Conditions Générales d'Utilisation

Signature

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 188 932 730 €.

Siège social : 7, promenade Germaine Sablon, 75013 PARIS

RCS n° 493 455 042.

SOMMAIRE

1 OBJET DU DOCUMENT

Ce document définit les **Conditions Générales d'Utilisation** (CGU) des certificats délivrés dans le cadre du processus de signature électronique par les autorités de certification *BPCE AC Signature* de BPCE, sous 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
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

Il existe quatre AC opérées par le Groupe BPCE et certifiées vis-à-vis de la norme *ETSI EN 319-411-1*, au niveau *Normalized certificate Policy* (NCP et NCP+).

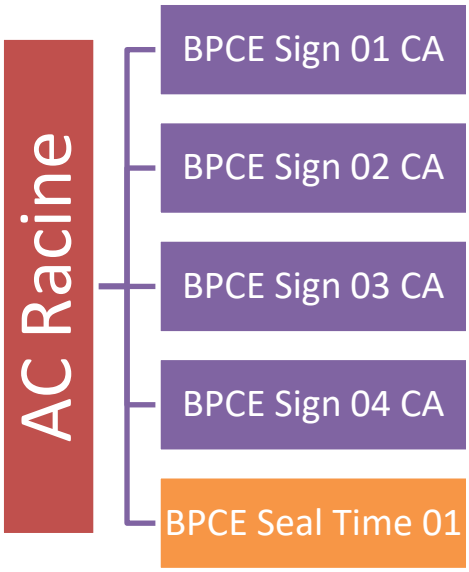
1.1 Acronymes

AC	Autorité de Certification
BP	Banques Populaires
BPCE	Banques Populaires Caisse d'Épargne
BPCE-SI	BPCE Solutions Informatiques
CE	Caisse d'Épargne
CGU	Conditions Générales d'Utilisation

DPC	Déclaration des Pratiques de Certification
ICG	Infrastructure de Confiance Groupe
OID	Object Identifier
PC	Politique de Certification
SIREN	Système Informatique du Répertoire des Entreprises
UCG	Usine à Certificat Groupe

2 CONDITIONS GÉNÉRALES D'UTILISATION

Contact de l'Autorité de Certification	Groupe BPCE Directeur de la Sécurité des Systèmes d'informations Groupe 7, promenade Germaine Sablon 75013 PARIS rssi-pssi-icg@bpce.fr

Type de certificats émis	Les certificats émis par l'AC sont des certificats de signature pour les clients des réseaux Caisse d'Épargne et Banques populaires et Filiales dans le cadre du processus de signature électronique. Il s'agit de certificats éphémères générés par l'AC au nom du porteur durant le processus de signature. Ces certificats ne peuvent être utilisés dans d'autres contextes. Les certificats sont émis à travers la chaîne de certification suivante :  Les certificats de la chaîne de certification sont disponibles à l'adresse suivante : • AC Racine : http://pro.d00.pki02.bpce.fr/bpce-root-ca.crt • *AC BPCE Sign 01 CA :* http://pro.d00.pki02.bpce.fr/BPCESIGN01CA.crt • *AC BPCE Sign 02 CA :* http://pro.d00.pki02.bpce.fr/BPCESIGN02CA.crt • *AC BPCE Sign 03 CA :* http://pro.d00.pki02.bpce.fr/BPCESIGN03CA.crt • *AC BPCE Sign 04 CA :* http://pro.d00.pki02.bpce.fr/BPCESIGN04CA.crt
Objet des certificats	Les certificats émis par l'AC sont des certificats à destination de personnes physiques, clients du Groupe BPCE. Ces certificats sont stockés dans un module de sécurité sous contrôle de l'AC et ne sont utilisables que durant la transaction de signature, c'est-à-dire quelques minutes.

Modalités d'obtention	L'obtention d'un certificat électronique de signature est entièrement intégrée au processus commercial de signature électronique entre les établissements Caisse d'Épargne et Banques Populaires et leurs clients. Le Client est identifié lors d'un face à face lors de l'entrée en relation et tout long de la relation client, conformément aux exigences bancaires réglementaires, sur la base de la présentation d'une pièce d'identité officielle (carte nationale d'identité, passeport…), dont une trace est conservée dans le dossier réglementaire du client. Le Client peut aussi utiliser tout moyen d'identification électronique de niveau de garantie substantiel ou élevé au sens du Règlement eIDAS[1], (conformément à l'Article R. 561-5-1, alinéa 1, du *Code monétaire et financier*). Enfin, un Client peut utiliser un moyen d'authentification qui lui a préalablement été remis de façon sécurisée, qui lui a été remis après la vérification d'identité réalisé soit en face-à-face en agence, soit de façon équivalente, comme le prévoit l'Article R. 561-5-2 du *Code monétaire et financier*, parmi le suivants : – *Authentification non rejouable par SMS basée sur le numéro de téléphone mobile ayant été vérifié de manière sécurisée,* – *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,* – *Authentification par Certificat matériel, le Certificat ayant été remis au Client lors d'un rendez-vous en Face-à-face. Les certificats sur support matériel sont des certificats référencés émis par une autorité de certification reconnue par le Groupe BPCE et conforme aux exigences RGS ou équivalent PAC,* – *Authentification basée sur deux moyens d'authentification sécurisés (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.*

[1] 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.

Acceptation	Le DN du certificat est présenté au client avant signature, qui peut accepter ou refuser le certificat. S'il le refuse, le certificat est révoqué par l'AC et le processus de signature est abandonné.
Modalités de renouvellement	Le certificat est délivré pour une durée de validité de 10 minutes. Il n'est donc pas proposé de processus de renouvellement.
Modalités de révocation	Le Client ou l'agent peut être à l'origine de la demande de révocation. La demande se fait par courrier postal à l'adresse mentionnée ci-dessus (« Contact de l'Autorité de Certification »).
Disponibilité des services	Le service de demande de révocation est disponible tous les jours H24 et 7J7. 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).
Limites d'usages	Les certificats délivrés ne sont utilisables que durant la transaction de signature. Ils sont générés pour une durée de dix minutes et ne sont donc plus utilisables au-delà de cette période. Les clés privées correspondantes sont également détruites des modules de sécurité soit à la fin de la transaction de signature si tout s'est correctement déroulé, soit suite à une erreur technique durant la transaction de signature. Les dossiers d'enregistrements et les journaux d'évènements sont archivés et conservés au minimum 10 ans.

Obligations des porteurs	Le porteur : – Doit communiquer des informations exactes et à jour lors de ses échanges avec le chargé de clientèle ; – Est en charge de s'assurer que les informations présentées dans le document à signer sont correctes ; – Doit accepter les Conditions Générales d'Utilisation qui lui sont présentées lors du processus de signature ; – Vérifier que les données présentes dans le certificat du document signé qui lui est remis sont correctes. – Doit contacter l'AC dans les plus brefs délais dans le cas où ses données ne sont pas correctes. – Consent à la conservation des données d'enregistrement de son certificat.
Obligations de vérification des certificats par les utilisateurs	Les utilisateurs des certificats doivent : – Vérifier l'usage pour lequel le certificat a été émis ; – Vérifier que le certificat utilisé a bien été émis par l'AC ; – Vérifier que le certificat n'est pas présent dans les listes de révocation de l'AC ; – Vérifier la signature du certificat, et de la chaîne de certification, jusqu'à l'AC Racine et contrôler la validité des certificats. La liste de révocation des certificats émis par l'AC est disponible aux adresses suivantes : ▸ AC Racine : – http://pro.d00.pki02.bpce.fr/BPCERootCA.crl – http://pro.d01.pki02.bpce.fr/BPCERootCA.crl – http://pro.d02.pki02.bpce.fr/BPCERootCA.crl ▸ *BPCE AC Signature :* – http://pro.d00.pki02.bpce.fr/bpcesign0*x*ca.crl – http://pro.d01.pki02.bpce.fr/bpcesign0*x*ca.crl – http://pro.d02.pki02.bpce.fr/bpcesign0*x*ca.crl Le « *x* » prend la valeur 1, 2, 3 ou 4, en fonction de l'AC qui a émis le certificat (*BPCE Sign 01 CA, BPCE Sign 02 CA, BPCE Sign 03 CA*, ou *BPCE Sign 04 CA*).

Limite de responsabilité	Sous réserve des dispositions d'ordre public applicables, BPCE ne pourra pas être tenue responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LAR et des LCR ainsi que de tout autre équipement ou logiciel mis à disposition. BPCE décline en particulier sa responsabilité pour tout dommage résultant d'un cas de force majeure tel que défini par les tribunaux français. BPCE décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.
Archivage	Les traces des événements liés au cycle de vie des certificats sont archivées par l'infrastructure de confiance Groupe (demande, dossier de demande, génération/révocation du certificat). Les données archivées sont conservées au minimum 10 ans.
Références documentaires	La Politique de Certification de l'AC est accessible à l'adresse suivante : https://www.dossiers-securite.bpce.fr
Conditions d'indemnisation	Sans objet
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.

Loi applicable	La Politique de Certification est soumise au droit français. En matière contractuelle, tout litige relatif à la validité, l'interprétation, l'exécution de la Politique de Certification (PC) et des présentes sera soumise aux tribunaux compétents du ressort du tribunal de Paris.
Audits et références applicables	L'AP proclame la conformité de la DPC à la PC sur la base des résultats de contrôles de conformité qui visent à s'assurer que les différentes procédures opérationnelles sont à jour et appliquées. L'AC s'engage à effectuer ce contrôle au minimum une fois tous les ans. Par ailleurs, avant la première mise en service d'une composante de son infrastructure ou suite à toute modification significative au sein d'une composante, l'AC fera également procéder à un contrôle de conformité de cette composante. Les certificats émis par l'AC sont certifiés conforme à la norme *ETSI EN 319411-1*, niveau NCP et NCP+ . L'AC a également obtenu la certification de son offre dans le cadre du programme *Adobe Approved Trusted List* (AATL).