NewBank : Merchant webapp

Equipe B

Yahiaoui Imène - Gazzeh Sourour - Ben aissa Nadim

Al Achkar Badr

Sommaire

Mises à jour de l'incrément :

Dans cet incrément :

- Nous avons encore modifié légèrement notre architecture en retirant la gestion des frais de notre PaymentGateway et les mettants dans un nouveau service FeesCalculator, et en ajoutant une base de données en mémoire pour la mise en cache des transactions au niveau de PaymentService.
- Nous avons ajouté explicitement les hypothèses manquantes et qui ont guidé notre conception

Les modifications apportées aux explications écrites déjà fournies sont indiquées en rouge. La partie ‘Proposition d’architecture du système’ est réécrite pour incorporer les interfaces externes et internes.

Introduction

Le présent rapport a pour but de mettre en lumière le sujet qui nous a été assigné, puis d'aborder la portée, les utilisateurs, les risques et les cas d'utilisation associés. De plus, nous avons élaboré un diagramme de composants qui sera présenté et expliqué.

Projet

La portée de ce projet englobe le développement et le déploiement d'une application web spécialement conçue pour les commerçants. Elle inclut l'intégration d'un kit de développement logiciel (SDK) pour faciliter les paiements par carte de débit et de crédit sur les sites web des commerçants. De plus, elle couvre la gestion des frais de transaction pour les transactions en ligne sans numéraire au sein du système bancaire.

Utilisateurs

1. Utilisateurs Principaux :
    - Commerçants : Ceux qui possèdent et exploitent des entreprises et qui utilisent l'application web pour gérer les transactions.
    - Clients : Individus effectuant des achats auprès des commerçants en utilisant des cartes de débit/crédit.
2. Utilisateurs Secondaires :
    - Administrateurs de la Banque : Responsables de la supervision du système bancaire en ligne sans numéraire.
    - Administrateurs Système : superviser la suppression de comptes et de cartes, de gérer les données sensibles et d'assurer la sécurité en cas de perte ou de vol.
    - Credit Card Network : ce réseau va nous solliciter afin d'autoriser une transaction chez nous (NewBank), notre système communiquera avec lui afin de lui demander de créer des cartes virtuelles.
    - Banques externes: Les banques externes nous solliciteront pour les transferts des fonds.

Risques Possibles

- Préoccupations en matière de sécurité : Risques liés à la gestion des transactions financières. Possibilité de violation de la sécurité des données sensibles des utilisateurs, ce qui pourrait entraîner des conséquences graves pour la confidentialité et la confiance des clients.

- Intégration : Difficultés pour intégrer de manière transparente le SDK dans divers sites web de commerçants.
- Scalabilité : S'assurer que le système peut gérer un grand nombre de clients (jusqu'à 1 million) sans problèmes de performance.
- Haute Disponibilité : De même, soutenir la gestion en temps réel d'un grand nombre de transactions.
- Extensibilité : Comme notre système interne sera étendu en premier lieu par un sdk fourni par nous.
- Robustesse : Comme le kit de développement est fourni par nous et permet l'utilisation de nos services par de nombreuses entreprises, c'est à nous de garantir la robustesse contre les entrées et les essais erronés pour faire tomber notre service.

Cas d'Utilisation

- Enregistrement et Intégration des Commerçants :

Description : Un commerçant s'inscrit sur l'application web, fournissant les détails nécessaires à l'intégration au sdk.

- Gestion des Comptes Clients :

Description : Les clients peuvent créer et gérer leurs comptes, y compris les comptes d'épargne. Ils ont la capacité d'effectuer des opérations telles que l'ouverture de nouveaux comptes, la consultation des comptes existants.

- Consultation de Solde et Historique des Transactions Client :

Description : Les clients peuvent consulter le solde et l'historique des transactions de leur compte. Cette fonctionnalité permet d'obtenir des informations détaillées sur les mouvements associés au compte client.

- Virement entre Comptes :

Description : Les clients ont la possibilité de réaliser des virements entre leur compte bancaire et le compte associé à la carte de notre service.

- Traitement des Transactions avec Cartes de Débit/Crédit :

Description : Les commerçants initient des transactions en utilisant les détails des cartes de débit/crédit, qui sont traités de manière sécurisée par le système.

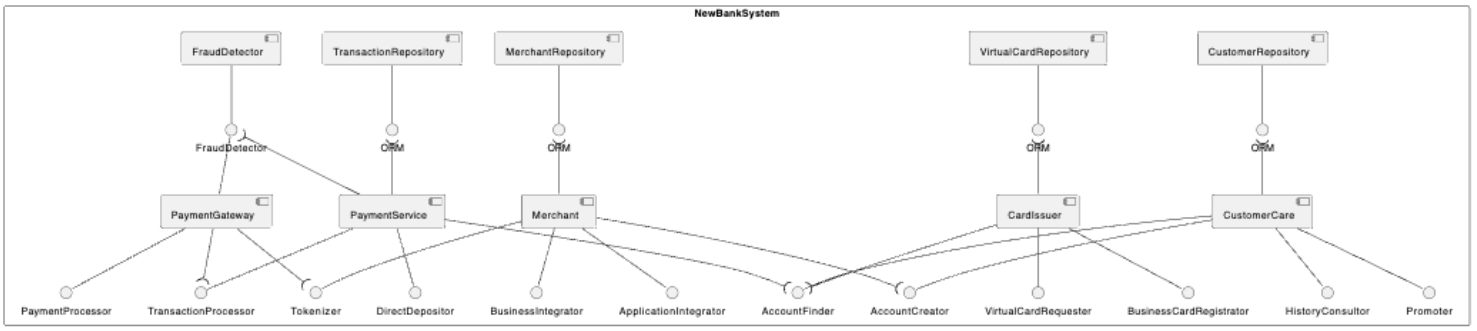
- Gestion des Frais de Transaction :

Description : Le système calcule et gère les frais de transaction associés à chaque transaction, assurant une facturation précise.

Diagramme de Composants :

Lien pour la version svg plus claire : architecture.svg

Pour démarrer notre conception architecturale, nous avons commencé par un diagramme de composants dans lequel nous avons essayé d'identifier les principaux composants métier qui entreront en jeu. Nous considérons ces composants comme les briques de notre compréhension de la logique métier que nous devrons mettre en œuvre.
C'est donc sur cette base que nos décisions en matière de conception architecturale émergeront.



Chaque composant est conçu pour jouer un rôle spécifique :

- CustomerCare : Ce composant gérera toute la logique liée à l'intégration des clients dans notre banque sans numéraire, de la création d'un compte à l'affichage de l'épargne et de l'historique des transactions.

- CardIssuer : Ce composant contiendra la logique d'émission de cartes virtuelles par la banque à ses clients, et permettra aux entreprises d'enregistrer différents types de cartes virtuelles qui pourraient leur servir à fidéliser leurs clients, par exemple des cartes-cadeaux, des cartes de restaurant, etc.

- Merchant : Ce composant assurera l'intégration des entreprises dans notre banque sans numéraire. Les entreprises qui souhaitent utiliser notre sdk, par exemple, devront avoir leur application enregistrée dans notre système. De même, les entreprises disposent d'une panoplie d'options diverses en ce qui concerne leurs comptes.

- FraudDetector : Comme son nom l'indique, ce composant sera chargé de détecter les activités suspectes et les tentatives de fraude. Ce composant sera utilisé par d'autres composants dans divers scénarios.

- PaymentService : Ce composant gère la logique du service transactionnel de base fourni par la banque. Il traite les demandes de paiement, qu'il s'agisse d'un débit ou d'un crédit d'un compte, gère l'autorisation et la logique de base des transactions et Il utilise le composant de détection des fraudes FraudDetector dans son processus..

- PaymentGateway : Cette composante est la partie exceptionnelle de notre système. C'est la variante sur laquelle nous allons travailler et elle gère toute la logique du traitement des paiements effectués à l'aide de notre sdk. Il sera chargé de contacter le réseau CreditCardNetwork pour la validation des cartes, de déduire les frais de transaction et d'utiliser le mécanisme de tokenisation fourni lors de l'intégration du merchant pour authentifier et crypter ce trafic. Il utilisera également le détecteur de fraude.

- Les repositories représentent des composants responsables de la gestion et du stockage des données.

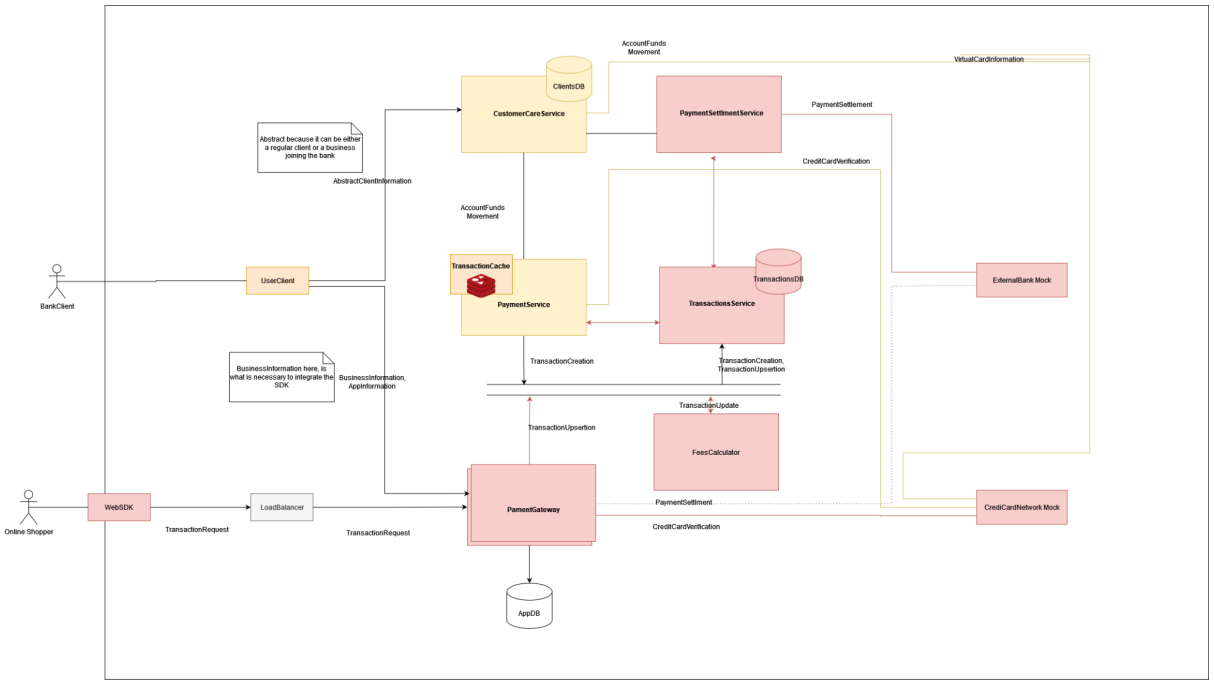
Hypothèses

- Les cartes virtuelles sont générées par les CCN, et par conséquent c'est le CCN qui se chargera de vérifier si un client possède une carte assignée à notre système NewBank pour nous appeler chez nous.
- Le SDK effectue le cryptage des données de la carte, la vérification de la validité du numéro de carte saisi, et la demande de paiement avec le token de l'application.
- La passerelle de paiement est chargée d'autoriser la transaction en effectuant les vérifications nécessaires sur l'appartenance du commerçant au système et en demandant l'autorisation externe le cas échéant pour les cartes de crédits des clients du marchand.
- Les frais appliqués à une transaction varient en fonction du montant dépensé. Nous envisageons de prendre en considération la localisation de la transaction, qui est attaché à une application par le marchand, pour gérer ces frais plus finement. (reste à valider par le client)
- L'autorisation d'une transaction génère un jeton d'autorisation de la banque cliente récupéré par le CCN et conservé par la passerelle de paiement, puis balance avec la transaction pour être utilisé pendant les règlements de fonds.
- Les frais qui doivent nous être versés sont calculés après l'autorisation de la transaction par la passerelle de paiement et avant son règlement par le service de règlement des paiements.
- La demande de règlement des fonds est envoyée avec le jeton d'autorisation à la banque commerçant/acquéreur par le service de règlement des paiements.
- Si le commerçant est un client de notre banque, le service de règlement des paiements effectue lui-même la demande de règlement.
- Aucune demande de règlement n'est effectuée avant que les frais ne soient calculés et joints.
- Le règlement des transactions, qu'elles concernent notre passerelle ou notre banque interne, est effectué périodiquement et non pas toute de suite. Un cronJob trigger le règlement de toutes les transactions effectuées les 12 heures passées.

Proposition d'architecture du système :

Vous trouverez ci-dessous notre diagramme d'architecture qui a été initialement dérivé du diagramme de composants conçu pour un monolithe et puis amélioré au fur et à mesure. Vous trouverez ci-après une explication détaillée des composants architecturaux, de leurs interfaces internes et de leurs interfaces externes.

Lien svg plus clair : [diagramme-archi]



Nous avons choisi une architecture orientée services afin que chaque service de ce découpage représente une vue cohésive et claire du domaine du métier traité et ait une responsabilité claire qui reflète des fonctionnalités recherchées par la banque en ligne. Les fonctionnalités sont une réponse au parallèle que sont les besoins métiers. Notre découpage est axé sur le découpage du domaine lui-même.

Voici une description du rôle et des cas d'utilisation de chaque service ainsi que ses interfaces externes et internes :

Composants principaux :

CustomerCareService :
Ce service sera chargé de tout ce qui concerne les relations avec les clients. Il créera des comptes d'utilisateurs, des comptes d'entreprises, gérera les mises à jour directes de leurs fonds et demandera des cartes de crédit

virtuelles pour ces clients à un service externe : le réseau de cartes de crédit (mock).

Composants et Interfaces Internes :

- AccountFinder : Tout ce qui concerne la recherche du compte d'un client est géré par cette interface
- AccountRegistration : En charge de l'intégration d'un client dans le système et de lui fournir son compte bancaire.
- ChequeAccountHandler : il déplace les fonds en cas de dépôt, de transfert ou de débit.
- SavingsAccountHandler : Différemment, il s'occupe de déplacer les fonds de l'épargne.
- VirtualCardRequester : Chargé de demander et d'émettre une carte bancaire virtuelle à un client.

Interface externes :

- **/POST /api/customers**
  request body:
  - firstName : String
  - lastName : String
  - email :String
  - phoneNumber : String
  - Birthdate : String
  - FiscalCountry : String
  - address : String

  response body:
  - id : Long
  - customerProfile: CustomerProfileDTO
  - balance: BigDecimal
  - savingsAccount: SavingAccountDTO
  - creditCard : CreditCardDTO null before the creation of a virtual card)

  /GET /api/customers/:id
  response body:
  - id : Long
  - customerProfile: CustomerProfileDTO
  - balance: BigDecimal
  - savingsAccount: SavingAccountDTO
  - creditCard : CreditCardDTO null before the creation of a virtual card)

  /POST /api/customers/:id/virtualcard

response body:

- id : Long
- customerProfile: CustomerProfileDTO
- balance: BigDecimal
- savingsAccount: SavingAccountDTO
- creditCard : CreditCardDTO
    - cardNumber: String
    - cardHolderName: String
    - expiryDate: String
    - cvv: String

/PUT /api/customers/:id/movetosavings
request body:

- amount: BigDecimal

/PUT /api/customers/:id/funds
request body:

- amount: BigDecimal
- operation : String (withdraw or deposit)

PaymentService :

Ce service est chargé d'autoriser la transaction réelle et la demande de paiement émanant d'une banque ou de notre réseau de cartes de crédit. Ce service effectue les contrôles de fraude nécessaires, par exemple, et les contrôles de fonds, car il demande les informations sur le client au service clientèle avant d'approuver la transaction. Il envoie également l'événement à une queue afin de créer la transaction et de la stocker dans la base de données par le service dédié qui écoute sur la queue.

Composants et Interfaces Internes :

- FundsHandler : application des contrôles nécessaires sur l'historique et le seuil des transactions, ainsi que vérification des fonds du compte.
- FraudDetector : Détecteur de fraude en cas, par exemple, de transactions multiples en même temps.
- TransactionProcessor : Traite la transaction proprement dite en vérifiant l'existence du panier ou de l'IBAN et en délivrant une autorisation en cas d'approbation. Il envoie ensuite la transaction dans la queue interne.

Interface externes :

/POST /api/payments/process
request body :

- cardholderName : String

- cardNumber : String
- expirationDate : String
- cvv : String
- toAccountIBAN : String
- toAccountBic : String
- amount : BigDecimal

response body :

- success : boolean
- message : String
- authToken : String

/POST /api/payment/checkCreditCard :

request body :

- cardNumber : String
- expirationDate : String
- cvv : String

response body :

- response : boolean
- message : String
- authToken : String

/POST /api/transfer/process

request body :

- fromAccountIban :String
- fromAccountBic : String
- toAccountIban : String
- toAccountBic : String
- amount : bigDecimal

response body :

- success : boolean
- message : String
- authToken : String

TransactionsService :

Ce service s'occupera des insertions et des mises à jour de notre base de données de transactions. Il effectuera beaucoup d'écritures et sera purement utilisé pour nous permettre d’effectuer des autorisations plus rapides dans d'autres services sans se soucier de la latence d'écriture directe et concurrente dans la base de données par ses services (PaymentService et PaymentGateway).

Composants et Interfaces Internes :

- Persister : gère le stockage des transactions, qu'elles soient effectuées par l'intermédiaire du processeur de paiement ou de notre passerelle de paiement.

Interface externes :

Il n’aura pas d’interface externe mais il va plutôt écouter les transactions qui arrivent sur la queue pour manipuler la db des transactions.

Il ecoute les transactions normales provenant du PaymentProcessor sur un topic ‘internal-transactions’, et les transactions en provenance du PaymentGateway sur un topic ‘external-transactions’.

PaymentSettlementService :

Ce service s'occupera des mouvements de fonds et du règlement de toute transaction en cours qui a été approuvée. Il recevra les demandes de transfert de fonds de nos comptes clients vers d'autres comptes bancaires, et inversement, il procédera également à la demande de règlement de fonds à partir d'autres comptes bancaires si ce sont nos clients qui recevront les fonds.

Composants et Interfaces Internes :

- TransactionsDétenteur : Cette interface contient la logique de règlement des paiements : elle vérifie s'il s'agit d'un paiement entièrement interne ou externe et, si c'est le cas, rappelle l'organisme externe pour régler la transaction.
- FondsDéducateur : Cette interface est chargée de lancer l’application des mouvements de fonds liés aux comptes respectifs, ainsi que de prendre la réduction qui a été calculée précédemment par notre calculateur de frais.

Interface externes :

/POST /api/settle

PaymentGatewayService :

Ce service a pour l'instant deux responsabilités. La première est d'intégrer une entreprise et son application, de générer le jeton et de permettre l'utilisation de notre sdk en l'utilisant. La seconde est le traitement des transactions effectuées par son intermédiaire, c'est-à-dire le calcul des frais, l'appel au CCN pour l'autorisation de paiement du client et le déclenchement du règlement des fonds après l'autorisation.

Il n'est pas divisé en deux services, car la seconde responsabilité dépend étroitement de la première. Pour pouvoir procéder à une transaction, le service doit vérifier à chaque fois que le jeton est valide, que le commerçant est dans notre système, etc…

Composants et Interfaces Internes :

- BusinessIntegrator : Intègre le commerçant dans notre système, à condition qu'il nous communique ses coordonnées bancaires.
- BusinessFinder : Gère la recherche des entreprises qui nous ont déjà rejoints.
- ApplicationIntegrator : gère l'intégration de l'application proprement dite en lui associant un apitoken, une clé publique et un commerçant.
- ApplicationFinder : gère la recherche de l'application qui a été précédemment intégrée à notre passerelle.
- Encrypter : Encrypter : Encrypter : Encrypter : Encrypter : Encrypter Gère l'aspect sécuritaire de la transaction, en chiffrant, déchiffrant et émettant les clés utilisées par l'interface de l'intégrateur d'applications.
- TransactionProcessor : Traite les transactions entrantes, délivre l'autorisation et demande une autorisation externe dans le cas où le client du commerçant utilisant notre sdk n'est pas un client de notre banque.

Interface externes :

/POST /api/gateway/authorize
request body :

- token : string
- amount : BigDecimal
- cryptedCreditCard : String

/POST /api/gateway/integration/merchants
request body :

- name : String
- email : String
- bankAccount :
    - IBAN : String
    - BIC : String

response body :

- id
- name : String
- email : String
- bankAccount :
    - IBAN : String
    - BIC : String

- application : Application (null before application creation)

/POST /api/gateway/integration/applications
request body :
- name : String
- email : String
- url : String
- description : String
- merchantId : String

response body :
- id : Long
- name : String
- email : String
- url : String
- description : String
- apiKey : String
- merchant : MerchantDto

/POST /api/gateway/integration/applications/{id}/token
response body :
- token : String

/GET /api/gateway/integration/applications/{id}/token
response body :
- token : String

FeesCalculatorService :
Ce service gère le calcul des frais qui doivent être appliqués à une transaction entrante et les rattache avant qu'elle ne soit réglée.

Composants et Interfaces Internes :
- FeesCalculator: gère les frais d'utilisation de notre passerelle et applique un forfait et un ratio en fonction du montant de la transaction.

Interface externes :

Il n'aura pas d'interface externe mais il va plutôt écouter les transactions qui arrivent sur la queue pour leur rattacher les frais calculés.

Il ecoute les transactions en provenance du PaymentGateway sur un topic 'external-transactions', et republie de nouveau les transactions avec les frais sur cette même queue.

Mocks :

ExternalBank Mock :
Ce service imitera un service bancaire typique : il autorise les paiements et demandera les règlements de fonds qui sont déclenchés.

Interface externes :

/POST /api/externalbank/authorize
request body :
- fromAccountIBAN : String
- toAccountIBAN : String
- amount : BigDecimal

response body :
- authorized : boolean

/POST /api/externalbank/add
request body :
- iban : String
- amount : BigDecimal

response body :
- settled : boolean

/POST /api/externalbank/deduce
request body :
- iban : String
- amount : BigDecimal

response body :
- settled : boolean

CreditCardNetwork Mock :
Ce service simulera un CCN, vérifiant la validité d'une carte et renvoyant un jeton d'autorisation si le client est autorisé dans le cas d'une transaction approuvée, et émettant des cartes de crédit virtuelles.

Interface externes :

/POST /api/payment/authorize
request body :
- cardNumber : String
- expirationDate : String
- cvv : String

response body :
- response : boolean

- message : String
- authToken : String
- AccountIBAN : String
- AccountBIC : String

Loadbalancer :
Ce composant supplémentaire fonctionne seul et fournit une sorte de proxy inverse pour accéder à la passerelle de paiement. Ce composant est placé devant la passerelle et répartit la charge sur ses différentes instances qui sont redondantes. Il sera chargé de limiter l'utilisation en cas de demandes élevées et étranges de la part d'un certain demandeur. Il réacheminera également les demandes vers une instance opérationnelle s'il détecte que l'autre instance en cours d'exécution a échoué.

Routes traitées :

/POST /api/gateway/integration/merchants
/POST /api/gateway/integration/applications
/POST /api/gateway/integration/applications/{id}/token
/GET /api/gateway/integration/applications/{id}/token

Choix technologiques :

- Le développement des services se fera en Java Spring Boot pour deux raisons : la familiarité de la stack technologique pour l'équipe et la robustesse de java (multithreading, strong typing,..).
- La base de données de transactions sera en Cassandra pour permettre un flux d'écriture intensif.
- Les autres bases de données seront en Postgres vu qu’elles seront sollicitées autant en écriture qu'en lecture.
- La technologie de la file d'attente décidée est Kafka vu sa capacité de traiter un débit très haut de messages, dans notre cas cela sera les transactions.
- Le reverse proxy du load balancer est implémenté avec Nginx.

Limitation des risques identifié

En commençant par l'extensibilité, nous avons utilisé REST pour que la fonctionnalité de notre passerelle soit facilement exposée par le biais d'un kit de développement logiciel.
L'exposition d'interfaces externes simples, conformes aux normes REST et fournissant des points d'accès à la passerelle basés sur des cas d'utilisation simples, facilite l'extension et l'intégration de SDK à la passerelle.

En ce qui concerne la robustesse, nous avons vu que, d'un point de vue fonctionnel, il s'agit de gérer les entrées erronées et les erreurs, qu'elles soient intentionnelles ou non. Mais d'un point de vue architectural, il est indispensable d'atténuer les problèmes tels que les pics de charge élevés et les essais d'effondrement du service. Soit en limitant l'utilisation, soit en la réacheminant vers d'autres instances moins débordées, soit en refusant simplement les demandes entrantes qui tentent d'affliger le système et d'arrêter le service.
Pour ce faire, nous avons ajouté un proxy inverse devant notre passerelle de paiement. Ce composant joue le rôle de gardien, limiteur de débit et équilibreur de charge.

Il convient de noter que pour parvenir à faire ce qui a été mentionné précédemment, nous allons faire recours à une redondance active-active de la passerelle de paiement derrière le proxy inverse.

SDK

Une clé api sera fournie à chaque client de l’SDK. Ce token JWT sera incorporé dans l'en-tête "Authorization" de chaque requête API envoyée au SDK. Si le token s'avère invalide, la gateway ne recevra aucune requête. En revanche, si le token JWT est valide, les transactions se déroulent sans accroc.

Concernant le cryptage des informations de carte, nous avons choisi d'employer l'algorithme RSA. Plus précisément, la gateway génère une paire de clés RSA, à savoir la clé privée et la clé publique. Le SDK utilise la clé publique pour chiffrer les données de carte avant de les transmettre à la passerelle. Ceci garantit une transmission sécurisée des informations sensibles.