
IBM
IBM SOA*
Summit
*Informations valorisées et SOA,
le couple gagnant.

IBM SOA Summit

IBM

Retour d’expérience de mise en oeuvre d’un Bus de Service

Eric Datei

Senior IT Architect – IBM Certified

Global Business Services

Agenda

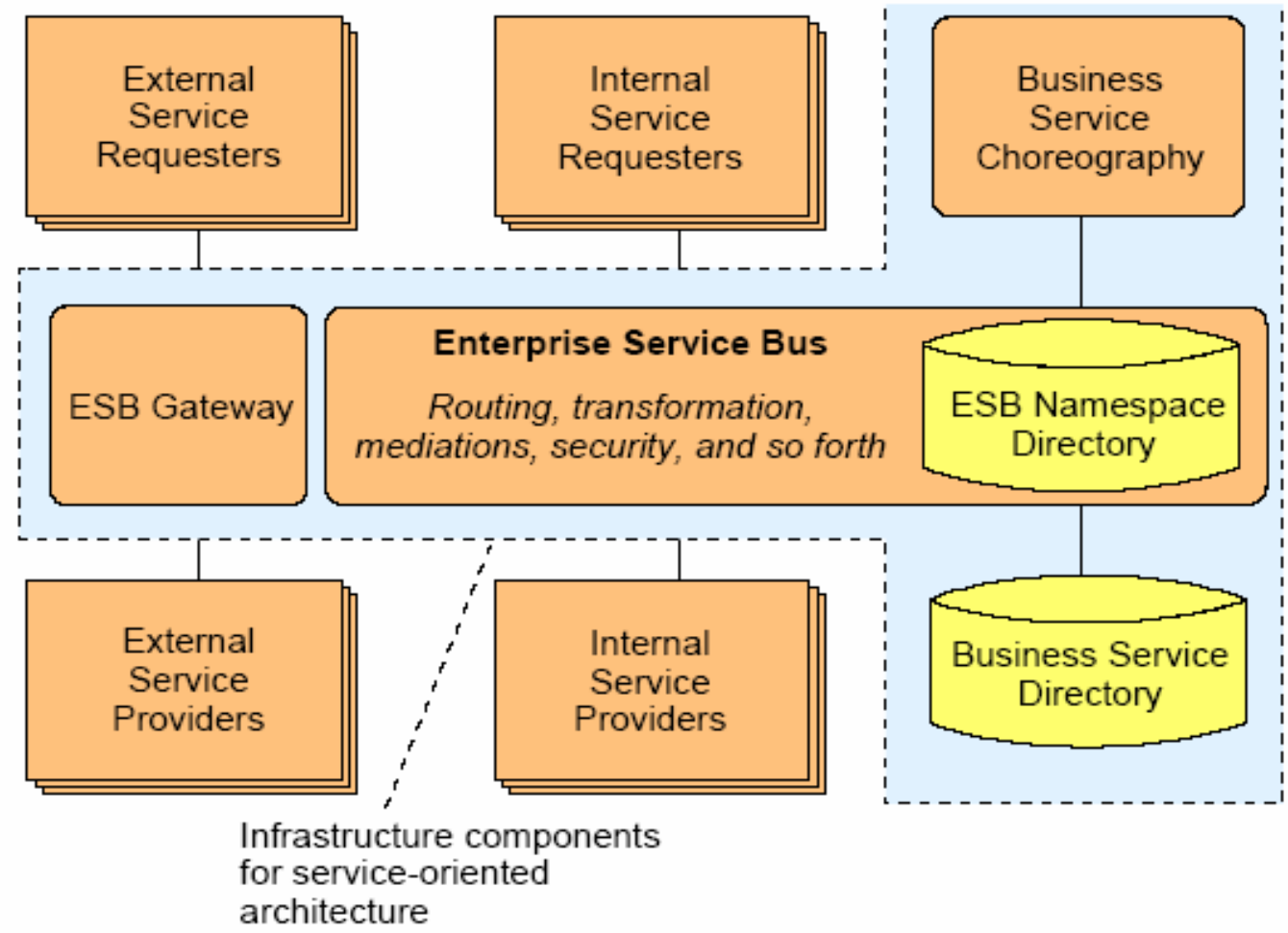
1. **Positionnement du Bus de service dans l'infrastructure SOA**

2. **Retour d'expérience issu d'un grand projet stratégique**
   1. Présentation des problématiques fonctionnelles et techniques
   2. Description des solutions mises en oeuvre
   3. Points durs et difficultés rencontrés

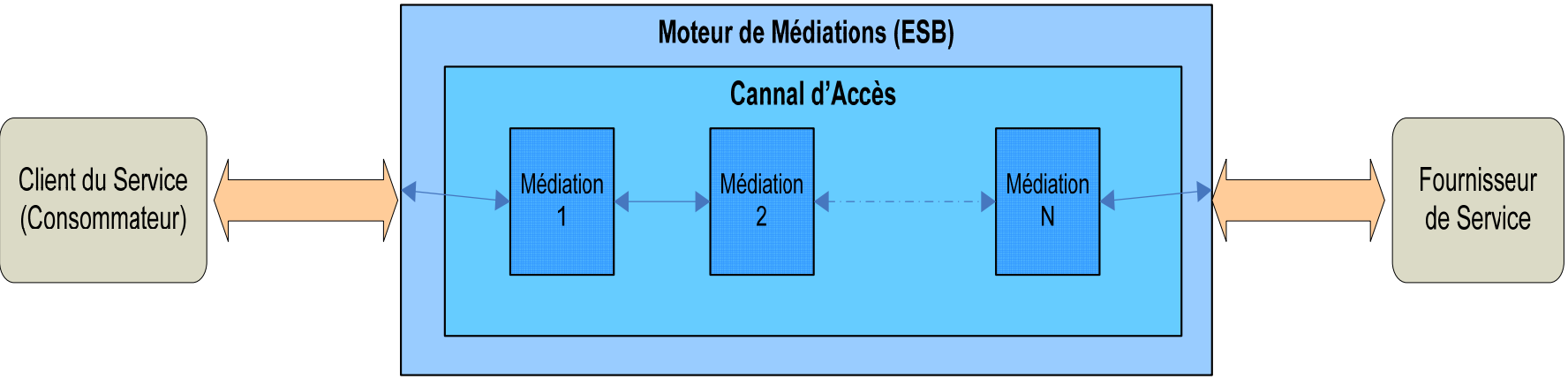
Les problématiques SOA

- **Interfaçage des services**
  - Mise en place d'une infrastructure permettant de définir une interface standard entre un service de la plate-forme et le bus de services
- **Exposition des services**
  - A travers le Bus de Service en supportant différents types d'interactions et différents protocoles
- **Sécurité**
  - Authentification, Autorisations, Confidentialité, Intégrité, Audit, Non répudiation …
- **SLA & Monitoring**
  - Gestion de la Qualité de Service & Supervision des services
- **Souscription aux Service & Facturation**
  - Auto souscription des clients du service
  - Génération de logs d'accès. Génération d'informations de facturations
- **Gestion de du cycle de vie des services**
  - Gestion des versions et du cycle de vie des services
  - Publication et découverte des Services
- **Haute disponibilité & Scalabilité**

Infrastructure SOA
Pourquoi un Bus de service



Infrastructure SOA
Mise en œuvre des services techniques



- **Support des Médiations**
  - Capacité à implanter des traitements additionnels s'effectuant au cours de l'acheminement d'une requête sans impacter le client ni le fournisseur du service
- **Des Médiations peuvent être utilisées pour implémenter diverses exigences fonctionnelles ou non fonctionnelles d'une manière non intrusive**
  - Sécurité
  - Logging
  - Supervision
  - Routage
  - …

Agenda

1. **Positionnement du Bus de service dans l'infrastructure SOA**

2. **Retour d'expérience issu d'un grand projet stratégique**
   1. Présentation des problématiques fonctionnelles et techniques
   2. Description des solutions mises en oeuvre
   3. Points durs et difficultés rencontrés

Construire un système qui se veut évolutif et flexible pour répondre aux nouveaux besoins du marché

- **Un établissement financier, dont les actionnaires sont les banques françaises majeures**

- **Objectif : Construire un nouveau système bancaire innovant**

  - Conforme aux évolutions réglementaires, connues ou **à venir**, des paiements en Europe (exemple : nouveaux formats d'opérations comme le Débit Direct Européen)

  - Apte à **exister,** donc à **se différentier** par son offre de services**,**

  - Tout en étant compatible (formats, performances, qualité de service) avec les formats actuels

- **D'où : construction d'un système d'Informations « from scratch » :**
  - Flexible et évolutif
  - Ouvert et mettant à disposition de nouveaux services

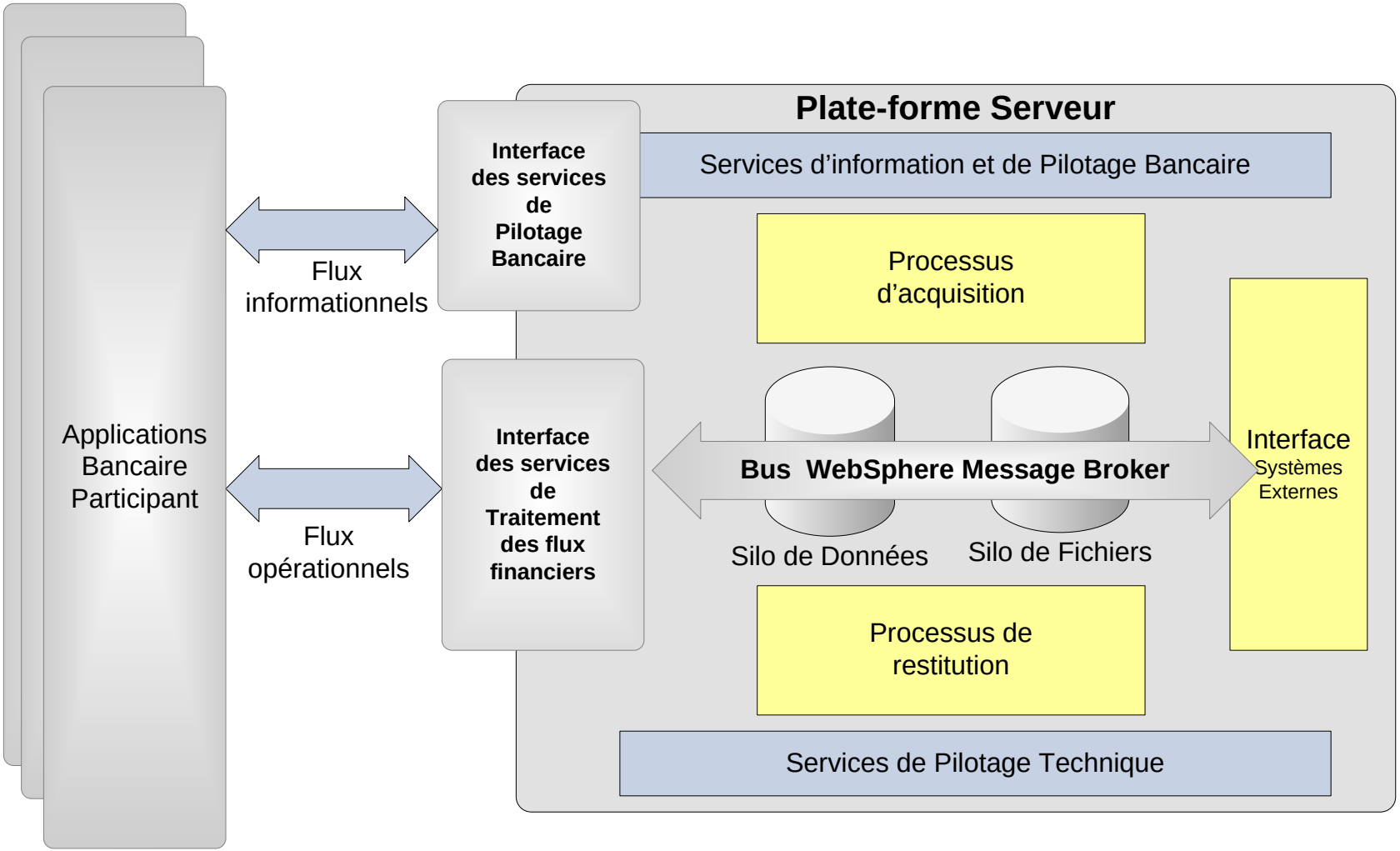
Problématiques fonctionnelles

- **L’ouverture programmée pour 2008 du marché Européen des paiements impose au projet des jalons prédéfinis de mise en production.**
- **La première exigence fonctionnelle est la livraison opérationnelle du système selon des jalons imposés par ce calendrier.**
- **Le système doit être capable d’évoluer rapidement afin de pouvoir se différencier par son offre de services, au sein d’un marché des paiements européen devenu fortement concurrentiel.**
- **Le système doit pouvoir supporter différentes communautés d’échanges de manière à pouvoir vendre les services à valeur ajoutée proposés par ce nouveau système à d’autres acteurs européens.**

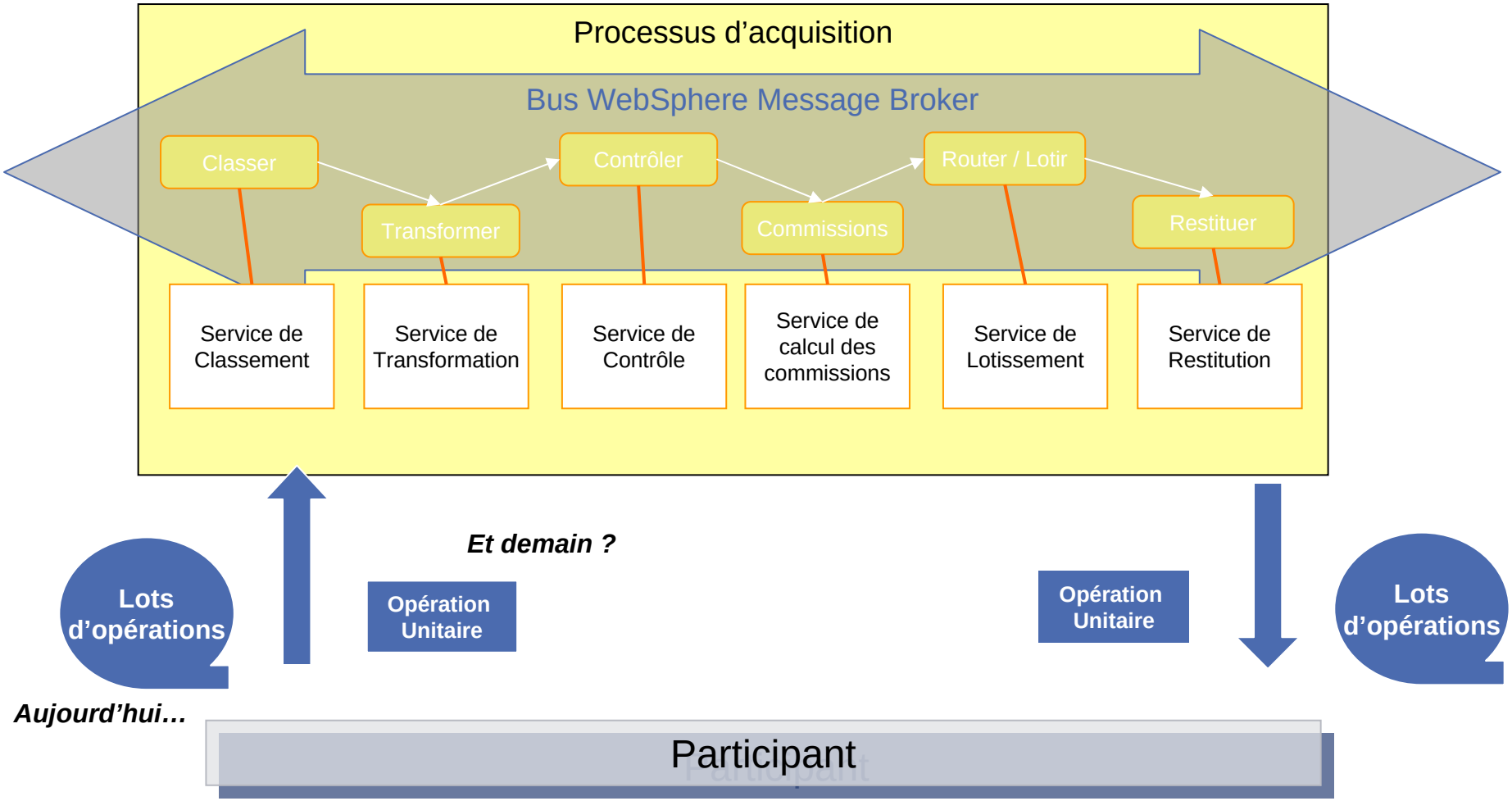
Problématiques techniques

- **La sécurité**
- **Les performances et la volumétrie des échanges**
- **La très haute disponibilité du système**
- **La fiabilité totale des échanges et du stockage**
- **La mise à disposition de mécanismes d'invocation des services compatibles avec les infrastructures techniques actuellement en place chez les clients de la plate-forme**

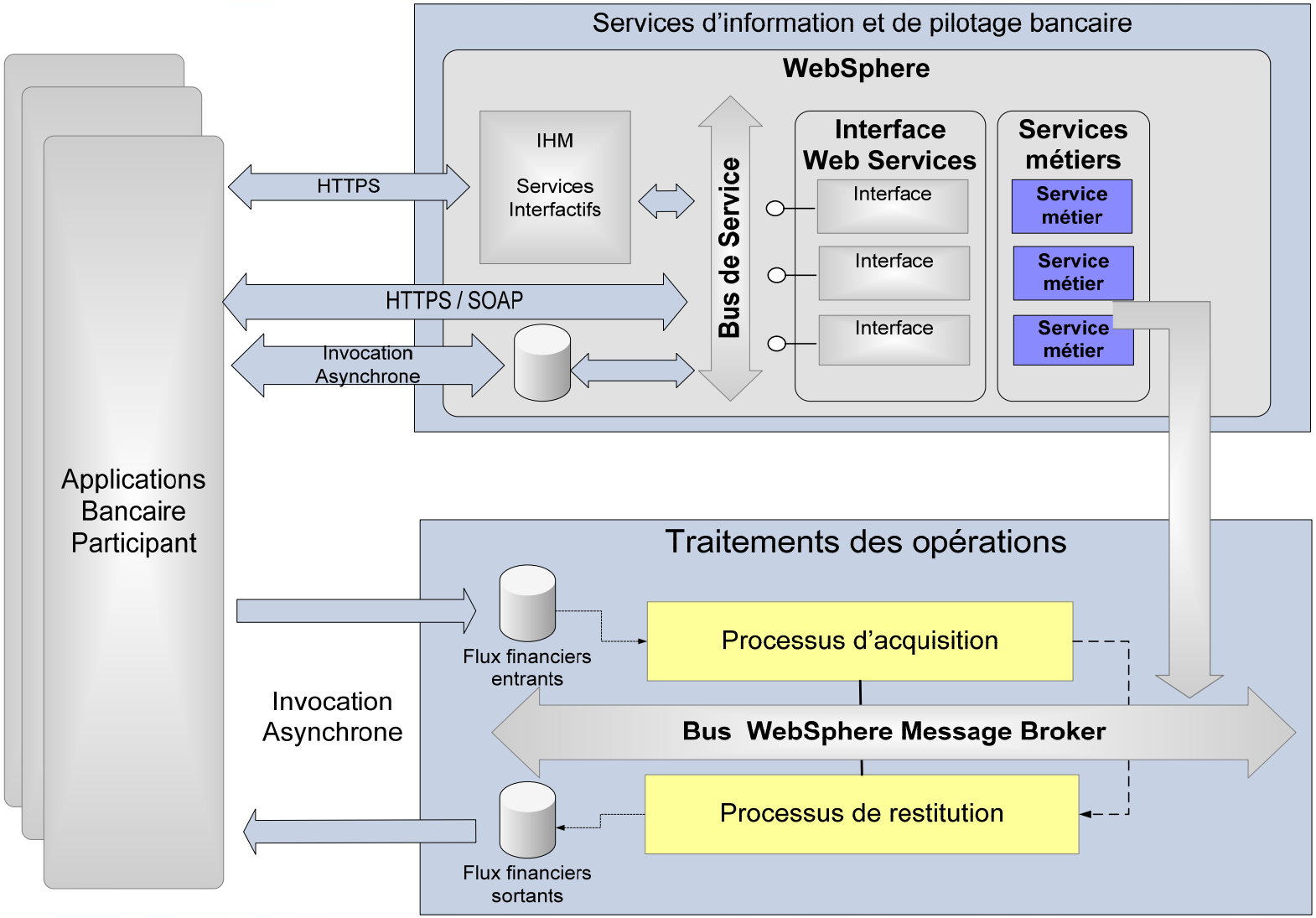
La construction du Système s'appuie d'emblée sur une approche orientée services



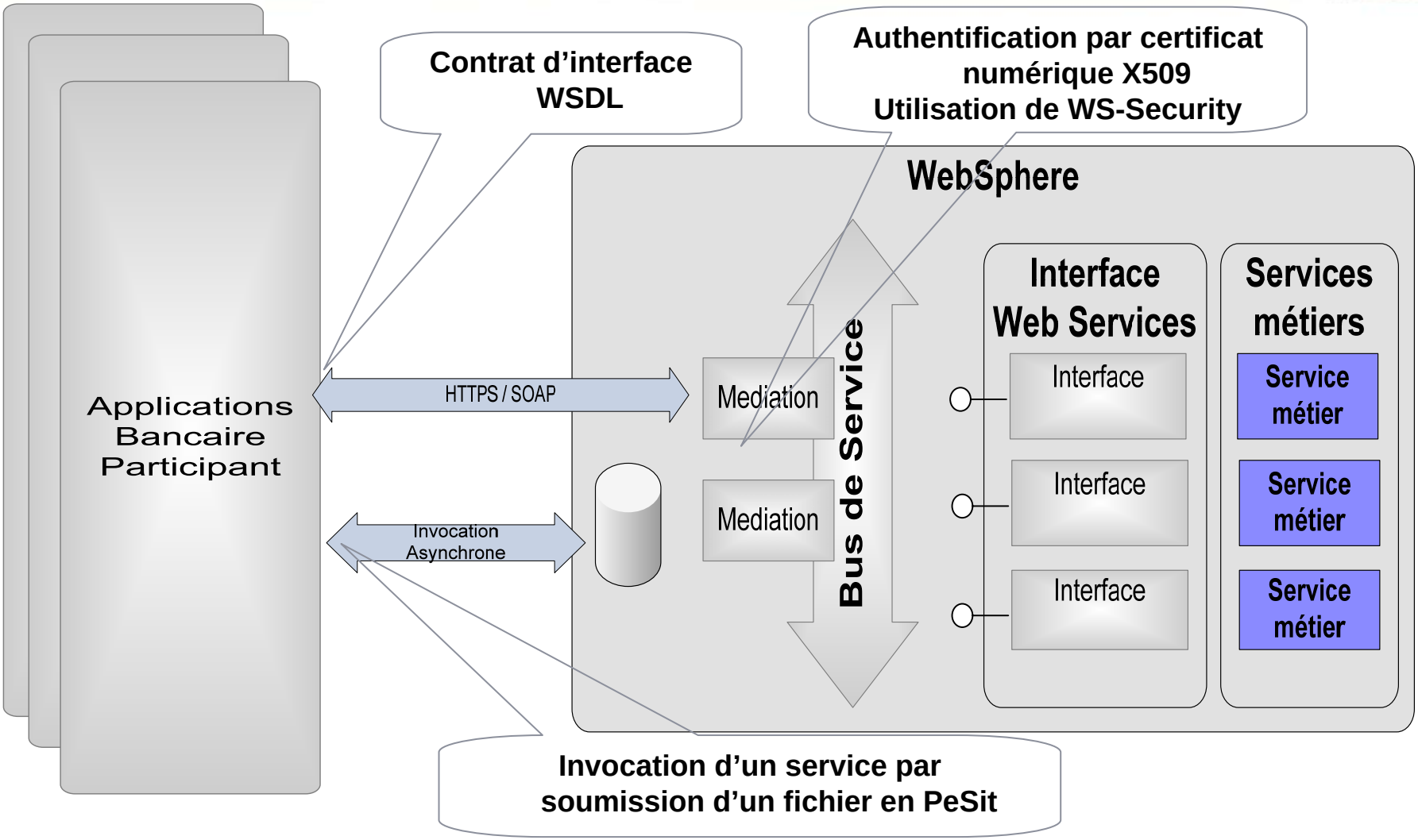
Flexibilité : Réponse à un besoin d'évolution d'un processus
Exemple : l'approche service permet l'évolutivité des traitements



Pour Informer et agir, le choix poussé par IBM, : Une architecture Orientée Services (Web services, ESB)



Une architecture orientée services basée sur des technologies standard mais supportant également les technologies existantes dans les banques



Mise en œuvre de la sécurité
Problématiques

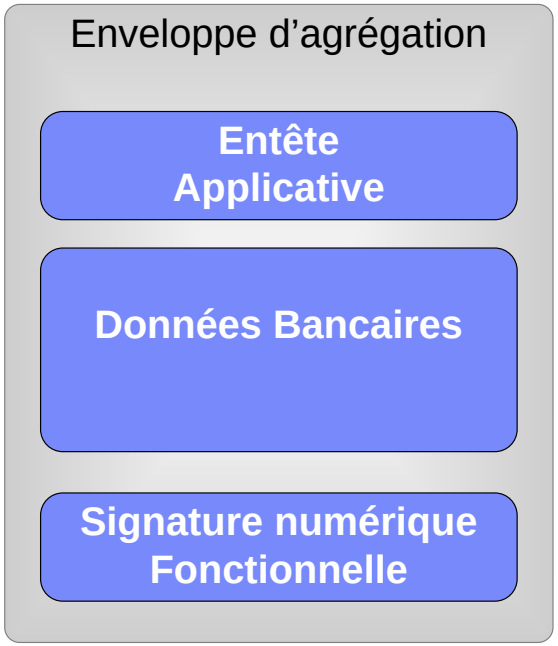
- **Garantir une authentification forte de tous les acteurs du système**
- **Mettre en place des contrôles d'habilitation strictes permettant de limiter les actions possibles en fonction du type d'utilisateur**
- **Garantir une confidentialité totale des données transmises de bout en bout de la chaîne de traitement**
- **Garantir l'intégrité des messages transmis et stockés**
- **Garder trace de toutes les actions effectuées sur le système**
- **Pouvoir associer chaque message traité et chaque action à un acteur de manière non équivoque**

Mise en œuvre de la sécurité
Mécanismes mis en œuvre 1/2

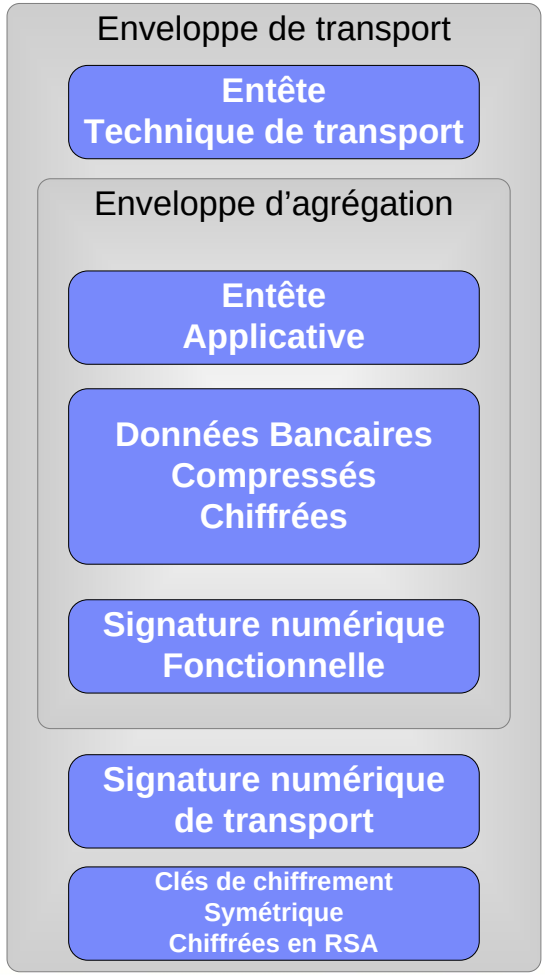
- **Authentification forte des utilisateurs et des applications émettrices de flux financiers par certificat X509**
- **Gestion des habilitations basé sur des profils stockés dans un annuaire LDAP**
- **La confidentialité est garantie par un chiffrement des flux en AES. Les données sont stockées chiffrées. Elles ne sont déchiffrées qu'au moment du traitement**
- **L' intégrité des messages échangés est garantie par la fourniture d'une signature numérique de l'émetteur et d'une signature apposée par la plate-forme assurant le transport du message**
- **Tous les échanges sont tracés et les acteurs authentifiés par leur signature permettant ainsi l'audit et la non répudiation**

Mise en œuvre de la sécurité
Mécanismes mis en œuvre 2/2

Données transmises par les clients de la plate-forme



Données échangées et stockées



Mise en œuvre de la sécurité
Principales difficultés rencontrées

- **La mise en œuvre de l'ensemble de ces mécanismes repose sur des technologies cryptographiques asymétriques nécessitant l'utilisation de clés RSA et de certificats numériques.**
  - Difficultés de mise en œuvre de ces mécanismes avec de clés issus des PKI des différents acteurs du systèmes (Banques françaises)
  - L'interopérabilité entre les implémentations est un élément très important pour le bon fonctionnement du système

- **Difficultés liées au déploiement des clés et à la gestion des secrets**
  - Pas d'utilisation de cartes HSM dans la première version du système

- **Les opérations de chiffrement asymétriques et de signature sont très consommatrices en ressource CPU.**
  - Impact fort sur les performances
  - L'infrastructure doit être dimensionnée en conséquence

- **Les données sont stockées et archivées chiffrées**
  - Difficultés liées à l'archivage des clés sur une longue période

Retour d'expérience sur la mise en œuvre d'une architecture SOA

- **Avantages**
  - Meilleure maîtrise des risques. L'architecture SOA conduit à un système plus structuré, mieux maîtrisé permettant ainsi
    - de réduire les temps de développement et de mise en œuvre
    - de minimiser les risques liés à l'effet tunnel
  - Flexibilité du système permettant une réactivité face aux besoins d'évolution métiers

- **Points de vigilance**
  - La définition de l'interface des services métier est un élément clé de la réussite
    - Les services doivent avoir la bonne granularité.
    - Cela nécessite une collaboration étroite entre experts métiers et architectes SI
  - La mise en œuvre performante d'une telle architecture nécessite une bonne maîtrise des technologies sous jacentes (Bus de Service, Web Services, Sécurité …)