Définir et promouvoir l'excellence pour les services financiers mobiles

Sommaire

Introduction

Certification GSMA relative à l'argent mobile

La Certification GSMA des services d'argent mobile est une initiative globale visant à fournir des services financiers plus sécurisés, transparents et résilients aux millions d'utilisateurs des services d'argent mobile dans le monde.

Au cours de la dernière décennie, l'argent mobile est passé du stade de produit de niche dans quelques pays à celui de véritable phénomène de société dans les marchés émergents, car il offre des services financiers fiables à des populations qui n'étaient pas bancarisées auparavant. Un milliard de dollars sont désormais échangés chaque jour au niveau du secteur de l'argent mobile à travers 690 millions de comptes enregistrés dans le monde, ce qui en fait la plateforme de paiement principale de l'économie numérique dans de nombreux marchés émergents.

La confiance a été un élément essentiel du succès de l'argent mobile. La certification va permettre au secteur de passer à l'étape suivante en améliorant la qualité des services et la satisfaction des clients, en facilitant la mise en œuvre de partenariats de confiance, en établissant des relations de confiance avec les régulateurs et en encourageant la mise en œuvre de normes réglementaires adéquates et proportionnelles.

Contexte

La Certification GSMA des services d'argent mobile est le fruit de plusieurs années de collaboration entre GSMA et les entreprises du secteur de l'argent mobile, dans le but d'améliorer la confiance et la transparence des services. Suite à la publication du Code de conduite fin 2014, la GSMA a collaboré avec des prestataires en Afrique, en Amérique Latine et en Asie pour comprendre les défis présentés par leurs services et les meilleures pratiques sur ces marchés.

Pour développer les critères de certification, la GSMA a piloté un processus consultatif sur trois ans impliquant des prestataires d'argent mobile et des consultants experts indépendants. Les critères ont été définis et testés via les auto-évaluations de 39 prestataires d'argent mobile. En 2017, GSMA a fait appel à Alliances Management, une entreprise de gestion de systèmes de certification indépendante, pour gérer le projet.

Les avantages de la certification

Les entreprises certifiées sont à l'avant-garde du secteur de l'argent mobile. Elles ont prouvé leur sérieux vis-à-vis de la protection des droits des consommateurs, de la diffusion de services fiables et sécurisés, et de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Leurs pratiques commerciales sont parmi les meilleures du secteur.

La certification vise avant tout à améliorer la confiance et à responsabiliser les consommateurs afin qu'ils prennent des décisions plus éclairées concernant leurs services financiers. Elle encourage l'adoption de l'argent mobile et fait progresser l'inclusion financière. Elle garantit aux partenaires financiers potentiels la présence de contrôles renforcés, ce qui facilite l'interopérabilité et encourage l'intégration dans l'écosystème financier. Le potentiel en matière de collaboration, d'innovation et d'intégration avec les partenaires commerciaux sera également amélioré.

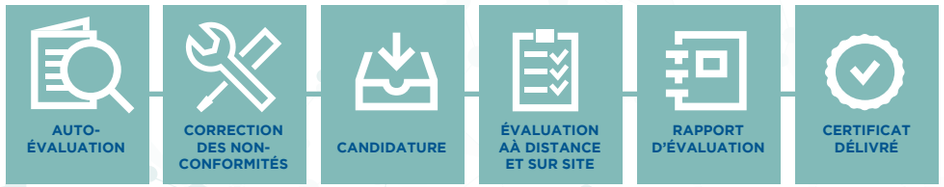
En définissant les meilleures pratiques du secteur, la certification vise à établir des relations de confiance avec les régulateurs et à encourager la mise en œuvre de normes réglementaires adéquates et proportionnelles. L'amélioration de la confiance vis-à-vis de l'argent mobile est dans l'intérêt commun du secteur privé, des gouvernements, des régulateurs et des consommateurs. La société dans son intégralité tirera parti de la numérisation des services financiers.

Les principes de la certification

La certification est fondée sur huit principes, eux-mêmes divisés en sous-principes, détaillés dans le corps de ce document. Les huit principes sont :

1.	**Finance :**	Protéger les fonds des clients contre le risque de perte
2.	**AML/CFT/Prevention de la fraude :**	Lutter contre le blanchiment de capitaux, le financement du terrorisme et la fraude
3.	**Personnes :**	Gérer correctement le personnel, les agents et les tiers
4.	**Opération :**	Garantir la bonne opération du service et sa fiabilité
5.	**Sécurité :**	Protéger la sécurité des systèmes supportant le service
6.	**Transparence :**	Communiquer les frais, les conditions générales et les informations de manière transparente aux clients
7.	**Service à la clientèle :**	Répondre de manière efficace aux demandes et aux plaintes des clients
8.	**Confidentialité des données :**	Protéger les données personnelles des clients

Le processus de certification



Pour plus d'informations sur la Certification GSMA des services d'argent mobile et le processus de certification, rendez-vous sur **gsmamobilemoneycert.com** ou contactez **mm@gsmamobilemoneycert.com**.

Principe 1 : Finance

Protéger les fonds des clients contre le risque de perte

1.1 Protection contre les pertes résultant de la défaillance d'une banque, d'un prestataire ou d'une autre partie

Les prestataires doivent prendre des mesures pour s'assurer que les fonds sont protégés en cas d'insolvabilité du prestataire, de la banque dépositaire ou d'une autre entité

1.1.1 Les prestataires doivent s'assurer que des sommes égales au montant total des engagements financiers correspondant à l'argent mobile en circulation sont conservées sur un ou plusieurs comptes de cantonnement pour le compte des utilisateurs de leur service d'argent mobile

1.1.2 Les prestataires doivent veiller à ce que les fonds des utilisateurs soient cantonnés afin d'empêcher leur saisie par les créanciers du prestataire en cas d'insolvabilité du prestataire

1.1.3 Les prestataires doivent prendre des mesures de prévention du risque de perte des fonds en cas d'insolvabilité de la banque, de l'émetteur obligataire ou de toute autre entité auprès de laquelle des fonds sont investis

1.2 Protection contre le risque de règlement

Les prestataires doivent prendre des mesures pour s'assurer que les fonds ne sont pas mis en danger en raison du processus de règlement avec des banques et autres partenaires financiers

1.2.1 Dans la mesure du possible, les prestataires n'autorisent que les opérations de client pour lesquelles le débit et le crédit des comptes d'argent mobile s'effectuent en temps réel

1.22 Les prestataires doivent régulièrement effectuer un rapprochement des transactions et régler leurs soldes auprès de leurs partenaires de l'écosystème financier*

* Dans le cadre de la Certification GSMA des services d'argent mobile, les « partenaires de l'écosystème financier » désignent les entités connectées au service d'argent mobile dans le but de fournir un service financier. Cela comprend par exemple, sans s'y limiter, les banques (banques dépositaires et autres établissements financiers détenteurs de comptes), les entités émettant ou recevant des paiements groupés, les agrégateurs, les commerçants utilisant des terminaux de point de vente, les prestataires de GAB et autres prestataires de services de paiement (nationaux ou internationaux).

Principe 2 : AML/CFT/Prevention de la fraude

Lutter contre le blanchiment de capitaux, le financement du terrorisme et la fraude

2.1 Effective AML/CFT policies and procedures
Les prestataires doivent élaborer des politiques et procédures efficaces pour lutter contre le blanchiment de capitaux et le financement du terrorisme (ML/FT)

2.1 Politiques et procédures AML/CFT efficaces
Les prestataires doivent élaborer des politiques et procédures efficaces pour lutter contre le blanchiment de capitaux et le financement du terrorisme (ML/FT)

2.2 Engagement de la direction générale à l'égard de la lutte contre le blanchiment de capitaux et le financement du terrorisme
La direction générale doit manifester son engagement à l'égard de la lutte contre le blanchiment de capitaux et le financement du terrorisme à travers une surveillance adaptée

2.3 Responsable désigné pour la lutte contre le blanchiment de capitaux et le financement du terrorisme (responsable de la lutte contre le blanchiment de capitaux)
Les prestataires doivent nommer une personne qualifiée chargée d'assurer la promotion et la surveillance du respect des obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme

2.4 Logiciel de surveillance des transactions
Les prestataires doivent mettre en place un système de surveillance des transactions pour letter contre le blanchiment de capitaux, le financement du terrorisme et la fraude

2.5 Vérification de l'indentité des clients (KYC) et plafonds d'opération et de solde de compte adaptés au niveau de risque
Les prestataires doivent obtenir des justificatifs d'identité, contrôler les clients et appliquer des plafonds d'opération et de solde de compte ou bloquer les opérations ou les comptes en fonction du niveau de risque

2.5.1 Les prestataires doivent dûment vérifier l'identité des clients

2.5.2 Les prestataires doivent appliquer des plafonds appropriés d'opération et de solde de compte en fonction du niveau de risque et des exigences de vérification et d'identification des clients

2.5.3 Les prestataires doivent pouvoir bloquer les opérations des comptes dans certaines circonstances

2.5.4 Les prestataires doivent passer tous les comptes au crible des listes nationales et internationales de sanction et de surveillance du blanchiment de capitaux et du financement du terrorisme

2.6 Procédures de formation du personnel et des agents à la lutte contre le blanchiment de capitaux et le financement du terrorisme
Les prestataires doivent former leur personnel et leurs agents aux procédures AML/CFT de lutte contre le blanchiment de capitaux et le financement du terrorisme, veiller au respect de ces procédures et prendre des mesures appropriées en cas de non respect

2.6.1 Les prestataires doivent veuiller à ce que leur personnel et leurs agents soient correctement formés aux procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme.

2.6.2 Les prestataires doivent veiller au respect des procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme par leur personnel et leurs agents

2.7 Gestion de la fraude
Les prestataires doivent développer des politiques et des mesures basées sur le risque afin de détecter et prévenir tout cas de fraude

Principe 3 : Personnes

Gérer correctement le personnel, les agents et les tiers

3.1 Politiques et procédures de vérifications préalables
Les prestataires doivent effectuer des vérifications préalables appropriées concernant leur personnel, leurs agents et les entités offrant des services de sous-traitance

3.2 Formation du personnel et des agents
Les prestataires doivent mettre en place des programmes de formation de leur personnel et de leurs agents

3.2.1 Les prestataires doivent développer et mettre en place des programmes de formation de leur personnel

3.2.2 Les prestataires doivent développer et mettre en place des programmes de formation de leurs agents

3.3 Accords contractuels
Les prestataires doivent mettre en place des accords écrits régissant leurs relations avec les agents et les entités fournissant des services en sous-traitance

3.3.1 Les prestataires doivent mettre en place des accords écrits régissant leurs relations avec les agents et les entités fournissant des services en sous-traitance

3.3.2 Les prestataires doivent assumer la responsabilité des actions effectuées en leur nom par leurs agents (et sous-agents éventuels) dans le cadre du contrat prestataire-agent

3.4 Gestion du personnel, des agents et des entités offrant des services de sous-traitance
Les prestataires doivent mettre en place des politiques et des procédures pour la gestion et la surveillance dans le temps de leur personnel, de leurs agents et des entités assurant des services de sous-traitance

Principe 4 : Opération du service

Garantir la bonne opération du service et sa fiabilité

4.1 Surveillance du service d'argent mobile par le conseil d'administration et la direction générale
Les prestataires doivent s'assurer que leur conseil d'administration et leur direction générale mettent en place un contrôle de gestion efficace

4.2 Gestion et suivi des niveaux de service
Les prestataires doivent gérer les activités commerciales et techniques en fonction des niveaux de service

4.2.1 Les prestataires et les partenaires doivent gérer l'opération des systèmes techniques de façon appropriée et gérer les niveaux de service

4.2.2 Les prestataires et les partenaires doivent gérer les opérations commerciales et les niveaux de service

4.3 Gestion des capacités
Les prestataires doivent prendre des mesures visant à s'assurer de l'adéquation des capacités de système et de réseau par le biais de prévisions, de mesures de surveillance et de tests

4.4 Gestion des incidents et des problèmes
Les prestataires doivent mettre en place un processus de gestion des incidents afin de restaurer le service conformément aux niveaux de service convenus et d'identifier les causes sous-jacentes des problèmes

4.5 Changement et gestion des configurations
Les prestataires doivent mettre en place des processus permettant de s'assurer que les systèmes et les applications restent robustes et sûrs à la suite de changements de système ou de configuration

4.6 Gestion globale des risques
Les prestataires doivent mettre en place un cadre de gestion du risque permettant la détection, l'évaluation et le contrôle des risques

4.7 Continuité de service
Les prestataires doivent mettre en place des plans efficaces de poursuite de l'activité en cas d'urgence ou de sinistre

Principe 5 : Sécurité

Protéger la sécurité des systèmes supportant le service

5.1 Gouvernance en matière de sécurité

Les prestataires doivent mettre en œuvre des mécanismes de gouvernance pour s'assurer que des politiques de sécurité soient définies et mises en œuvre dans le cadre d'une supervision continue

5.1.1 Les prestataires doivent définir et mettre en œuvre une politique formelle de sécurité des services d'argent mobile et l'examiner périodiquement

5.1.2 Les prestataires doivent former le personnel vis-à-vis de leurs responsabilités en matière de sécurité

5.1.3 Les prestataires doivent veiller à ce que des politiques soient en place pour assurer un traitement sécurisé des informations et des actifs

5.1.4 Les prestataires doivent assurer la protection des actifs accessibles aux fournisseurs ou à des tiers

5.2 Conception et mise en place d'un réseau, de systèmes et d'applications sécurisés

Les prestataires doivent s'assurer que le réseau, les systèmes et les applications utilisés pour l'argent mobile soient conçus et développés dans une optique de sécurité

5.2.1 Les prestataires doivent veiller à ce que les données soient protégées au moyen de la cryptographie et de systèmes de contrôle de la sécurité des réseaux

5.2.2 Les prestataires doivent s'assurer que les systèmes et les applications soient conçus et développés de façon sécurisée et fassent l'objet de tests rigoureux

5.3 Opérations de sécurité

Les prestataires doivent mettre en place des processus de gestion securisée de l'ensemble des systèmes

5.3.1 Les prestataires doivent identifier, évaluer et surveiller les risques en matière de sécurité

5.3.2 Les prestataires doivent correctement identifier et authentifier les utilisateurs du système du service d'argent mobile

5.3.3 Les prestataires doivent limiter l'accès aux données clients aux personnes qui en ont besoin

5.3.4 Les prestataires doivent restreindre l'accès physique aux systèmes

5.3.5 Les prestataires doivent s'assurer du fonctionnement correct et sécurisé du traitement des informations

5.3.6 Les prestataires doivent mettre en place des processus garantissant l'enregistrement de toutes les opérations et actions des utilisateurs avec des pistes d'audit appropriées

5.3.7 Les prestataires doivent effectuer des tests périodiques de leurs systèmes et de leurs procédures de sécurité

5.3.8 Les prestataires doivent assurer une sécurité continue des informations

5.3.9 Les prestataires doivent mettre en place un processus de détection, de traitement et de surveillance des incidents de sécurité et des réclamations liées à la sécurité

Principe 6 : Transparence

Communiquer les frais, les conditions générales et les informations de manière transparente aux clients

6.1 Communication efficace et transparente

Les prestataires doivent s'assurer que des informations claires, visibles et opportunes soient fournies aux clients concernant la tarification et les conditions générales du service

6.2 Éducation des clients concernant la sûreté et la sécurité

Les prestataires doivent éduquer les clients sur la manière d'utiliser les services d'argent mobile en toute sécurité

Principe 7 : Service à la clientèle

Répondre de manière efficace aux demandes et aux plaintes des clients

7.1 Politiques et procédures du service clientèle

Les prestataires doivent élaborer et publier les politiques et procédures relatives au service à la clientèle

7.1.1 Les prestataires doivent élaborer des politiques et procédures relatives au service à la clientèle

7.1.2 Les prestataires doivent informer les clients de l'existence de politiques et procédures relatives au service à la clientèle

7.1.3 Les prestataires doivent mettre en place des politiques spécifiques pour le traitement des annulations d'opération

7.2 Disponibilité de l'assistance à la clientèle

Les prestataires doivent mettre à la disposition de la clientèle un mécanisme approprié pour répondre aux questions et problèmes de celle-ci

7.3 Mécanismes de recours extérieurs

Les prestataires doivent spécifier un mode de résolution des litiges en cas d'échec des mécanismes internes

Principe 8 : Confidentialité des données

Protéger les données personnelles des clients

8.1 Gouvernance en matière de confidentialité des données

Les prestataires doivent se conformer aux bonnes pratiques et aux réglementations applicables en matière de confidentialité des données des clients

8.2 Transparence de la confidentialité des données

Les prestataires doivent veiller à ce que des informations claires, visibles et opportunes sont fournies aux utilisateurs sur les pratiques de protection de leurs données personnelles

8.3 Contrôle des données personnelles par les clients

Les prestataires doivent veiller à ce que les clients soient informés de leurs droits et qu'ils aient la possibilité d'exercer un véritable choix et contrôle sur les informations les concernant

8.4 Minimisation de la collecte et de la conservation de données

Les prestataires doivent limiter les informations personnelles collectées auprès des clients et conservées, utilisées ou partagées

Annexe : Définition de l'argent mobile

L'argent mobile est un service transformationnel qui utilise les technologies de l'information et de la communication pour élargir la diffusion de services financiers auprès de clients ne pouvant pas être touchés par les services financiers traditionnels distribués par le biais de succursales bancaires.

Un service est considéré comme Service d'argent mobile s'il répond aux critères suivants :

1. Le service doit permettre le transfert d'argent et le paiement à l'aide d'un téléphone portable.
2. Le service doit être disponible pour les personnes non bancarisées, par ex. les personnes n'ayant pas accès à un compte formel dans une institution financière.
3. Le service doit proposer au moins l'un des produits suivants :
   a) Transfert national ou international ;
   b) Paiement mobile, y compris les paiements de factures, les versements groupés et les paiements aux commerçants ;
   c) Stockage de valeur.
4. Le service doit fournir un réseau de points de transaction physiques en dehors des succursales bancaires et des GAB de manière à rendre le service accessible au plus grand nombre.

Services non considérés comme des Services d'argent mobile :

1. Les services bancaires mobiles qui utilisent le téléphone portable comme un canal supplémentaire pour accéder à un produit bancaire traditionnel.
2. Les services de paiement liés aux produits bancaires traditionnels ou cartes de crédit.

Pour plus d'informations sur la Certification GSMA des services d'argent mobile et le processus de certification, rendez-vous sur **gsmamobilemoneycert.com** ou contactez **mm@gsmamobilemoneycert.com**.

GSMA
MOBILE MONEY
CERTIFICATION