

HOBUX Consulting SARL

INFORMATIQUE-MONÉTIQUE

Audit-Conseil-Assistance-Sécurité-Intégration

Ingénierie logicielle-Formation-Recrutement



**DÉPARTEMENT
FORMATION-RECRUTEMENT**

**COURS
AUDIT D'UN SYSTÈME MONÉTIQUE**

Version 5.0 - Novembre 2014

Introduction

I. Systèmes monétiques

1. Composants matériels
2. Composants logiciels
3. Gammes de produits carte
4. Focus « Cartes prépayées »
5. Composantes d'un système monétique
6. Personnalisation de cartes

II. Schématisation des transactions

1. Transactions privatives
2. Transactions régionales
3. Transactions internationales

III. Procédures monétiques

1. Stockage et conservation des cartes
2. Remise des cartes et des codes PIN
3. Traitement des plaintes des porteurs
4. Traitement des cartes avalées
5. Approvisionnement des DABs/GABs
6. Comptabilisation des opérations

IV. Fraude monétique

1. Back-office monétique
2. Points de vulnérabilités
3. Menaces potentielles
4. Formes/techniques de fraude
5. Systèmes d'alerte



V. Risques monétiques

1. Catégories de risques
2. Dispositifs à mettre en place
3. Maîtrise du comportement client
4. Tableaux de bord de gestion des risques

VI. Evaluation d'une activité monétique

1. Formation et recyclage des acteurs
2. Sécurité du système d'information
3. Pertinence des procédures opérationnelles
4. Contrôle de la comptabilisation des opérations
5. Pertinence des niveaux de contrôle
6. **Service après-vente de la monétique**

VII. Outils d'audit monétique

1. Questionnaire d'évaluation de l'activité monétique
2. Questionnaire d'évaluation du système d'information
3. Sondage sur le respect des procédures opérationnelles
4. Sondage sur le traitement des cartes et des codes
5. Sondage sur le traitement des plaintes et des litiges
6. Sondage sur la satisfaction des porteurs de cartes

VIII. Normes - Référentiels

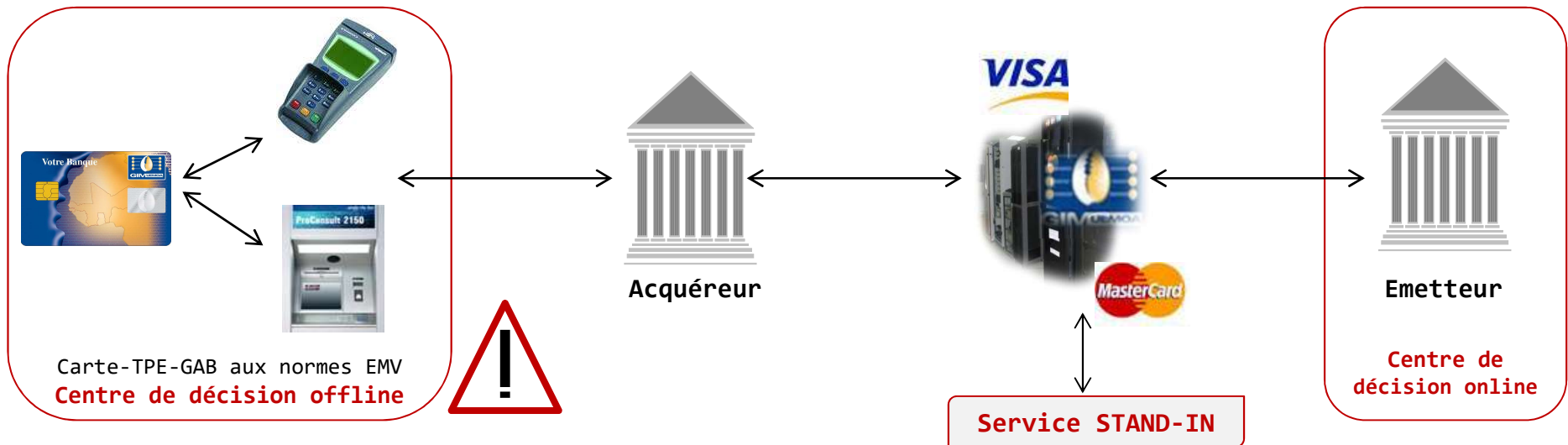
1. EMV
2. PCI DSS
3. Débat « EMV vs PCI DSS »
4. Autres normes et référentiels

JOUR
2

INTRODUCTION

Transaction en mode « online »

Transaction nécessitant une communication entre les systèmes (bancaires et monétiques) lors du processus de demande d'autorisation



Transaction en mode « offline »

Transaction ne nécessitant pas de demande d'autorisation. Les « centres de décision offline » assurent le service demandé.

STAND-IN

Délégation de la délivrance des autorisations au **serveur monétique** ou à un **réseau de paiement** en raison d'une indisponibilité (**et sur la base de paramètres et données prédéfinis** : fichiers soldes périodiques, montant maximum à chaque transaction, nombre maximal de transactions, ...)

QUIZZ



1. Quelle différence existe-t-il entre CVV2 et CVC2 ?
2. Quelles sont les formes possibles de porte-monnaie électronique ?
3. Citer quelques exemples de porteurs secondaires de cartes bancaires
4. Dans quelles types de transactions le cryptogramme visuel est demandé/exigé ?
5. Après la fabrication d'une carte, le cryptogramme visuel peut-il être modifié ?
6. Quelle différence existe-t-il entre un accepteur et un acquéreur ?
7. Le mode « OFFLINE » et le mode « STAND-IN » sont-ils équivalents ?
8. Un serveur monétique est-il un actif informatique ?
9. Un DAB/GAB est-il actif monétique ?
10. Un logiciel avec des bugs constitue-t-il une faille exploitable ?
11. Un collaborateur mal formé constitue-t-il une menace pour l'activité monétique ?

I. SYSTÈMES MONÉTIQUES

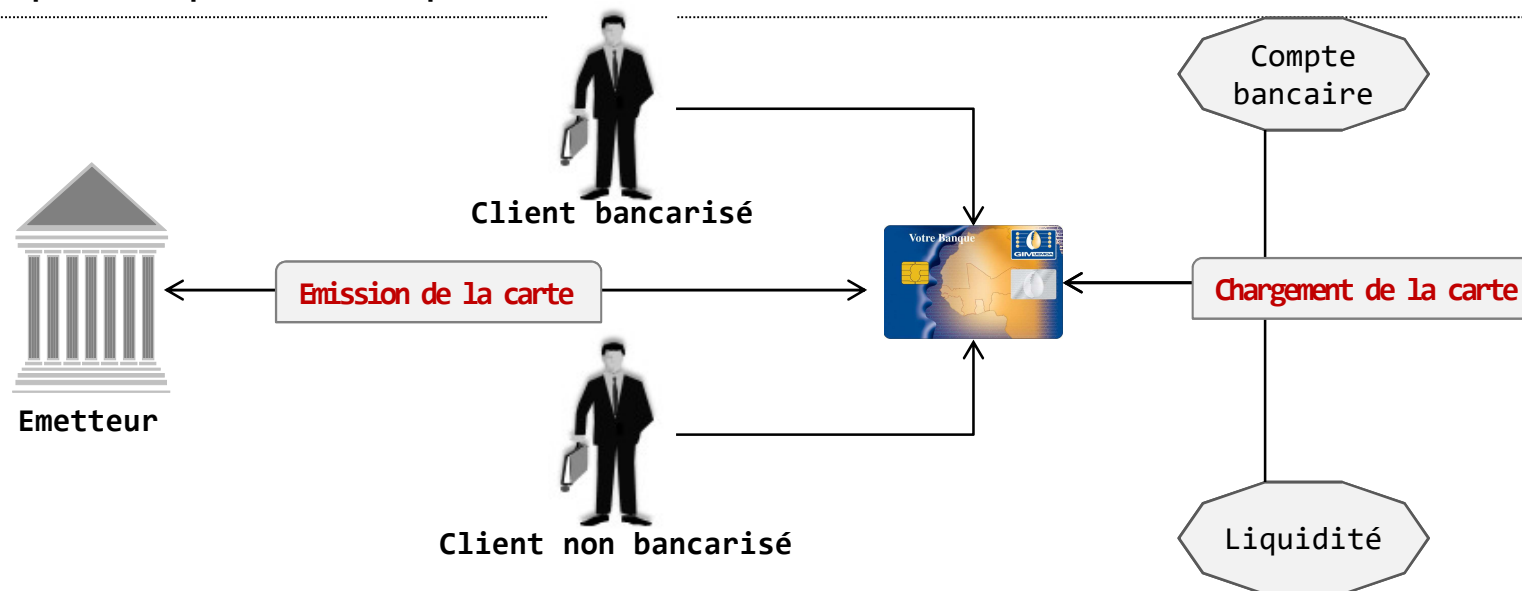
4. Focus « Cartes prépayées »

▪ Porteurs potentiels

- Client détenteur d'un compte bancaire
- Porteur secondaire (carte salaire, carte « argent de poche », ...)
- Personne physique (ou personne morale) hors du monde bancarisé (**personnes en interdicts bancaires**, adolescents, touristes, ...)

▪ Pourquoi une carte prépayée ?

- Facilité d'obtention, simplicité dans l'utilisation
- Possibilité de transfert de liquidité de carte à carte
- Meilleure sécurité pour l'utilisation sur internet
- Carte de « secours » ou seconde carte lors des déplacements
- Outil pédagogique pour initier les enfants aux cartes bancaires
- Option pour les paiements de salaire *(et fini le billetterie)*



I. SYSTÈMES MONÉTIQUES

4. Focus « Cartes prépayées »

▪ Risques associés

• Utilisations inappropriées

- Fraude fiscale
- Blanchiment d'argent

→ pouvant engendrer le financement d'activités illicites

→ pouvant affaiblir les possibilités de contrôles fiscaux

• Complexité de la traçabilité des opérations

- Faible régulation des acteurs (dans le domaine du prépayé)
- Anonymat des échanges de monnaies « électroniques »
- Difficultés de contrôle des flux de capitaux transfrontaliers

→ pouvant engendrer une perte de contrôle des autorités monétaires, des difficultés dans la régulation financière

• Suivi approximatif des mouvements

- Absence de relevés bancaires associés
- Négligence des porteurs ou manque d'information
- Sensibilisation souvent insuffisante

→ pouvant engendrer des pertes financières énormes pour les porteurs

• Incidents de règlement

- Insuffisance du solde du compte de règlement
- Fraude massive sur les cartes prépayées
- Fortes utilisations des détenteurs de cartes prépayées

→ pouvant engendrer des pertes financières énormes pour l'émetteur, une perte d'image auprès des réseaux de paiement



I. SYSTÈMES MONÉTIQUES

5. Composantes d'un système monétique

- **Volet « Emission de cartes »**
 - Promotion de cartes régionales
 - Promotion de cartes internationales
- **Volet « Acquisition »**
 - Installation de DABs/GABs
 - Placement de TPEs chez les commerçants
- **Volet « Réseaux de paiement »** (principaux réseaux dans l'UEMOA)
 - GIM-UEMOA
 - VISA
 - MasterCard
- **Volet « Compensation et Règlement »**
 - GIM-UEMOA (compensation régionale) / BCEAO (règlement régional par STAR-UEMOA)
 - VISA / MasterCard (compensation et règlement des opérations internationales)
- **Volet « Fabrication et Personnalisation »**
 - Fabrication des plastiques, des puces, ...
 - Intégration des données porteur, des données de sécurité, ...
 - Génération des codes PIN, expédition des PIN mailers, ...



I. SYSTÈMES MONÉTIQUES

5. Composantes d'un système monétique

- Volet « **Systèmes logiciels** »
 - Solution bancaire
 - Gestion des soldes des comptes
 - Gestion du lien « cartes/comptes »
 - Solution monétique
 - Gestion des cartes bancaires
 - Gestion des autorisations
 - Gestion de la fraude
 - Gestion des litiges
- Volet « **Pilotage et Régulation** »
 - Normes interbancaires
 - Règles d'interopérabilité
 - Lutte contre la fraude



Un système
monétique est un
assemblage de
sous-systèmes



1. Suivi de la fabrication des cartes

- Chez le personnalisateur : cartes avec les visuels de la banque
- Livrées à la banque, non remises aux clients, non dispatchées
- Livrées à la banque, non remises aux clients et stockées en agence
- Nombre de cartes défectueuses reçues
- Nombre de PIN mailers inopérants

2. Composants logiciels d'un système monétique (cartographie des applications)

- Documentation des composants logiciels
- Tests des composants logiciels à chaque évolution
- Sauvegardes de données avant chaque mise à jour
- Interactions entre les différents composants logiciels
- Analyse des incidents et de leurs origines techniques ou organisationnelles
- Sécurisation des différents composants logiciels

3. Composants matériels d'un système monétique (cartographie du matériel)

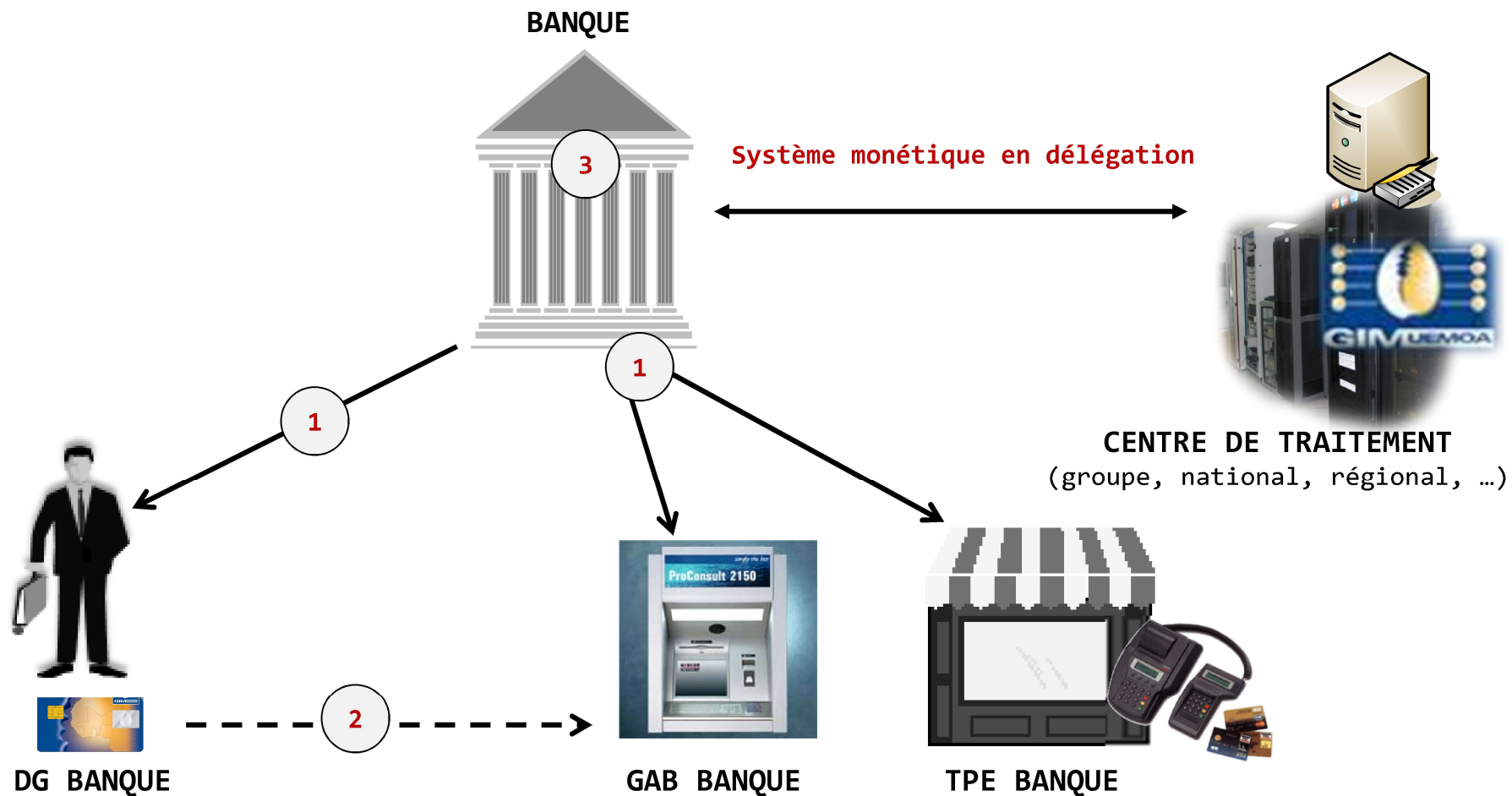
- Sécurité des composants matériels
- Locaux des DABs/GABs : caméras internes et externes
- Analyse des incidents et de leurs origines techniques ou organisationnelles
- Paramétrage des DABs/GABs et des TPEs (comptes commerçants)

4. Cartes prépayées

- Volume de cartes en circulation et créances associées
- Etat périodique des demandes d'autorisation (acceptées, rejetées)
- Etat périodique des plus gros rechargements
- Suivi de l'activité « fraude » sur les cartes prépayées

II. SCHÉMATISATION DES TRANSACTIONS

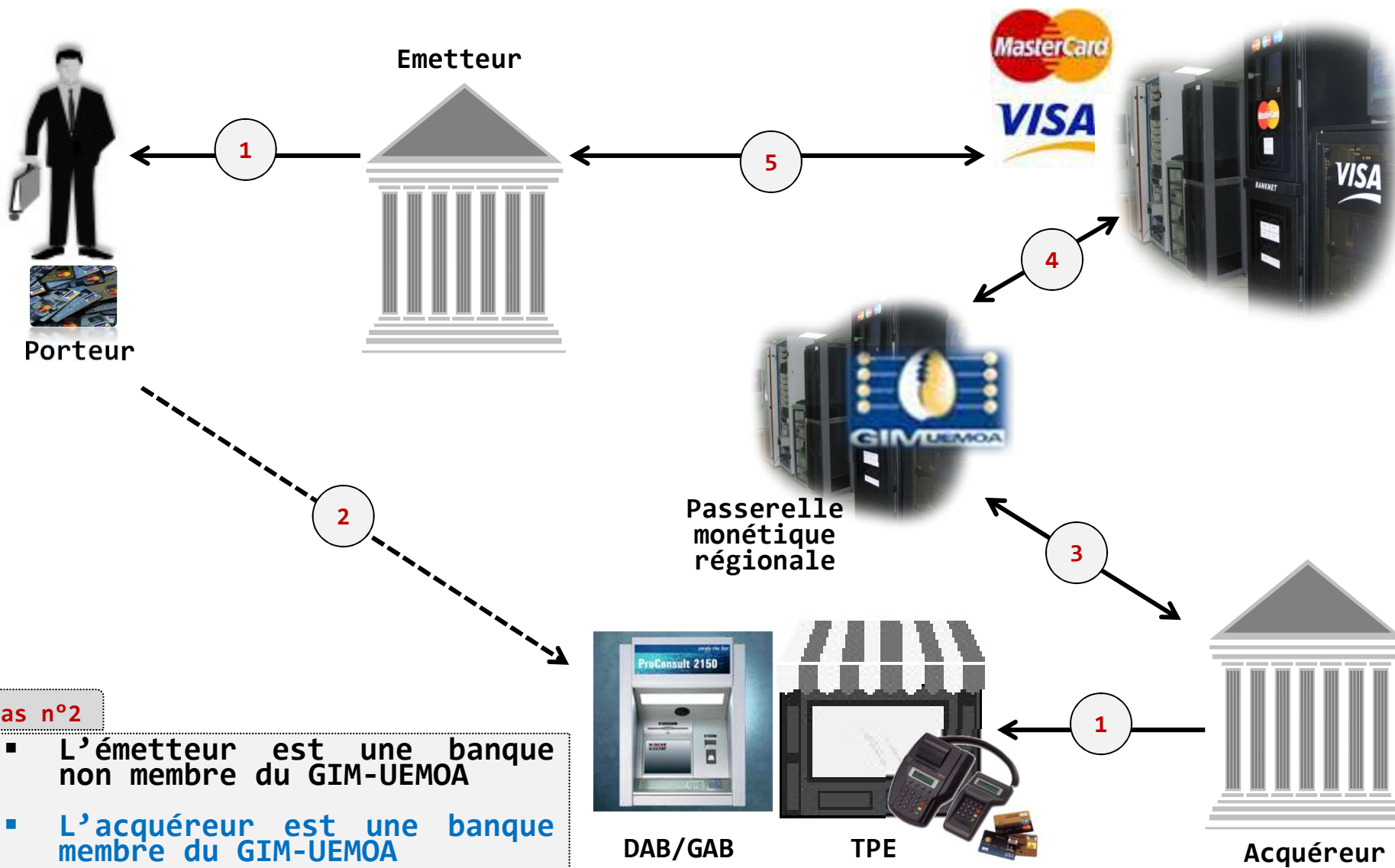
1. Transactions privatives (système monétique en délégation)



- La **délégation** consiste à la **sous-traitance d'une partie du traitement monétique** à un centre de traitement (exemple : GIM-UEMOA, GIMAC, ...)
- Il s'agit notamment d'une **partie du volet technique** de la monétique

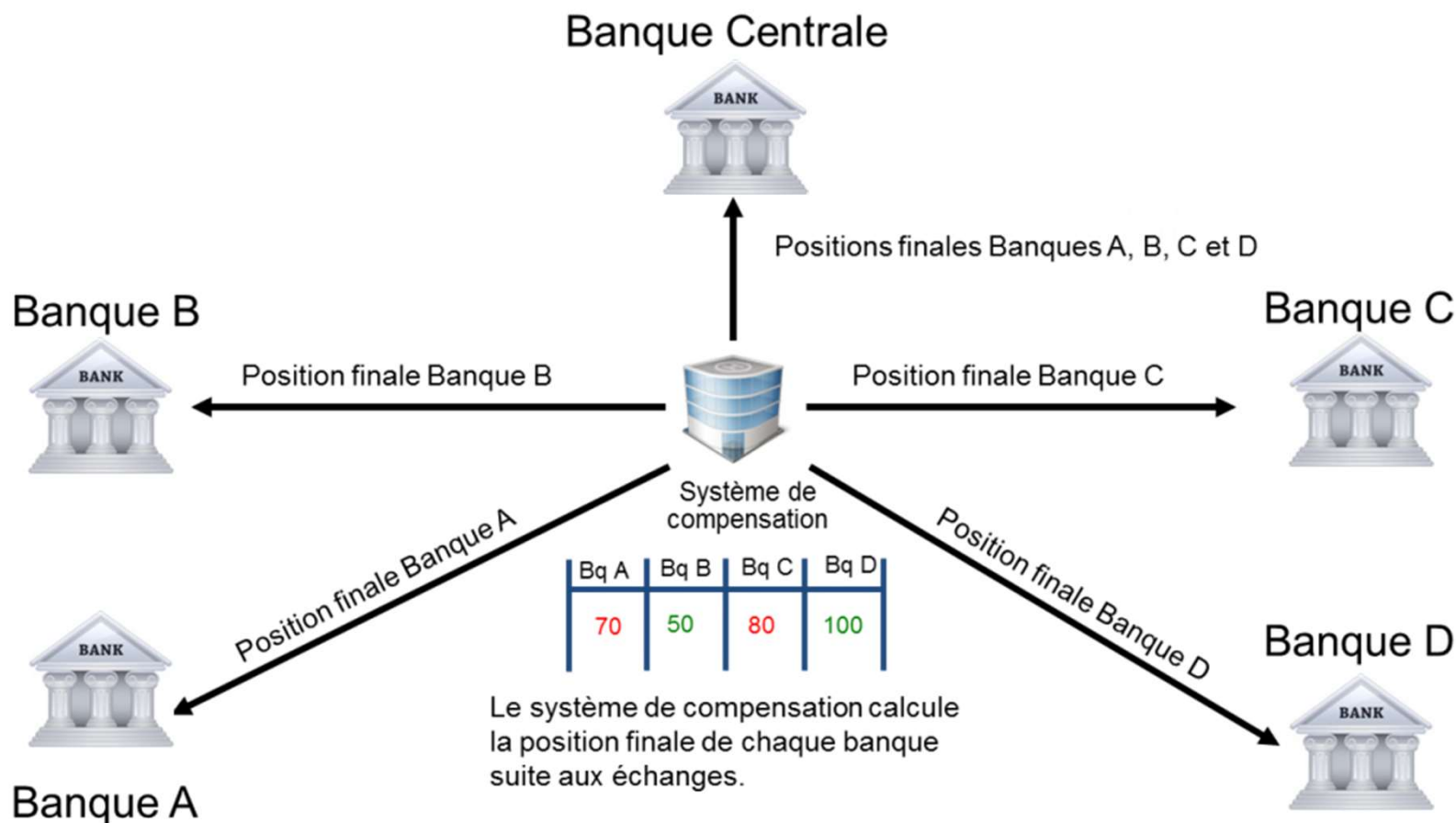
II. SCHÉMATISATION DES TRANSACTIONS

3. Transactions internationales



III. PROCÉDURES MONÉTIQUES

6. Comptabilisation des opérations

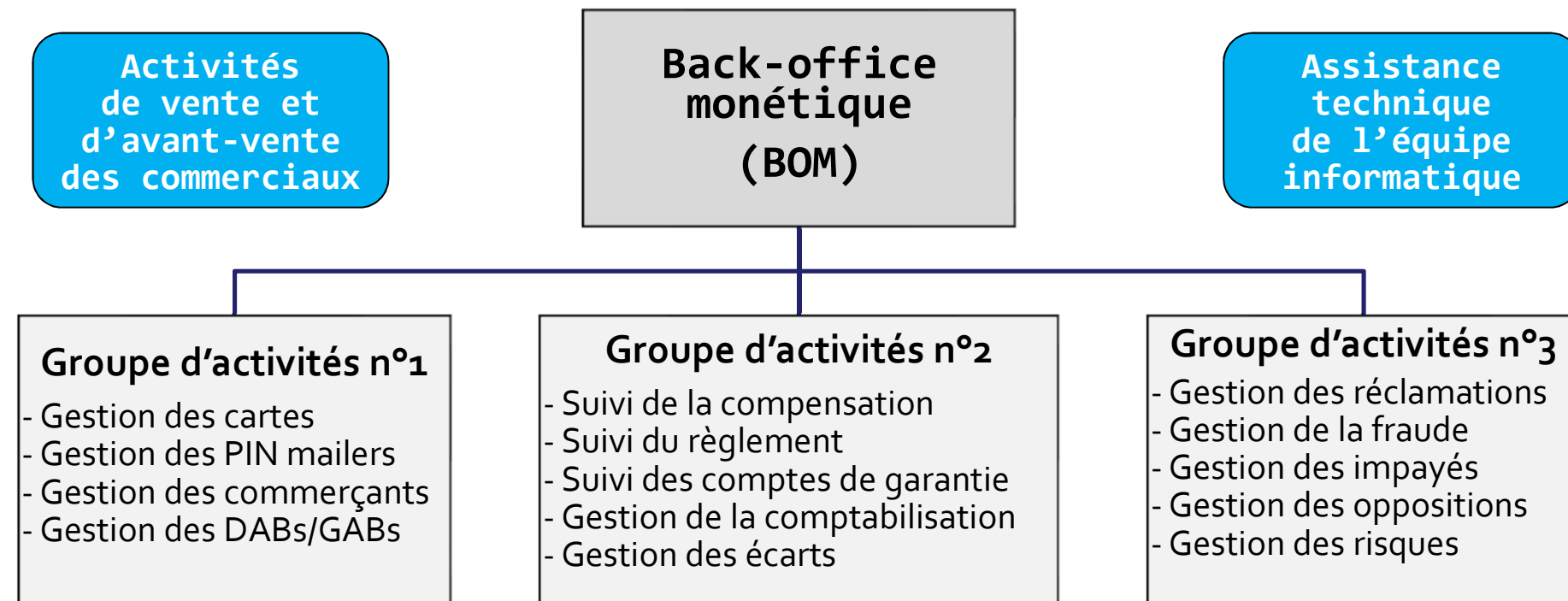


▪ Compensation multilatérale

- L'heure d'arrêt des opérations est fixée par le compensateur
- L'autorité de compensation est la « **contrepartie fictive** » de chaque banque participante à la journée de compensation

IV. FRAUDE MONÉTIQUE

1. Back-office monétique



L'organisation (**organigramme, dimensionnement, découpage de l'activité, procédures**) d'un BOM dépend fortement des paramètres ci-dessous :

- L'**organisation générale de la banque**
- La **stratégie de développement de la monétique**
- Les ressources disponibles pour une allocation au BOM

NB : les groupes d'activités n°1 à n°3 peuvent nécessiter 2, 3 ou 4 collaborateurs en prenant en compte les paramètres cités plus haut.



1. Vulnérabilités

- Analyse des vulnérabilités d'ordre organisationnel
- Analyse des vulnérabilités d'ordre humain
- Analyse des vulnérabilités d'ordre logiciel ou matériel (sur la base des cartographies réalisées)

2. Système d'alerte

- Analyse des flux monétiques (paiement, autorisation, mise en opposition, ...)
- Echanges avec les banques locales, avec le GIM-UEMOA
- Echanges avec les autres banques du Groupe
- Existence d'un système d'alerte (mis à jour et régulièrement amélioré)

3. Formation/Sensibilisation

- Formations des acteurs internes sur la monétique
- Formations des commerciaux (front office)
- Formations spéciales au back office monétique
- Mise à niveau périodique sur l'information monétique
- Participation aux différents salons sur la monétique

4. Contrôle interne

- Mise en place des mécanismes adéquats
- Maîtrise des systèmes et des opérations monétiques
- Disponibilité des ressources nécessaires à la conduite d'une mission de contrôle interne

V. RISQUES MONÉTIQUES

1. Catégories de risques

- **Risques internes liés aux comportements du personnel**
 - Complicité avec des acteurs externes
 - Emission de cartes sur des comptes « dormants »
 - Retards dans les opérations de mise en opposition sur cartes
- **Risques liés à l'émission et à la gestion du cycle de vie des cartes bancaires**
 - Emission de cartes sur des comptes « inappropriés »
 - Emission de cartes avec des plafonds trop élevés
 - **Emission de cartes pour des clients « douteux »**
 - Modification inadéquate des plafonds de retrait/paiement
 - Non annulation de cartes avant la clôture effective des comptes associés
- **Risques liés aux opérations de compensation/comptabilisation**
 - Oubli dans l'envoi et/ou la récupération des fichiers
 - Intégration partielle des fichiers de comptabilisation
 - Prise en compte incomplète des opérations en raison d'un système logiciel inadéquat entraînant un traitement manuel additionnel
- **Risques liés à la maîtrise/au suivi des comptes monétiques**
 - Schémas comptables inadaptés (vu les objectifs de contrôle de la banque)
 - Opérations monétiques non maîtrisées en raison d'un défaut de formation
 - Comptes monétiques non suivis en raison d'une charge d'activité
 - Incident de règlement en raison d'un solde insuffisant au niveau du compte d'opérations

V. RISQUES MONÉTIQUES

4. Tableaux de bord de gestion des risques

- **Tableau de bord n°1 : gestion des cartes**
 - Statistiques des cartes commandées
 - Statistiques des cartes reçues
 - Statistiques des cartes en circulation
 - Statistiques des cartes en stock
- **Tableau de bord n°2 : contrôle interne**
 - Liste des comptes fermés sur une période donnée
 - Preuve de l'annulation des cartes adossées aux comptes fermés
 - Destruction des cartes récupérées
- **Tableau de bord n°3 : gestion des impayés monétiques**
 - Liste des impayés traités + implications (financières, ...)
 - Liste des impayés en cours de traitement
 - Mise à jour du plan d'actions de gestion des impayés
- **Tableau de bord n°4 : comptabilisation des opérations**
 - Preuve de l'intégration régulière des fichiers reçus
 - Epuration des comptes monétiques
- **Tableau de bord n°5 : approvisionnement des DABs/GABs**
 - Etat des arrêtés
 - Etat des approvisionnements
 - Croisement avec les comptes caisse associés
 - Listing des anomalies
 - Gestion clés et codes d'accès aux DABs/GABs