International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 10 Issue 7 July - 2026, Pages: 183-187

Interoperability of University-Bank Information Systems: Preliminary Study for a Dynamic Web Platform for Integrated Management of Academic Fee Payments

Jacques KIZA DIMANDJA

Assistant Deuxime Mandat
Email: Jacques.kiza.dimandja@uka.ac.cd
University : Our Lady of Kasayi University (U.KA),

Licencié en Sciences Informatiques (Orientation: Conception des systèmes Informatiques) , Assistant Scientifque à l'Université Notre-Dame du Kasayi (U.KA), Kasaï Central, Kananga(RDC)

Abstract: *This paper presents a preliminary study on the interoperability between academic and banking information systems for the integrated management of university tuition fee payments. The traditional manual verification of paper receipts introduces critical vulnerabilities, including document fraud, administrative delays, and complex financial reconciliation (Kiza Dimandja, 2024). This study establishes a theoretical and technical framework based on RESTful Web services, mutual TLS authentication, HMAC transaction signing, and NoSQL log storage (Kleppmann, 2018). The proposed architecture guarantees transactional idempotency, data consistency across Wide Area Networks (WAN), and complete auditability. This work defines the essential semantic and structural specifications required prior to the deployment of a dynamic web platform (Laudon & Laudon, 2020).*

Keywords— Interoperability; REST Web Services; Financial Reconciliation; NoSQL Logging; Transactional Security; Academic Information System.

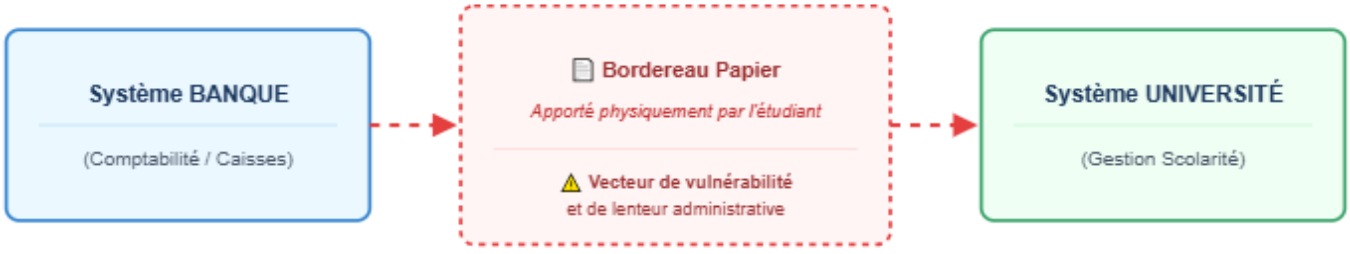
Interopérabilité des systèmes d'information Université-Banque : Étude préalable pour une plateforme Web de gestion intégrée des paiements de frais académiques

Résumé— *Les processus traditionnels de recouvrement des frais académiques, fondés sur des vérifications manuelles de pièces justificatives papier, exposent les institutions à des risques élevés de fraude documentaire, d'erreurs de réconciliation et de goulots d'étranglement administratifs (Kiza Dimandja, 2024). Cet article présente une étude préalable sur l'interopérabilité des systèmes d'information (SI) hétérogènes Université-Banque. Nous formalisons un cadre architectural fondé sur des services Web RESTful, une architecture orientée événements et un modèle de persistance NoSQL dédié à l'auditabilité des transactions (Akoka & Comyn-Wattiau, 2006). Cette étude établit les exigences théoriques, sémantiques et sécuritaires indispensables au déploiement ultérieur d'une plateforme Web dynamique de gestion intégrée (Laudon & Laudon, 2020).*

Mots-clés— *Interopérabilité des SI; Services Web REST; Réconciliation financière; Stockage NoSQL; Sécurité transactionnelle; Système d'Information Académique*.

1. Contextualisation et Problématique : La Rupture de la Chaîne d'Information

Dans une architecture d'entreprise traditionnelle non intégrée, l'Université et la Banque fonctionnent comme deux **îlots décisionnels étanches** (Laudon & Laudon, 2020).



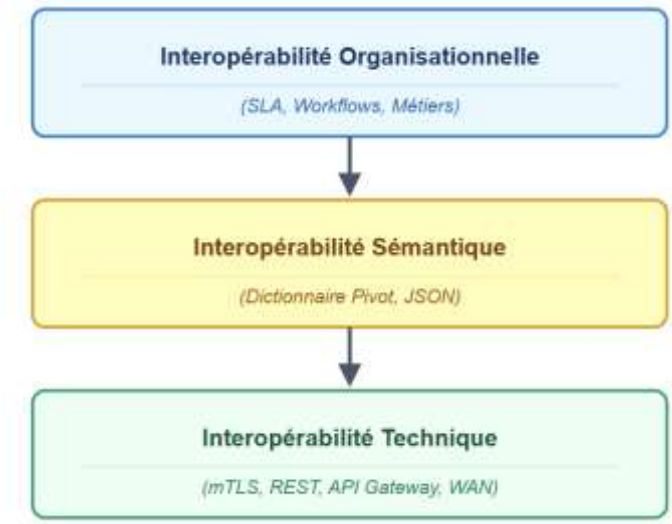
L'Analogie du "Courrier Postal vs la Téléphonie Directe"

- **Modèle Manuel (Courrier Postal) :** L'étudiant agit comme un "messager physique" transportant un bordereau papier du guichet bancaire au guichet académique. Ce transfert asynchrone introduit un délai important (souvent plusieurs semaines) et repose sur un support papier vulnérable aux altérations (falsification de tampons, modification de montants) (Kiza Dimandja, 2024).

- **Modèle Interconnecté (Téléphonie Directe) :** L'Université et la Banque établissent un canal crypté en temps réel. Dès qu'un paiement est encaissé à la banque, l'information est notifiée instantanément au système de scolarité sans intervention humaine intermédiaire.

2. Les Trois Piliers Scientifiques de l'Interopérabilité

Pour interconnecter deux Systèmes d'Information (SI) d'entreprises aux architectures logicielles et matérielles hétérogènes, l'interopérabilité s'articule autour de trois niveaux fondamentaux (Akoka & Comyn-Wattiau, 2006) :



A. L'Interopérabilité Technique (Couche Transport et Protocole)

- **Problème :** La banque peut utiliser un réseau bancaire propriétaire sous mainframe (ex. AS/400) ou Java, tandis que l'Université exploite un serveur Web sous PHP/Linux.

  Solution : Utilisation du style architectural **REST (Representational State Transfer)** s'appuyant sur HTTP/2 (Fielding, 2000). Les échanges s'effectuent via des payloads légers au format JSON, consommables universellement quel que soit le langage de programmation sous-jacent.

B. L'Interopérabilité Sémantique (Dictionnaire Pivot de Données)

- **Problème :** Pour la banque, la donnée clé est un Numéro de Compte ou un Code Transaction. Pour l'Université, la donnée pivot est le Matricule Étudiant et le Code Promotion.
- **Solution :** Définition d'un schéma d'échange unifié (Dictionnaire de données pivot).

  Exemple de Payload JSON Unifié :

payload_transaction_pivot.json

```
{
   "transaction_ref"   : "BNK-2026-089452"     ,
   "student_id"        : "UKA-2025-CS-0142"    ,
   "amount_paid"       : 250000.00   ,
   "currency"          : "CDF"  ,
   "fee_type"          : "FRAIS_ACADEMIQUES"     ,
   "timestamp"         : "2026-07-20T11:45:00Z"
}
```

C. L'Interopérabilité Organisationnelle (Engagements et Workflows)

- Alignement des processus métiers : Définition précise du niveau de service (SLA) fixant la tolérance de panne, le temps maximal de réponse de l'API (ex. < 2000 ms) et la gestion des échecs de paiement.

3. Sécurité Transactionnelle et Intégrité sur Réseau WAN

Le réseau étendu (WAN) reliant la banque à l'université est par nature non sécurisé. Deux mécanismes cryptographiques fondamentaux sont théoriquement et pratiquement requis pour garantir la confiance :

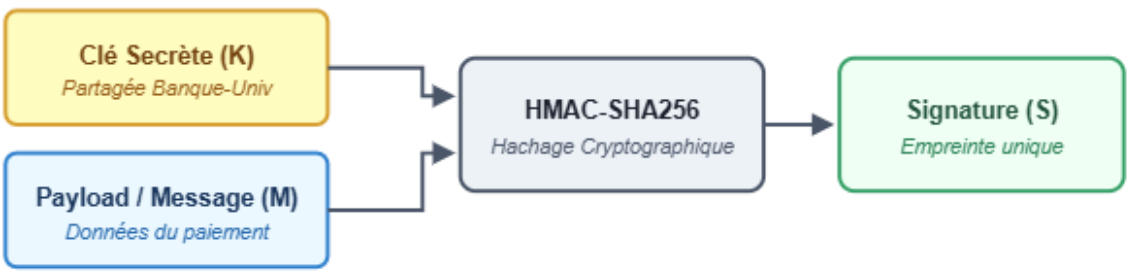
3.1 Authentification Forte Mutuelle (mTLS)

Contrairement au HTTPS classique où seul le serveur prouve son identité au client (navigateur), le **mTLS (Mutual TLS)** exige que la banque ET l'université présentent un certificat numérique $X.509$ valide émis par une Autorité de Certification (CA) (Chappe & Bideau, 2021). Tout serveur tiers non autorisé est immédiatement rejeté au niveau de la couche transport.

3.2 Signature Cryptographique des Messages (HMAC-SHA256)

Pour garantir la **non-répudiation** et l'**intégrité** des données bancaires lors du transit, la banque calcule une empreinte numérique sécurisée à partir d'une clé privée partagée K et du contenu du message M :

$$S = HMAC\text{-}SHA256(K, M)$$



International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 10 Issue 7 July - 2026, Pages: 183-187

Si un pirate intercepte le paquet sur le réseau et modifie le montant du paiement (ex. transforme 25 000 en 250 000), le serveur de l'Université recalcule S' à la réception. Comme $S' \neq S$, la transaction est rejetée immédiatement et l'alerte est enregistrée.

4. Garantie d'Idempotence et Résilience Réseau

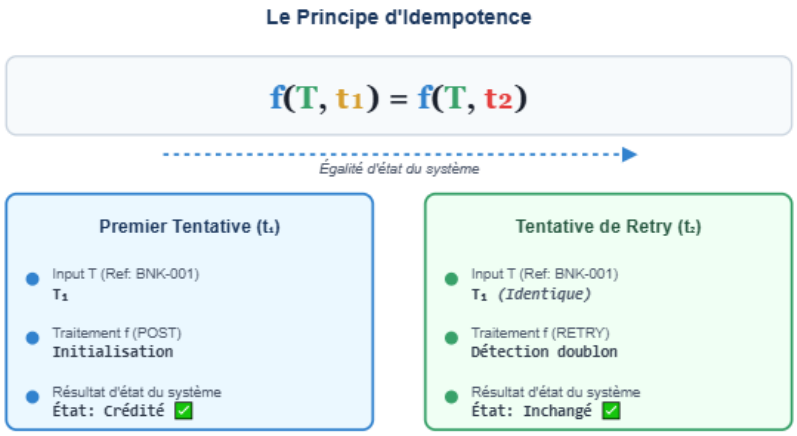
Sur un réseau étendu (WAN), des pannes intermittentes ou des pertes de paquets peuvent survenir. Si la banque envoie une confirmation de paiement mais que le réseau se coupe avant de recevoir la réponse de l'Université, la banque va **réessayer** d'envoyer la même requête.

- **Le Danger : Le Double Paiement (Non-Idempotence)**

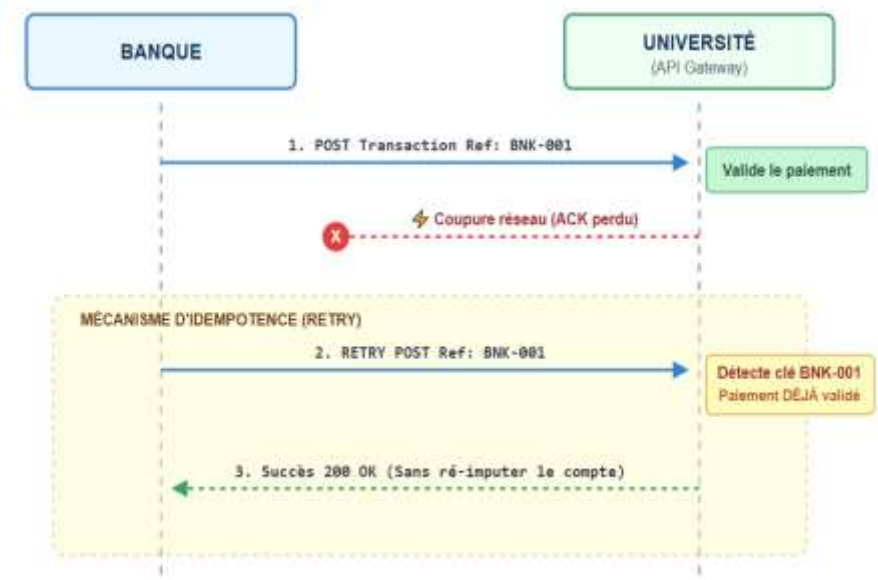
Sans mécanisme de contrôle, l'Université risquerait de créditer deux fois le compte de l'étudiant pour un seul versement bancaire réel.

- **La Solution Scientifique : L'Idempotence Algorithmique**

Une opération est dite **idempotente** si le fait de la répéter plusieurs fois produit le même résultat que de l'exécuter une seule fois (Kleppmann, 2018) :

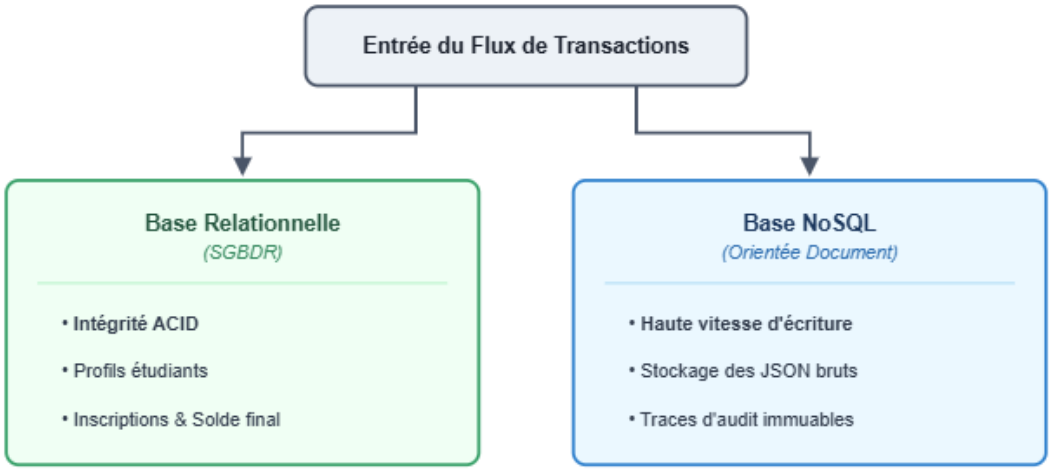


Le Use Case diagram presente les differents actions en image ci-dessous :



5. Architecture Hybride de Données : SGBDR vs NoSQL

Le système repose sur un découplage des responsabilités de stockage (Gardarin, 2003) :



1. **SGBDR (ex. MySQL / PostgreSQL) :** Maintient l'intégrité référentielle stricte des données académiques (Étudiants, Promotions, Frais dus, Solde validé) conformément aux propriétés ACID (Atomicité, Cohérence, Isolation, Durabilité).
2. **NoSQL Orienté Document (ex. MongoDB) :** Sert de journal d'audit temps réel (*Audit Log Store*). Il ingère sans contrainte de schéma toutes les requêtes brutes JSON, les entêtes HTTP, les adresses IP et les signatures HMAC (Kleppmann, 2018). Cela permet une traçabilité judiciaire totale en cas de litige financier.

Conclusion et Perspectives

Cette étude préalable démontre que l'interopérabilité des systèmes d'information Université-Banque ne réside pas uniquement dans le codage d'une interface Web, mais dans le **déploiement d'une architecture orientée services (SOA/REST) robuste, idempotente et cryptographiquement sécurisée**.

Les spécifications théoriques et sécuritaires ainsi établies fournissent le cadre rigoureux indispensable à la phase suivante : la conception logicielle et le déploiement opérationnel de la plateforme Web dynamique intégrée.

Références bibliographiques

- **Akoka, J. et Comyn-Wattiau, I.**, *Encyclopédie des systèmes d'information*, 1re éd., Paris, 2006.
- **Chappe, S. et Bideau, E.**, *Sécurité informatique et réseaux : Cours et exercices corrigés*, 2e éd., Paris, 2021.
- **Fielding, R. T.**, *Architectural styles and the design of network-based software architectures*, Thèse de doctorat, Irvine, 2000.
- **Gardarin, G.**, *Bases de données : Objet et relationnel*, 4e éd., Paris, 2003.
- **Kiza Dimandja, J.**, *SQL Injection Attack Prevention Methodology: Best Practices and Strategies*, International Journal of Academic Multidisciplinary Research (IJAMR, Vol. 8, N° 5), Kananga, 2024.
- **Kleppmann, M.**, *Concevoir des applications intensives en données : Les principes fondamentaux des systèmes fiables, évolutifs et maintenables*, 1re éd., Paris, 2018.
- **Laudon, K. et Laudon, J.**, *Management des systèmes d'information*, 16e éd., Paris, 2020.
- **Tannenbaum, A. et Van Steen, M.**, *Systèmes distribués : Principes et architectures*, 2e éd., Paris, 2008.