

1. PREAMBULE

Les présentes CGU, décrivent les conditions générales d'utilisation du service de délivrance de certificat de Signature simple et Avancée Chaabi eSign -Signature Cert, que la Banque populaire offre à ses clients 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. OBJET

Ces CGUs ont pour but de détailler les conditions d'utilisation du service de délivrance de certificat pour des besoins de signature électronique, les certificats peuvent être fournis, soit à des particuliers, soit à des professionnels, les certificats et les clés privées associées sont fournis sous format logiciel PKCS12 ou sur dispositif physique qualifié pour les certificats avancés, ils sont émis par l'AC « Chaabi eSign - Certs CA » placée sous l'AC Racine « Chaabi eSign – Root CA ». L'OID de la présente CGU est 1.2.504.1.1.2.1.3.10.6

3. DEFINITION

Les termes ci-dessous définis auront entre les Parties la signification suivante :

« Application Utilisatrice » : désigne les services applicatifs utilisant des Certificats émis par BCP pour des besoins de Signature électronique simple et avancé du Porteur « Autorité de Certification » ou « AC » : désigne l'entité émettrice des certificats. Elle est garante de la gestion des certificats délivrés (génération, diffusion, renouvellement, révocation.). Elle s'appuie pour cela sur une infrastructure technique :

AC désigne la BCP, personne morale en charge, au nom et sous la responsabilité, l'application d'une Politique de Certification et a qualité pour émettre des Certificats électroniques avancés et simples, au titre de cette Politique de Certification et de son agrément

« Bi-clé » : désigne le couple de clés composé d'une Clé Publique et d'une Clé Privée, généré dans le cadre d'une infrastructure de type PKI
Autorité d'enregistrement (AE) : constitue l'interface entre l'utilisateur et l'autorité de certification. Elle est chargée d'identifier de façon certaine les demandeurs ou les porteurs de certificat et de s'assurer que les contraintes liées à l'usage d'un certificat soient remplies.

L'AE est responsable de la vérification des informations d'identification du futur Porteur et/ou du Porteur d'un Certificat, ainsi qu'éventuellement d'autres informations spécifiques, avant de

transmettre la demande correspondante à l'A.C. Elle a également en charge, la -vérification des informations du Porteur lors du renouvellement du Certificat de celui-ci. transmettre la demande correspondante à la fonction adéquate de l'IGC ;

« Certificat » : document établi sous forme électronique attestant du lien entre les données de vérification de signature électronique et le signataire, attestant qu'une Bi-clé appartient au Client, à son mandataire, au porteur ou à l'Utilisateur du Certificat ou à l'élément matériel ou logiciel identifié dans le Certificat. Le Certificat est signé par l'Autorité de Certification ;

« Clé Privée » : désigne une clé mathématique que le Porteur doit conserver secrètement

« Clé Publique » : désigne une clé mathématique rendue publique et qui est utilisée pour vérifier la signature d'une donnée reçue ;

« Contrat » : ensemble contractuel constitué des présentes Conditions Générales d'Utilisation, du formulaire de demande ou de demande de renouvellement de Certificat ainsi que de la Politique de Certification, applicables à la date de conclusion du contrat., ainsi que des éventuels avenants à ce Contrat.

« Client » : désigne une personne morale / professionnelle/particulier signataire des présentes Conditions Générales d'Utilisation et du contrat d'achat de Certificats, qui habilite le Porteurs (personne physique) à utiliser des Certificats, lequel Porteur peut donner mandat à une autre personne physique afin de le représenter pour la gestion des Certificats.

« Compromission » : désigne la divulgation ou suspicion de divulgation ou de perte d'informations confidentielles résultant de la violation d'une mesure de sécurité et conduisant à une possible perte de confidentialité et/ou d'intégrité des données considérées ;

« Conditions Générales » ou CGU : désigne le présent document devant être signé par le Porteur et/ou le Client ou son Mandataire souhaitant acquérir des Certificats ou habiliter des Porteurs à les utiliser.

« Données Confidentielles » : désigne ensemble la Clé Privée du Certificat, le code d'activation de la Clé Privée, qui sont des données strictement personnelles au Client, le Mandataire et le Porteur qui devront être impérativement gardées secrètes ;

« Entité » : désigne toute autorité administrative ou entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations ;

Comme prestation. « Infrastructure de Gestion des Clés » ou « IGC » : désigne l'ensemble des composantes, fonctions et procédures dédiées

à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance ;

« LAR » : désigne la liste des Certificats d'Autorité de Certification révoqués ;

« Liste des Certificats Révoqués ou LCR » : désigne la liste des Certificats Révoqués. Cette liste contient les coordonnées des Certificats qui ont été révoqués ainsi que la date et l'heure du jour de la révocation desdits Certificats. Cette liste est accessible sur internet 24 heures sur 24 et 7 jours sur 7. Ces listes sont mises à jour régulièrement selon la Politique de Certification et à chaque révocation de Certificat. Le Client doit disposer d'internet pour la vérification de la validité de son Certificat.

Mandataire : désigne une personne, physique ayant par procuration du Représentant Légal, le pouvoir de faire l'acquisition de certificats ou de révoquer les Certificats utilisés par le(s) Porteur(s). A défaut de désignation expresse, le mandataire social est Mandataire. Le Mandataire doit être préalablement enregistré pour l'obtention d'un Certificat.

« OID » : désigne le numéro d'identifiant d'objet unique désignant la Politique de Certification de l'Autorité de Certification ;

« Politique de Certification » ou « PC » : désigne l'ensemble des règles et exigences, identifiées par un OID, auxquelles BCP se conforme dans le cadre des présentes et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes ;

Porteur : désigne la personne physique identifiée dans le Certificat et qui est le détenteur de la Clé Privée correspondant à la Clé Publique qui est dans ce Certificat ;

Prestataire de services de confiance (PSCO) : désigne la personne morale responsable de la gestion de Certificats électroniques tout au long de leur cycle de vie, vis-à-vis des Porteurs et Utilisateurs de ces Certificats.

Le PSCO est BCP « Représentant Légal » : désigne le représentant légal du Client, personne morale

« Révocation » : désigne l'action qui a pour but l'extinction de la validité d'un Certificat. Un Certificat qui a fait l'objet d'une révocation est inscrit sur la LCR

Services de confiance : Un service de confiance est un service électronique normalement fourni contre rémunération qui consiste : en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de

certificats relatifs à ces services; ou en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services.

« Signature Électronique » : désigne l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache, conformément à la législation applicable ;

« Support » : désigne le support physique contenant notamment le(s) Certificat(s) du Porteur.

« Utilisateur du Certificat » : désigne l'Entité ou la personne physique qui reçoit un Certificat et qui s'y fie pour vérifier une Signature Électronique provenant du Porteur.

Acceptation des C.G.U

Avant de signer électroniquement le Client reconnaît :

Avoir lu et approuvé les présentes CGU ainsi que la PC de l'AC « Chaabi eSign - Certs CA »

Avoir pris connaissance de la Politique de Signature et de Gestion de Preuve en vigueur

4. ENTREE EN VIGUEUR

Les présentes CGU sont applicables dès la première utilisation du service par un utilisateur et pour toute la durée d'utilisation des services.

Le Contrat est renouvelable par tacite reconduction pour une durée égale à la durée de vie du certificat demandé sauf non renouvellement adressé par l'une des Parties à l'autre Partie par lettre recommandée avec accusé de réception, trois mois avant la date d'échéance.

Les CGU sont opposables au Client dès leur signature impliquant l'acceptation pleine et entière des CGU et documents associés par le Client.

Le Contrat est constitué :

- Les Présentes CGUs
- La politique de certification accessible sur le lien suivant
- [http://www.gbp.ma/Documents/PC_Chaabi_eSign_Certs_C A.pdf](http://www.gbp.ma/Documents/PC_Chaabi_eSign_Certs_CA.pdf)

5. 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 la politique de certification associée. Le Porteur s'engage à utiliser les Certificats et les Supports Physiques cas d'un certificat avancé sur des postes informatiques répondant aux

spécifications minimales figurant dans la procédure d'installation des Certificats.

Le Client reconnaît pleinement que ces spécifications minimales pourront être mise à jour. Toutefois, si malgré les dispositions et tests mis en œuvre afin que les Certificats et Supports Physiques distribués fonctionnent sur les configurations minimales indiquées par les fabricants de ces Supports Physiques, ils ne fonctionnaient pas, ceci sans aucune faute imputable à et sans que ce dernier ne soit en mesure de proposer une solution alternative en

6. 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 du dossier, 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.

7. OBLIGATIONS DU CLIENT

Le Client et son Mandataire sont responsables de la gestion des Certificats délivrés aux employés, délégataires ou agents du Client dans le cadre du Contrat et s'engagent à faire en sorte que tout Porteur de Certificat respecte les obligations prévues par les CGU et qu'aucune fraude ou erreur n'est commise. A ce titre, le Client et son Mandataire s'assurent notamment que le Porteur :

- N'utilise pas les Certificats à des fins personnelles ;
- Communique les informations utiles à la création du Certificat

- Respecte la procédure de Révocation décrite dans les présentes CGU ;

Conserve et de manière sécurisée, les données confidentielles et le Support Physique du Certificat.

Le Client et son Mandataire s'engagent à fournir toutes informations utiles, exactes et à jour pour la création et la gestion des Certificats.

Le Client et le Mandataire s'engagent à informer l'AE de toute modification des informations contenues dans le Certificat, par courrier avec les pièces justificatives requises, dans un délai de 30 jours à compter de leur survenance. A défaut, BCP se réserve le droit, le délai écoulé, de Révoquer le Certificat et résilier le Contrat.

Le Client et le mandataire sont garants de l'exactitude des informations fournies et de l'exhaustivité des pièces justificatives nécessaires à l'enregistrement des Certificats.

Le Client et son le mandataire reconnaissent et acceptent 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.

Le Client s'engage à payer le prix convenu dans les conditions prévues

8. OBLIGATIONS DU PORTEUR

Le Porteur s'engage à fournir toutes informations utiles, exactes et à jour pour la création et la gestion du Certificat.

Le Porteur est garant de l'exactitude des informations fournies et de l'exhaustivité des pièces justificatives nécessaires à l'enregistrement du Certificat

Le Porteur reconnaît et accepte que les informations fournies à ce sujet soient conservées et utilisées par BCP pour la gestion du cycle de vie de son Certificat dans les conditions prévues par la loi et en particulier celles relatives à la protection des données personnelles.

Le Porteur reconnaît être informé des conditions d'installation du Certificat et de la procédure d'installation fournie à ce titre.

Le Porteur s'engage à respecter les usages autorisés des Bi-clés et des Certificats.

Le Porteur s'engage à protéger son Support Physique ou logiciel contenant son Certificat par ses propres moyens.

Il s'engage également à ne pas communiquer à un tiers son code PIN.

Le Porteur respecte les conditions d'utilisation de sa Clé Privée et du Certificat correspondant.

Le Porteur doit faire, sans délai, une demande de Révocation de son Certificat en cas de Compromission ou de suspicion de Compromission de sa Clé Privée.

Le Porteur s'engage à ne pas délivrer le Certificat qui lui est attribué et

divulguer les codes de protection de ce Certificat.

Le Porteur est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de Révocation.

9. OBLIGATIONS DES

UTILISATEURS DE CERTIFICATS

Les Utilisateurs de Certificats s'engagent à respecter les stipulations des CGU.

Les Utilisateurs de Certificats respectent l'usage pour lequel un Certificat a été émis.

Pour chacun des Certificats de la chaîne de Certification, du Certificat du Porteur jusqu'à l'Autorité de Certification racine, les Utilisateurs du Certificat vérifient l'état du Certificat et notamment la signature numérique de l'AC Chaabi eSign – Certs CA de BCP, émettrice du Certificat considéré, et contrôlent la validité de ce Certificat.

Les Utilisateurs de Certificats vérifient et respectent les obligations des Utilisateurs de Certificats exprimés dans la PC applicable.

10. 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.

Les modes de règlement acceptés sont les suivants :

- Carte Bancaire
- Virement
- Chèque

Le prix du Certificat et du Support sont réglés par le Client dès réception de la facture qui correspond à la validation du dossier de demande de Certificat.

Le Client reconnaît expressément que le prix du service est dû en totalité nonobstant la Révocation du Certificat avant son terme, quelle que soit la cause de la Révocation.

Toutefois l'AC reconnaît engager sa responsabilité en cas d'erreur technique, faute ou négligence, de sa part ou de l'une de ses composantes, et procédera à la révocation du certificat et la génération d'un autre à ses propres frais.

Le Client reconnaît expressément que le prix du service est dû en totalité nonobstant la Révocation du Certificat avant son terme, quelle que soit la cause de la Révocation.

Toutefois l'AC reconnaît engager sa responsabilité en cas d'erreur technique, faute ou négligence, de sa part ou de l'une de ses

composantes, et procédera à la révocation du certificat et la génération d'un autre à ses propres frais.

11. 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

12. 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.

13. CONFIDENTIALITE

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

14. 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

15. 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 PSCO 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.

16. 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

17. 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.

18. 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

19. 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.

20. 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.