

Conditions d'utilisation des solutions de paiement mobile

1. Champ d'application/Aperçu des prestations

Les présentes conditions s'appliquent lorsqu'une carte de débit ou un moyen de paiement ayant la même finalité (ci-après «**carte**») de Credit Suisse AG ou de Credit Suisse (Suisse) SA (ci-après «**banque**») sont déposés et utilisés électroniquement dans une solution de paiement mobile (ci-après «**Wallet(s) mobile(s)** »).

Les conditions d'utilisation sont considérées comme ayant été acceptées dès que le client s'est enregistré via le Wallet mobile (cf. ch. 2).

Les conditions contractuelles du fournisseur respectif (ci-après «**fournisseur**») s'appliquent au Wallet mobile, à l'appareil sur lequel le Wallet mobile est utilisé et, le cas échéant, aux comptes numériques utilisés par le client de la banque et par les utilisateurs autorisés par ses soins d'une carte, telle que, p. ex., une carte de partenaire (ci-après «**utilisateur**»). La banque n'est pas le fournisseur de la solution de paiement mobile: elle permet uniquement à l'utilisateur de déposer sa carte dans le Wallet mobile du fournisseur en tant que moyen de paiement. La banque n'a aucune influence sur le fonctionnement, la disponibilité ou l'étendue des fonctions du Wallet mobile auquel le fournisseur concerné peut apporter des modifications conformément à ses propres conditions contractuelles. Ceci comprend également la possibilité qu'a le fournisseur de limiter et/ou de suspendre temporairement ou définitivement la possibilité d'utilisation du Wallet mobile. Tout droit à un Wallet mobile en état de fonctionnement est donc, en tout état de cause, exclu vis-à-vis de la banque.

Les présentes conditions complètent les autres dispositions applicables à la relation contractuelle entre la banque et l'utilisateur, en particulier les Conditions générales en vigueur de la banque et les Conditions applicables aux cartes de débit (consultables à l'adresse suivante: www.credit-suisse.com/ch/fr/legal.html). En cas de dispositions contradictoires, les présentes conditions prévalent sur d'autres conditions contractuelles de la banque.

La banque se réserve à tout moment le droit de modifier les présentes conditions. Les modifications seront portées à la connaissance de l'utilisateur sous une forme appropriée et seront considérées comme approuvées si, au moment de l'entrée en vigueur de la modification, l'enregistrement d'une carte de l'utilisateur existe conformément au ch. 2.

2. Inscription

Un Wallet mobile ne peut être utilisé pour le paiement sans espèces par carte (ci-après «**transaction Wallet mobile**») qu'après que cette carte a été inscrite dans le Wallet mobile respectif.

Pour l'inscription, l'utilisateur est invité à indiquer le nom figurant sur la carte, le numéro de la carte, la date d'expiration, le code de vérification de la carte (CVV, CVC) et d'éventuelles données supplémentaires exigées par l'opérateur du Wallet mobile (ci-après «**données de la carte**»). Celles-ci doivent être saisies manuellement, le cas échéant au moyen d'une lecture des données de la carte par caméra ou d'autres procédés de lecture automatique des données de la carte, par exemple via une application (fonction In-App Provisioning) ou de toute autre manière selon la réglementation de l'opérateur du Wallet mobile. Après la saisie complète des données de la carte, diverses vérifications sont effectuées par le réseau de cartes mondial, p. ex., Mastercard (ci-après «**société de réseau de cartes**»), l'opérateur du Wallet mobile, la banque ou son prestataire de services.

Une fois ces vérifications effectuées, des démarches supplémentaires en vue de l'authentification de l'utilisateur peuvent avoir lieu. L'achèvement réussi de l'inscription est confirmé à l'utilisateur par la banque, soit directement dans le Wallet mobile, soit par SMS ou de toute autre manière. La banque est libre de refuser l'inscription de la carte sans indication de motifs.

Après avoir procédé avec succès à l'inscription de la carte, un numéro de carte numérique est généré (ci-après «**numéro de carte numérique**») et déposé dans le Wallet mobile (ci-après «**dépôt électronique**»).

3. Transaction Wallet mobile et approbation de la transaction

Un Wallet mobile peut être utilisé par le client comme moyen de paiement dans le commerce stationnaire, dans des dispositifs automatiques, dans des boutiques en ligne et dans des applications chez un commerçant ou un prestataire de services acceptant le Wallet mobile comme moyen de paiement (ci-après «**commerçant**»).

La manière et le moment où une transaction est considérée comme approuvée (p. ex. via la saisie d'un NIP ou de données biométriques telles que le scan d'empreintes digitales ou la reconnaissance faciale, ou par la simple utilisation de l'appareil) sont déterminés par les directives des fournisseurs.

Le client est conscient du fait et reconnaît que toute personne qui se légitime en accédant au terminal et en utilisant le Wallet mobile (p. ex. en saisissant le code approprié) et/ou qui confirme une transaction via le terminal, qui dépose le Wallet mobile comme mode de paiement auprès de commerçants ou qui utilise le Wallet mobile de toute autre manière, est, vis-à-vis de la banque, considérée comme étant en droit d'effectuer des transactions avec le Wallet mobile. Cela vaut même si cette personne n'est pas le propriétaire effectif du terminal.

4. Devoir de diligence du client

Lors de l'utilisation du Wallet mobile, le client doit respecter les obligations de diligence suivantes:

- a. L'utilisateur doit prendre les mesures nécessaires pour protéger son terminal contre toute utilisation ou manipulation non autorisée (p. ex. verrouillage de l'appareil ou de l'écran).
- b. L'utilisateur doit garder ses moyens de légitimation personnels secrets. Il ne doit pas transmettre ses moyens de légitimation à des tiers. Aucun moyen de légitimation de tiers (p. ex. données biométriques – telles que les empreintes digitales – d'un tiers) ne doit être enregistré sur l'appareil respectif pour le déverrouillage ou dans le Wallet mobile.
- c. S'il y a des raisons de croire que des personnes non autorisées ont accès au code de verrouillage de l'appareil ou de l'écran, les moyens de légitimation pour le verrouillage de l'appareil ou de l'écran doivent alors immédiatement être modifiés.
- d. En cas de perte ou même de simple suspicion de perte du terminal, notamment en cas de vol, il convient d'en faire immédiatement le signalement afin que le numéro de carte numérique puisse être bloqué. L'utilisateur doit en outre immédiatement bloquer la carte SIM (ou la faire bloquer par l'opérateur de réseau) et si possible, faire également bloquer l'appareil par le fabricant.
- e. Toute neutralisation des structures de sécurité via l'installation d'applications ou d'un système d'exploitation non officiellement disponibles (jailbreak) ou toute autre manipulation similaire sur le terminal (p. ex. configuration d'un accès au niveau système du terminal) ainsi que toute installation d'applications non autorisées par le fournisseur du système d'exploitation (p. ex. car celles-ci rendent le terminal plus vulnérable aux virus et logiciels malveillants) est proscrite. Toute manipulation entreprise sur le terminal se fait aux risques et périls de l'utilisateur et sous sa responsabilité, et toute responsabilité de la banque pour des dommages consécutifs ou liés à ladite manipulation est exclue.
- f. Le client est tenu, avant la transmission (temporaire ou durable) de l'appareil (p. ex. vente, cadeau, prêt, consignation, mise en gage, réparation), de supprimer toutes les données de la carte et de transactions.
- g. S'appliquent également les devoirs de diligence et d'information prévus dans les Conditions applicables aux cartes de débit ainsi que dans les conditions contractuelles de l'opérateur du Wallet mobile applicables à l'utilisateur.

L'utilisateur ou le client de la banque assume la totalité des risques et conséquences découlant de l'utilisation – même abusive – de tout Wallet mobile (p. ex. par des personnes non autorisées ou à des fins non autorisées). La prise en charge d'un dommage conformément aux conditions applicables aux cartes de débit demeure réservée.

5. Modifications de la carte ou du dépôt électronique

Le renouvellement, la résiliation, le blocage ou le déblocage de la carte se répercute en principe également sur son utilisation par le biais du Wallet mobile.

Le dépôt électronique peut – indépendamment de la carte émise physiquement – être révoqué, bloqué ou débloqué pour chaque appareil séparément et ne change rien au statut de la carte mais doit cependant, contrairement à ce qui est prévu dans les Conditions applicables aux cartes de débit, être effectué séparément pour chaque carte par le titulaire respectif du Wallet mobile. Les paiements effectués jusqu'au moment du blocage sont considérés comme validés et ne peuvent être annulés.

L'utilisateur peut, si cela est prévu par l'opérateur du Wallet mobile, mettre fin au dépôt électronique selon la réglementation et les instructions de l'opérateur du Wallet mobile (p. ex. via la suppression des données relatives à la carte dans le Wallet mobile). L'utilisateur peut, si cela est prévu par le fabricant de l'appareil, mettre fin au dépôt électronique en supprimant le Wallet mobile de l'appareil ou en restaurant l'appareil aux paramètres d'usine (suppression de toutes les données saisies par le client).

La banque se réserve le droit de mettre fin ou de restreindre en tout temps, en tout ou partie, sans indication de motifs, le dépôt électronique dans des Wallets mobiles spécifiques ou dans tous les Wallets mobiles.

6. Coût

Il incombe aux seuls titulaires de carte de s'assurer qu'ils disposent bien d'appareils compatibles capables de prendre en charge l'utilisation du Wallet mobile.

La totalité des coûts, frais et dépenses prélevés pour la téléphonie mobile et/ou pour des prestations de services de télécommunication en rapport avec l'installation et/ou l'utilisation du Wallet mobile sont à la charge de l'utilisateur ou du client de la banque.

7. Protection des données

Le traitement d'informations relatives au client, notamment les données du client, de la carte et des transactions ainsi que le numéro de carte numérique (ci-après «**données de clients**») est, par principe, régi par la Déclaration sur la protection des données de la banque, laquelle peut être consultée à l'adresse suivante: www.credit-suisse.com/ch/fr/legal.html.

Lors de l'inscription et de l'utilisation, des informations sur l'appareil, des données d'une carte SIM ou d'une carte mémoire et des géodonnées (ci-après collectivement «**données de l'appareil**») ainsi que des informations provenant de la relation d'affaires du client avec l'opérateur du Wallet mobile (également en sa qualité de fabricant de l'appareil ou d'opérateur d'un système d'exploitation installé sur l'appareil, ci-après «**données de l'opérateur du Wallet mobile**») peuvent également être traitées aux fins décrites dans les présentes conditions d'utilisation.

Dans le cadre de l'inscription, du renouvellement, de la résiliation, du blocage et du déblocage du dépôt électronique et/ou dans le cadre de transactions Wallet mobile, des données de clients ou de l'appareil ainsi que des données de l'opérateur du Wallet mobile peuvent être échangées entre la banque, l'opérateur du Wallet mobile et la société de réseau de cartes aux fins suivantes:

- contrôle de l'autorisation du dépôt électronique,
- vérification et comparaison de l'identité du client et du détenteur de l'appareil,
- prévention d'abus et d'escroqueries, et enquête à ce sujet,
- respect de dispositions du droit de la surveillance (p. ex. sanctions nationales/internationales),
- établissement ou mise à jour du numéro de carte numérique et comparaison d'informations quant au statut (renouvellement, résiliation, blocage ou déblocage, etc.) de la carte et du dépôt électronique,
- établissement d'un relevé des transactions passées dans le Wallet mobile (p. ex. informations sur le point d'acceptation, montant et date de la transaction).

Les conditions contractuelles de l'opérateur du Wallet mobile peuvent prévoir que les données mentionnées au présent chapitre peuvent être collectées, traitées et transmises par l'opérateur du Wallet mobile (y compris d'éventuels tiers) à d'autres fins. La banque n'est pas responsable de la collecte, du traitement et de la transmission de données par l'opérateur du Wallet mobile, la société de réseau de cartes ainsi que les tiers auxquels ceux-ci ont recours. Ces questions sont régies par leurs conditions contractuelles.

8. Transfert de données et communication électronique

L'utilisateur prend acte du fait que les opérateurs de Wallets mobiles, les sociétés de réseaux de cartes, les points d'acceptation ainsi que les tiers mandatés par ceux-ci ou par la banque peuvent se trouver à l'étranger et que des données peuvent être traitées dans le monde entier – y compris en dehors de l'Europe. Les données de clients et de l'appareil ainsi que les données de l'opérateur du Wallet mobile sont transmises en règle générale sous forme cryptée et/ou par le biais d'un canal sûr et, le cas échéant, dans le monde entier, lors de l'inscription, dans le cadre de modifications de la carte ou du dépôt électronique et lors de transactions Wallet mobile. Les communications de la banque destinées à une authentification supplémentaire de l'utilisateur ainsi que pour la confirmation de l'achèvement réussi de l'inscription sont toutefois transmises sans cryptage, par le biais d'un réseau ouvert, accessible à tous (p. ex. Internet, SMS).

La banque est autorisée à informer ou contacter l'utilisateur dans le cadre de l'inscription ou dans le but de communiquer des modifications des présentes conditions d'utilisation par SMS, par e-mail, par courrier postal, par pop-up dans le Wallet mobile ou par le biais d'autres moyens de communication.

L'utilisateur prend acte du fait que, par les communications non cryptées qui sont transmises par le biais d'un réseau ouvert, des tiers peuvent conclure à l'existence d'une relation contractuelle ou de toute autre relation juridique avec la banque, et qu'il n'est donc pas possible de partir du principe que la confidentialité de la communication et, par là même, le secret bancaire sont garantis. L'utilisateur prend notamment acte des risques suivants: lors de l'utilisation d'un réseau (p. ex. Internet), des virus informatiques et autres peuvent contaminer le terminal lorsque celui-ci communique avec le réseau. Le recours à des logiciels de sécurité disponibles sur le marché peut aider le client à mettre en œuvre des mesures de protection appropriées et est donc recommandé. Il existe un risque qu'un tiers accède au terminal à l'insu de l'utilisateur pendant l'utilisation en ligne. En outre, des lacunes dans la connaissance du système et des mesures de sécurité insuffisantes sur le terminal peuvent faciliter les accès non autorisés. Les opérateurs de réseau (p. ex. fournisseur d'accès à Internet) ont la possibilité d'établir quand et avec qui un utilisateur est entré en contact. Il est important d'utiliser uniquement des logiciels provenant de sources fiables.

Même lorsque l'expéditeur et le destinataire se trouvent dans le même pays, la transmission de données par le biais de tels réseaux s'effectue souvent en passant par des États tiers, c'est-à-dire également par des pays qui ne disposent pas du même niveau de protection des données que l'État de domicile de l'utilisateur ou que le lieu où ce dernier séjourne. Les données peuvent être perdues ou captées par des tiers non autorisés, manipulées et faire l'objet d'une utilisation abusive au cours de leur transmission ou l'identité de l'expéditeur peut être usurpée ou manipulée. La responsabilité de la banque ne saurait être engagée pour les dommages qui pourraient en résulter.

Aucun dispositif de sécurité, même issu des développements les plus récents de la technique, ne saurait garantir une sécurité absolue tant du côté de la banque que de celui de l'utilisateur. Le terminal de l'utilisateur fait partie intégrante du système mais il échappe au contrôle de la banque et peut, de ce fait, constituer un point faible du système. Malgré toutes les mesures de sécurité, la banque ne peut pas, pour des raisons techniques, assumer de responsabilité en ce qui concerne ce terminal.