

1. PREAMBULE

Les présentes CGU, décrivent les conditions générales d'utilisation du service de Cachet simple et Avancée, que la Banque populaire offre à ses entités clientes notamment les Banques Populaires Régionales (BPR) et ce conformément aux exigences de la loi 43-20. Toute utilisation des services proposés suppose la consultation et l'acceptation préalable et sans réserve des présentes conditions Générales d'utilisation.

2. DEFINITION ET ACRONYMES

AC : Autorité de certification

AE : Autorité d'enregistrement

MC : Mandataire de certification

RCC : Responsable du certificat Cachet

IGC : Infrastructure de gestion des clés

PC : Politique de certification

LAR : Liste des Autorités révoqués

LCR : Liste des certificats révoqués

Autorité de certification (AC) - Au sein d'un Prestataire de Service de Certification Électronique (PSCE), une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuier" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et le terme d'AC est le seul utilisé.

Autorité d'enregistrement (AE) - Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat de celui-ci.

Infrastructure de Gestion de Clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Liste des Autorités Révoquées (LAR) - Liste contenant les

Identifiants des certificats d'autorités subordonnées révoquées ou invalides.

Liste des Certificats Révoqués (LCR) - Liste contenant les identifiants des certificats révoqués ou invalides.

Mandataire de certification (MC) - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des **RCC** et des serveurs informatiques de cette entité (il assure notamment le face-à-face pour l'identification des RCC lorsque celui-ci est requis)

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles un AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs, les responsables de certificats et les utilisateurs de certificats.

Le porteur de certificat est la personne physique représentant une personne morale identifiée dans le certificat. C'est la personne qui va en faire usage : signer et cacheter des documents selon le certificat électronique choisi, quand le porteur est non humain c'est le terme cachet qui est utilisé.

Responsable du certificat de cachet (RCC) - La personne physique responsable du certificat de cachet, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat.

Utilisateur de certificat - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du porteur du certificat.

3. OBJET

Ces CGUs ont pour but de détailler les conditions d'utilisation du service de signature électronique utilisé par la banque pour ses clients dans le cadre de la « Dématérialisation de l'ouverture de compte » au niveau des agences CPM, et également pour les besoins de signature électronique des clients des partenaires conformément à la politique de certification et politique de signature associée.

L'OID de la présente CGU est 1.2.504.1.1.2.1.3.10.5

Les certificats émis par l'AC Chaabi - eSign Seals CA sont des certificats cachet au nom de personnes morales destinés aux BPR et autres entités clientes et sont hébergés sous formats X.509 au sein des HSMs de la BCP.

4. Contact de l'Autorité de Certification BCP

Les demandes d'informations ou commentaires sur ces CCGU doivent être adressés au responsable de l'IGC à l'adresse suivante :

responsablepki@groupebcp.com

Banque Centrale Populaire Angle Mohamed El Bakri & Angle
Mohamed Diouri Casablanca Maroc

5. Acceptation des C.G.U

Le RCC, l'Utilisateur du Certificat et le porteur reconnaissent avoir lu, et approuvé les CGU ainsi que la PC de l'AC « Chaabi – eSign Seals CA », acceptent leur contenu et reconnaissent être liés par la totalité des dispositions y afférentes.

- Disposer de la compétence et des moyens nécessaires pour utiliser les Certificats.
- Avoir pris connaissance de la nature, et des modalités d'utilisation des Certificats.

6. ENTREE EN VIGUEUR

Le Contrat est conclu à compter de la signature du formulaire de nomination du RCC et de demande de certificat qui engendre la validation effective du dossier du demandeur par la BCP.

Le Contrat est constitué de :

La politique de certification accessible sur le lien suivant

- http://www.gbp.ma/Documents/PC_Chaabi_eSign_Seals_CA.pdf
- La politique de signature et gestion de preuve http://www.gbp.ma/Documents/Politique_Signature_Gestion_de_preuve_CPM_Digital.pdf
- Formulaire de nomination RCC Et Demande de certificats signés

La durée de vie du Certificat est de 3 ans à compter de la date de l'émission du certificat.

7. DEMANDE DE CERTIFICAT

L'AE de la BCP met à disposition des BPRs et entités clientes le formulaire de demande de certificat et /ou de nomination, de renouvellement de RCC

Un certificat est demandé par un représentant légal de l'entité ou un

MC dûment mandaté pour cette entité, et ce avec le consentement préalable du futur RCC.

Les informations suivantes doivent au moins faire partie de la demande de certificat :

- Le nom du service de création de cachet à utiliser dans le certificat ;
- Les données personnelles d'identification du RCC ;
- Les données d'identification de l'entité (sauf si l'enregistrement est effectué par l'intermédiaire d'un MC).
- Le dossier de demande est établi soit directement par le futur RCC à partir des éléments fournis par son entité, soit par son entité et signé par le futur RCC.
- Si l'entreprise n'a de MC, le dossier est transmis directement à l'AE de la BCP.

Si l'entreprise a mis en place un MC, le dossier lui est remis. Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le MC ou le futur RCC du certificat

8. RENOUELEMENT

Le RCC et/ou le MC est informé de l'expiration du certificat par mail au moins 3 mois avant l'expiration.

La procédure de renouvellement mise en place est la suivante :

- Révoquer le certificat précédent ;
- Faire une nouvelle demande de certificat conformément au processus initial.

9. CONDITIONS D'USAGE

En acceptant les conditions décrites dans le présent document, l'utilisateur reconnaît que le certificat est uniquement à usage de « Signature » et ne peut être utilisé que dans le cadre de la signature électronique comme précisés dans les politiques de certification associées aux certificats et la politique de signature et gestion de preuve que ce dernier ne soit en mesure de proposer une solution alternative en cohérence avec la PC, la responsabilité de la BCP sera limitée au remboursement du prix d'achat du service consommé par le Client.

10. REVOCATION DU CERTIFICAT

Les personnes pouvant demander la révocation d'un certificat de cachet sont les suivantes :

- Le MC
- Le RCC

Un représentant légal de l'entité

La demande de révocation se fait par mail à l'adresse suivante
responsablepki@groupebcp.com

Le demandeur de la révocation doit fournir les informations suivantes :

- Le nom du service qui utilise le cachet, informations à faire figurer dans le certificat ;
- Le nom et Prénom du demandeur de la révocation en plus d'un justificatif montrant sa capacité de pouvoir faire la demande.
- Le numéro de série du certificat et toutes autres informations permettant de retrouver rapidement et sans erreur le certificat à révoquer ;
- La cause de la révocation

11. LIMITES D'USAGES

Les certificats cachets émis par l'AC Chaabi -eSign Seals CA ne sont utilisables qu'à des fins de signature au nom de la personne morale identifié dans le certificat et ce Les certificats sont émis pour une durée de 3 ans ;

Les certificats cachet ne doivent pas être utilisé dans les circonstances suivantes

- S'ils ont été révoqués ;
- Si l'Autorité de certification émettrice est en cessation d'activité ;
- Signer des documents ou données autres que ceux générés par les applications identifiées et autorisées et ce uniquement dans le cadre du service de signature électronique fourni par la BCP

12. OBLIGATIONS Du PSCo

Le PSCo s'engage à mettre en œuvre les moyens nécessaires pour :

- Faire évoluer l'OID en cas d'évolution de sa PC.
- Que l'AE contrôle l'identification du Porteur se présentant physiquement pour l'enrôlement ;
- S'assurer, lors de l'enregistrement, que les informations et documents dont elle dispose sont de nature à établir l'identité du futur signataire
- créer et émettre des Certificats contenant des informations réputées exactes au porteur
- Procéder à la Révocation des certificats dès lors que la demande de Révocation est effectuée dans les conditions
- Assurer la publication sous format électronique de la

version en vigueur de la PC et des présentes Conditions Générales d'utilisation,

- Assurer la publication sous format électronique de la LCR.
- Informer dans les plus brefs délais en cas de Compromission de la Clé Privée de l'AC, et par tout moyen l'ensemble des Porteurs concernés que leurs Certificats ne sont plus valides.
- fournir au Client toute la documentation nécessaire à l'utilisation du Certificat.

13. OBLIGATIONS DU CLIENT

- Le Client, ou le Porteur s'engage à respecter les stipulations des CGU
- Le Client s'engage à fournir toutes informations utiles, exactes pour la création et la gestion des Certificats pour la Signature.
- Le Client est garant de l'exactitude des informations fournies et de l'exhaustivité des pièces justificatives nécessaires à l'enregistrement des. Le Client reconnaît et accepte que les informations fournies à ce titre soient conservées et utilisées par BCP pour gérer les Certificats dans les conditions prévues par la loi et en particulier celles relatives à la protection des données personnelles.

14. PRIX ET FACTURATION

Le prix est déterminé dans les conditions tarifaires émises par la Banque Populaire et communiqués aux Clients (partenaire)et annexé au présent document.

15. ETENDUE DES

RESPONSABILITES

Le Client demeure à l'égard de la BCP, le seul responsable du respect des droits au titre des documents contractuels ainsi que du bon accomplissement de leurs obligations.

La BCP ne pourrait en aucun cas être tenue responsable dans le cas d'un non-respect par le Client, le Porteur de leurs obligations notamment en cas de :

- Demande de Révocation tardive auprès de l'AE ;
- Utilisation d'un Certificat dans le cadre d'une application ou transaction autre que celles prévues aux termes de la PC et des documents contractuels

La BCP n'endosse aucune responsabilité au titre des conséquences liées à des retards, altérations ou pertes que pourraient subir le Client

dans la transmission de tous messages électroniques, lettres ou documents. De même, la BCP n'assume aucune responsabilité quant aux conséquences liées à la Révocation d'un Certificat

16. ASSURANCE

BCP atteste avoir souscrit une assurance Responsabilité Civile et Professionnelle concernant les prestations résultant de son activité de PSCo

Aux termes du contrat d'assurance souscrit par BCP et dans les limites et conditions de ce contrat, si le Client subit un dommage direct suite à une faute professionnelle de la BCP ou de ses préposés dument prouvée, le Client est dédommagé à la hauteur du prix du Certificat et du Support cumulé.

17. CONFIDENTIALITE

Toutes informations ou toutes données communiquées par les Parties par écrit relativement au service de signature électronique sont considérées comme confidentielles

Toutes informations ou toutes données communiquées par les Parties par écrit relativement aux Certificats sont considérées comme confidentielles (ci-après « Informations Confidentielles »).

- La Clé Privée du Certificat,
- Le code d'activation de la Clé Privée,
- Les données collectées dans le cadre de la demande de certificat

Les Parties s'engagent à :

- Traiter les Informations Confidentielles avec le même degré de protection qu'elles accordent à leurs propres informations confidentielles de même importance ;
- Garder les Informations Confidentielles et qu'elles ne soient pas divulguées ni susceptibles de l'être directement ou indirectement à tout tiers
- Éviter que les Informations Confidentielles ne soient ni copiées, ni reproduites, ni dupliquées, en partie ou en totalité, lorsque de telles copies, reproductions ou duplications ne sont pas directement liées à l'exécution des présentes

18. PROPRIETE INTELLECTUELLE

La souscription au service de signature électronique Chaabi -eSign Signature ne donne aucun droit de propriété aux Clients. Ces derniers s'engagent à respecter et à faire respecter les droits d'auteur et de propriété intellectuelle et industrielle de la BCP qui est seul

propriétaire des noms, logos, marques ou tout autre signe distinctif lui appartenant.

A l'exception de l'utilisation des Certificats prévue par les CGU, le Client et le Porteur ne pourront faire état ou usage des marques, logos, documents ou tout autre droit de propriété intellectuelle appartenant à la BCP qu'avec l'autorisation expresse, écrite et préalable de celle-ci

19. DONNEES A CARACTERE

PERSONNEL

BCP reconnaît que les obligations visées au premier paragraphe de l'article 23, de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, lui incombent également.

Les données personnelles ne peuvent faire l'objet d'une opération de traitement de la part de la BCP d'une personne placée sous son autorité ou d'un de ses sous-traitants, que sur instruction des personnes concernées, sauf en vertu d'obligations légales.

Ainsi, BCP ne peut traiter les données à caractère personnel que pour la production, la fourniture, et la gestion des Certificats électronique et les services y afférents notamment la signature électronique simple et avancée.

Les données à caractère personnel sont les informations nominatives de la personne concernée enregistrées au sein du dossier d'enregistrement, et du portail d'enrôlement sur le certificat électronique et sur tous les supports de traitement de la gestion du cycle de vie du certificat.

Des procédures techniques, fonctionnelles et organisationnelles sont mises en place pour assurer la protection des données à caractère personnel à partir de l'enregistrement du dossier et pendant toutes les étapes de gestion du cycle de vie des Certificats.

Toute collecte de données à caractère personnel par BCP dans le cadre de son activité de PSCE est réalisée dans le strict respect de la loi 09-08 relative à la protection des données personnelles.

Toute personne relevant de la BCP qui, dans l'exercice de ses fonctions, aurait connaissance de données à caractère personnel traitées, est tenue de respecter le secret professionnel même après avoir cessé d'exercer fonctions, dans les termes prévus par les lois en vigueur.

20. RESILIATION

Dans le cas où l'une des Parties n'exécute pas l'une quelconque de ses obligations en vertu des présentes Conditions Générales, l'autre Partie lui notifiera d'exécuter ladite obligation. Si la Partie

défaillante ne remédie pas à son manquement dans un délai de trente (30) jours suivant la réception de cette notification, l'autre Partie pourra résilier le Contrat sans préjudice d'éventuels dommages-intérêts qu'elle pourrait réclamer.

Si la Partie défaillante remédie à son manquement dans le délai de trente jours, elle pourra être tenue au règlement des dommages-intérêts de retard.

En cas de résiliation anticipée pour un motif non imputable à la BCP le prix payé par le Client à la souscription reste acquis à la BCP

21. CONSERVATION DES ARCHIVES

La BCP conservera les documents relatifs à la preuve du contrôle d'identification des signataires pendant les délais prévus dans la Politique de Certification.

Les journaux d'évènement sont conservés sur site pendant une durée de 30 jours. Après leur génération, ils sont archivés et conservés pendant sept ans.

Les Certificats d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins cinq ans après l'expiration de ces Certificats.

22. NULLITE

Si une ou plusieurs clauses des CGUs sont tenues pour non valables ou déclarées comme telles par une loi, un règlement ou par suite d'une décision définitive d'une juridiction compétente, les autres clauses conserveront leur pleine validité sauf en cas de caractère indissociable avec la stipulation litigieuse

23. INTEGRALITE

Les Parties reconnaissent que la version en vigueur des Conditions Générales d'Utilisation, la version en vigueur de la PC et toutes les procédures organisationnelles représentent l'intégralité des accords entre elles à l'égard de la réalisation de l'objet des présentes, abrogent et changent tous accords et propositions antérieurs ayant le même objet quelle qu'en soit la forme, sous réserve des avenants ou annexes qui viendraient ultérieurement les modifier ou les compléter.

24. MODIFICATION DES DISPOSITIONS CONTRACTUELLES

La BCP peut être amenée à ajuster et à apporter des modifications aux dispositions des présentes Conditions Générales et des

documents contractuels relatifs au Certificat qui lui sembleraient nécessaires pour répondre aux évolutions techniques et commerciales de son offre et en vue de l'amélioration de la qualité des services de Certification ou qui seraient rendues nécessaires par la modification de la législation de la réglementation en vigueur. Les changements apportés à un document contractuel seront portés à la connaissance du Client par tout moyen, au moins un mois avant leur entrée en vigueur, le Client ayant alors la possibilité de résilier son Contrat en cas de désaccord

Le présent Contrat et l'ensemble des documents contractuels sont régis par la Loi marocaine. Tout litige relatif à la validité, à l'exécution ou à l'interprétation des présentes Conditions Générales ou des dispositions de l'intégralité des accords entre les Parties sera soumis à la compétence des tribunaux marocains du ressort de l'Autorité de Certification.

25. REGLEMENT DES LITIGES – TRIBUNAL

Les Présentes CGU, Politique de Certification est soumise au droit Marocain

Tout litige relatif à la validité, l'interprétation, l'exécution des présentes CGU et Politique de certification sera soumis aux tribunaux compétents du ressort du tribunal de Casablanca

26. AUDIT ET RÉFÉRENCE APPLICABLE

Un contrôle de conformité de la PC associée à ces CGU peut être effectué à tout moment, et sur demande du comité de pilotage PSCo de la BCP.