CONDITIONS GENERALES DU SERVICE DE BANQUE EN LIGNE

acme Banque et Assurance offre à sa clientèle sur son site Web, et avec accord de la banque, un service en ligne, ci-après désigné le « Service », permettant à distance :

- La souscription de produits et services bancaires et extra bancaires,
- La consultation et la gestion de compte ainsi que la réalisation d'opérations bancaires

Dans les termes et conditions prévus dans les présentes.

Utilisation du Service

L'accès au service en ligne acme s'effectue à partir d'un terminal connecté au réseau Internet.

L'acquisition ou la location du terminal, son installation et sa maintenance ainsi que les frais d'accès et d'utilisation du réseau ne sont pas à la charge de acme.

Accès au service et règles de preuve

Les règles d'accès et de preuve du Service ont pour objet de préciser et définir les moyens mis à disposition du client pour effectuer un certain nombre d'opérations via les services de banque en ligne par Internet de acme. Dans ce cadre et afin de permettre l'utilisation de ses services en ligne, acme délivre des Authentifiants au client, dans les termes et conditions définis aux présentes.

Ces Authentifiants ont pour objectif de permettre au Client de réaliser les opérations telles que décrites ci-dessous dans les termes et conditions définis dans la présente convention :

- accéder au service, notamment pour consulter ses comptes,

- signer des transactions bancaires,

- signer des documents contractuels ou précontractuels (conventions, formulaires,…).

Cette convention relève des conditions générales du contrat de banque en ligne, ainsi que des Dispositions Générales de Banque clientèle des particuliers, des conditions générales propres à chaque convention de compte, contrats de produit ou service concernés.

Définitions

Les termes mentionnés dans la présente convention comportant une majuscule ou édités en caractères italiques sont définis comme ci-après :

Identification du client : procédure consistant à reconnaître le client dans les systèmes informatiques de acme à partir d'un identifiant.

Identifiant : élément communiqué au client par acme lui permettant de reconnaître le client de manière certaine.

Authentification du client : procédure consistant à vérifier par des moyens appropriés, ci-après définis comme des Authentifiants, l'identité déclarée par le client. L'authentification permet d'apporter la preuve de l'identité déclarée par le client lors de l'identification.

Authentifiants : éléments propres au client prenant la forme notamment d'un code personnel d'accès ou d'une clé privée associé à un certificat, permettant aux systèmes informatiques de acme de réaliser l'authentification en ligne dudit client. Cette liste n'est pas exhaustive. Les Authentifiants peuvent être amenés à évoluer dans le temps en fonction de l'état de l'art et de la technique, considérant que le client sera informé par tout moyen de toute évolution dans un délai d'un (1) mois à compter desdites modifications.

Certificat du client : document électronique contenant des éléments permettant d'identifier le client, attestant du lien entre le client et sa clé privée. Un certificat est signé électroniquement par acme en tant qu'autorité de certification ; acme atteste ainsi que le client dont l'identité est mentionnée dans le certificat, est en possession de sa clé privée.

Clé privée du client : document électronique personnel et confidentiel, propre au client, conservé sous le contrôle exclusif du client, sur son ordinateur ou tout autre support électronique de stockage de son choix qui lui est propre. Une clé privée est liée logiquement et de manière irrévocable au certificat correspondant.

Révocation : procédure consistant à déclarer le certificat du client et sa clé privée comme étant invalides, donc inutilisables. Les références du certificat sont alors publiées sur une liste des certificats révoqués : la responsabilité du client en cas d'utilisation frauduleuse du certificat révoqué est alors dégagée.

La révocation d'un certificat entraîne celle de l'ensemble des certificats délivrés par acme au client.

Certificat client valide : caractère d'un certificat en cours de validité (non révoqué) qui est signé électroniquement par acme, en tant qu'autorité de certification.

Le certificat client valide a une durée de vie déterminée.

Autorité de certification : L'Autorité de certification est une entité qui a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).

Une Infrastructure de Gestion des Clés (IGC): est un ensemble de composants et de procédures visant à gérer le cycle de vie des certificats électroniques.

Les fonctionnalités principales des IGC en ce qui concerne la gestion des certificats de clés publiques sont :

- l'enregistrement de demande et vérifications des critères d'attribution,
- la création des certificats électroniques et leur renouvellement,
- la diffusion des certificats,
- la gestion des listes de révocation,
- l'archivage des certificats.

Procédure de Délivrance des Authentifiants

Les Authentifiants délivrés par acme prennent la forme soit d'un Code personnel d'accès, soit d'un Certificat client valide.

Obligations à la charge des clients

Le client s'engage à respecter l'ensemble des règles de sécurité ci-après décrites, à savoir :

- respecter et mettre en œuvre les conseils de sécurité concernant ses moyens d'authentification communiqués sur le site Sécurité acme, notamment en mémorisant le code ou le *mot de passe* sans l'écrire, en ne le transmettant à personne et en conservant son certificat sur son ordinateur personnel,

- mettre en œuvre tous les moyens à sa disposition pour s'assurer que son ordinateur est raisonnablement sécurisé

La responsabilité de acme ne peut être engagée en cas de piratage et/ou utilisation frauduleuse des Authentifiants du client du fait d'une erreur de manipulation de la part du client, de la négligence de celui-ci, ou d'un virus affectant l'ordinateur utilisé. Le client est donc seul responsable du matériel informatique qu'il utilise, ainsi que de l'usage et de la conservation de ses Authentifiants qui lui sont personnels et dont il s'interdit de les transmettre à quiconque.

Utilisation des Authentifiants

Les clients peuvent utiliser les Authentifiants qui leur sont remis, dans les termes et conditions ci-après définies pour :

- accéder au service acme
- signer des transactions dites sensibles
- signer des documents précontractuels ou contractuels présentés par acme dans le cadre des relations liant le client à la banque

Signature de transactions sensibles

Après avoir accédé au service acme, le client a la possibilité d'effectuer un certain nombre d'opérations bancaires entrant dans le périmètre du contrat acme qu'il aura souscrit. En cas de saisie d'opérations par le client sur son compte ou celui de son mandant (notamment virement, …) un récapitulatif de l'opération demandée est présenté au client, avant sa prise en compte par acme, afin qu'il puisse la confirmer ou l'annuler.

Confirmation d'opération par signature électronique

Le récapitulatif de l'opération est présenté sous la forme d'un document au format texte, au sein d'une application de signature électronique qui prend en charge techniquement l'opération de signature électronique sur l'ordinateur du client. Le client prend connaissance du document présenté, puis s'il décide de confirmer et valider son opération, il choisit le certificat à utiliser pour signer la transaction. Il doit alors cocher la case ad hoc présentée sur son écran pour confirmer son consentement et cliquer ensuite sur le bouton « signer » avant de saisir sur son ordinateur le mot de passe de sécurité afférent audit certificat, pour en activer la clé privée. Le document est alors signé électroniquement puis renvoyé aux systèmes informatiques de acme.

Les systèmes informatiques de acme vérifient alors notamment :

- que le document signé n'a pas été modifié depuis sa signature électronique et que le client a bien été en possession de la clé privée correspondant au certificat joint au document,

- que le certificat du client est valide au moment de la réception du document signé par acme. Cette vérification est faite notamment en validant la signature apposée par acme sur le certificat présenté, en contrôlant ses dates de validité et en vérifiant son absence sur la liste des certificats révoqués,

- que le document signé par le client est bien celui qui lui a été présenté, sans modification, ajout ou suppression autre que l'apposition de sa signature.

L'opération demandée par le client est autorisée si ces conditions sont toutes vérifiées. Dans l'hypothèse contraire, elle sera refusée. Le document signé par le client, ainsi que les résultats de cette vérification et les éléments ayant permis de réaliser la vérification sont consignés dans des enregistrements techniques horodatés. Ces enregistrements sont techniquement contresignés par le système informatique de acme réalisant la validation de signature.

La signature électronique du client prend la forme d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du Code civil. Il est convenu entre acme et le client que la fiabilité de ce procédé est présumée jusqu'à preuve contraire.

Signature de documents contractuels ou précontractuels

Après l'accès au service (tel que décrit à l'article 4.1 des présentes), dans le cadre du service acme, il est donné au client la possibilité de souscrire à des produits ou services proposés par acme donnant lieu à signature de documents contractuels, le client pouvant par ailleurs être amené à accéder à des services nécessitant la signature de documents précontractuels tel des questionnaires ou des formulaires.

Dans les cas de figure précités, les systèmes informatiques de acme préparent un document à signer (suivant le cas une proposition commerciale, un document contractuel ou bien un formulaire à signer) sur lequel est apposé un cachet électronique de acme. Les systèmes informatiques présentent le document au client. Ce dernier peut alors en prendre connaissance, le compléter si cela est demandé et le cas échéant y consentir en apposant sa signature.

L'acte à signer est présenté sous la forme d'un document électronique au format PDF, au sein d'une application de signature électronique qui prend en charge techniquement l'opération de signature électronique sur l'ordinateur du client. Le client prend connaissance du document présenté, puis s'il décide de le signer, choisit le certificat à utiliser pour signer ledit document, coche une case pour confirmer son consentement et clique sur le bouton « signer ».

Le document est alors signé électroniquement au format PDF puis renvoyé aux systèmes informatiques de acme.

Les systèmes informatiques de acme vérifient alors notamment :

- que le document signé n'a pas été modifié depuis sa signature électronique et que le client a bien été en possession de la clé privée correspondant au certificat joint au document,

- que le certificat du client est valide au moment de la réception du document signé par acme. Cette vérification est faite notamment en validant la signature apposée par acme sur le certificat présenté, en contrôlant ses dates de validité et en vérifiant son absence sur la liste des certificats révoqués,

- que le document signé par le client est bien celui qui lui a été présenté, sans modification, ajout ou suppression autre que l'apposition de sa signature. Cette vérification est effectuée par la validation du cachet électronique apposé par acme.

Si ces conditions sont toutes vérifiées, un exemplaire du document est mis à disposition du client sous forme de document PDF comportant le cachet électronique acme ainsi que la signature électronique du client. Il peut le stocker sur son ordinateur, et également en réaliser une copie papier.

Si les conditions ne sont pas toutes vérifiées, l'acte est détruit et est considéré comme nul et non avenu.

Le document signé par le client, ainsi que les résultats de cette vérification et les éléments ayant permis d'en réaliser la vérification sont consignés dans des enregistrements techniques horodatés. Ces enregistrements sont techniquement contresignés par le système informatique de acme en charge de la validation de la signature.

DUREE ET MODIFICATION

Durée et conditions de résiliation

La convention de service acme est conclue pour une durée indéterminée et peut être dénoncée par l'une ou l'autre des parties, à tout moment, moyennant le respect d'un préavis de 15 jours suivant notification écrite.

La clôture du compte à l'initiative de l'une ou l'autre des parties, entraînera toutefois la résiliation de la convention, sans formalité ni délai, de même que le transfert du compte dans une agence acme du réseau physique.

Modifications

Le client peut demander d'apporter des modifications à sa convention (notamment liste des comptes, plafond des virements). Celles-ci seront effectives sous réserve d'acceptation par acme.

Le service peut être complété et ses conditions d'utilisation sont susceptibles d'évoluer en fonction notamment des progrès technologiques ou pour améliorer la qualité ou la sécurité des services.

Le client sera informé de ces évolutions par tout moyen et tout document approprié mis à sa disposition. Elles sont considérées comme acceptées, à défaut de résiliation de la convention dans le délai précité.

Signature de l'organisation