La monétique

(en 180 secondes)

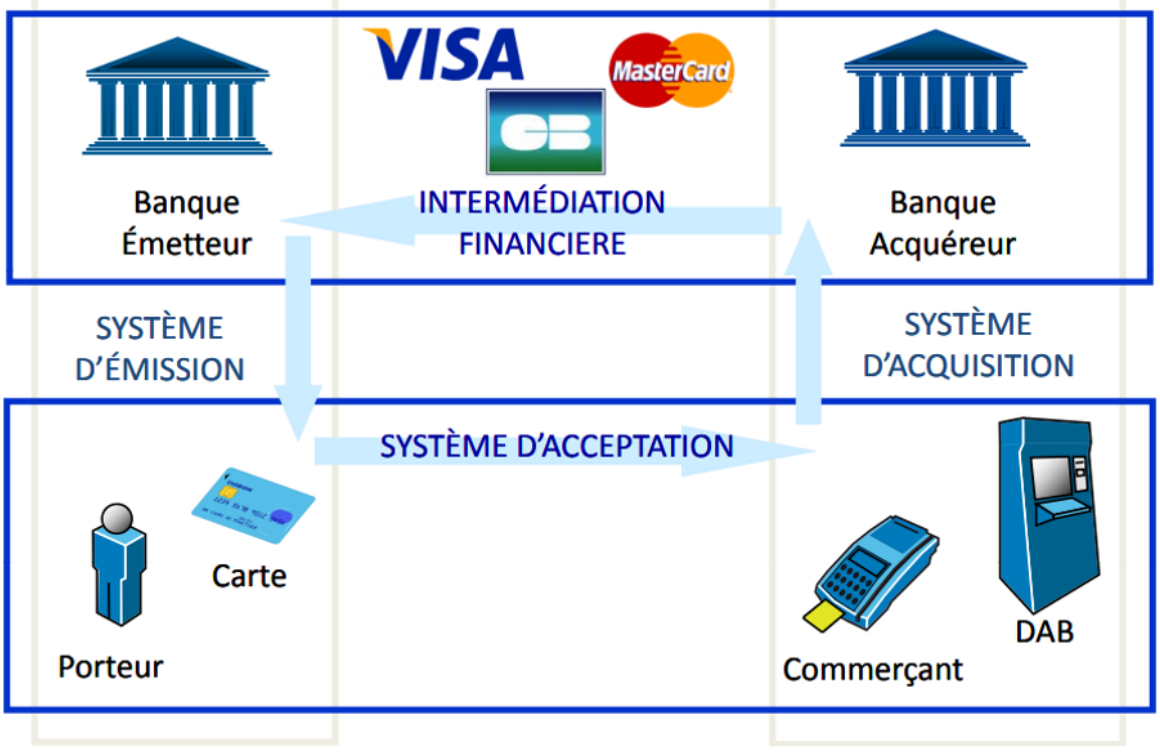
BIA
GROUPE

L'architecture du système monétique

La monétique est un écosystème de technologies variées s'appuyant sur de multiples acteurs, qu'ils soient institutionnels, industriels ou simples particuliers.

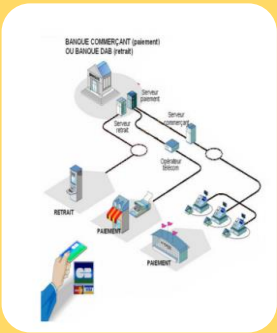
Les paiements électroniques sont devenus une référence en terme de sécurité de systèmes complexes dont les solutions sont très souvent utilisées dans d'autres domaines.

Le fonctionnement du système monétique est souvent présenté comme un système « quatre coins » (parfois en trois coins) qui met en œuvre les cinq principaux acteurs d'une opération de paiement : porteur, accepteur, acquéreur, système de paiement et émetteur.



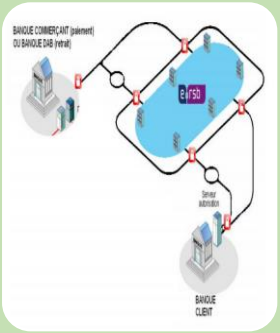
Les réseaux monétiques

Les réseaux monétiques sont les réseaux d'information reliant l'ensemble des acteurs du système monétique.



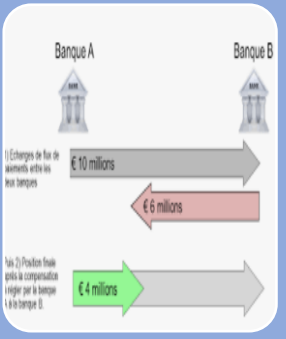
Les réseaux d'acquisition et de paramétrage

- Les réseaux d'acquisition et de paramétrage sont ceux mis en place entre l'accepteur et l'acquéreur.
- Ils permettent de véhiculer localement les demandes d'autorisation générées par les paiements. Ils sont également le support des actions de gestion de réseau, de télécollecte et de téléparamétrage.



Les réseaux de routage des autorisations interbancaires

- Les réseaux de routage des autorisations interbancaires sont ceux mis en place entre acquéreurs et émetteurs afin de véhiculer les demandes d'autorisation de transaction.
- En France, le réseau e-rsb (Réseau de Service aux Banques) exploité par la Société d'Exploitation de Réseaux et de Services Sécurisés (SER2S) véhicule la quasi-totalité des demandes d'autorisation effectuées sur le territoire national avec une moyenne de plus de 13 millions de demandes par jour. Lorsqu'une banque émettrice est étrangère ou en cas d'accord commerciaux hors Cartes Bancaires, des réseaux de routage tiers sont utilisés, tels que Visanet de Visa ou le MasterCard Worldwide Network de Mastercard.



Les réseaux de compensation

Les réseaux de compensation interbancaire sont ceux mis en place entre institutions financières (ex. acquéreurs et émetteurs) afin de permettre des opérations de compensation interbancaire (calculer un solde net à partir de différentes transactions, dont celles de paiement/retrait par carte).

Les normes en monétique

La norme SEPA

La mise en place d'un espace unique de paiement en euros (Single Euro Payments Area (SEPA)) par le conseil européen des paiements (European Payments Council - EPC) sur demande de la commission européenne.

Le support Plastique

- La norme ISO 7816-1
- L'Interface visuelle de la carte de paiement (l'ISO 7810 , l'ISO 7811-1, l'ISO 7811-2, l'ISO 7812-1, l'ISO 7816-2)

L'interface Magnétique

- La norme ISO 7813

Le sans contact

- La norme ISO 14443

La norme EMV

- Standard international de paiement et retrait capable de :
  - S'assurer que les fonctions de paiement et retrait sont exécutées de façon sécuritaire dans le terminal point de vente
  - Définir les fonctions minimales assurant l'interopérabilité internationale entre carte et terminal
- Destiné à une utilisation mondiale de la puce
- Définit conjointement par Europay Mastercard et Visa

La norme PCI DSS

PCI-DSS est un standard de sécurité des données visant à limiter les risques de fuites des données bancaires comme le numéro de carte. Actuellement à sa version 3.1, ce standard est rédigé par les membres de PCI SSC, autrement dit par les réseaux bancaires (American Express, Discover, JCB, MasterCard et Visa). Ces derniers ont donc réussi à s'accorder sur un programme de sécurité qu'elles souhaitent voir appliquer dans la communauté.

3D Secure

Face à l'augmentation des fraudes sur la vente à distance, les acteurs de la monétique ont mis en place une authentification renforcée du porteur. Cette authentification, rendue possible par le protocole 3D-Secure est assurée par « ce que sait le porteur » (mot de passe, date de naissance) ou « ce qu'il possède » (carte contenant des codes d'identification, équipement d'authentification – token – ou en encore téléphone portable).

La DSP 2

L'authentification forte se caractérise par une vérification d'identité utilisant la combinaison d'au moins 2 facteurs parmi les 3 catégories suivantes :

– Connaissance : quelque chose que seul le client connait (ex : mot de passe)

– Possession : quelque chose que seul le client possède (ex : appareil mobile)

– Inhérence : quelque chose que seul le client est (ex: empreinte digitale)