Projet INF 561
Modélisation d'une Banque en ligne

Léopold BOUDARD – Numa CROSTHWAITE
12/12/2006

Table des matières

1 Introduction

Une petite banque privée gère des comptes pour une dizaine de milliers de particuliers et veut offrir à ses clients la possibilité de consulter leurs comptes à distance et d'effectuer certaines opérations résumées dans le diagramme de cas d'utilisation ci-dessous (cf. figure 1).

La banque dispose déjà d'un site web qui présente des informations générales sur ses services et ses produits. On se propose ici de réaliser l'architecture fonctionnelle du service internet sécurisé permettant aux clients de gérer leurs comptes. On modélise dans un premier temps un système bancaire. On donne ensuite un schéma conceptuel de données sur lequel nous nous baserons pour détailler les processus en jeu dans notre application.

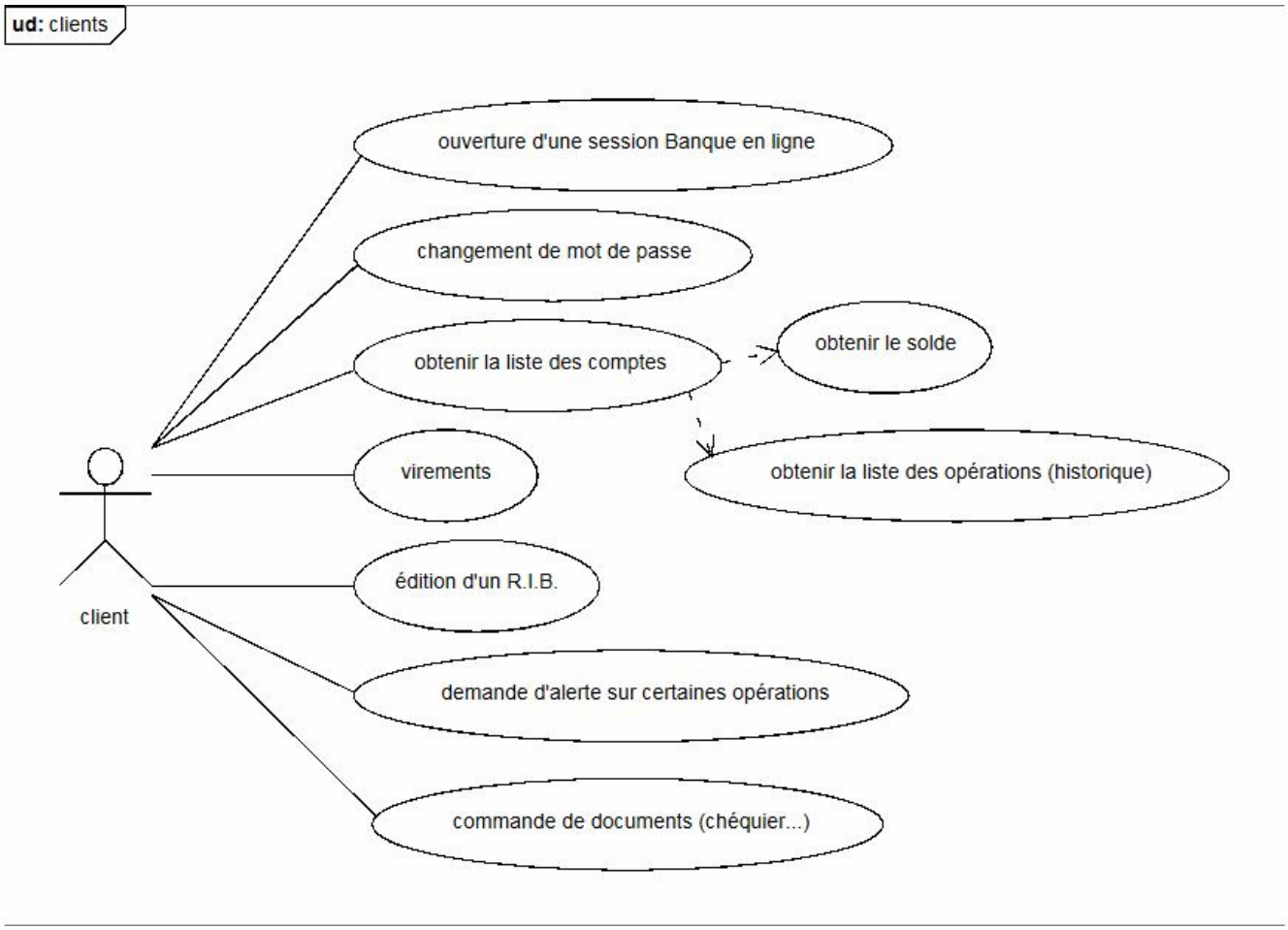


Figure 1: cas d'utilisation de l'application banque en ligne.

2 Modélisation du système bancaire

2.1 Acteurs

Plusieurs types d'acteurs interagissent:

- Les **clients** (particuliers).
- Les **conseillers** interviennent dans la création des comptes et peuvent se substituer aux clients.
- Les **administrateurs** supervisent l'activité du site, mettent à jour son contenu
- Les **services de gestion** des opérations de la banque.
- Le **marché extérieur**. On entend par marché extérieur, le marché boursier sur lequel la banque passe ses ordres d'achat ou de vente de titres, mais également les autres banques et leurs clients.
- L'**application de Banque en ligne** ou bank on line (BOL)

2.2 Flux entre les acteurs

Une modélisation des interactions entre les acteurs est proposée dans le tableau 1 en appendice.

2.3 Modèle de données

Le schéma de la figure 2 ci-dessous représente la structure des données du système d'une banque modélisée à l'aide de DBdesigner. Les entités ont été regroupées en plusieurs sous-ensembles :

- Les acteurs
- Les historiques des comptes mensuels
- Les référentiels comptes et titres
- Les demandes d'opérations
- L'historique opérations
- Les alertes

Il s'agit d'une représentation abstraite qui doit aider à mettre en exergue les processus mis en oeuvre lors du déroulement de l'application.

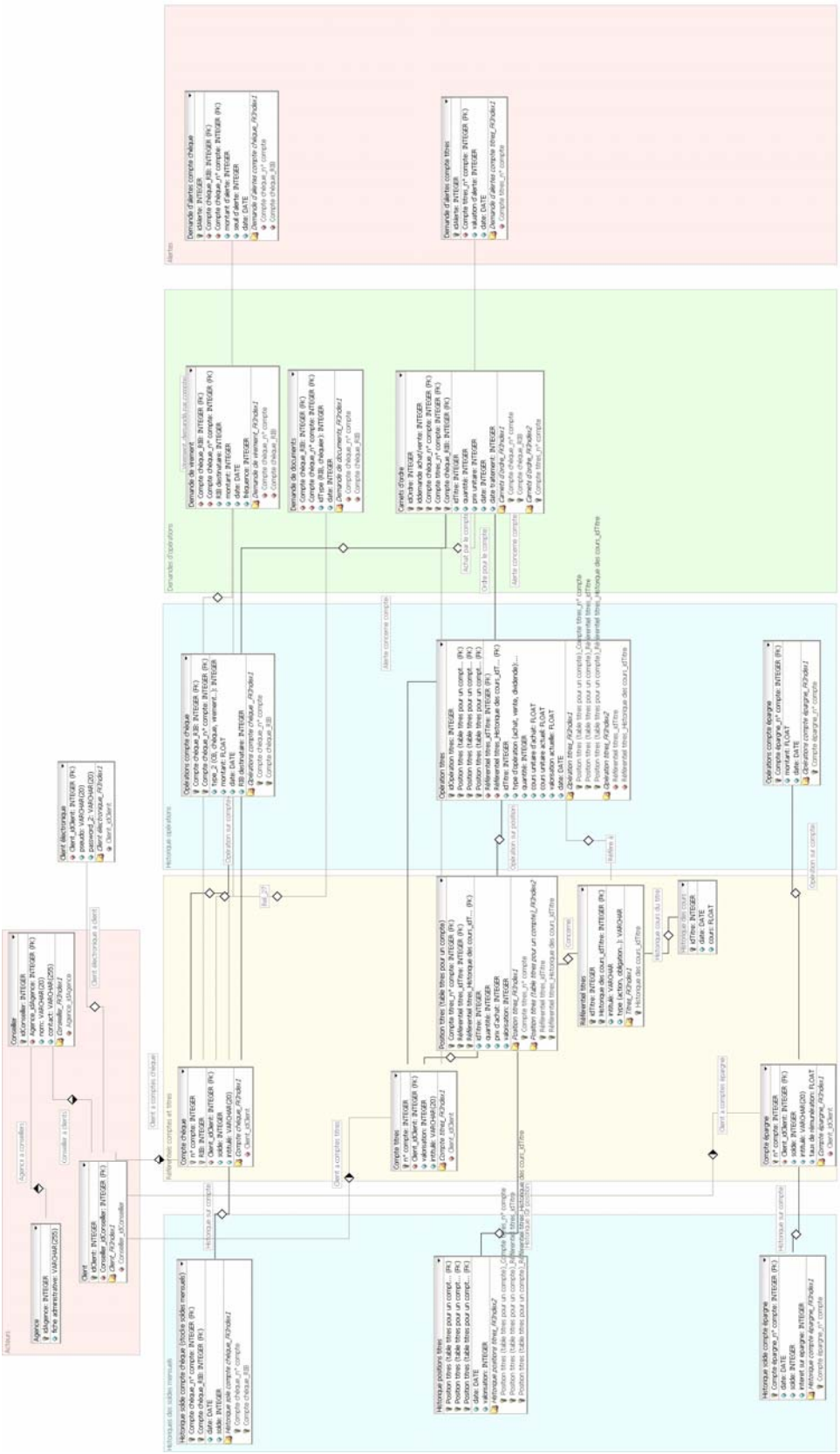


Figure 2: modèle de données.

3 Architecture fonctionnelle

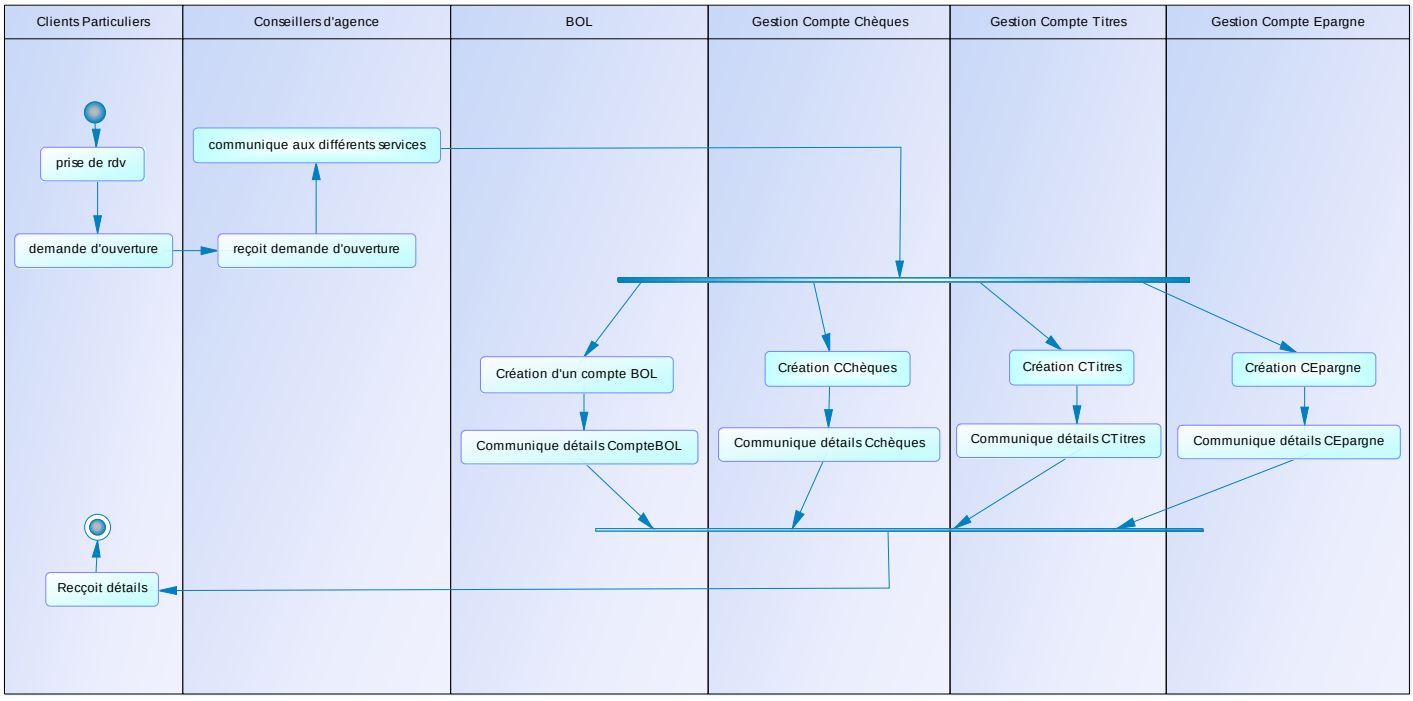
Nous décrivons l'architecture fonctionnelle du logiciel en modélisant les processus du système bancaire qui impliquent l'application BOL. Nous utilisons les normes de la *Business Process Modeling Notation* BPMN et en particulier le concept de « swimlanes » pour représenter la répartition des activités entre les différents acteurs. Les diagrammes ont été réalisés avec la version d'essai de Power Designer de Sybase.

3.1 Processus de « background »

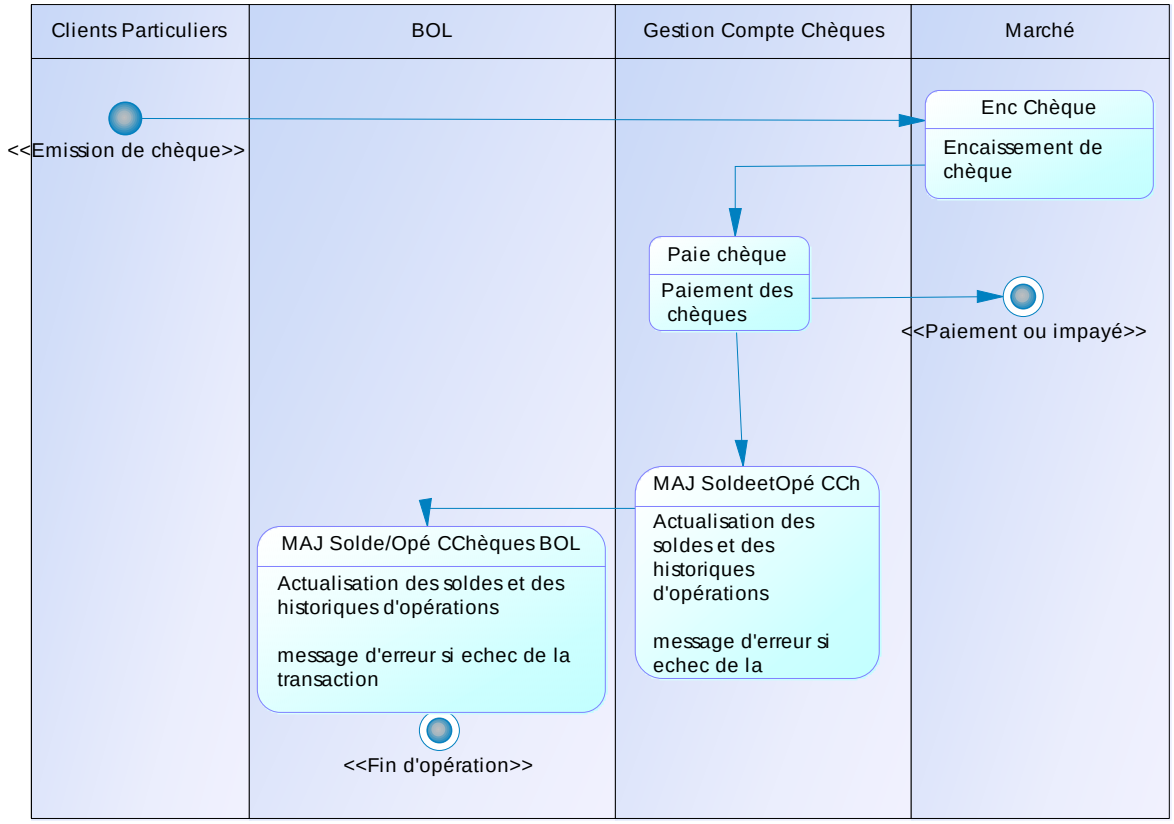
Nous appelons processus de «background » des processus généraux qui décrivent l'activité des comptes d'un client. Ces processus impliquent l'actualisation des bases de données de l'application Banque On-Line (BOL) mais ne découlent pas de l'utilisation du service web.

3.1.1 Ouverture d'un compte

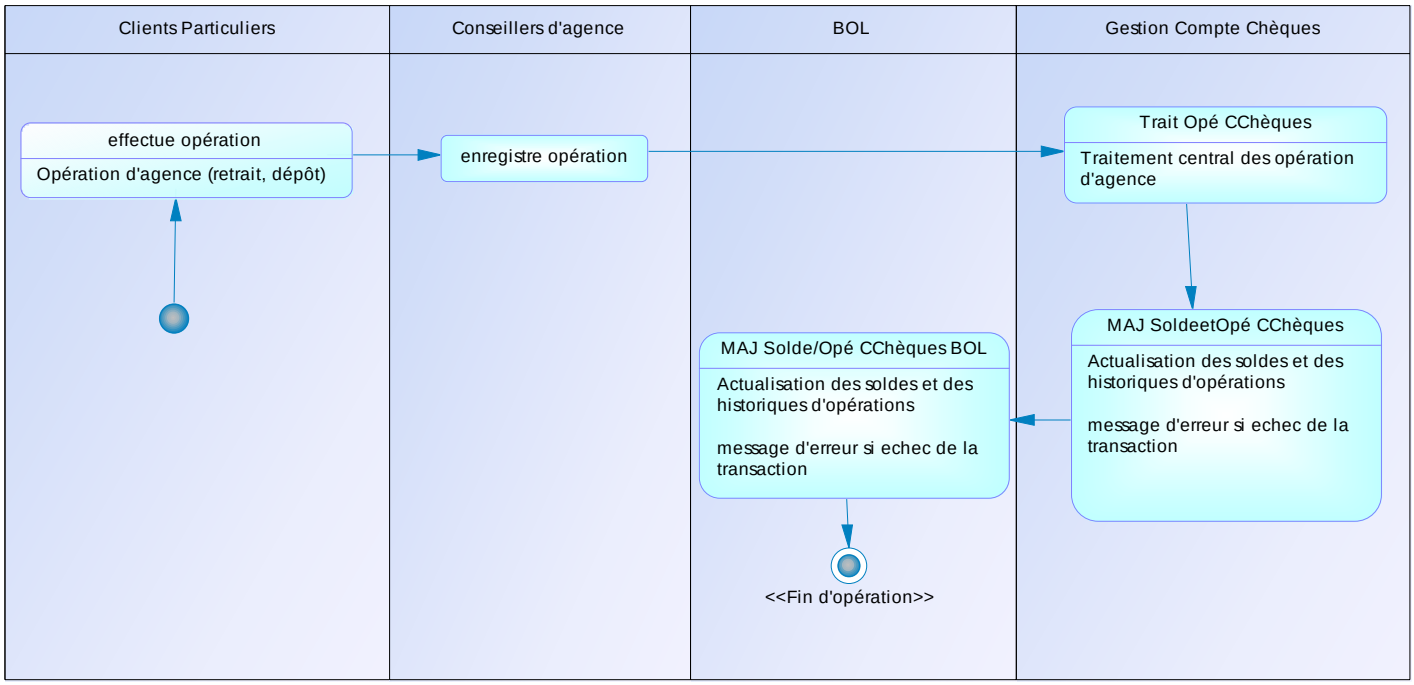
L'ouverture du compte de banque en ligne s'effectue en même temps que l'inscription d'un client à la banque. Elle se fait par l'intermédiaire d'un conseiller (dans une agence) qui transmet la demande d'ouverture aux services de gestion de la banque. Les informations sont ensuite répercutées au client qui récupère entre autre son login et son mot de passe du service BOL.



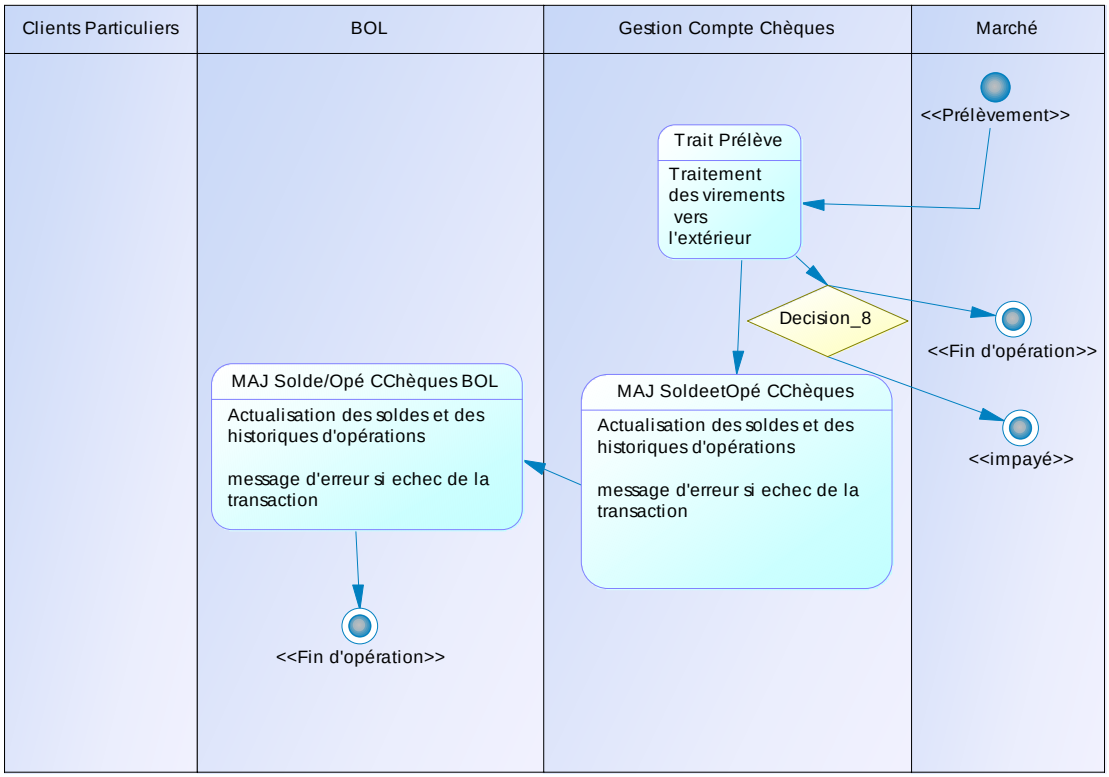
3.1.2 Emission d’un chèque



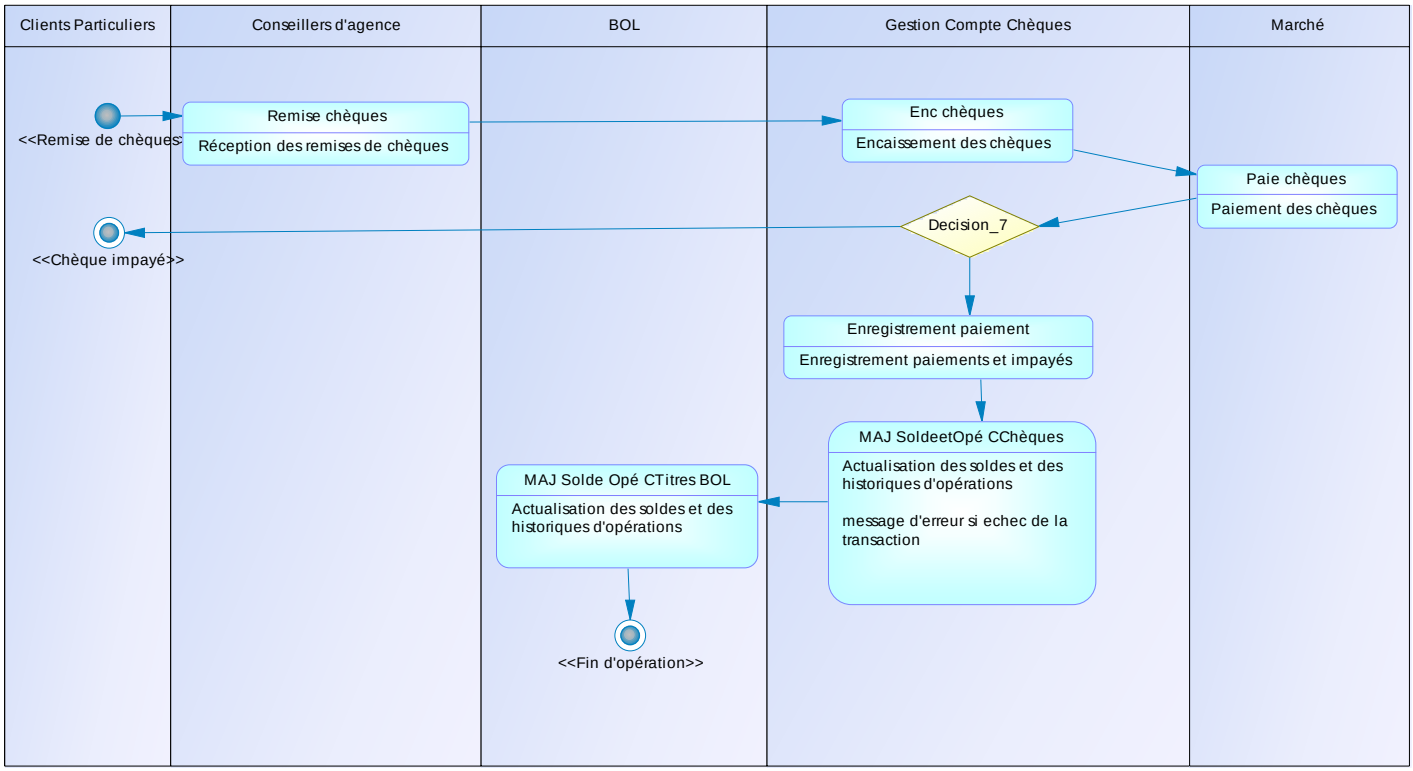
3.1.3 Opérations d'agence



3.1.4 Prélèvements



3.1.5 Remise de chèques



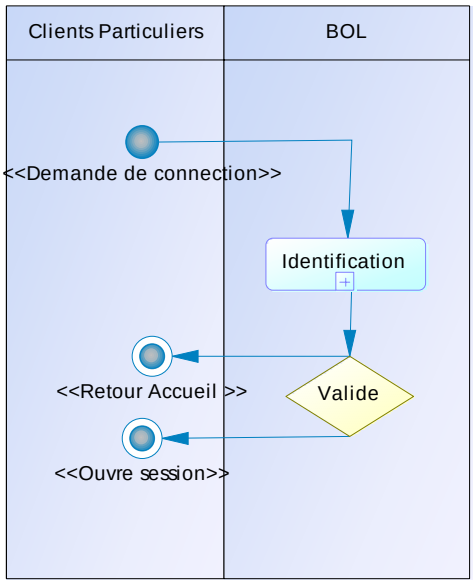
3.2 Processus de « foreground »

Nous désignons par processus de « foreground » les processus qui décrivent les fonctionnalités de l'application web. On modélise par conséquent les fonctions données dans le cas d'utilisation de la figure 1 : démarrage d'une session, modification du mot de passe, demande de mot de passe oublié, achat et vente de titres, consultation des opérations et du solde sur les différents types de compte, demande d'alertes, virements, édition d'un R.I.B et commande de chéquier.

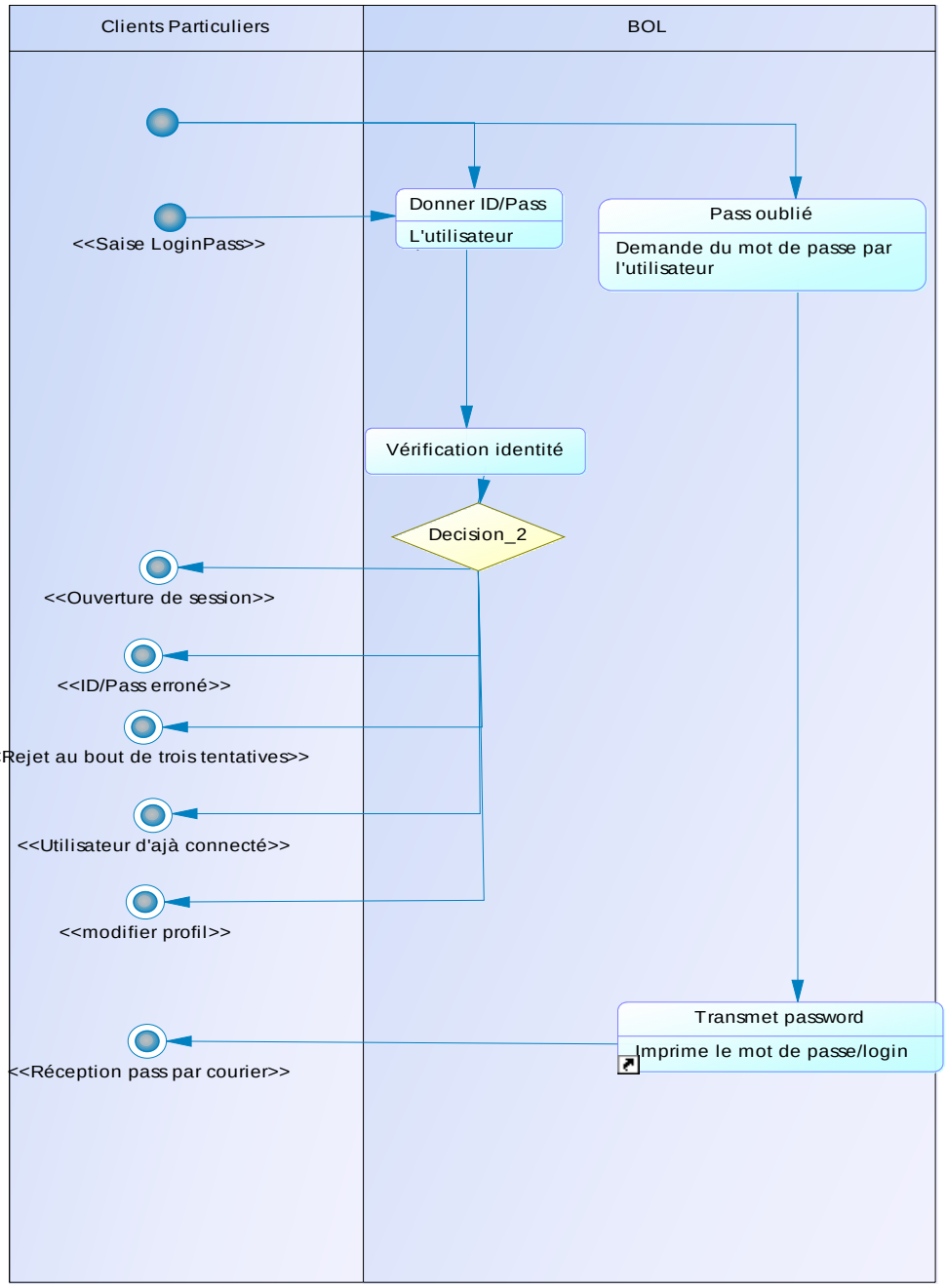
3.2.1 Démarrage d'une session – connexion

Le client dispose d'un login et d'un mot de passe qui lui ont été communiqués lors de l'ouverture de son compte. Il dispose de trois tentatives pour se connecter. S'il oublie son mot de passe, ce dernier peut lui être communiqué à nouveau par courrier. Ce dernier processus est détaillé plus bas (mot de passe oublié).

La connexion initialise une session BOL et précède donc tous les processus décrits ci-après.

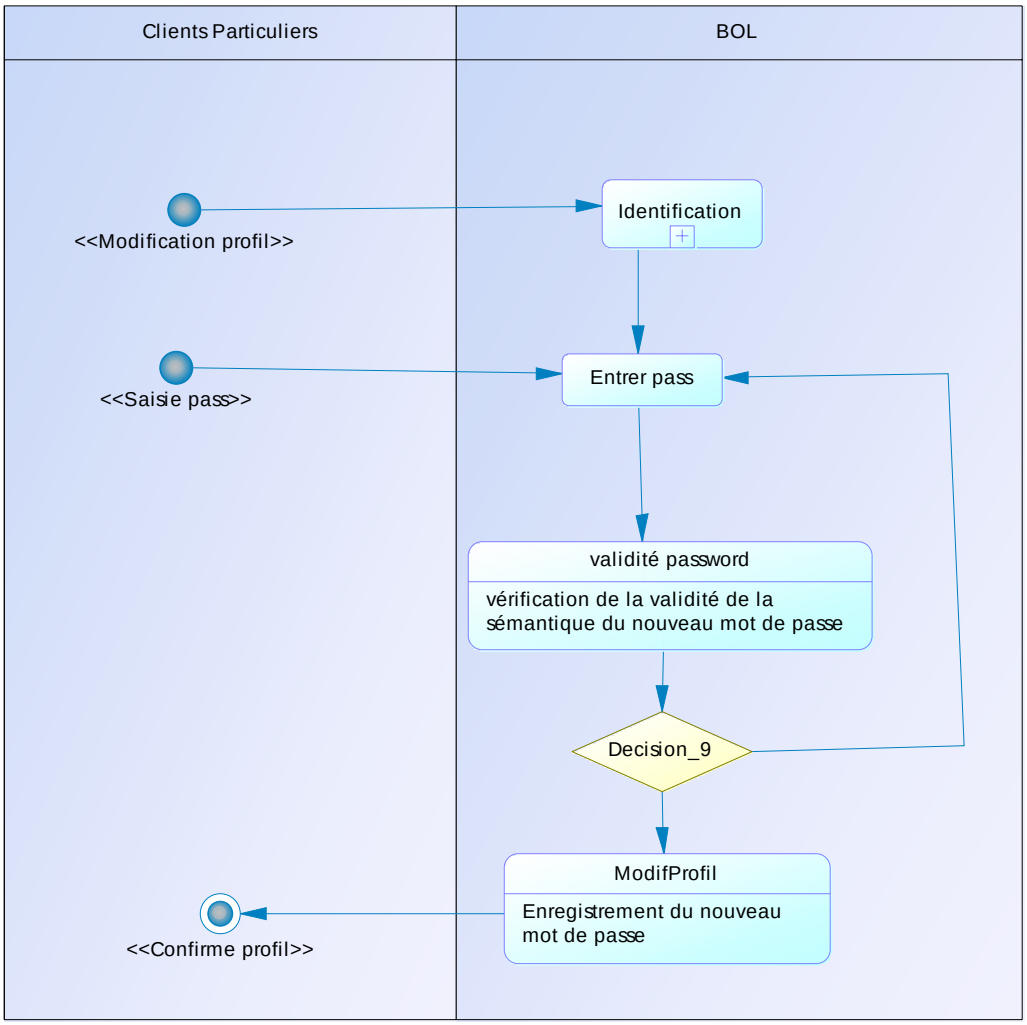

Clients Particuliers
BOL
<<Demande de connection>>
Identification
<<Retour Accueil >>
Valide
<<Ouvre session>>

3.2.1.1 Processus d’identification

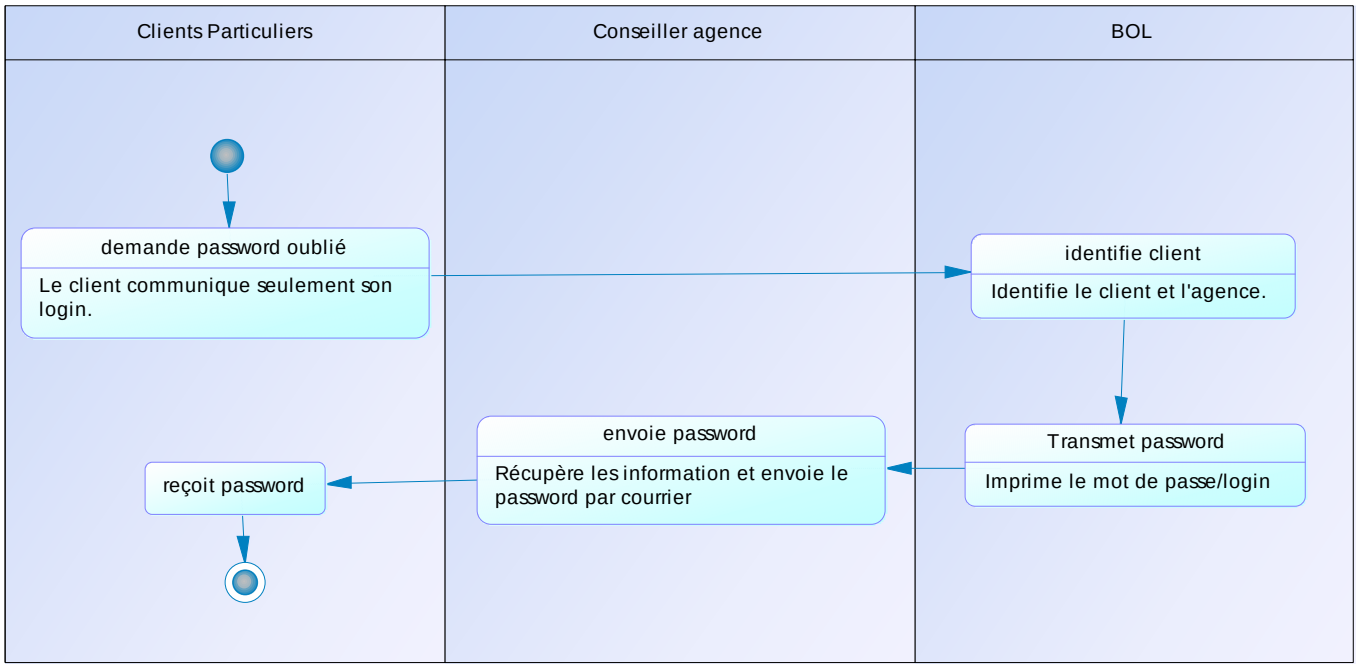


3.2.2 Modification du mot de passe

Le client a la possibilité de modifier son mot de passe. Pour cela, il doit s’identifier à nouveau et entrer un nouveau mot de passe qui respecte des contraintes sémantiques prédéfinies (e.g. doit contenir 10 caractères dont au moins trois chiffres).

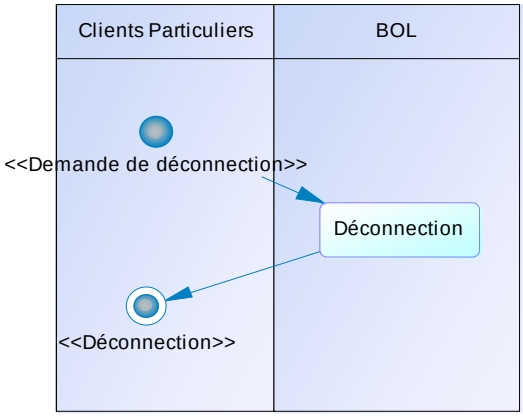

Clients Particuliers
BOL
<<Modification profil>>
Identification
<<Saisie pass>>
Entrer pass
validité password
vérification de la validité de la sémantique du nouveau mot de passe
Decision_9
ModifProfil
Enregistrement du nouveau mot de passe
<<Confirme profil>>

3.2.3 Demande de mot de passe oublié



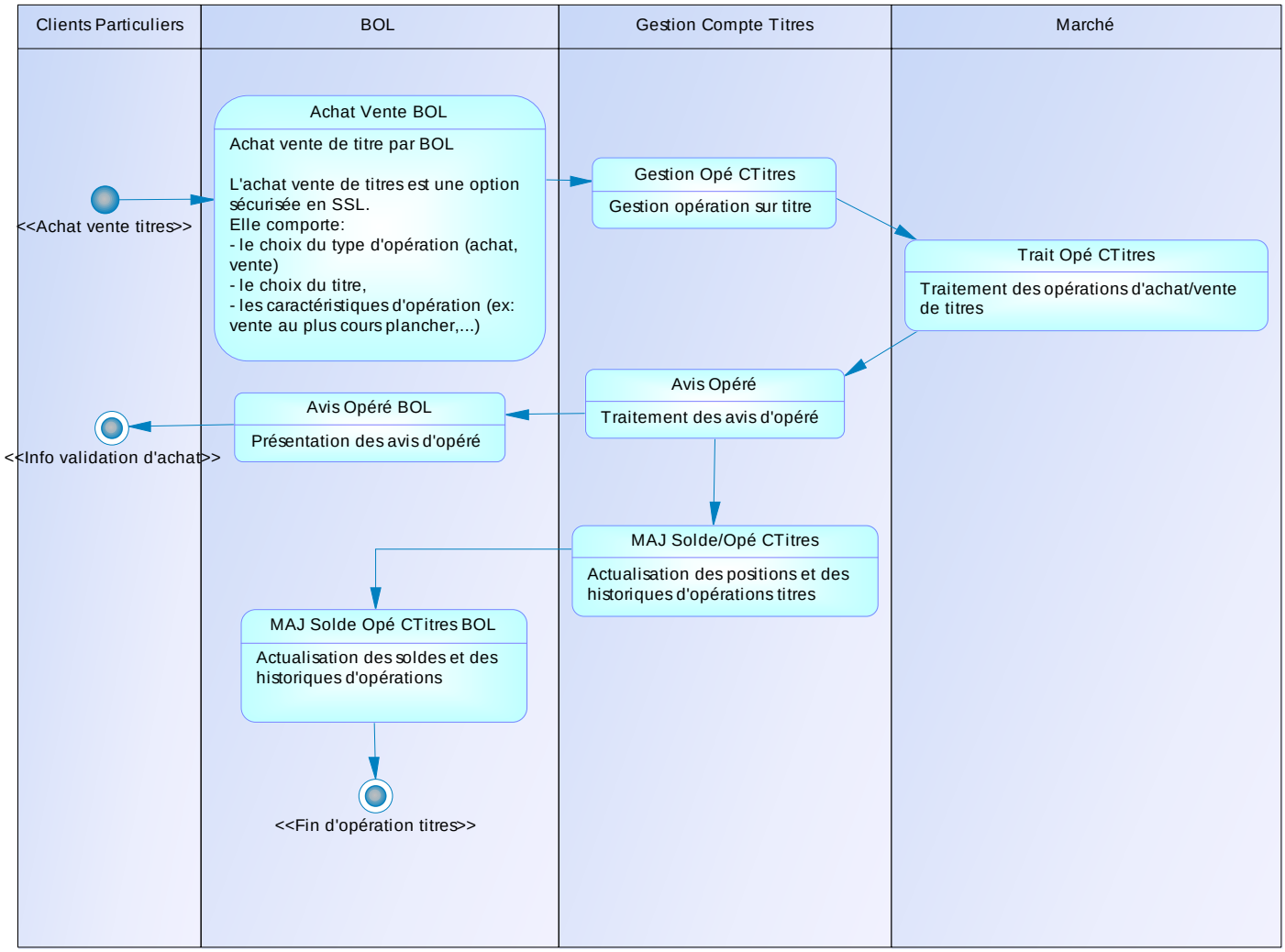
3.2.4 Déconnexion

Une fois qu'il a opéré ses transactions en ligne, le client termine sa session en se déconnectant. Cette déconnexion s'effectue aussi en cas de terminaison involontaire de la session (panne d'ordinateur).



3.2.5 Achat et vente de titres

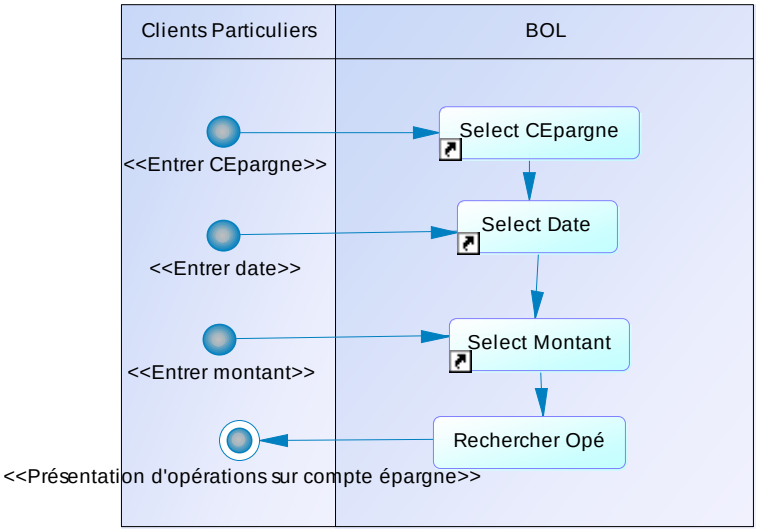
Le client a la possibilité de passer des ordres d'achat ou de vente de titres.



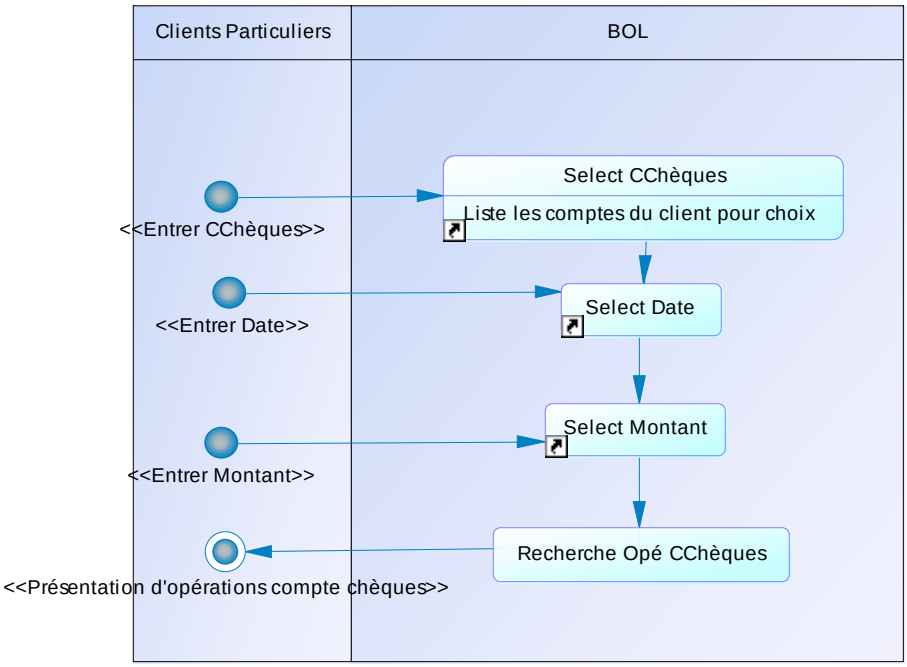
3.2.6 Consultation d'opérations

Le site de la BOL offre la possibilité de retrouver les détails d'opérations effectuées sur les différents comptes en fonction de différents critères. Pour les comptes chèques et épargne, l'utilisateur choisit la date de l'opération et son montant. Pour le compte titres, il choisit un titre, une valorisation et la quantité achetée ou vendue.

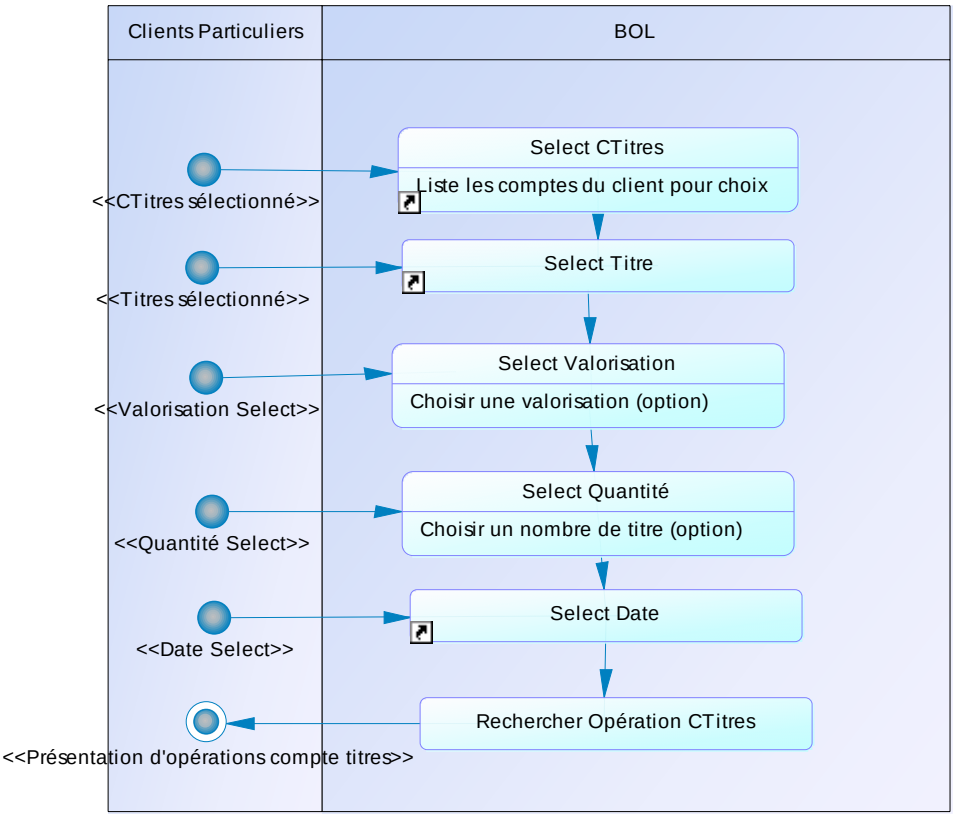
3.2.6.1 sur le compte épargne



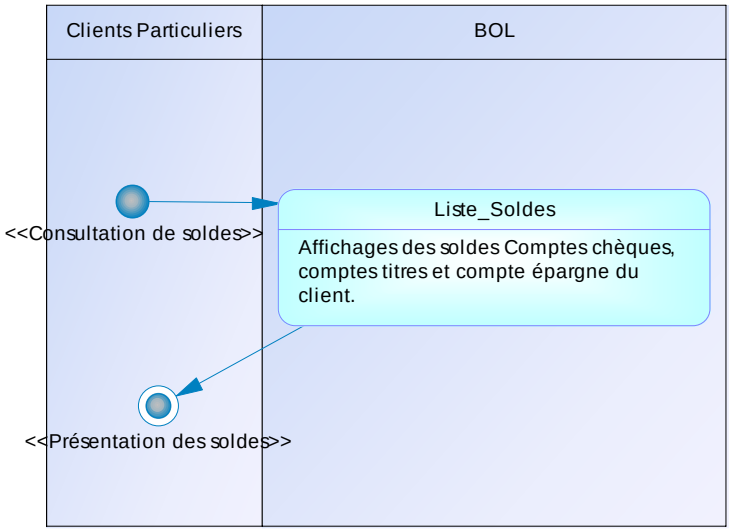
3.2.6.2 sur le compte chèques



3.2.6.3 sur le compte titres

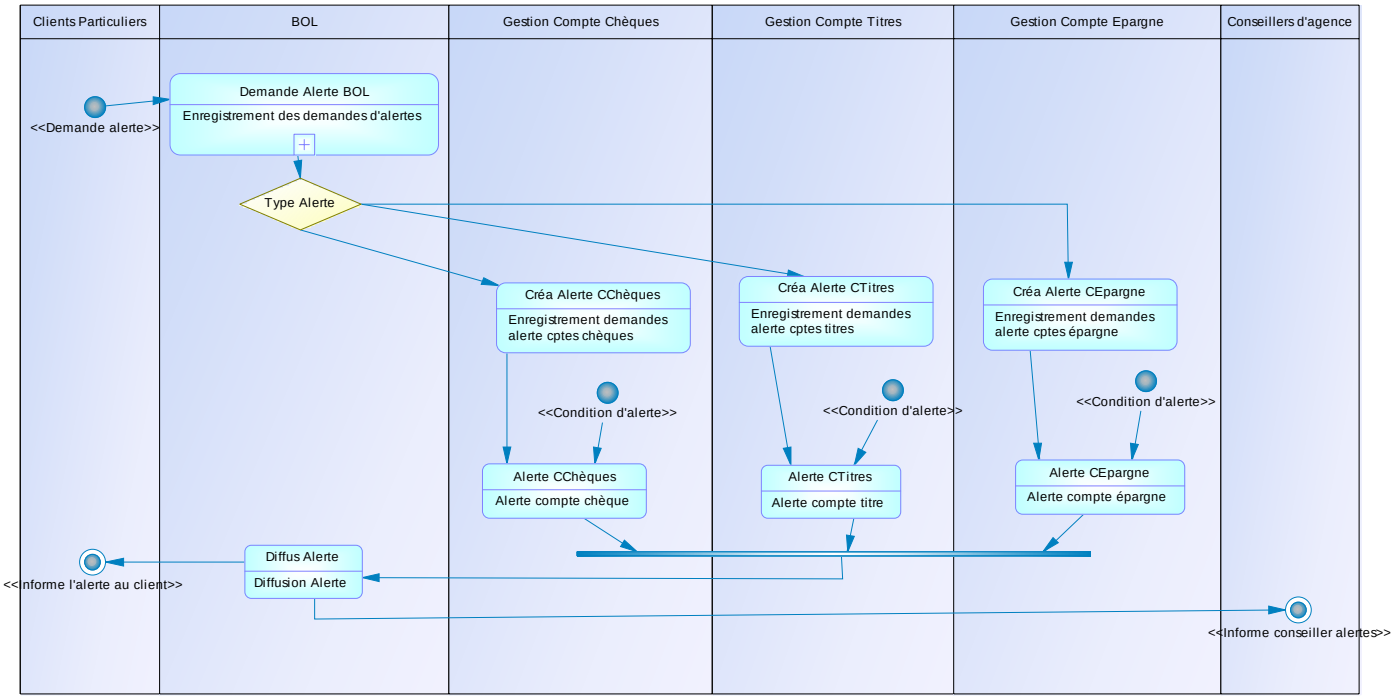


3.2.7 Consultation soldes

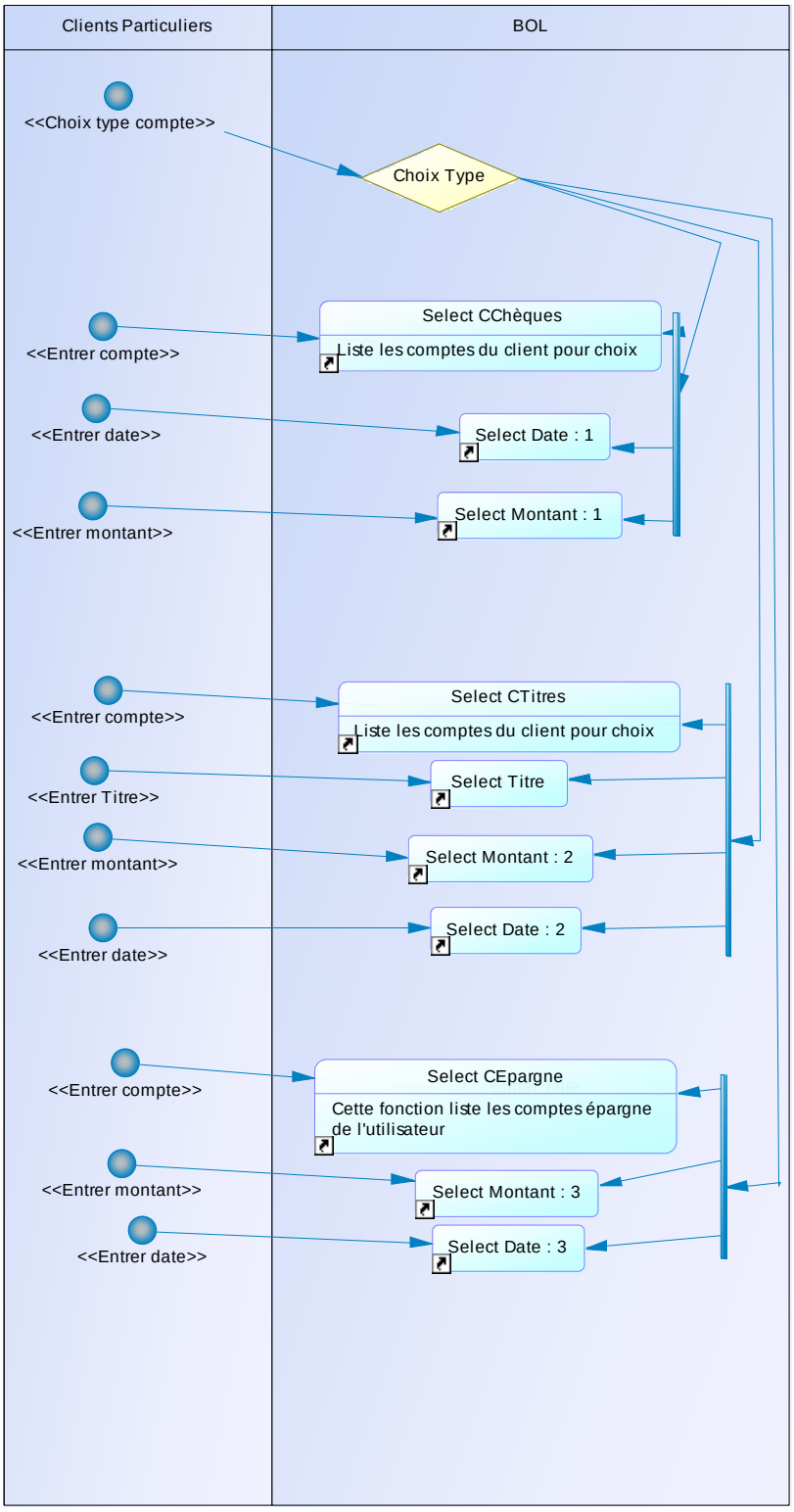


3.2.8 Demande d'alerte

Le client peut demander à recevoir des “alertes” par email ou SMS lorsque des opérations dépassent un certain montant ou, dans le cas du compte titres, lorsqu’une action descend en dessous d’un certain seuil. La période pendant laquelle l’alerte est valide peut être spécifiée (celle-ci peut être rétroactive).

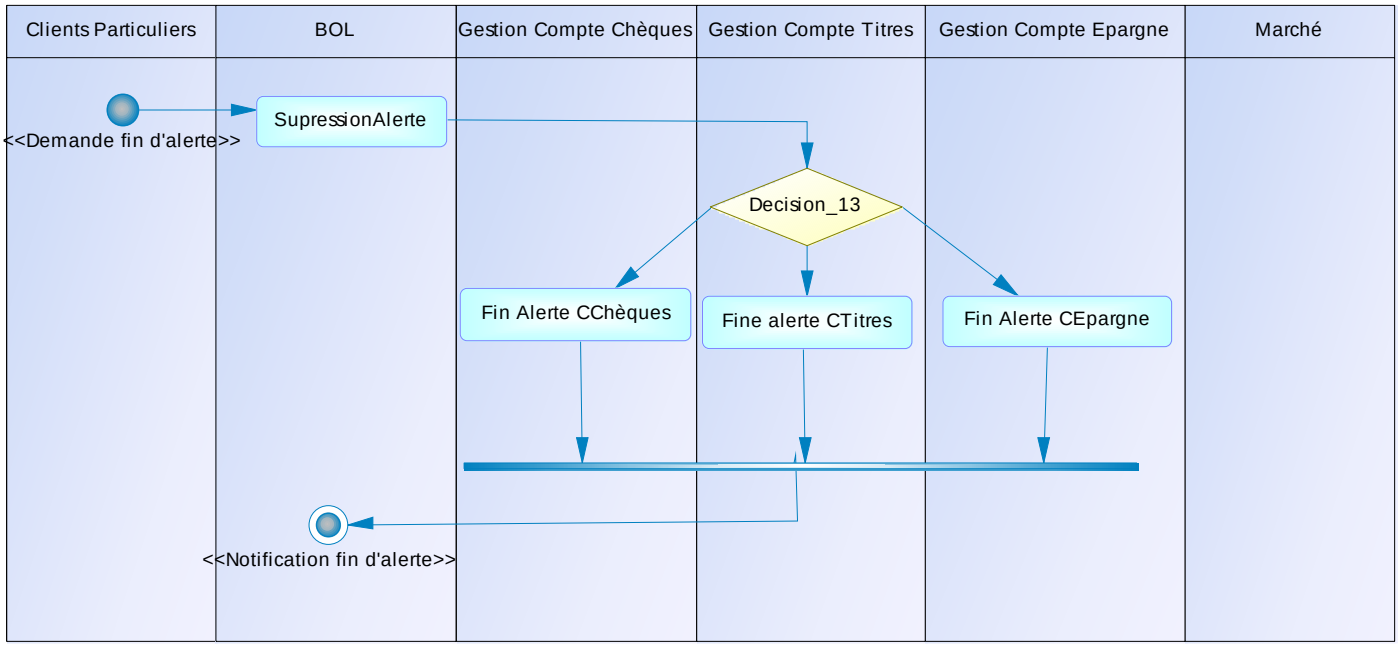


3.2.8.1 Traitement de la demande d'alerte par la BOL



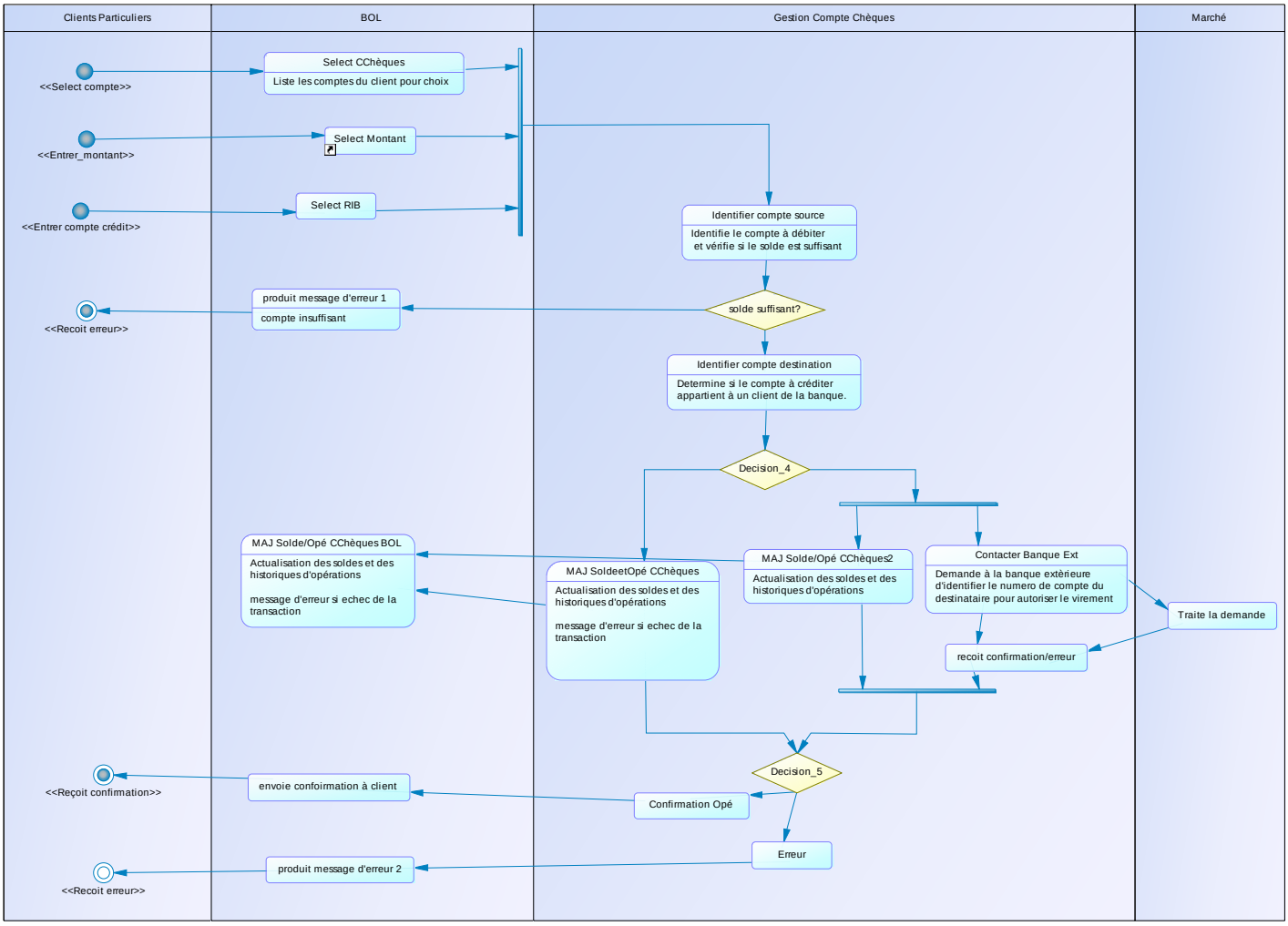
3.2.9 Demande de fin d'alerte

Lorsque le client juge qu'une alerte n'est plus pertinente, il peut la supprimer.

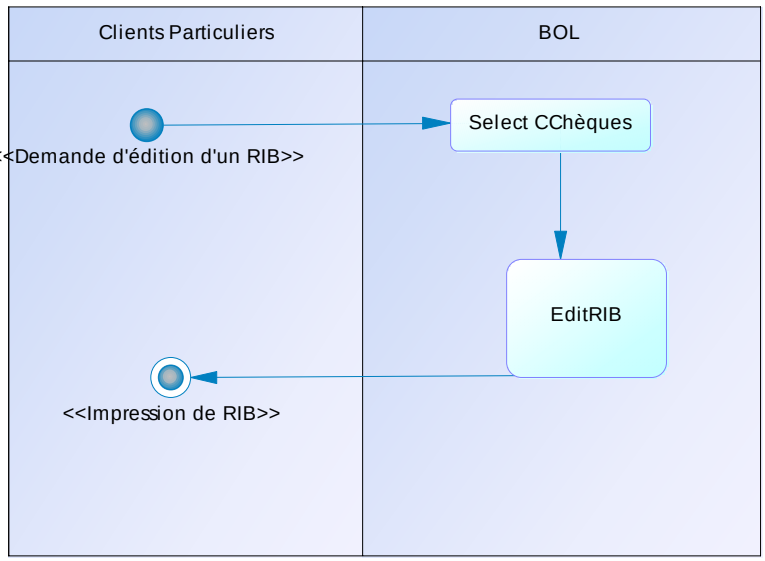


3.2.10 Demande de virement

La possibilité d'effectuer des virements en ligne représente une fonctionnalité importante. L'utilisateur choisit le compte qu'il souhaite débiter, le montant du virement et donne le RIB du compte du destinataire (les virements vers l'étranger ne sont pas pris en compte). Les services de gestion de la banque gèrent les aspects de la transaction qui impliquent des échanges avec d'autres banques. Le diagramme ci-dessous ne détaille donc pas ces aspects et en particulier les mécanismes complexes de compensation entre les banques. Les virements peuvent évidemment également s'effectuer entre clients de la banque ou entre les comptes d'un même client (du compte chèque vers le compte courant par exemple).

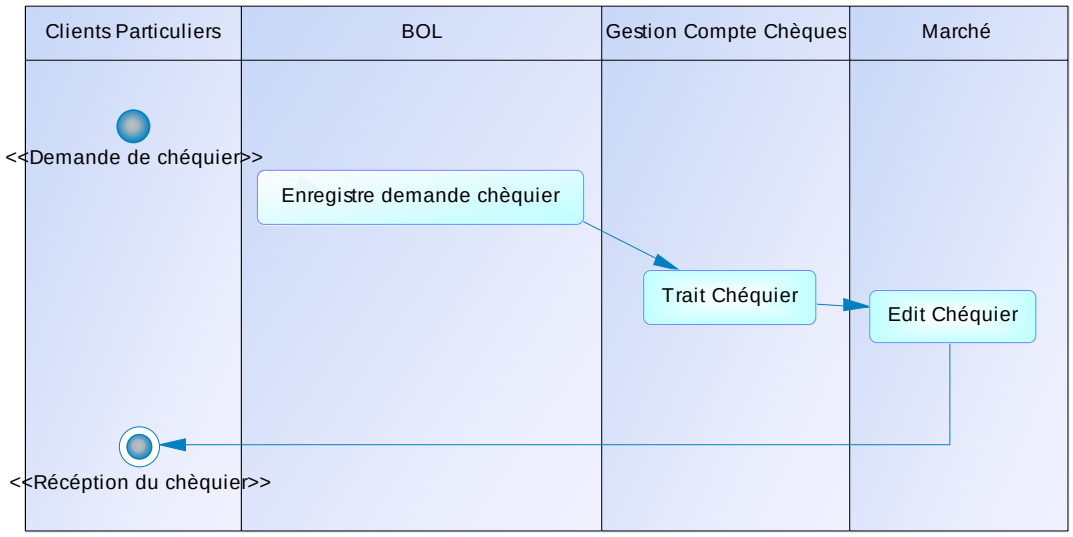


3.2.11 Edition d'un RIB



3.2.12 Demande de chéquier

Le client peut commander certains documents en ligne et en particulier un chéquier qui lui est envoyé par courrier à son domicile.



4 Architecture technique

4.1 Structure du site web

Dans un article intitulée *exploiting UML extensibility in the design of web information systems*, E. Gorshkova décrit une méthode pour modéliser la structure et le contenu de pages web à partir d'un diagramme de composition, un cas particulier des diagrammes des classe UML. Cette méthode permet également de montrer comment elles sont liées aux objets métiers qu'elles représentent.

La figure 3 ci-dessous présente le diagramme de composition de notre site de banque en ligne. Le contenu d'une page peut être représenté par une classe. Ces classes sont stéréotypées `<<page>>`. Les éléments de la page sont présentés comme des attributs. Un contenu commun à plusieurs pages peut être représenté par une classe séparée. C'est le cas dans notre application de la classe menu qui permet d'accéder aux différentes pages.

Certaines pages requièrent que l'utilisateur entre des données. Ces pages sont stéréotypées `<<formulaire>>`. Les attributs d'un formulaire correspondent aux données d'entrée qui sont transmises aux serveurs de la banque après validation (les attributs stéréotypés `<<submit>>` correspondent à de boutons de confirmation). Les entrées peuvent se faire au moyen d'un menu déroulant (`<<select>>`) ou directement au clavier (`<<edit>>`). Certaines pages présentent une liste d'objets qui peuvent être le résultat d'une requête. Ces pages ont le stéréotype `<<liste>>`. Les classes de ce stéréotype ont au moins un attribut de stéréotype `<<tableau>>` qui correspond à un tableau d'objets qui disposent de liens vers des pages présentant leur détail. Par exemple, chaque compte dans le tableau de la liste des comptes renvoie à l'historique du compte correspondant.

Le diagramme présente également les liens entre les différentes pages. Une association entre une page source et une page cible est désignée par le stéréotype `<<lien>>`.

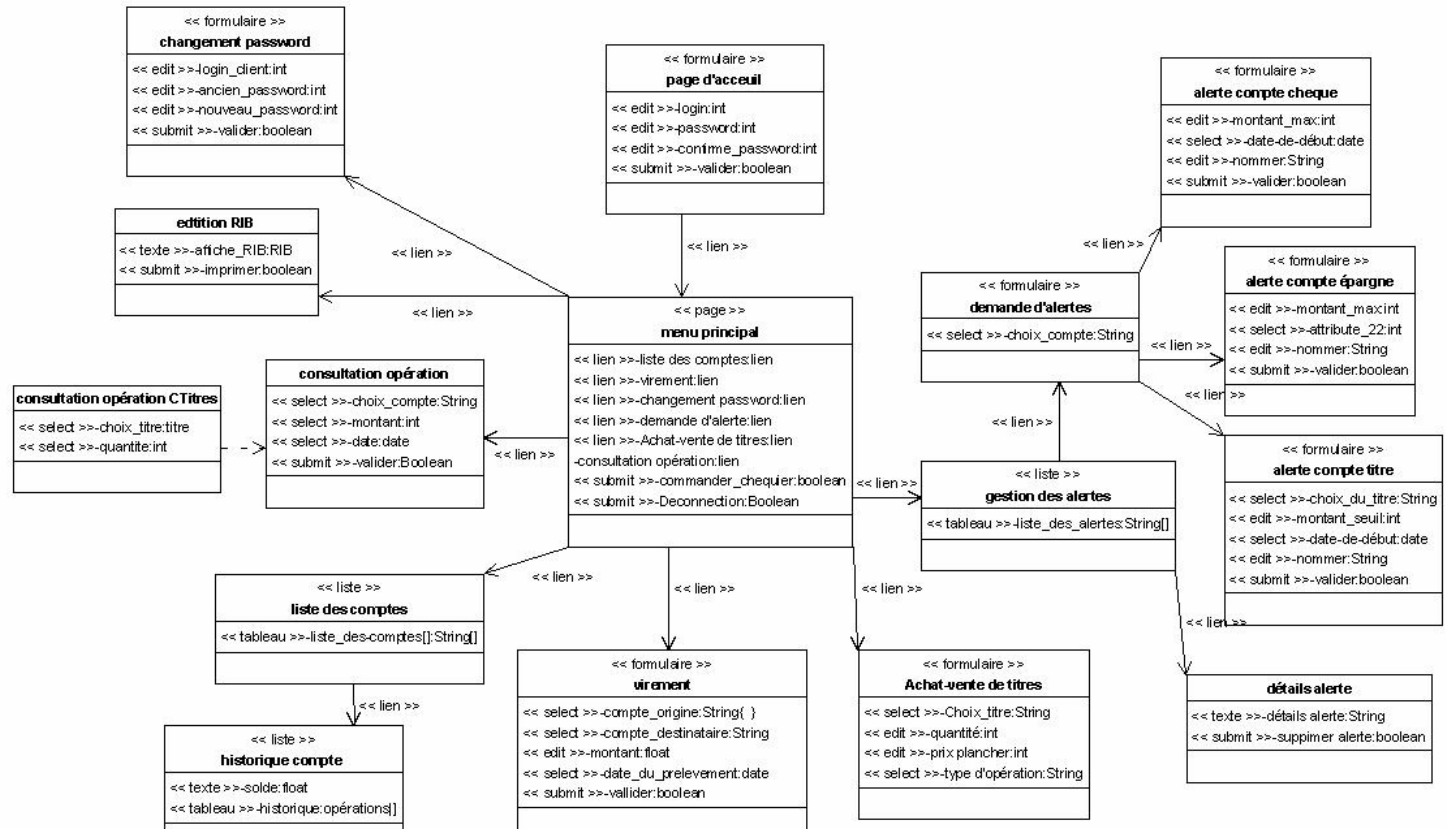


Figure 4 : diagramme de composition du site de banque en ligne

4.2 Sécurité

Dans le cadre de notre application, les questions de sécurité interviennent à différents niveaux :

- sécurité du login et du mot de passe de connexion
- confidentialité des transactions et des informations du client sur la banque en ligne
- protection et garantie des informations échangées avec les services de gestions de la banque et les agences
- protection et garantie des informations transmises au client
- protection de la session

Chacun de ces problèmes met en question différents processus qui nécessitent d'être traités un par un, selon le niveau de flexibilité et de sécurité qu'on souhaite apporter aux opérations. La garantie

du bon fonctionnement du serveur , et notamment la résistance aux attaques, est également nécessaire et inhérente à l'architecture technique et logicielle.

4.3 Sécurité du login et du mot de passe

Compte tenu du fait qu'on donne la possibilité à l'utilisateur de réaliser des transactions vers l'extérieur, il est nécessaire d'introduire un haut niveau de sécurité dans la connexion du client. Le login et le mot de passe devront correspondre à des normes de sécurité élevées. A un client correspondra un seul et unique login.

Pour éviter les attaques, on limitera le nombre de tentatives de connexion, avec éventuellement un changement de mot de passe en cas d'échec. La transmission du login et du mot de passe initial devra être effectuée directement par l'agence par courrier.

4.3.1 Confidentialité des transactions et des informations du client sur la banque en ligne

Pour garantir la confidentialité des transactions et des informations (login, mot de passe) données par le client, il sera nécessaire d'établir une connexion cryptée SSL, durant toute la durée d'une session:

- le client connecté au site déclenche une requête de formulaire sécurisé ;
- le client crée une clé privée qu'il conserve durant toute la durée de la session et une clé publique envoyée au serveur ;
- le serveur crée une clé de session en cryptant un message aléatoire à partir de la clé publique et l'envoie au client ;
- le client crypte la clé de session avec sa clé privée et la renvoie au serveur qui en vérifie l'authenticité avec sa clé publique ;
- le reste des transactions est alors effectué avec la clé de session

En dehors du login et du mot de passe, aucune information concernant un client ne sera stockée dans les bases de données du serveur. Aucun cookie ne sera envoyé pour l'identification, on interdira au navigateur de retenir le login ou le mot de passe.

Éventuellement, un niveau de sécurité supplémentaire devra être introduit dans les couches de transaction (virement et achat de titre). Un password pourra être généré pour chaque transaction, et envoyé, via l'agence, par courrier électronique certifié.

4.3.2 Protection et garantie des informations échangées avec les services de gestions de la banque et les agences

Toutes les demandes de transactions effectuées sur la banque en ligne doivent circuler vers les services de gestion de la banque via un réseau privé et sûr (sans faille de panne matérielle ou de concurrence).

Les mises à jour d'historiques et d'opérations pourront transiter sur le web avec une connexion sécurisée.

4.3.3 Protection et garantie des informations transmises au client

Les informations transmises aux clients font appel à 3 niveaux de sécurité :

- les informations sur les comptes, tels que les historiques et les RIB, sont protégées de l'extérieur avec la connexion SSL. Ces informations devront être protégées au mieux contre la copie; ne permettant à l'utilisateur qu'une impression ou une consultation sur site.
- les informations de login et mot de passe doivent rester confidentielles. Il est préférable pour les demandes de mot de passe de passer systématiquement par l'agence qui déclenche un envoi par courrier.
- les alertes pourront être envoyées par courrier électronique via l'agence.

4.3.4 Protection de la session

Pour éviter les situations bloquantes et limiter les problèmes de concurrence, nous n'acceptons qu'une seule session par utilisateur. Nous limitons également la durée de connexion à 30 minutes.

4.4 Langage envisagé

Compte tenu des contraintes de sécurité, et notamment de la protection des informations transmises, et de volume, J2EE est sans doute le plus adapté pour la création du site de banque en ligne.

Pour des questions de coût et de facilité de dialogue avec les bases de données, une solution de type LAMP serait également tout à fait envisageable en ce qui concerne le serveur. La question du dialogue avec les services de gestions et les agences reste néanmoins ouverte.

5 Conclusion

L'enjeu principal de la modélisation du logiciel de banque en ligne BOL réside dans la multiplicité des fonctionnalités offertes à l'utilisateur tout en gardant en point de mire les problématiques de sécurité. La description des processus en jeu dans l'application, ainsi que la modélisation de l'architecture du site que nous proposons ici permettront d'aboutir à la production d'une application facilement modulable. Il apparaît effectivement facile d'élargir le champs de l'application en offrant par exemple la possibilité d'effectuer des virements périodiques ou en étendant le nombre d'opérations boursières réalisables.

L'architecture proposée, si elle est relativement complète au point de vue des fonctionnalités proposées à l'utilisateur, reste néanmoins très superficielle ; il est désormais à la charge des ingénieurs logiciel de rentrer dans le détail de l'application, en suivant la démarche de raffinements des processus. Il est notamment nécessaire de s'intéresser aux fonctions mises en œuvre par les processus et à la nature des flots d'information.

Enfin, les solutions aux problèmes de sécurité abordés dans la dernière partie doivent être traités plus en détails avant l'implémentation.

APPENDICE

	Particuliers	Banque						Opérateurs de Marché, tiers
		Conseillers d'agence	Administrateurs BDL	BDL	Gestion des Cpte Chèques	Gestion des Cptes Titres	Gestion des Cptes Epargne	
Particuliers		.Demande ouverture/MAJ client/compte .Operations d'agence .Demandes opposition .Demande de mot passe oublié	.Demande de mot de passe	.Consultation de soldes de compte .Consultation d'opérations Edition de RIB .Commandes de document .Demandes de virement .Demandes d'Achat/Vente de titres .Demandes d'alertes .Demande de contact du conseiller .Information sur les produits .Modification profil et mot de passe .Demande de mot passe oublié				.Opérations bancaires
Conseillers d'agences	.Communication de mot de passe oublié		.Demandes ouverture/maj client compte	.Demandes d'opposition .Demande de mot de passe oublié	.Opérations d'agence	.Opérations d'agence	.Opérations d'agence	
Administrateurs BDL	.Envoi du mot de passe initial	.Communication de mot de passe oublié		.Supervision de l'activité du site .Mise à jour de contenu du site				
BDL	.Présentation de soldes de comptes .Présentation d'opérations .RIB imprimables .Information sur les produits .Mots de passe oublié	.Demandes de contact du conseiller			.Commandes de documents .Demandes de virements .Demandes d'alertes	.Demandes d'achat/Vente de titres .Demandes d'alertes		.Virements .Achats/ventes de titres
Gestion des Cpte Chèques	.Documents commandés .Cpte rendus de virements .Alertes sur solde ou sur opération			.Soldes cpte chèques actualisés .Historiques d'opérations	.Virements internes		.Virements internes	
Gestion des Cptes Titres	.Cpte rendus d'opération titres .Alertes sur titres			.Soldes de positions titres .Historiques d'opérations achat/vente .Historiques de dividendes/coupons				
Gestion des Cptes Epargne				.Soldes de comptes Epargne .Historiques d'opérations .Décomptes d'intérêts				
Opérateurs de Marché, tiers					.Opérations bancaires	.Compte rendu achat/vente de titres .Dividendes/Coupons versés		

Tableau 1: tableau des flux entre acteurs