Berthoulat Rémi
Sanchez Arnaud
Thévenoux Rémi
Werlen Maxime

AUTOMATISATION D'UN PROCESSUS DE PAIEMENT
ARCHITECTURE TECHNIQUE

Date de création	22/10/08	Version	1
Date de dernière modification	07/11/08	Révision	61
Titre	Automatisation d'un processus de paiement		
Sujet	Architecture technique		
Mots-clés	Infrastructure, réseau, performances, securité, exploitation, déploiement, carte à puce, lecteur de carte, dimensionnement, plan de reprise d'activité, sauvegarde		
Validé			

TABLE DES MATIÈRES

I Spécification des performances attendues

a Capacité du système d'information et architecture technique

Le système doit pouvoir supporter une charge de 6 000 000 de cartes en bases de donnée, 500 000 paiement par jour répartis sur des tranches horaires réduites. Le système devra pouvoir traiter au moins un débit de 300 paiement par seconde en garantissant une qualité de service maximale et 500 paiement par seconde en garantissant une qualité de service dégradée (plus lent) tout en conservant la contrainte de rapidité des transactions.

b Rapidité des transactions

La durée d'une transaction est un élément essentiel de la réussite de l'adoption par le public. Le paiement doit s'effectuer au plus vite. Trois cas sont prévus :

•Qualité de service optimale : le paiement est effectuée en moins de 5 secondes ;

•Qualité de service moyenne : le paiement est effectué en moins de 15 secondes ;

•Qualité de servie dégradée : le paiement est effectué en plus de 15 secondes.

L'objectif est d'avoir un maximum de paiement effectué en moins de 5 secondes. En cas de charge anormale élevée, le système pourra passer en service moyen.

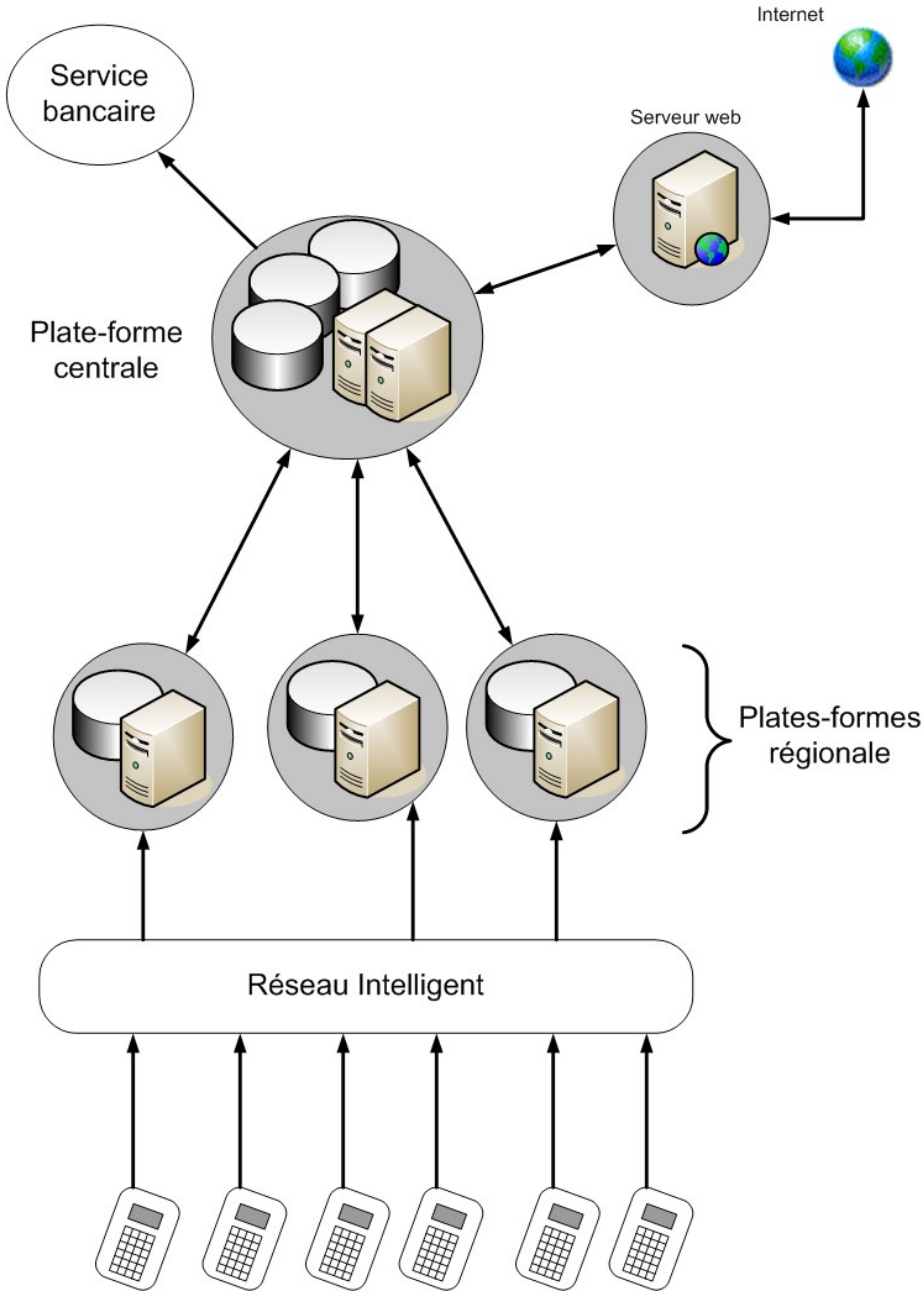
Il doit être prévu un service dégradé fonctionnel si le service normal ne peut être assuré.

II Description de la solution technique

a Architecture

ARCHITECTURE GLOBALE

Le système sera réparti entre trois pôles. Premièrement les TPE installés chez les commerçants, les plates-formes régionales de traitements des transactions, d'une plate-forme centrale, et d'un service internet.



TERMINAUX DE PAIEMENT

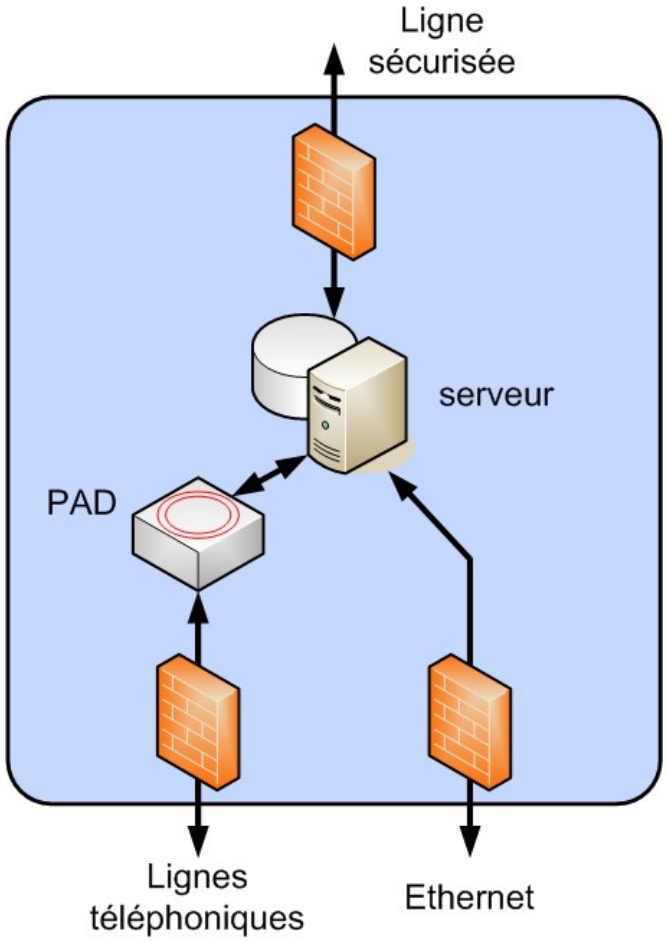
Nous allons réutiliser les TPE déjà présent chez les commerçants en y ajoutant un module spécifique qui permettra de traiter les transactions avec la carte SODEXO. Les TPE communiqueront avec le reste du système soit via une connexion téléphonique, soit via IP pour les plus récents.

PLATES-FORMES RÉGIONALES

Les plates-formes régionales auront pour tâche de traiter l'ensemble des transactions. Pour cela elles disposeront d'un ensemble de PAD traitant les communications provenant du système téléphonique (RNIS).

Les communications via IP (sécurisé par le protocole SSL) et celles traitées par les PAD seront alors analysées par un ensemble de serveurs qui communiqueront avec deux bases de données : la base client et la base transaction.

Afin d'accélérer les traitements, chaque plate-formes régionales aura quotidiennement une réplique de la base client issu de la plate-forme centrale. Chaque transaction sera stocké dans une base, et la plate-forme centrale fera une « télécollecte » sur chaque plate-forme régionale pour mettre à jour ces différentes bases, dont la base client qui sera alors répliqué sur les plates-formes régionales.



RÉPARTITION ENTRE LES PLATES-FORMES RÉGIONALES

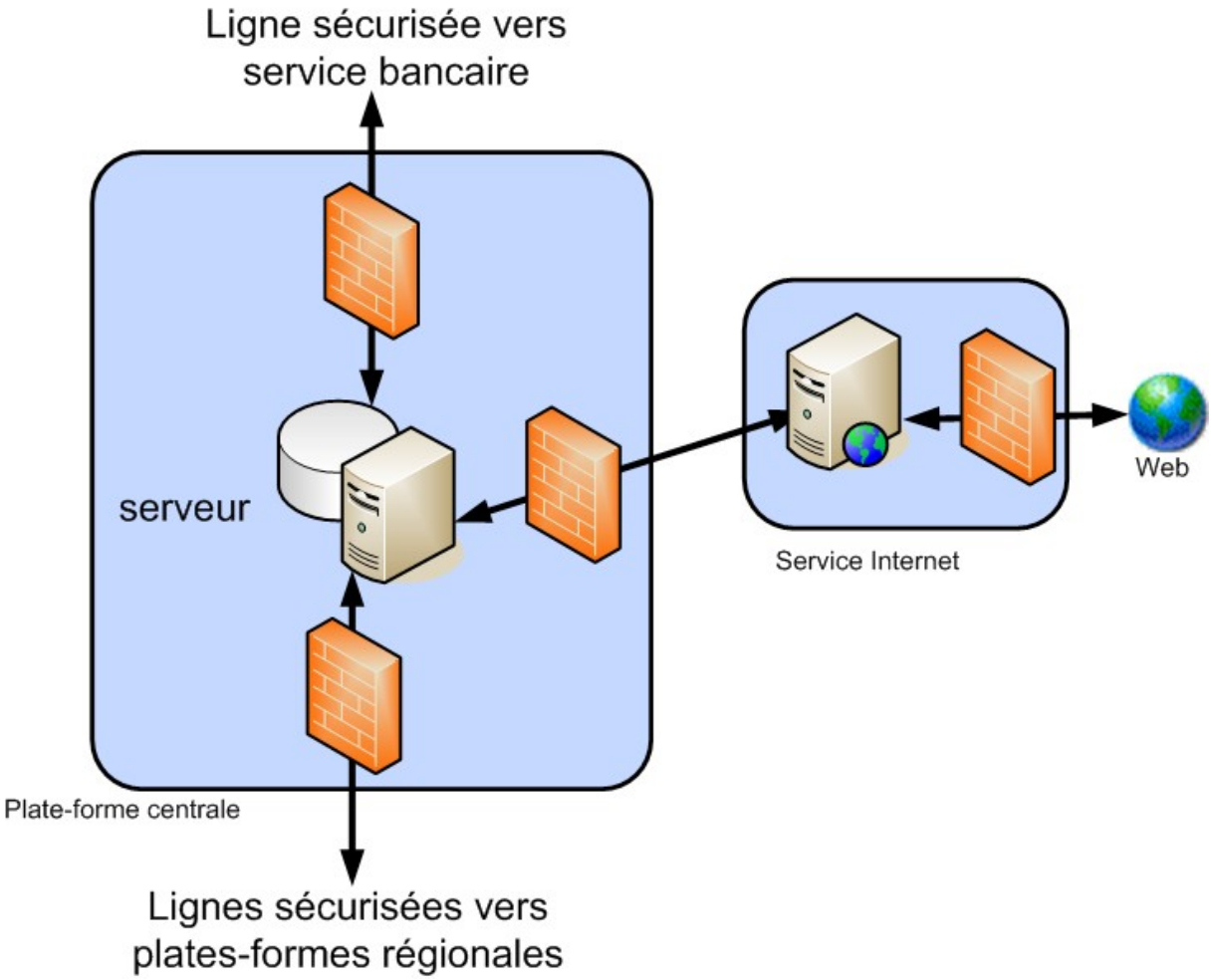
Nous utiliserons le Réseau Intelligent de France Télécom qui permet de répartir automatiquement le flux en provenance des TPE vers les plates-formes les moins sollicitées.

Ce système permet d'optimiser les temps de traitements, mais aussi de gérer automatiquement les problèmes de redirections lorsqu'une plate-forme ne sera plus opérationnelle.

Enfin le système permet de simplifier la programmation des TPE en n'utilisant qu'un numéro national pour toutes les plates-formes.

PLATE-FORME CENTRALE

La plate-forme centrale aura pour mission la télécollecte auprès des plates-formes régionales, la gestion des compensations ainsi que des différentes activités commerciales (achat des cartes, gestion des commerçants, ...)



Ainsi chaque soir, cette plate-forme exécutera une télécollecte auprès des autres plates-formes, puis mettra à jour les bases clients, commerçants et transactions. Lors de cette opération, les bases transactions des plate-formes régionales seront « vidées » et les transactions seront stockées avec une attention particulière sur la plate-forme centrale.

Une fois cette opération terminée, les serveurs analyseront la base commerçants pour détecter les compensations a exécuter, puis communiquera celles-ci via une ligne sécurisée à sa banque les opérations à mettre en place (les méthodes de transfert de données seront étudiées plus tard, dans le dossier EDI).

Les serveurs devront en parallèle traiter les requêtes issues du service web.

SERVICE INTERNET

Le service internet doit permettre de gérer le site web. Il n'agira pas directement sur les bases de données, mais communiquera avec la plate-forme centrale via des protocoles tels que SOAP.

b Description des bases de données

BDD TRANSACTIONS

Cette base stocke l'ensemble des transactions effectuées entre un client et un commerçant. Elle contient la date, la valeur de la transaction, et les identifiants du commerçant et du client.

BDD CLIENTS

Cette base stocke les données relatives au client final (porteur de carte) tel que le numéro de la carte, le solde, la valeur d'un repas, et le débit de la journée.

BDD COMMERÇANTS

Cette base contient les informations relatives aux commerçants, dont son identifiant, la liste des comptes pour les compensations, des informations commerciales et bancaires.

BDD COMPENSATIONS

Cette base enregistre l'ensemble des compensations effectuées par Aventix donc une date, un montant, l'origine et le bénéficiaire.

c Dimensionnement

NOMBRE DE CENTRES DE TRAITEMENT

Les plate-formes de traitements sont dupliqués pour que la charge d'une plate-forme indisponible soit réparti sur les autres afin de permettre de ne pas interrompre le service à cause de l'indisponibilité d'une plate-forme du à la maintenance, les mises à jours, test ou de causes prévues ou imprévues.

Les indisponibilités prévisibles seront programmées pendant la nuit sur une partie seulement des centres de sorte à maintenir le service 24h/24h et d'avoir la plus grande capacité de traitement pendant le pic du déjeuner.

Ainsi nous estimons que dans la pire situation envisageable, et vues les nombreuses

mesures de protection mises en œuvre sur chacune des plate-formes, il ne peut y avoir que deux plate-formes indisponible en même temps : l'une subissant une maintenance lourde qui ne peut être faite durant la nuit, l'autre devenant indisponible pour une cause imprévisible.

Vus les frais fixes associés à la mise en place d'une plate-forme (locaux, équipe technique,...), la solution la plus économique est d'implanter 5 plates-formes. Chacune doit ainsi pouvoir traiter 33% du trafic global.

PLATES-FORMES RÉGIONALES

Le premier équipement à mettre en place sera une batterie de PAD pouvant traiter les communications avec les TPE. Les TPE peuvent se connecter soit par ligne téléphonique classique, les PAD permette alors d'interfacé les communications. Les TPE plus récent pourront se connecter directement via le système IP à notre serveur.

Les modèles tels que le RA3120 de CRX peut traiter 120 connexions simultanées. Lors des pics, il y a 30 000 connexions à la minute, avec une moyenne haute de 10s par transaction, il faut traiter environs 5 000 connexions simultanées.

Les plates-formes devant pouvoir traiter 33% du flux, il faut donc au moins 14 PAD de 120 connexions.

Les bases de données du serveur devront contenir une copie de la base clients et une base de transactions. Il y a seulement 500 000 transactions par jour (la base est vidée quotidiennement) et 6 000 000 clients. Donc un disque dur de quelque Go sera amplement suffisant. Il faudra lui adjoindre des disques de sauvegardes.

Si l'espace mémoire n'est pas une contrainte, il faut en revanche optimiser le temps d'exécution. On optera donc pour un serveur multi-processeur afin de paralléliser les tâches. Cependant le verrou étant les temps de communication on se limitera à des processeurs de l'ordre 2 GHz.

SERVEUR WEB

Le site Web ne stockera pas particulièrement de données hormis le site lui-même. On se limitera donc à un espace de l'ordre du Go pour l'espace de stockage. De même, il n'y a pas de traitement particulièrement important fait par le serveur (traitement d'une commande, affichage d'informations, demande de modification de données, etc.). Nous limiterons donc aussi la puissance à quelque GHz.

PLATE-FORME CENTRALE

Cette plate-forme nécessitera des moyens de stockage bien plus important. En effet, il nous faudra garder toute les transactions pendant 20 ans. Vu l'évolution rapide des moyens de stockage, on ne planifiera le stockage que sur les premières 5 ans.

A raison de 500 000 transactions par jour, en estimant une transaction à 128 octets, il faudrait donc environ 120 Go pour les données pures.

Pour la base clients (6 millions de clients) on peut estimer un tupple à 512 octets soit un total de 3 Go

Pour la base commerçants on estime un enregistrement à 2 Ko, donc un espace total de 600 Mo.

Enfin la base compensations peut être estimée à 30 000 ligne par jour (une compensation en moyenne tout les 10 jours). Tout comme les transactions, nous allons garder ces données 20 ans, mais prévoir leur stockage que sur les 5 premières années. Avec 128 octets par ligne, il faut prévoir 7 Go.

- Transaction 120 Go
- Clients 3 Go
- Commerçants 600 Mo
- Compensation 7 Go
- **TOTAL 130,6 Go**

En ajoute 20% pour le SGBD on arrive donc à un espace d'au moins 160 Go à prévoir pour le stockage de l'ensemble des données métiers.

À cela, on doit adjoindre les informations de comptabilité et les données de gestion. On optera pour des disques de 300 Go, qui offrir une certaine liberté par rapport à l'ajout de nouvelles données.

Dématérialisation des documents

Les inscriptions en base de données, ne sont pas des pièces juridiques à part entière. Il faut donc conserver des documents à des fins comptables. Ces documents étant extrêmement importants, nous ferons appel à une société spécialisée pour l'hébergement de document sécurisé. Nous ne nous occupons pas du stockage de ces données chez nous.

d Réseau

Serveur Web – Internet

On peut estimer les connexions par les commerçant et les entreprises à environs 1500 par jour avec des pointes à 200 connexions simultanées. En considérant que les pages Internet sont d'environs 150 Ko. Il faut alors un débit de 30 Mo/s.

Serveur Web – Plate-forme centrale

On installera une ligne sécurisée entre le serveur Web et la plate-forme centrale. On peut estimer les requêtes à 512 octets, donc en reprenant un pic de 200 connexions, il faut prévoir un débit minimum de 200Ko/s

Plate-forme centrale – Plate-forme régionale

On installera aussi des lignes sécurisées entre la plate-forme centre et les régionales. Le trafic principal sera le transfert de la base client de 3Go. Si l'on décide qu'elle doit être transmise en moins de 10 minutes, il faut un débit de minimum de 5Mo/s

Plate-forme centrale – Banque

Les communications avec les banques se feront via des lignes sécurisées.

Plate-forme régionales – TPE

Les TPE pourront être connectés grâce au réseau téléphonique classique ou via une connexion internet. Il prévu de traiter 5000 connexions en parallèle, il faudra donc autant de ligne téléphonique par plate-forme. On prévoira aussi une connexions internet de 512Ko/s pour traiter le connexions via IP.

III Spécification du déploiement

a Installation minimale initiale

Afin de fonctionner, chacune des plate-formes régionales doit posséder un équipement minimal : quelques appareils de réception des communications TPE et un serveur de transaction.

Le site principal doit lui aussi être équipé du minimum : l'architecture liée à la gestion d'Aventix (serveur d'application et de base de données, serveur WEB) et un serveur de compensation.

b Augmentation de la capacité de traitement des plate-formes régionales

Lorsque l'activité d'Aventix se développera (au bout de six moins, puis au bout d'un an, ...), il faudra revoir la capacité des plate-formes régionales en ajoutant de nouveaux équipements de communication avec les TPE et de nouveaux serveurs de transaction. Afin de pouvoir procéder aux changements, une plate-forme pourra être rendue indisponible et déléguer ses transactions aux autres plate-formes.

c Augmentation de la capacité de traitement du site central

On ajoutera principalement de l'espace pour les bases de données liées aux transactions et aux comptes clients. Pour les comptes clients, l'emplacement d'un compte sur un serveur est calculé par un algorithme prenant en compte le nombre de serveurs disponibles. Il faudra revoir cet algorithme en mettant à jour le nombre de serveurs de base de données. Lors d'une intervention technique sur le système, on pourra fonctionner avec le site central secondaire.

IV Politique de sécurité

Pour assurer une sécurité maximum, nous devons cibler les éléments les plus importants du système qui devront faire l'objet d'une attention particulière. Nous pouvons isoler deux points principaux :

•La sûreté du traitement des paiements, il faut pour cela que le système soit toujours disponible pour les lecteurs de carte à puce. Une indisponibilité en heure de pointe serait désastreuse pour l'image d'Aventix.

•La sécurité des données : les comptes commerçants, le solde des cartes et les transactions sont des données confidentielles qui ne doivent pas être lues ou modifiées par une personne non habilitée.

Pour nous prémunir de ces deux risques principaux nous allons utiliser d'une part un dimensionnement adapté et une architecture sécurisée.

a Disponibilité du système

SUPPORT DE CHARGE

Le support de charge est décrit dans les spécifications de l'infrastructure. Elle repose sur un système de plates-formes séparées géographiquement. Chaque plate-forme possède une charge nominale inférieure à sa capacité réelle. Sa surcapacité est prévue pour pouvoir traiter le flux provenant d'une plate-forme défaillante. Ainsi la défaillance d'une plate-forme est transparente. Le réseau intelligent de France Télécom permettant de répartir intelligemment le flux entre les plates-formes en fonction de leur temps de réponse.

SÛRETÉ DES PLATES-FORMES TECHNIQUES

Pour prendre en compte toutes les causes qui pourraient empêcher le système de fonctionner, nous allons gérer les risques au niveau de chaque plate-forme et prévoir en cas de problème la possibilité de fermer la plate-forme sans pénaliser le système. Les pannes d'une plate-forme peuvent venir :

•d'une panne physique de réseau, pour cela nous pouvons prévoir un double câblage des bâtiments à deux points d'entrée (fourreaux) différents ;

•d'une panne d'électricité, sur le même principe nous pouvons prévoir une double alimentation électrique géographique séparée ;

•d'une inondation, le site ne sera pas situé en sous-sol et bénéficiera d'un sol surélevé pour permettre l'évacuation de l'eau.

Le fonctionnement multi-sites multi-plates-formes permet, en cas de catastrophe naturelle ou de dysfonctionnement grave, la fermeture d'une plate-forme. Comme expliqué dans l'infrastructure, la charge de la plate-forme défectueuse sera alors répartie sur les autres.

Sûreté des machines

Tous les serveurs du système d'information disposent de disques redondés pour faire face à un possible dysfonctionnement matériel. Il ne faut absolument pas perdre les logs des paiements.

Les machines disposent aussi d'une alimentation redondée et de dispositifs logiciels d'alertes préventives de défaillance matérielle.

Pour éviter les erreurs logicielles, nous mettrons l'accent sur la qualité et les tests lors du développement.

b Sécurité des données

Sécurité des transactions

Les transactions doivent rester privée, sans possibilité de espionnage des données transitant sur le réseau public. Toutes les communications devront être encryptées par des moyens de sécurisation des données. L'utilisation de connexions SSH est un minimum à fournir.

Protection contre les attaques externes

Pour assurer la protection contre les attaques externes, le système disposera de firewall et d'un IDS (Intrusion Detection System). Les points d'entrée sur le système étant bien définis, les firewall pourront être correctement réglé par des spécialistes.

Pour les accès d'exploitation aux machines, où les flux sont bien plus hétérogène, nous pouvons utiliser un bastion. C'est une machine dont le but est de servir de point d'entrée unique sur le réseau. C'est la seule machine acceptant les communications en SSH avec clés autorisées expressément par les administrateurs. Cette machine est la seule à pouvoir se connecter sur le réseau. Aucune autre route réseau ne peut parvenir depuis l'extérieur jusque sur les serveurs.

Protection contre les attaques internes

Le bastion permet de logger toutes les connexions des personnels jusqu'aux machines. Toutes les données transitant vers ou depuis les machines sont enregistrée. Les flux sont identifiés par les clés SSH des personnels. Ces accès sont strictement réservés aux personnes compétentes : administrateurs et ingénieurs maintenance accrédités. Si une agression interne était commise, le fautif serait immédiatement identifié. Il est nécessaire de communiquer sur l'importance des données, pour que les personnes accréditées changent régulièrement de mots de passe, ferment correctement leurs connexions...

V Processus d'exploitation et de maintenance

a Accès aux machines

L'accès aux machines se fait par l'intermédiaire de bastions, qui sont la seule porte d'accès au réseau interne du système d'information. Pour accéder à cette machine, il faut disposer d'une clé SSH accréditée sur la machine. La clé permet d'identifier son propriétaire et donc de lui attribuer des droits en conséquence.

b Accréditation

Le processus d'accréditation est assez strict, seuls les administrateurs d'une machine peuvent avoir accès aux machines de production. Les équipes de développement ont accès à la plate-forme de test. Les accès sont réglementés, font l'objet d'une formation préalable et renouvelée régulièrement. Les mots de passe ont une durée de vie courte. Toutes les personnes ayant un accès sont informées des risques encourus par une utilisation frauduleuse ou erronée.

c Exploitation

L'exploitation correspond aux tâches régulières ou imprévisibles mineures qui ne peuvent pas attendre une modification des applications ou qui ne sont pas automatisables. Cela peut-être par exemple le redémarrage d'une application qui aurait cessé de fonctionner, le réglage des paramètres réseaux ou applicatifs (mémoire allouée, options...).

d Maintenance

La maintenance correspond à la production de nouvelle version des applications répondant à la nécessité préventive ou curative de correction d'anomalies. Pour la production et les tests des nouvelles versions, une plate-forme de test est prévue. Elle comporte la même architecture que les plate-formes de production, mais avec moins de serveurs en parallèle.

Les mises à jour des plate-formes de production se déroulent pendant la nuit, lorsque l'activité est la plus faible. Lorsque la charge est particulièrement faible, une plate-forme peut supporter la charge totale. On sépare donc les plate-formes en deux groupes, l'un est mis à jour pendant que l'autre assure le traitement des paiements, puis on inverse. Ce système permet de ne pas interrompre le service.

VI Plan de sauvegarde

a Objectifs du plan de sauvegarde

Le plan de sauvegarde s'inscrit dans la démarche de réalisation d'un plan de reprise d'activité visant à spécifier les dispositions (techniques et humaines) à prendre afin de garantir d'une part la non-perte de données en cas de dysfonctionnement du système d'information et à organiser le processus de récupération de données en cas de perte irréversible d'information et d'autre part à définir les procédures d'archivage des données.

b Démarche pour réaliser le plan de sauvegarde

Les étapes d'élaboration du plan de sauvegarde sont les suivantes :

- recherche des données à protéger ;
- définition du type de sauvegarde souhaité ;
- contrôle de la qualité des données sauvegardées ;
- définition de l'emplacement physique et géographique des sauvegardes.

RECHERCHE DES DONNÉES À PROTÉGER

Il est capital d'identifier les données à sauvegarder et leur fréquence. En effet, il paraît peu concevable de sauvegarder systématiquement toutes les bases de données du système d'information. Pour cela, il faut identifier les données dites « sensibles ». Cette étude doit se faire au niveau de la direction pour la décision relève de la stratégie. En pratique, les propositions sont faites par les informaticiens et validées par la direction.

On identifie aussi les contraintes liées à la sauvegarde de ses informations : volumétrie des bases de données, état de la base de données (certains SGBD ou applications demandent à ce que la base de donnée soit fermée pour que la sauvegarde puisse être réalisée).

DÉFINITION DU TYPE DE SAUVEGARDE SOUHAITÉ

Il s'agit de préciser quel type de sauvegarde il faut mettre en place : on peut imaginer des sauvegardes complètes mais il faut prendre en compte le temps nécessaire et l'espace disque requis, on peut aussi imaginer des solutions dites de sauvegarde « différentielle » où seules les modifications depuis la dernière sauvegarde sont enregistrées.

Les éléments à prendre en compte dans le type de sauvegarde à mettre en place sont divers et variés :

- la capacité de stockage nécessaire ;
- la vitesse de sauvegarde souhaitée ;
- la fiabilité du support (pour les sauvegardes sur le long terme – plusieurs années) ;
- la facilité à restaurer les données ;
- le coût de la solution.

Contrôle de la qualité des données sauvegardées

Il ne suffit de dire comment doit on sauvegarder, encore faut il s'assurer que les données soient bel et bien sauvegardées. Un contrôle de qualité des données sauvegardées permet de s'assurer de la bonne exécution des tâches de sauvegarde. En pratique, il peut suffire de faire une restauration d'une sauvegarde et tester que tout fonctionne comme attendu pour s'en assurer.

Définition de l'emplacement physique et géographique des sauvegardes

Lorsqu'on défini un plan de sauvegarde, on le fait en connaissance des risques liés à l'exploitation des locaux (incendie, inondation, …). De ce point de vue, il paraît logique de ne pas conserver les sauvegardes au même emplacement géographique de les données d'origine.

On fait aussi des choix en matière de stockage physique : les données peuvent être stockées sur un serveur, sur bandes magnétiques, sur Internet, sur des supports tels les CDROM, DVD ou clés USB ...

En fonction de la sensibilité des données et de l'importance qu'on y accorde, on déploiera des moyens nécessaires. Comme lorsqu'on souhaite s'équiper d'un système de sécurité (firewall, …), il ne faut pas que les moyens soient démesurées par rapport aux données à sauvegarder.

c Éléments pour la réalisation du plan de sauvegarde d'Aventix

Recherche des données à protéger

Les données les plus sensibles sont certainement celles liées aux transactions. En effet, on ne peut accepter aucune perte d'information sur les transactions réalisées entre les employés et les commerçants sinon, nous ne serons pas en mesure d'effectuer la compensation ce qui aura pour conséquence grave la perte de confiance des commerçants et l'abandon de notre solution.

Le tableau ci-dessous fait l'inventaire des données à protéger :

Type de données	**Source des données**	**Criticité des données (1 à 5)**	**Tolérance perte (en heures)**
Transactions	Serveur de transaction	1	0
Comptes clients	Serveur compte clients	2	0
Comptes des commerçants	Serveur comptes commerçants	2	0
Comptabilité	Logiciel de finances	3	24
Ordres de paiement	Serveur comptes commerçants	3	24
Données de gestion (fournisseurs, entreprises, commerçants, commandes, ...)	Serveur applicatif	4	24
Données propres au portail Internet	Serveur WEB	5	24

Définition du type de sauvegarde souhaité

On choisira une sauvegarde de type **incrémentiel**. Toutes les données sont sauvegardées une fois par semaine. Chaque jour, on sauvegarde uniquement les données ayant été modifiées. Cette technique à l'avantage de rendre plus rapide le processus de sauvegarde (effectué la nuit, en période de plus basse activité) puisqu'on ne copie pas systématiquement toutes les données. L'inconvénient est que en cas de restauration, il faudra restaurer la sauvegarde de début de semaine ainsi que toutes les sauvegardes journalières effectuées depuis la dernière sauvegarde..

Contrôle de la qualité des données sauvegardées

Le contrôle se fera par restauration des données sauvegardées et tests fonctionnels sur une architecture matérielle test. Si les résultats sont concluants, on validera la procédure de sauvegarde. Ci-dessous quelques critères pour la validation de la procédure de sauvegarde :

- les données ont été restaurées sans erreur ;
- tests d'intégrité et de cohérence des données validés ;
- les tests des applications sont concluants.

Définition de l'emplacement physique et géographique des sauvegardes

Les sauvegardes se trouvent sur des serveurs de sauvegarde. Ces serveurs de sauvegarde peuvent se trouver n'importe où du moment qu'ils ne sont pas au même emplacement géographique que les données sources. De plus, il faut réunir un certain nombre de conditions d'hébergement des serveurs (salle blanche, climatisée située au minimum au 1er étage du bâtiment).

Les serveurs de sauvegarde sont des services de type NAS ayant les caractéristiques suivantes :

- 2 disques dur en RAID 1 de 300 Go
- Accessible par Ethernet Gigabit

d Gestion instantanée des données

Nous l'avons dit, on ne peut pas se permettre de permettre certaines données. La seule solution pour parer une défaillance du système est de dupliquer ces données.

Ainsi, chaque plate-forme régionale (n) duplique ses données sur la plate-forme régionale voisine (n+1). En fin de journée, les données de chaque site sont collectées par le site central pour effectuer la mise à jour des comptes clients et commerçants et pouvoir ordonner les compensations. Cette solution garantie une non-perte des données de transaction.

Pour les données critiques stockées au site central, nous disposerons d'un site central secondaire.

VII Plan de reprise d'activité (PRA)

Le plan de reprise d'activité ou PRA permet d'assurer, en cas de panne du système, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'Aventix.

Le plan de reprise d'activité doit permettre, en cas de sinistre, de basculer sur un système capable de prendre en charge les besoins informatiques nécessaires à la survie de l'entreprise. Il peut y avoir un mode de fonctionnement dégradé sur lequel seules les transactions pourraient être effectuées, les autres fonctionnalités de gestion étant temporairement suspendues jusqu'à rétablissement du système de base.

a Rappel sur l'architecture du système informatique

La France est divisée en cinq plate-formes régionales qui traitent toutes les transactions réalisées grâce à la carte restaurant. Cette division permet de répartir la charge puisque le système doit pouvoir supporter 500 000 transactions par jour.

Un site central regroupe les transactions effectuées dans la journée et traite les compensations. C'est aussi le cœur de l'entreprise Aventix avec les serveurs WEB et d'application.

b PRA lors d'un incident sur une plate-forme régionale

Les cinq plate-formes régionales sont identifiées par un numéro n allant de 1 à 5. Les données de chaque site n sont synchronisées avec le site n+1. Ainsi, lorsqu'une transaction arrive sur le serveur 3, elle est enregistrée de façon synchrone sur le serveur 4. Si le site n tombe (grosse panne, inondation, incendie, ...), le site n+1 conservera les transactions initialement crées sur la plate-forme n.

Le réseau intelligent de France Télécom permet de re-router automatiquement les appels (ou les transactions) vers les plate-formes disponibles si une plate-forme ne répond pas elle ne recevra plus de flux. Une fois la plate-forme défaillante de nouveau opérationnelle, le flux lui arrivera de nouveau automatiquement.

c PRA lors d'un incident sur le site central

En cas de panne du site central, on ne peut pas compter sur les plate-formes régionales qui ne sont pas équipés des applicatifs nécessaires et surtout qui ne possèdent pas toutes les informations du site central. Ainsi, il convient d'avoir un site central secondaire qui est synchronisé avec le site central principal.

Si l'incident sur le site central n'est pas réparé dans la journée (ce que nous allons exiger de notre partenaire informatique), les données des sites régionaux seront rapatriées sur le site central secondaire. Une mise à jour des données du site central principal sera donc nécessaire.

VIII Étude de l'existant

a Cartes à puces

On peut diviser les cartes à puces en trois grands groupes technologiques :

Les cartes à mémoire (T1G ou T2G)

Il s'agit du modèle le plus simple, la carte n'est pas programmable, mais une logique câblée permet d'implémenter un simple compteur. Le compteur pouvant uniquement être lu ou décrémenté. Les premières cartes téléphoniques utilisaient ce type de technologie. Ce type de carte est cependant devenu rare, car la carte est facilement copiable et falsifiable, la rendant trop peu sûre.

Les cartes à micro contrôleur (Smart Card)

Sur ce type de carte, un micro contrôleur minimaliste permet de doter la carte d'un minimum d'intelligence. La carte est donc capable d'exécuter des opérations simples, la sécurité de la carte est ainsi améliorée puisque elle peut être équipée de fonctions de cryptographies.

Les cartes Java (Javart)

Il s'agit d'une technologie permettant d'exécuter de manière sécurisée, sur une carte à micro contrôleur, plusieurs programmes écrits avec un sous-ensemble du langage développé par Sun Microsystems : Java. Un système d'exploitation permet de gérer les différents programmes de la carte qui est donc plus performante qu'une carte à microcontrôleur simple. Le développement d'application sur de telles cartes est simplifié par l'utilisation du langage Java qui offre un plus haut niveau d'abstraction et une portabilité plus importante, ce qui accroît la réutilisation des applications.

Cartes à bande magnétique

Il existe aussi les **cartes à bande magnétique**, ces cartes jouent le même rôle que les cartes à mémoire, sauf que la mémoire est magnétique, au lieu d'être électronique. Ces cartes sont aujourd'hui un peu désuètes par rapport aux cartes électroniques car elles sont moins fiables. Elles peuvent s'effacer plus facilement.

Il existe trois types de support physique principaux pour les cartes à microcontrôleurs :

- Puce seule (carte SIM de téléphone portable)
- Carte sur support rigide (Carte bancaire, carte téléphonique)
- Carte sans contact (Télépéage, transport en commun, badge sécurité), la technologie RFID étant la plus répandue.

Dans notre cas nous nous intéresserons en particulier aux cartes à puces à support rigide, ce qui nous permettra d'utiliser des lecteurs de carte bancaires pour notre application. Ces cartes présentent les caractéristiques physiques suivantes :

- Dimensions : 85.60 x 53.98 x 0.76 mm
- Matière : PVC ou ABS
- Position et contacts de la puce standardisés

	Carte à mémoire	Carte à Microprocesseur	Carte Java
Sécurité	+	+++	+++
Adaptabilité	+	++	+++
Facilité mise en œuvre	+++	++	+
Prix d'achat	+++	++	+

b Lecteurs de carte

Un terminal de paiement électronique (aussi appelé TPE) est un appareil électronique capable de lire les données d'une carte bancaire, d'enregistrer une transaction, et de communiquer avec un serveur d'authentification à distance.

Un TPE peut lire une carte grâce à son lecteur de carte à puce ou par son lecteur de piste magnétique. Il a la possibilité de se connecter à un serveur d'authentification grâce à son modem. La carte lue peut-être une carte bancaire (de type B0' ou EMV par exemple), un porte-monnaie électronique (par exemple, système Moneo en France), ou tout autre carte à puce (carte vitale) ou une carte au format SIM (par exemple, contenue dans un téléphone mobile, système déployé par NTT DoCoMo au Japon).

Illustration 1: Terminal de paiement électronique fixe avec son pin-pad

En France, les différents logiciels de paiement sont développés à partir de spécifications techniques présentées dans le Manuel du Paiement Électronique (MPE) établi par le groupement des cartes bancaires (GIE CB).

Pour utiliser un TPE, un commerçant doit passer un contrat avec sa banque par lequel sont fixés un montant maximal de transaction au-dessus duquel une autorisation est obligatoire, ainsi que le montant que la banque prélèvera sur chaque paiement effectué (commission).

COMMUNICATION AVEC LES SERVEURS

Via une ligne analogique

Il peut être accompagné d'un pinpad, petit clavier numérique sur lequel le client saisit son code confidentiel. Déclinaisons sur TPE autonome portable via socle (liaison entre le TPE et le socle en IR ou DECT) Les temps d'autorisations pour une transaction en autorisation est en moyenne de 12 secondes. Gestion possible de la liaison caisse en cas de TPE fixe.

Via le réseau GPRS

Le TPE dispose d'une carte SIM MtoM incluant un forfait télécom 1 ou 2 Mo) Il peut être accompagné d'un pinpad, petit clavier numérique sur lequel le client saisit son code confidentiel et insère sa carte (si présence de puce). Le forfait télécom correspond aux communications (télécollectes et autorisations) il est forfaitisé dans la prestation de la location du TPE GPRS fixe ou portable ou représente un forfait après la première année en cas d'achat. Attention, dans une solution GPRS, une passerelle agréée GIE CB devra être utilisée (certifiée Double SSL) Gestion possible de la liaison caisse en cas de TPE fixe Le temps d'autorisation pour une transaction est en moyenne de 7 secondes.

Via le réseau Internet

IP NATIF (le TPE utilise le lien ADSL déjà en magasin et mutualise ainsi le moyen télécom existant) Le moyen télécom est accès ADSL fourni par n'importe quel Provider du marché. Il peut être accompagné d'un pinpad, petit clavier numérique sur lequel le client saisit son code confidentiel et insère sa carte (si présence de puce) Les temps d'autorisations pour une transaction en autorisation est en moyenne de 7 secondes. Attention, dans une solution TPE IP NATIF, une passerelle agrée GIE CB devra être utilisée (certifiée Double SSL). Le TPE peut être chargé avec une liste des cartes opposées ; il refusera alors toute carte se trouvant dans la liste. L'éventail des cartes lues dépendra des applications chargées dans la mémoire du TPE.

Pour fonctionner les cartes doivent être associées à un lecteur de carte à puce. C'est le lecteur qui fournit l'alimentation électrique à la carte (même dans le cas des cartes sans contact). Les lecteurs programmables peuvent lire différents types de cartes suivant les logiciels dont il est équipé, ils possèdent plusieurs types d'interface avec l'extérieur :

- Port série / USB, pour assurer la communication avec un ordinateur
- Connecteur pour carte à puce (basée sur les protocoles T=0, T=1 et T=CL)
- Lecteur de bande magnétique
- Ligne spécifique pour communiquer avec des systèmes bancaires (notamment par ligne téléphonique)

Il n'y a malheureusement pas de standard définissant la manière de communiquer avec un lecteur de carte. Mais la majorité des lecteurs de carte peut être mise à jour par le biais d'un ordinateur ou d'une clé USB. Il faudra donc créer une application spécifique à nos besoins qui sera exécuté sur le lecteur de carte, il est probable qu'il faille en créer une par modèle de lecteur. Le commerçant sélectionne ensuite le programme à exécuter sur son terminal. Le programme lit la carte et une vérification de sa validité est mise en œuvre.

c Sécurité

Notre application étant relativement critique, nous avons besoin de nous assurer que les cartes utilisées par les utilisateurs finaux sont bien des cartes Aventix valides. Dans le cas d'une carte à mémoire, nous ne pouvons uniquement stocker un identifiant sur la carte, même si l'identifiant est crypté, il est toujours possible de falsifier la carte en faisant une copie. Dans le cas des cartes à micro-contrôleurs ou des cartes Java, il est possible d'implémenter un algorithme de cryptographie qui permettra de s'assurer de la validité de la carte.

d Adaptabilité

Il est possible que les informations que l'on souhaite stocker sur la carte évoluent dans le futur. Il est donc important d'avoir investit dans des cartes permettant de faire ces évolutions. Les cartes à mémoires sont assez limitées dans cette optique.

e Facilité de mise en œuvre

Certaines technologies sont plus délicates que d'autre à mettre en œuvre : les cartes à mémoire ne nécessitent par exemple pas l'implémentation d'un programme sur la carte. Les cartes Java, à l'inverse, bien qu'offrant de meilleures performances et une base plus stable pour les applications complexes, nécessitent une certaine expertise technique.

f Prix

Étant donné que les cartes seront distribuées à un très grand nombre d'exemplaire, il est difficile d'estimer le prix réel d'une carte à puce. Il faudra donc demander un devis aux différents fournisseurs pour avoir une estimation plus précise. Motechno semblent être un des rares revendeurs à donner des prix pour les grandes quantités de cartes à puce personnalisées. La mise en place du processus de fabrication est facturée 300€, les cartes quant à elles coûtent 0,30€ l'unité. Un lecteur de carte à puce, du type terminal pour carte bancaire, pouvant s'adapter correctement à nos besoins, coûte environ 150€.

g Fournisseurs

Les principaux fournisseurs de carte à puce et terminaux de paiements sont :

- Gemalto (fusion de Gemplus et Axalto) : http://www.gemalto.com/france/
- Oberthur Card Systems : http://www.oberthurcs.com/
- Sagem Sécurité : http://www.sagem-securite.com/

Ces fournisseurs ont généralement des revendeurs locaux agréés, par exemple, Gemalto revend ces produits en France par l'intermédiaire de NIS (http://www.nis-infor.com) qui propose d'ailleurs un service de personnalisation graphique des cartes et qui assure la livraison chez le client. La prochaine étape serait donc de demander un devis chez les différents fournisseurs locaux, afin de pouvoir faire une étude financière plus précise.