Conditions Générales d'Utilisation

Cachet Serveur & Horodatage

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 l'Autorité de Certification *BPCE AC Cachets* de BPCE, sous les OID suivants :

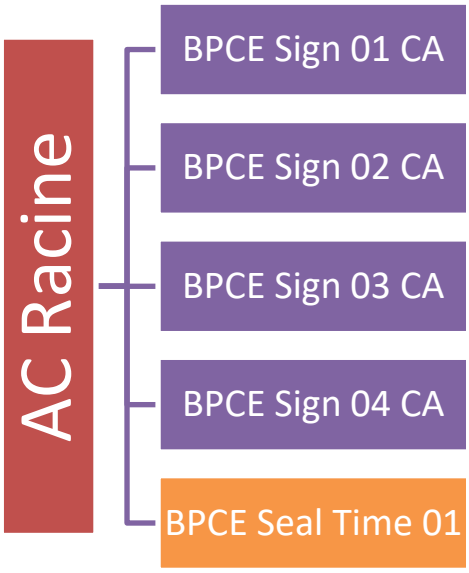
Politique de certification	OID
Cachet Serveur	*1.3.6.1.4.1.40559.1.0.1.31.210.1.1*
Horodatage	*1.3.6.1.4.1.40559.1.0.1.31.211.1.1*

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+).

1.1 Acronymes

AC	Autorité de Certification
BP	Banques Populaires
BPCE	Banques Populaires Caisse d'Épargne
CE	Caisse d'Épargne
CGU	Conditions Générales d'Utilisation
DPC	Déclaration des Pratiques de Certification
ICG	Infrastructure de Confiance Groupe
IT-CE	Informatique & Technique Caisse d'Épargne
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 sont des certificats de cachet (entité morale). 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* • BPCE AC Cachets : *http://pro.d00.pki02.bpce.fr/BPCESEALTIME01.crt*

Objet des certificats	**CERTIFICAT CACHET SERVEUR** La clé privée associé au certificat sert pour la signature de : ᔓ Documents au nom de l'Établissement ; ᔓ CSR (format PKCS#10). **CERTIFICAT HORODATAGE** La clé privée associé au certificat sert pour : ᔓ L'horodatage de document au nom du Groupe BPCE ; ᔓ La signature de CSR (format PKCS#10).
Modalités d'obtention	Les cachets serveurs sont émis au nom des établissements du Groupe BPCE. L'identification et l'authentification du contact technique (CT) est effectuée par l'AE en face à face. Le CT appartient forcément à l'ICG (DPM-PCL-STR-ICG). Les informations suivantes figurent dans la demande de certificat Cachet Serveur : ᔓ Le nom et prénom du CT ; ᔓ Une pièce d'identité en cours de validité ; ᔓ Les informations permettant à l'AE de contacter le CT et d'authentifier le CT (numéro de téléphone, courriel…) ; ᔓ Un code de révocation pour le certificat demandé ; ᔓ Pour les certificats d'Horodatage : Une copie du P.-V. de la cérémonie des clés ; ᔓ La CSR pour la clé publique à certifier. La demande de certificat est traitée par l'AE dans un délai de deux semaines calendaires. Le CT notifié par courriel de la mise à disposition du certificat sur l'outil Venafi. À réception, le CT vérifie les informations du certificat et l'accepte ou le refuse par retour de courriel.
Acceptation	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.

Modalités de renouvellement	Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales.
Modalités de révocation	Une demande de révocation contient les informations suivantes : - Le code de révocation, fourni par l'AE lors de la délivrance du certificat - 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'identité du CT à travers la messagerie d'entreprise. 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. 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.
Disponibilité des services	Le service de demande de révocation est disponible tous les jours H24 et 7J7. Une demande de révocation, authentifiée et dûment établie par l'AE, émise par le CT est traitée dans un délai inférieur à 24 heures.
Limites d'usages	L'utilisation des certificats émis par l'AC, à d'autres fins que celles décrites dans ce document, n'est pas autorisée. Les dossiers d'enregistrements et les journaux d'évènements sont archivés et conservés au minimum 10 ans.

Obligations des porteurs	Le CT : – Doit communiquer des informations exactes et à jour lors de ses échanges avec l'AE ; – Doit accepter les présentes Conditions Générales d'Utilisation qui lui sont présentées lors du processus de demande ; – Vérifier que les données présentes dans le certificat qui lui est remis sont correctes ; – Doit utiliser un matériel cryptographique pour générer et conserver sa clé privée et garder celle-ci sous son contrôle exclusif ; – Doit utiliser un algorithme et des paramètres conformes au standard ETSI TS 119 312 ; – Doit cesser d'utiliser sa clé privée dès lors que le certificat associé a été révoqué ; – Doit cesser d'utiliser sa clé privée dès lors que le certificat est réputé compromis ; – Doit contacter l'AC dans les plus brefs délais dans le cas où ces données ne sont pas correctes.

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 Cachets :* – *http://pro.d00.pki02.bpce.fr/bpcesealtime01ca.crl* – *http://pro.d01.pki02.bpce.fr/bpcesealtime01ca.crl* – *http://pro.d02.pki02.bpce.fr/bpcesealtime01ca.crl*
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	Le service juridique BPCE traitera des différends relatifs aux certificats entre entités du Groupe.
Loi applicable	La présente Politique de Certification est soumise au droit français. En matière contractuelle, tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique de Certification (PC) 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+. L'AC a obtenu la certification de son offre dans le cadre du programme *Adobe Approved Trusted List* (AATL).