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

Le client peut être à l'origine de la demande de révocation.

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 Client

La demande se fait par courrier postal à l'adresse suivante :

Groupe BPCE Directeur de la Sécurité des Systèmes d'informations Groupe 7, promenade Germaine Sablon, 75013 PARIS

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 Client

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.

4.9.5.2 Certificat Client

Une demande de révocation est traitée dans un délai inférieur à 24 heures après réception et validation par l'AC. L'AC informe l'AED par courriel de la révocation du certificat, l'AED informe ensuite le Client concerné par le moyen le plus adapté (processus bancaire).

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 LAR.

Il appartient aux UC de vérifier l'état de validité d'un certificat client 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 60 minutes.

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 LCR 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

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 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.

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 LCR (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 Client et l'AC

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

Se référer aux mesures communes [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 définie 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'ICG 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, décrites dans la politique de signature (voir [PSGP] et, pour rappel, 3.2.3.3).

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée n'est pas transmise au porteur.

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.

6.1.4 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 d'AC est publié par le SP.

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 3072 bits.

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

Si l'algorithme utilisé est ECDSA la courbe utilisée devra être la courbe P-384.

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

La qualité des clés générées et des paramètres employés sont garantis par le matériel cryptographique utilisé.

6.1.7 Objectifs d'usage des bi-clés

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

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

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 AC est réalisé par au moins deux (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 clients et des LCR, sans diminuer la sécurité apportée aux bi-clés.

6.2.2.2 Bi-clés Client

Les bi-clés sont sous le contrôle exclusif des clients.

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 celui utilisé 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.

6.2.5 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 chiffrée. 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 AC sont déployées en ligne uniquement afin de signer des certificats de clients et les LCR 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/DPC.

6.2.6.2 Bi-clés Client

La clé privée ne fait pas l'objet d'un transfert hors de ou vers un module cryptographique.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées sont générées, conservées et utilisées dans le même type de matériel cryptographique tout au long de leur cycle de vie.

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 Client

Le client utilise le moyen et les données d'authentification qui lui ont été remis lors de son enregistrement pour activer sa clé privée. L'AED 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).

Les bi-clés des clients sont activées dans un HSM (6.2.1) après l'authentification réussie du client.

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.

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, s'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.

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

Voir 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.

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 par celle de l'AC Racine.

6.3.2.2 Bi-clé et certificat Client

Les bi-clés et certificats Client 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. 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 Client

Le type de données d'activation qu'utilise le client est décrit dans la politique de signature.

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 clients de données d'activation sont responsables de leur gestion et de leur protection. Un client 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.

6.4.3 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.

6.5 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]. Se référer à 1.2 pour la liste des OID.

8 AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

Voir [MCOM].

9 AUTRES PROBLÉMATIQUES MÉTIER 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 :

- 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,

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.

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 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 Client,

- Identité du Client,
- Demande (renseignée) d'émission de Certificat,
- Fichier de preuve de l'AE,
- Demande (complétée) 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.

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 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
- 7, promenade Germaine Sablon, 75013 PARIS
- 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,
- N'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 emploient 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, remédient 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 :

- Gère le réseau d'AED,
- Collecte auprès des AED des éléments de traçabilités des dossiers d'enregistrement des porteurs avant de les transmettre vers l'AC.
- Authentifie la demande de certificat,
- Authentifie les demandes de révocation,
- Transmet la demande de certificat,
- 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,
- 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 de l'AED

L'AED :

- Collecte auprès des clients les éléments de traçabilités des dossiers d'enregistrement des porteurs avant de les transmettre à l'AE,
- Vérifie les données du client et met à jour le dossier d'enregistrement du client,
- Met à jour et vérifie périodiquement que le moyen d'authentification utilisé par le client est toujours le sien (numéro de téléphone, par exemple),
- 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,
- 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.

9.6.7 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/DPC,
- Garantit que les informations qu'il fournit à l'AED 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'AED en cas de besoin de révocation de son Certificat.

9.6.8 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.

9.6.9 Obligations et garanties des autres participants

9.6.9.1 Obligations et garanties de l'UC

L'UC :

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

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.

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

Voir [MCOM].

9.11 Amendements à la PC/DPC

Voir [MCOM].

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 client.

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 client, il est du ressort de l'AED de gérer et de résoudre le litige. L'AP s'assure que l'AED 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/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.

9.15 Disposition diverses

9.15.1 Accord global

Aucune exigence spécifique.

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 PLARement 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 PLARement 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 LCR

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

10.5PSGP

[PSGP] *Politique de Signature et de Gestion de Preuves*, publié à l'adresse www.dossiers-securite.bpce.fr
(OID : 1.3.6.1.4.1.40559.1.0.3.3.0.1.2)