République Tunisienne
Ministère de l'enseignement supérieur et de
la recherche scientifique
Université de Virtuelle de Tunis

Mastère en Optimisation et Modernisation des Entreprises MOME

MEMOIRE

Pour l'obtention du diplôme de mastère professionnel

Les exigences de sécurité informatique de la plateforme de la carte à puce privative pétrolière

Elaboré par:

Mr Amor Mrabet

Encadré par :

Dr Hanene Idoudi **UVT**

Mme Sonia Rekik **SNDP-AGIL**

Année Universitaire 2014/2015

Dédicaces

A la mémoire de mes parents

A ma femme, à mes enfants.....

Remerciements

Au début de cette mémoire de fin d'étude de mastère,
J'adresse mes sincères remerciements à mes encadreurs
Dr Hanene Idoudi de l'UVT et
Madame Sonia Rekik Directrice responsable de la sécurité du système d'information et des grands projets IT à la SNDP.

C'est un agréable devoir pour moi aussi d'exprimer à tous mes enseignants de l'UVT ma reconnaissance et ma gratitude.

SOMMAIRE

Table des figures

Introduction générale

Danièle Linhart (1994) sociologue et auteur du livre "La modernisation des entreprises" (au édition La découverte) soutient que la modernité commande l'introduction de distinctions et de différenciations dans les organisations et c'est dans cet objectif de recherche de modernité que durant ces deux dernières décennies le paysage des entreprises industrielles et commerciales s'est transformé suite à l'adoption de nouvelles pratiques d'organisation du travail comme le juste-à-temps, les démarches de qualité, l'investissement dans la recherche et le développement, l'innovation et la modernisation de leurs moyens de paiement.

Parmi les moyens moderne de paiement il y a la carte à puce privative qui constitue un moyen rapide, facile d'utilisation et sécurisé. C'est une carte de crédit distribuée par une enseigne de la distribution et dont l'utilisation est limitée aux points de vente de la chaîne ou du réseau (stations services). La carte permet généralement de régler des achats soit au comptant, soit à crédit. Elle est également utilisée comme carte de fidélité par les enseignes.

Pour réussir son projet de mise en circulation de sa carte privative une organisation doit disposer entre autre des composants matériels et logiciels nécessaires mais doit prendre en considération une composante fondamentale qui est la sécurité de l'information pour le périmètre de sa plateforme.

Le travail objet de cette mémoire est de présenter un ensemble de mesures de sécurité de l'information organisationnelles et techniques selon la norme ISO/CEI 27002 version 2013 et selon les expériences vécues dans le projet de la carte privative AGILIS de la SNDP-AGIL.

Cette mémoire s'articule autours de six chapitres dont le première traite du cadre global du travail et pose les problématiques des moyens de paiement de la SNDP-AGIL, le deuxième introduit la solution à ces problématiques qui est le projet de la carte à puce privative pétrolière AGILIS, le troisième chapitre présente l'état de l'art de la carte à puce. Dans le quatrième chapitre on introduit les normes de sécurité de l'information. Le cinquième chapitre présente les mesures et recommandations organisationnels physique et environnementale de sécurité de l'information pour sécuriser le périmètre de la carte à puce. Et dans le dernier chapitre d'autres mesures plutôt techniques informatiques pour offrir un cadre de sécurité technique à la plateforme de la carte.

Chapitre 1 : Le cadre global du travail les moyens de paiement à la SNDP

Introduction

La **SNDP** utilise les bons carburants comme moyen de paiement réservé à sa clientèle pour régler leurs achats sur le réseau de stations services AGIL. Le gérant de la station service utilisera ces bons pour payer partiellement ses achats de carburants auprès de la S.N.D.P. Ces Bons feront l'objet d'une facturation au client final.

1.1 Présentation de la SNDP-AGIL

La **SNDP** est la société nationale de distribution des pétroles, créée en 1960 par le Groupe ENI de la Société Internationale AGIP S A, acquise à 50% par l'Etat Tunisien en 1963. En 1975 la conclusion d'un accord avec le groupe ENI a été ratifiée par la loi 75-81 du 20 décembre 1975 pour le rachat du reste du capital.

Ayant comme mission le stockage et la commercialisation des produits pétroliers sous le label AGIL, c'est une SA d'un capital de 32 millions DT sous la tutelle du ministère de l'industrie.

En développant ses activités, AGIL S.A. a fini par occuper la première place parmi les entreprises du secteur, tant par le volume de ses ventes que par l'importance de son chiffre d'affaires et le savoir-faire de ses ressources humaines et s'emploie constamment à consolider cette position en offrant à ses clients la meilleur qualité de produit et de service.

AGIL SA a obtenu sa certification selon le référentiel ISO 9001 version 2000 en octobre 2005, pour ses activités de commercialisation et distribution des hydrocarbures liquides, de jet A1, de carburant, de lubrifiant et de GPL en vrac. En 2012 AGIL SA a renouvelé cette certification.

1.2 La SNDP-AGIL en chiffre

- Elle a un effectif total de 1125 agents : 321 cadres, 421 maitrises, 373 exécutions. (2013)
- Chiffre d'affaire en 2010 : 1253 million DT
- Part de marché : 43.3%
- 200 stations-services réparties sur tout le territoire national
- 50 stations de port de pêche et de plaisance
- 70 distributeurs de bouteilles de gaz
- 7 dépôts de kérosène dans les aéroports tunisien
- 3 centres de stockage et d'emplissage de GPL bouteille
- Plus de 2000 clients du secteur privé (personne morale et physique) ainsi que la totalité des établissements étatiques.
- Une flotte de près de 200 véhicules lourds et légers sillonne le territoire national pour assurer notamment le ravitaillement des stations de service.
- La SNDP-AGIL possède le certificat ISO 9001.

1.3 Activité de la SNDP

Les activités principales de la SNDP/AGIL sont le stockage et la distribution des hydrocarbures liquides et gazeux et également leurs dérivés.

- Jet A1 : représente l'hydrocarbure liquide pour les transports Aériens sous la marque « AGILAIR » ;
- Lubrifiants : représentant les huiles.
- Carburant : représentant les hydrocarbures liquides
- Gaz : représentant la GPL (gaz des pétroles liquéfiés)
- Le fuel lourd et BTS (pour les bateaux et les cimenteries)
- Les produit spéciaux (xylène : d'hydrocarbures aromatiques dérivés méthyles du benzène)

1.4 Stratégies de la SNDP

La SNDP a élaboré au cours des dernières années une vaste stratégie visant à renforcer la présence commerciale de l'entreprise. Cette stratégie s'articule autour de trois axes principaux : le client, les ressources humaines et l'environnement.

La stratégie de la SNDP s'oriente totalement vers le client et porte également sur la promotion de l'image de marque de l'entreprise, à travers une série d'action de marketing.

La stratégie future porte aussi sur l'amélioration de son système d'information, du savoir-faire et de la compétence de son personnel ainsi que sur la consolidation de son ouverture sur les milieux universitaire et de la recherche.

Parallèlement, la SNDP qui fait de la protection de l'environnement une de ses priorités a mis en place dans ces stations services un système de récupération des huiles utilisés des véhicules, a mis aussi en place un système de management environnemental pour obtenir la certification de conformité par la norme ISO 140000.

1.5 Etude de l'existant

1.5.1 Système de payement par carte bon & Bon Valeur de la S.N.D.P

La clientèle Bon Valeur et carte bon est composée d'entreprises publiques, d'administrations et de privés clients passagers, de l'extra réseau et des privés. Le personnel de ces entreprises cliente de la S.N.D.P est habilité à consommer dans les stations-service AGIL. Le règlement s'effectue avec le moyen de paiement CB & BV S.N.D.P.

- B.V sont des bons libellés en dinars tunisiens par carnets de 24 bons ayant une valeur de 10, 15 ou de 25 dinars par bons.
- Les bons sont édités et imprimés suite à la demande du client auprès du guichet unique de la S.N.D.P.
- L'impression et le codage des bons se font en CMC7.
- La facturation et le paiement sont faits à la livraison des carnets Bons Valeur.
- Au retour au siège lecture des lignes CMC7 pour le contrôle de vraisemblance et la mise à jour de la base de données.

Figure 1 Un spécimen de Bon Valeur

1.5.2 Processus de circulation des Bons Valeur

Le processus de circulation des B.V suit les phases suivantes :

1. Les clients passent leurs commandes au siège de la S.N.D.P.
2. Saisie de la commande et de l'ordre de service par un opérateur.
3. Validation des ordres de service et établissement des ordres de traitement.
4. Création logique des bons.
5. Impression et massicotage des bons.
6. La S.N.D.P livre les bons aux clients.
7. Les clients distribuent ces bons à leurs personnels.
8. Les bons sont regroupés par les gérants des stations après avoir procuré leurs produits aux clients.
9. Les gérants des stations livrent ces bons, sous forme d'un bordereau gérant, aux chauffeurs des camions d'approvisionnement pour les remettre aux dépôts.
10. Ces bons seront acheminés ensuite vers le siège au centre de traitement des bons.
11. facturation des bons consommés aux clients et génération d'une note de débit/crédit au gérant en cas de différence entre les bons lus et le montant déclaré par le gérant

Ci-dessous un schéma qui résume les phases de circulation des B.V

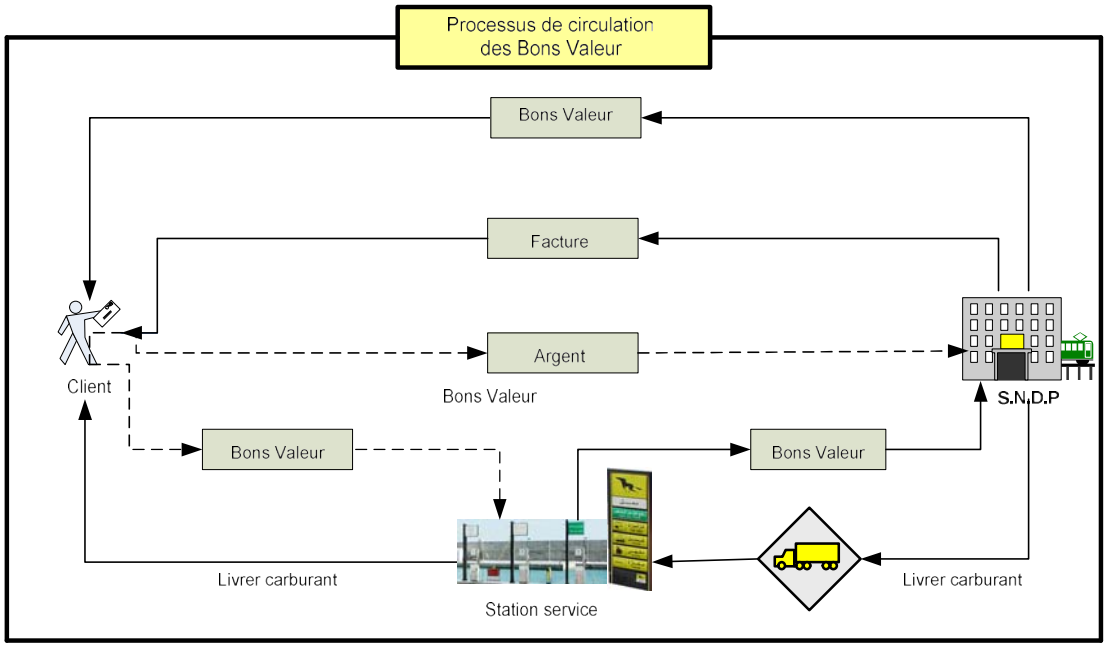


Figure 2 Le processus actuel de circulation des B.V

1.6 Critique de l'existant

On remarque clairement des sections précédentes, que les BV font l'objet d'un traitement complexe en amont et en aval de leurs consommations. Les inconvénients du processus actuel de paiement par B.V peuvent être énumérés comme suit :

- Le client est contraint à se déplacer vers le siège de la S.N.D.P pour commander des Bons.
- Le client est amené à visiter à plusieurs reprises le service d'édition des bons de la S.N.D.P, pour consulter l'état d'avancement de sa commande.
- Le client peut perdre un ou plusieurs bons
- Les bons peuvent être volés ou falsifié
- Les bons peuvent entre détériorés par l'eau ou autre produit
- Les services d'édition et de collecte des Bons sont confrontés à un travail fastidieux et routinier. En effet, l'ensemble des Bons consommés sur le réseau de stations services AGIL, sur tout le territoire, doit passer par un lecteur qui vérifie leur authenticité et les insère dans la BD (voir figure 4). Le nombre très important de Bons à traiter provoque un retard pouvant atteindre 4 à 5 mois. C'est-à-dire que les Bons livré à la S.N.D.P à une date D sera traité à une date D+4 mois (voir figure 4).

Figure 3 Lecteur Optique de B.V

Figure 4 Des milliers de bons en attente de traitement

1.7 Proposition de solutions

En vue des problèmes soulevés précédemment et dans sa ligne de stratégie de modernisation de ces moyens de paiement, la SNDP a envisagé un projet de paiement par carte à puce en remplacement des bons. Ce projet a été programmé par le plan stratégique de l'entreprise pour la période 2013-2018.

Chapitre 2 : Modernisation des moyens de paiement de la SNDP

Introduction

Dans le cadre de sa stratégie de modernisation de ces moyens de paiement et pour palier au différents insuffisances des bons carburant la SNDP lance son nouveau moyen de paiement par carte à puce privative pétrolière électronique présentant toutes les qualités de sécurité, de souplesse, de proximité et d'économie et qui pourrait être personnalisé en fonction des besoins de chaque client

Cette nouvelle carte pétrolière AGILIS, avec ces deux variantes post et pré payée est une avancée commerciale et technologique qu'AGIL met sur le marché et qui présente des fonctionnalités offertes aux clients tunisiens pour la première fois.

Le service de la carte AGILIS est disponible sur le plus grand réseau de distribution de carburant en Tunisie soit plus de 200 stations services repartie sur tout le territoire.

On présentera dans ce chapitre tout les aspects de ce projet.

2.1 Présentation du projet AGILIS

Ce projet a été envisagé depuis des années et programmé par le plan stratégique de l'entreprise pour la période 2013-2018.

Ce système vise à offrir aux clients AGIL, un moyen de paiement qui permet de:

- Moderniser le système de paiement par la dématérialisation des transactions et l'élimination des inconvénients du support papier des bon carburant et par conséquent l'amélioration de l'image de marque AGIL.
- Assurer une meilleure sécurité des moyens de paiement de la SNDP : face aux multiples opérations malveillantes de fraudes et de falsifications enregistrées ces derniers temps touchant les cartes bons et les bons valeurs.
- Diminuer le volume des transactions cash (manipulation d'argent liquide) et les risques y afférents tant pour les clients, pour les gérants ainsi que pour les transporteurs. Risque de vol, de perte, de fraude et des éventuelles erreurs de comptage.
- Elargir l'offre commerciale de la SNDP et de rattraper la concurrence.
- Fidéliser la clientèle AGIL.

2.1.1 Les composantes du projet

La solution se présente comme suit

2.1.1.1 Une composante matérielle constituée de :

- Terminaux de paiement électronique fixe (IP/GPRS).
- Terminaux de paiement électronique (IP) intégrés aux distributeurs carburants
- Lot de 10000 cartes à puce.
- un réseau local informatique mis en place dans 55 stations
- une plateforme composée de serveurs, équipements réseau et des équipements de sécurité informatique

Figure 5 Deux types de TPE autonome et intégré

2.1.1.2 Une composante logicielle constituée de:

- Une Application web Back office pour la gestion interne de la carte pétrolière,
- Un Système de télécollecte basé sur des services web
- Une Application Front Office publié sur le web destiner la l'accès des clients pour gérer tout les aspects de leurs cartes : recharge, consommation, itinéraires, kilométrage,...
- Un module SMS pour l'identification du client
- Un module Interfaçage interne avec l'ERP de l'entreprise

2.1.1.3 Un service de personnalisation des cartes (encodage et embossage).

La SNDP a fait le choix de confectionner (encodage et embossage) des cartes chez notre partenaire qui a fournit l'ensemble de la solution applicative de la carte privative pétrolière.

2.1.2 Les schémas fonctionnel par acteurs du projet

2.1.2.1 Schéma fonctionnel du projet carte privative pétrolière : Pour le Client

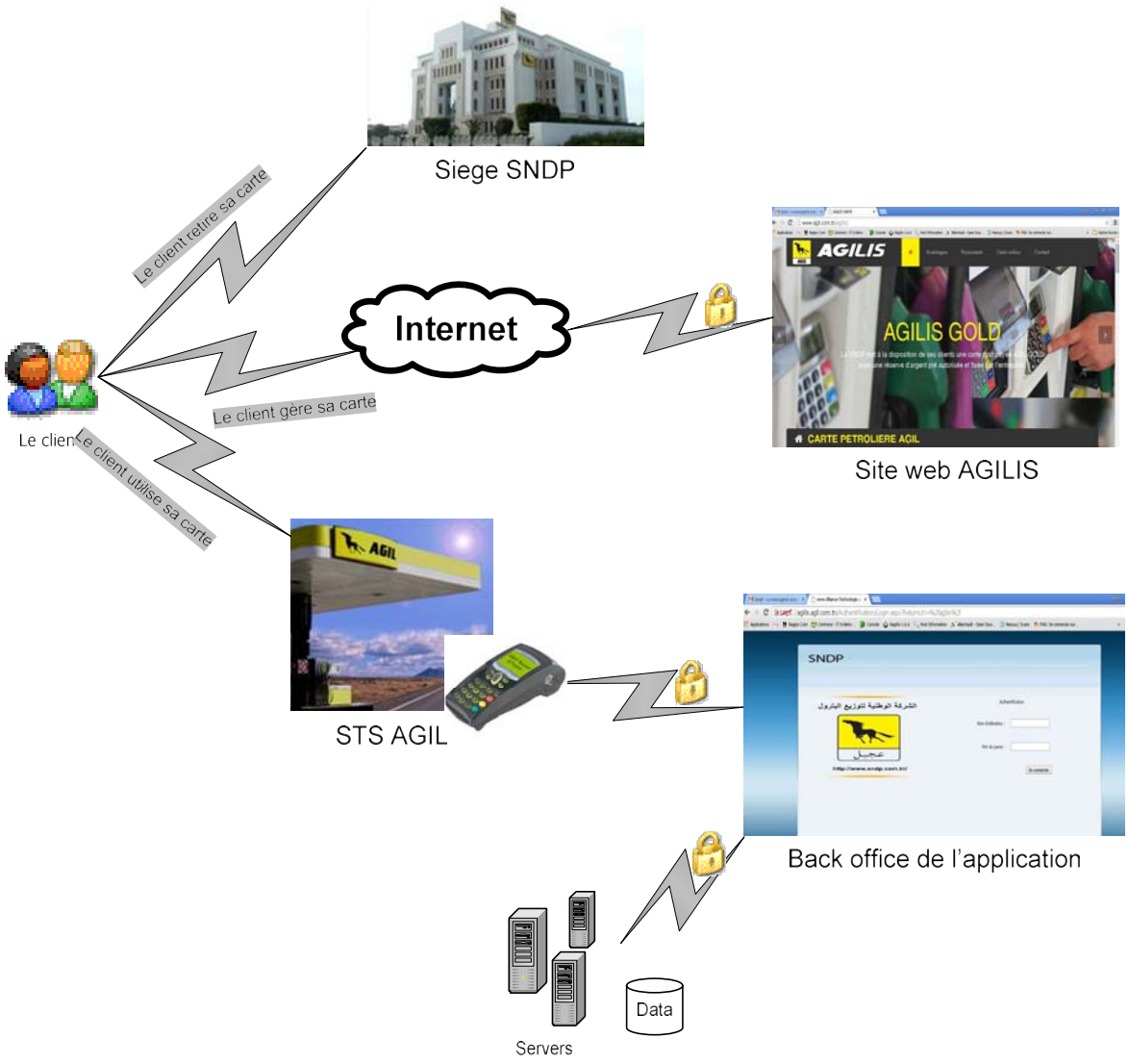


Figure 6 Schéma fonctionnel CP pour le client

- Le client retire sa carte privative pétrolière auprès des bureaux de vente de Tunis, Sousse ou Sfax
- Le client recharge sa carte via le site agilis.tn sur internet
- Il peu aussi via ce site faire une opposition sur sa carte, gérer les recharges d'une carte mère vers des cartes filles, surveiller sa consommation, son kilométrage, ...
- Quand le client s'approvisionne avec sa carte il est au fait mis en contact avec son compte sur le Back Office donc la base de données pour l'autorisation de la transaction.

2.1.2.2 Schéma fonctionnel de la carte pétrolière : Pour le Gérant de la Station

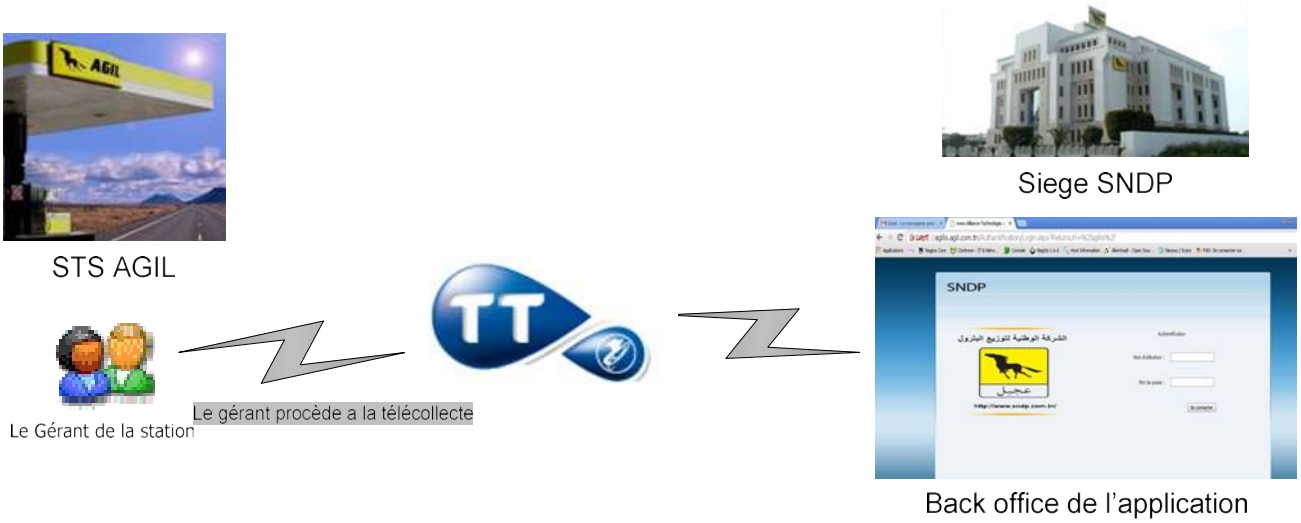


Figure 7 Schéma fonctionnel CP pour le Gérant

- Le Gérant effectue par intervalle de temps la télécollecte des ses ventes par la carte privative pétrolière.
- Le Gérant est alors en contact avec son compte sur le Back Office pour préparer son bordereau de vente par carte

2.1.2.3 Schéma fonctionnel de la carte pétrolière : Pour la SNDP

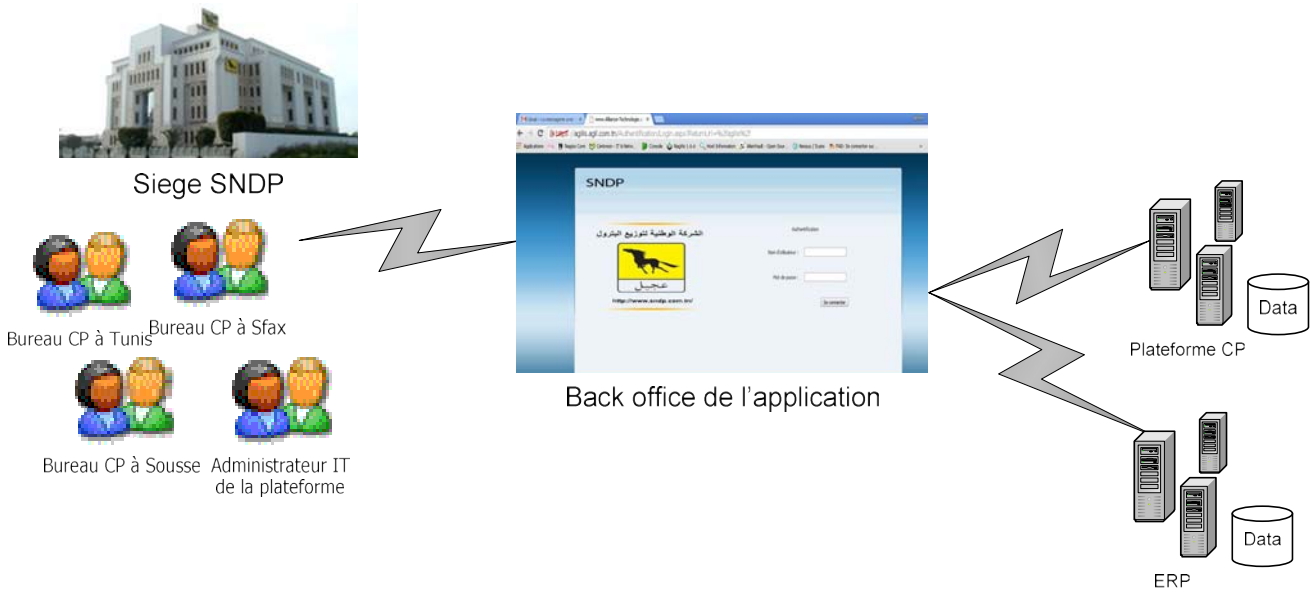


Figure 8 schéma fonctionnel CP pour la SNDP

- Les agents SNDP dans les bureaux de vente et facturation de Tunis, Sousse ou Sfax son en contact avec l'application Back Office pour les différents demandes des clients.

- les administrateurs de la plateforme sont en contact avec le back Office pour le contrôle, les mises à jour, les réclamations IT client, les mouvements avec l'ERP, le déblocage des cartes, la relation avec l'opérateur,...

2.1.2.4 Schéma global de la plateforme de la carte à puce privative pétrolière

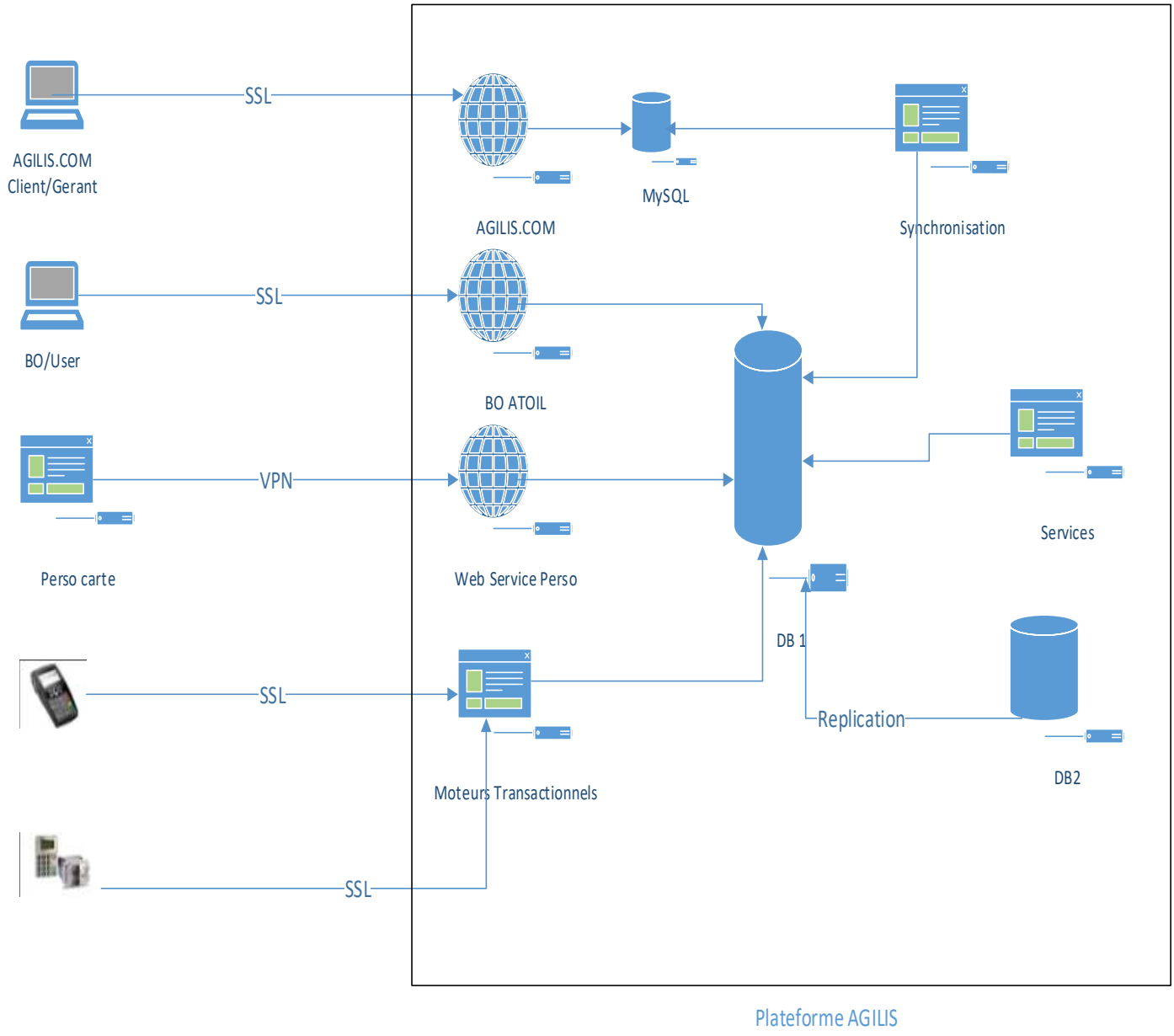


Figure 9 schéma global plateforme carte à puce

2.1.2 Avantages fonctionnels de la carte

Il existe trois types de cartes :

- **Carte prépayée** : ou porte monnaie électronique

La valeur monétaire est stockée dans la carte. C'est une recharge d'un montant déterminé à validité illimitée qui peut également être effectuée à distance via le portail web mis à la disposition des clients. C'est la meilleure solution permettant d'offrir un avantage pratique et sécurisé aux cadres et usagers des véhicules utilitaires d'une entreprise. La facturation et le paiement se feront au moment du chargement.
Cette carte peut être personnalisée ou anonyme.

- **Carte post payée** : La réserve d'argent est pré autorisée et fixée par l'entreprise

Il est délivré à l'utilisateur de la carte un plafond mensuel constitué du crédit que la SNDP lui a octroyé. La carte est alors programmée pour un rechargement automatique plafonné à hauteur du crédit alloué. La facturation et le paiement se feront après consommation selon les conditions commerciales octroyées au client.

- **Carte pré-facturée** (administration) : qui est pré-chargée en litrage valorisé, facturée le jour du chargement et payée à échéance.

Figure 10 AGILIS GOLD

PRÉ PAYÉE

- **Litrage/Valeur**
- **Pre-facturée**
- **Post-facturée**
- **Anonyme**
- **Recharge à distance**

Figure 11 AGILIS CASH

POST PAYÉE

- **Litrage/Mono Produit**
- **Valeur/Multi produit**
- **Post-facturée**
- **Plafond autorisé**

2.1.3 Les Caractéristiques de la Carte Pétrolière AGILIS

Proximité :

La carte est utilisable dans **toutes les stations services AGIL**, plus de 207 stations du réseau de distribution, minutieusement réparties dans tous les gouvernorats dans le but d'être le plus proche du client.

Personnalisé :

Les paramètres de la carte peuvent être personnalisés pour répondre aux besoins des clients :

- Le choix parmi différents produits carburant et lubrifiant,
- La décision des jours d'utilisation autorisés
- La limitation des transactions, selon les convenances du client, à des stations-service déterminées.
- La fixation de plafonds individuels pour chaque véhicule ou utilisateur.
- La fixation de ces plafonds peut être faîte par jour, par semaine et/ ou par mois.
- La Désactivation des fonctionnalités de la carte selon les exigences du client.
- La modification des plafonds, selon les besoins du client dans la limite de son solde, sans avoir à refaire la carte. Ce service est gratuit.

Figure 12 Explication sur les champs sur la carte

Sécurité :

- La carte est équipée d'une puce électronique de dernière génération garantissant une utilisation simple avec une sécurité maximale,
- Un code confidentiel est attribué à chaque utilisateur sans lequel aucune transaction ne peut être validée il est possible d'associer à chaque carte un code PIN et plusieurs codes chauffeurs sécurisés pour que chacun ait un code unique,
- La carte sera bloquée si on saisit un faux code trois fois consécutivement. Toute carte en opposition sera automatiquement refusée par le TPE,
- Toutes les transactions sont effectuées online, en cas de défaillance du réseau reliant le TPE au serveur, une seule transaction offline est autorisée,
- Les transactions sont cryptées de bout en bout,
- Toutes les transactions sont détaillées par véhicule, par utilisateur et par point de vente. Le suivi de ces opérations d'approvisionnement en carburant peut également être fait quotidiennement à travers notre solution web

Economie :

- La facture mensuelle permet une récupération de la TVA sur les achats de carburants. A la fin de chaque mois, le client recevra par courrier une facture détaillée de toutes les transactions passées.
- Le suivi quotidien de la consommation de la flotte du client à travers le site internet, permet de réagir à temps en cas d'utilisation anormale ou abusive et donc d'économiser sur les dépenses en carburants.
- L'option "Saisie Kilométrage" calcule la consommation moyenne de carburant par véhicule, (en litres par 100 kilomètres) permettant ainsi de détecter toute anomalie d'utilisation ou de consommation, le client peut visualiser directement l’impact du type de trajet et de toute modification dans son style de conduite sur la consommation.
- Le client peut consulter en toute confidentialité les transactions, et les télécharger sur fichier Excel, au jour le jour à travers le portail web de la solution, télécharger les factures, les relevés de comptes en format PDF

Chapitre 3 : Etat de l'art de la carte à puce

Introduction

La carte à puce est aujourd'hui omniprésente dans notre environnement : télécartes, cartes bancaires, cartes SIM, cartes de décryptage de télévision par satellite ainsi que toutes les versions de cartes privatives de diverses enseignes commerciales sont autant de cartes à puce issues d'une même technologie.

Nous présentons dans ce chapitre toutes les informations relatives aux cartes à puce : les normes, les différents types de cartes, les lecteurs et programmateurs et les logiciels.

3.1 Dimensions

Nous ne connaissons aujourd'hui que deux formats principaux de cartes à puce : celui de la carte bancaire ou celui de la carte dite mini ou micro SIM des téléphones portables; il existe théoriquement trois tailles physiques normalisées appelées ID 1, ID 00 et ID 000. Ces trois formats sont présentés, avec leurs dimensions respectives, sur les figures ci-dessous

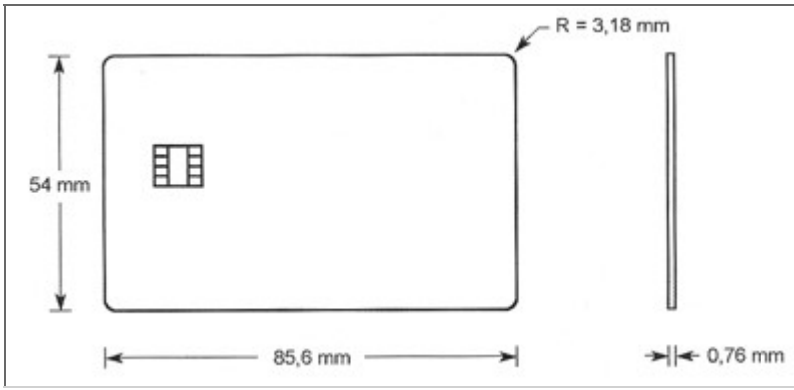
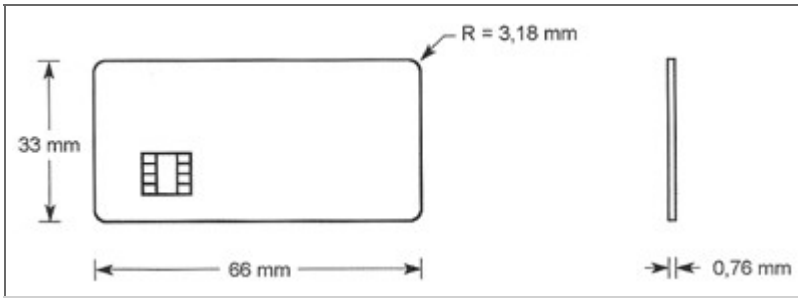
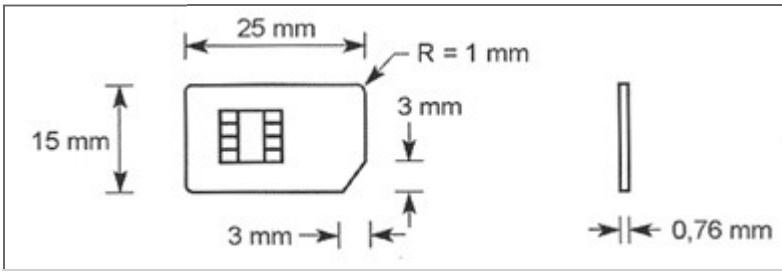
Format ID 1	
Format ID 00	
Format ID 000	

Figure 13 Dimensions des cartes privatives

L'examen de ces trois figures montre immédiatement que les cartes à puce "normales", c'est à dire les cartes bancaires, sont au format ID 1 tandis que les cartes mini ou micro SIM des téléphones portables sont au format ID 000.

3.2 Position des contacts

Encore plus peut-être que les dimensions des cartes, les contacts de connexion avec la puce doivent avoir une position parfaitement normalisée faute de pouvoir lire n'importe quelle carte dans n'importe quel lecteur.

Position AFNOR	Position ISO

Figure 14 Position des contacts sur la carte

3.3 Brochage

Les huit contacts, repérés C1 à C8 sur les figures de la page Position des contacts sont définis dans la norme ISO 7816-3 de la manière suivante :

- C1 porte l'appellation normalisée VCC ce qui correspond donc à la tension d'alimentation positive de la carte, fournie par le lecteur
- C2 porte l'appellation normalisée RST et correspond à la commande de reset de la carte, fournie par le lecteur. L'utilisation de cette entrée par la carte n'est pas obligatoire avec certaines cartes à mémoire
- C3 s'appelle quant à lui CLK ce qui est bien sûr l'abréviation de clock et correspond à l'horloge fournie à la carte par le lecteur. Bien que la norme précise ici encore que ce signal est optionnel, il est présent sur toutes les cartes, que ce soient de simples cartes à mémoire ou des cartes à microcontrôleurs car c'est lui qui rythme les échanges de données entre la carte et son lecteur
- C4 et C8 s'appellent RFU ce qui signifie tout simplement Reserved for Future Use. Même si vous n'êtes pas anglophone vous aurez compris que ces contacts sont donc réservés à une utilisation future
- C5 s'appelle GND et correspond bien évidemment à la masse électrique de la carte
- C6 s'appelle VPP et correspond à une tension de programmation de la carte fournie par le lecteur. Cette tension n'est plus jamais utilisée de nos jours. Sa présence vient du fait que les premières cartes à puce qui ont été produites intégraient de la mémoire EPROM, c'est à dire

de la mémoire programmable électriquement, qui nécessitait une tension de 21 volts pour cela. C'est cette « haute » tension, que l'on appelait tension de programmation, qui justifiait la présence de cette entrée VPP. Aujourd'hui, et même si quasiment toutes les cartes intègrent de la mémoire EEPROM, c'est à dire programmable et effaçable électriquement, la haute tension n'est plus nécessaire car la technologie actuelle permet de se satisfaire de la seule tension d'alimentation normale VCC

- C7 enfin est peut être le signal le plus important de tous puisqu'il s'appelle I/O et qu'il correspond donc aux entrées et sorties de données en provenance ou à destination de la carte. Cette ligne étant seule pour réaliser les entrées et sorties de données, elle est évidemment bidirectionnelle

Ce brochage, normalisé et universellement respecté, est présenté sous forme plus visuelle sur la figure ci-dessous.

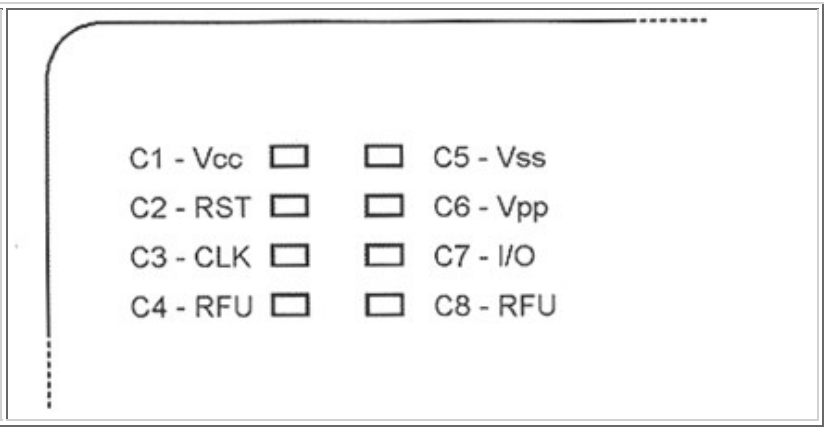
Brochage des cartes à puce	

Figure 15 Brochage des cartes à puce

3.4 Normes des cartes à puces

Pour définir une carte à puce, il faut au moins normaliser trois types de paramètres différents :

- Des paramètres physiques qui indiquent la taille de la carte et la position de la puce et de ses contacts
- Des paramètres électriques qui précisent les tensions d'alimentation et niveaux électriques mis en œuvre ainsi que le brochage de la puce sur la carte
- Des paramètres logiciels qui définissent le mode de dialogue avec la carte, les commandes qu'elle peut interpréter et son comportement face à ces dernières

En ce qui concerne la carte à puce, les trois normes principales sont :

- la norme ISO 7816 – 1 précisant les caractéristiques physiques de la carte
- la norme ISO 7816 – 2 définissant la position et le brochage des contacts de la carte à puce
- la norme ISO 7816 – 3 définissants les niveaux électriques et les chronogrammes de bas niveau qui régissent le dialogue avec les cartes à puce
- la norme ISO 7816 – 4 enfin, définissant les différentes commandes de base des cartes à puce

La plus intéressante de ces normes est évidemment l'ISO 7816-4 qui permet de comprendre le dialogue entre une carte à puce et son lecteur

3.5 Les différents types de cartes

Les deux principales familles de cartes qui cohabitent sur le marché sont :

3.5.1 Les cartes à mémoire ou cartes synchrones

La première famille, qui est aussi la plus ancienne, est la carte à mémoire appelée aussi carte synchrone en raison de son protocole de dialogue. Bien que ce soit une carte à puce, puisqu'une mémoire est bel et bien une puce de circuit intégré ; cette famille de carte est cantonnée à des applications relativement simples. Elle ne contient en effet que de la mémoire. En fait, cette famille peut aujourd'hui être scindée à son tour en deux sous-familles avec les cartes à mémoire "simples" appelées cartes à mémoire "tout court" et les cartes dites à mémoire protégée.

Ces cartes sont plus sûres que les cartes précédentes mais elles ne permettent pas la mise en place des applications les plus complexes que sont les cartes bancaires, les cartes SIM ou bien encore les cartes de décryptage TV. Il faut en effet pour cela que la carte dispose d'une "intelligence" locale que n'ont pas les cartes à mémoire.

3.5.2 Les cartes à microcontrôleur ou cartes asynchrones

L'intelligence locale qui fait défaut aux cartes à mémoire existe seulement dans les cartes à puce à microcontrôleur, appelées aussi cartes asynchrones en raison de leur protocole de dialogue. Ces cartes sont désignées aujourd'hui sous le vocable unique de cartes à puce, ou smart cards. Les cartes à puce "intelligentes" renferment un microcontrôleur complet ; c'est à dire l'association en un seul circuit d'une unité centrale de microprocesseur, de mémoire morte, de mémoire vive, de mémoire EEPROM, d'une interface d'entrée/sortie série et de toute la logique nécessaire pour faire fonctionner tout cela.

C'est donc bien un véritable petit micro-ordinateur complet qui est contenu dans ces cartes ; micro-ordinateur dénué de clavier et d'afficheur et dont le seul moyen de communication avec le monde extérieur est sa ligne d'entrée/sortie unique et bidirectionnelle I/O.

3.5.3 Les cartes vierges, personnalisables ou à OS ouvert

Parmi les cartes asynchrones, c'est à dire les cartes à microcontrôleur, il faut encore distinguer trois catégories différentes :

- Les cartes à puce "vierges" ou "spécifiques" dont la mémoire de programme du microcontrôleur ne contient rien lorsque vous les achetez. C'est donc à vous d'écrire l'intégralité de leur OS (operating system). Cela demande beaucoup de travail mais permet de disposer de cartes réellement "sur mesure". Les cartes Gold, Silver, Fun ou bien encore Jupiter font partie de cette famille

- Les cartes à puce dites "personnalisables". Dans ces cartes, le fabricant à programmé un OS (operating system) qui connaît un certain nombre de commandes et qui dispose d'un système de gestion de fichiers. Tout cela est personnalisable dans des limites plus ou moins larges selon la carte choisie. Ces cartes permettent de développer très rapidement une application quasiment sans programmer. En contrepartie, certaines applications ne peuvent pas être réalisées avec de telles cartes.

- Les cartes à puce dites "à OS ouvert". Dans ces cartes, le fabricant à programmé un interpréteur de P-code ; ce P-code provenant lui-même de la compilation de langage évolué tel que Java dans la Java Card ou Basic dans la Basic Card®. Comme pour les cartes à puce vierges, on peut ainsi réaliser une application "sur mesure" mais avec une programmation plus facile car elle est réalisée en langage évolué et non en langage machine. En outre, l'interpréteur de P-code prend en charge tous les protocoles de dialogue de bas niveau que l'on n'a pas ainsi à programmer

3.6 Les lecteurs de cartes

Si on utilise des cartes vierges telles que les cartes Gold, Silver, Fun ou Jupiter, il nous faut un programmateur, au moins pendant la phase de développement de l'application. C'est en effet ce programmateur qui va programmer le microcontrôleur de la carte et/ou sa mémoire EEPROM. Une fois cette carte programmée, et si on a écrit un programme compatible des normes ISO 7816 3 et 4, un lecteur classique pourra ensuite être utilisé pour lire et écrire dans votre carte.

Un programmateur classique en boîtier Le Multipro 2000	
	
Le lecteur CyberMouse d'ACS	Le lecteur ACR 30 d'ACS

Figure 16 Les lecteur et programmateur de carte à puce

Notez bien que tous les lecteurs de cartes à puce sont capables d'écrire dans les cartes à puce, pour peu que ces dernières l'autorisent. Le programmateur en tant que tel n'est nécessaire que pour les cartes initialement vierges car, tant qu'elles sont vierges, elles ne peuvent pas dialoguer avec quoi que ce soit.

3.7 Le logiciel nécessaire

Pour piloter un lecteur classique il faut disposer de ses pilotes sous le système d'exploitation qu'on utilise (Windows ou Linux par exemple). En outre, ces pilotes sont très bien documentés (en anglais) et des exemples de programmes qui les utilisent sont même fournis

3.7.1 Pilotes propriétaires ou PC/SC

Jusqu'à présent, et même si de nombreux lecteurs compatibles d'un environnement Windows étaient disponibles sur le marché, pour le développement d'application ; tout changement de lecteur impliquant en effet bien souvent de devoir réécrire tout ou partie de l'application.

Afin de mettre un terme à cette situation et de standardiser en quelque sorte le lecteur de cartes à puce au même titre que les autres périphériques reconnus par Windows, un groupe de travail s'est constitué, sous le nom de PC/SC Workgroup. Ce groupe a mis sur pied une spécification, appelée PC/SC pour PC Smart Card, qui permet de définir une interface "standard" pour l'utilisation de lecteurs de cartes à puce sous Windows. Même si on peut critiquer une fois de plus la domination de Microsoft, il faut reconnaître que cette standardisation simplifie le travail des développeurs d'applications cartes à puce devant fonctionner sous Windows.

En effet, si on décide de travailler dans le respect de la compatibilité PC/SC, nous n'avons plus à nous soucier du type de lecteur qui sera employé ni du fait qu'il utilise telle ou telle API pour dialoguer avec notre application. Cela permet de rendre véritablement celle-ci portable et indépendante du matériel.

[1] La source des informations concernant l'état de l'art de la carte est dans ce lien

Chapitre 4. Les normes de sécurité de l'information

Introduction

Dans ce chapitre on va aborder les normes de sécurité de l'information qui réglemente tout les aspects de sécurité informatique dans une organisation. On évoquera leurs champs d'application ainsi que les principes directeurs de ces normes.

Figure 17 L'ensemble des normes ISO 2700x

4.1 La Norme ISO/CEI 27002 Les bonnes pratiques

L'ISO 27002:2013 donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation.

L'ISO 27002:2013 est élaborée à l'intention des organisations désireuses de sélectionner les mesures nécessaires dans le cadre du processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon l'ISO/CEI 27001; de mettre en œuvre des mesures de sécurité de l'information largement reconnues; et d'élaborer leurs propres lignes directrices de management de la sécurité de l'information.

4.1.1 Evolutions de la version ISO 27002:2013

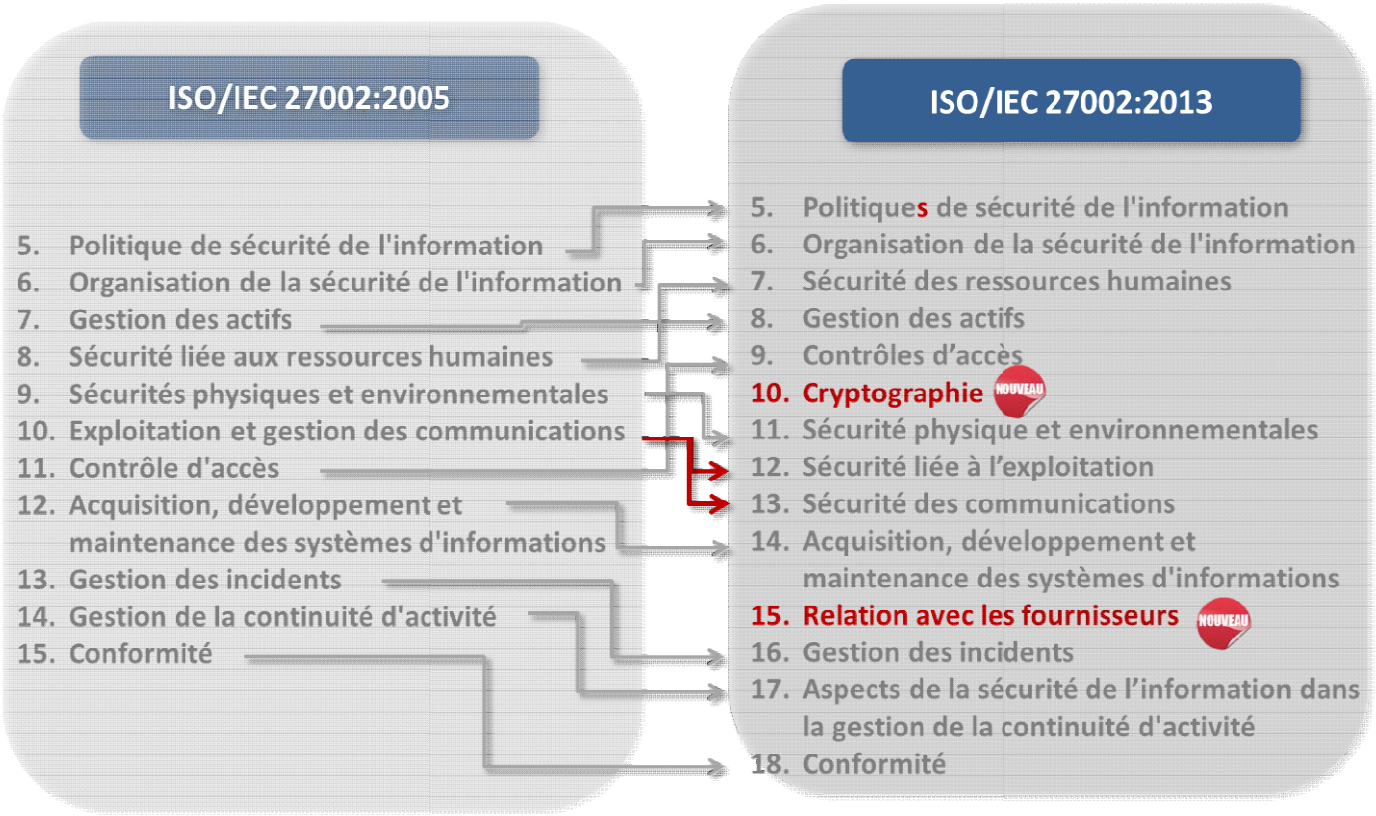


Figure 18 Evolution de l'ISO 27002 version 2013

4.2 La Norme ISO 27005 Risk management

L'ISO/CEI 27005:2011 contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

Cette norme est conçue pour aider à une mise en place de la sécurité de l'information basée sur une approche méthodique de gestion du risque. En effet, la norme ISO 27005 vient directement en appui des concepts généraux énoncés dans la norme ISO 27001, qu'elle complète donc en précisant les exigences portant sur la gestion des risques.

L'ISO/CEI 27005:2011 est applicable à tous types d'organisations (par exemple les entreprises commerciales, les agences gouvernementales, les organisations à but non lucratif) qui ont l'intention de gérer des risques susceptibles de compromettre la sécurité des informations de l'organisation.

4.2.1 Contenu de la norme

- Chapitre 7 Etablissement du contexte

    7.1 Considérations générales
    7.2 Critères de base
    7.3 Domaine d'application et limites
    7.4 Organisation de la gestion du risque en sécurité de l'information

- Chapitre 8 Appréciation du risque en sécurité de l'information

    8.1 Description générale de l'appréciation du risque en sécurité de l'information
    8.2 Analyse du risque
        8.2.1 Identification du risque
        8.2.2 Estimation du risque
    8.3 Evaluation du risque

- Chapitre 9 Traitement du risque en sécurité de l'information

    9.1 Description générale du traitement du risque
    9.2 Réduction du risque
    9.3 Maintien du risque
    9.4 Évitement du risque
    9.5 Transfert du risque

- Chapitre 10 Acceptation du risque en sécurité de l'information

- Chapitre 11 Communication du risque en sécurité de l'information

4.2.2 Démarche proposée

ISO 27005 propose une démarche de gestion des risques itérative, alignée sur les quatre phases Plan - Do - Check - Act. La tâche la plus importante reste cependant dans la phase de mise en place initiale, avec l'appréciation du risque.

Les activités décrites dans le standard et le processus générique de gestion des risques sont représentés dans le schéma ci-dessous :

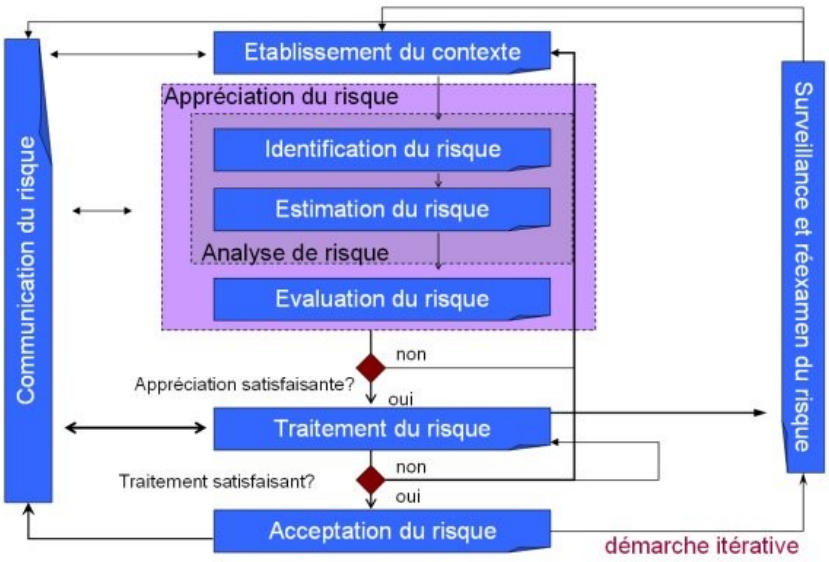


Figure 19 Démarche de l'ISO 27005

4.3 La Norme ISO/CEI 27001 SMSI

La norme ISO/CEI 27001 décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs informationnels. L'objectif est de protéger les informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion. Cela apportera la confiance des parties prenantes.

Le premier intérêt est d'aligner l'existant en termes de sécurité par rapport aux enjeux des métiers :

- Participer à la mise en place d'une véritable gouvernance du SI incluant la sécurité
- Aligner les besoins de protection des actifs (en DIC) avec les enjeux métiers
- Responsabiliser les métiers et les autres acteurs de la DSI sur les aspects sécurité

Le deuxième domaine d'intérêt concerne le fait d'impliquer les métiers dans la gestion des risques qui pèsent sur le système d'information.

- Renforcer l'engagement de la direction dans la conduite du plan de traitement de risques
- Planification budgétaire cohérente avec les pratiques de gouvernance

Enfin, faire connaitre auprès de tiers, des clients et de ses partenaires sa gouvernance concernant la protection de son patrimoine et le respect des contraintes réglementaires.

4.3.1 Evolutions de la version ISO 27001:2013

Par rapport à la version 2005, cette évolution de la norme apporte des simplifications et des clarifications :

- l'élaboration de la politique de sécurité est de la responsabilité du Top Management
- diminution du nombre de documents imposés (PGSI, Politique SMSI, ..)
- possibilité d'utiliser une méthode de gestion des risques non documentée de façon formelle
- indication claire que l'annexe A des mesures de sécurité peut être complétée par des mesures de sécurité adaptées aux enjeux

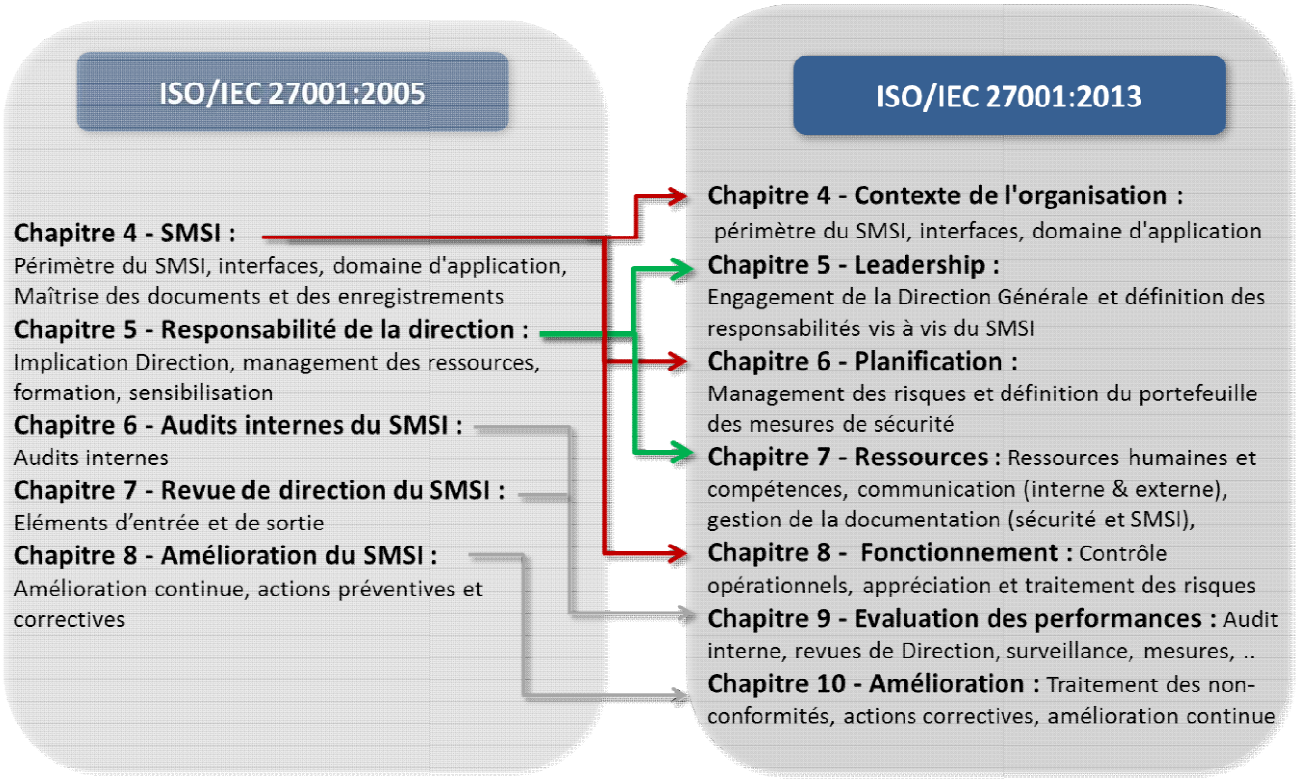


Figure 20 Evolution de la Norme ISO 27001 version 2013

Chapitre 5. Les exigences organisationnelles de sécurité informatique de la plateforme de carte à puce privative selon la norme ISO 27002

Introduction

Nous abordons dans ce chapitre les différentes exigences de sécurité de l'information organisationnelle et physique pour le périmètre de carte à puce privative qu'on appellera plateforme en se basant sur la norme ISO/CEI 27002 :2013.

5.1 Définition du périmètre de la plateforme de la carte à puce privative pétrolière

Nous définissons la plateforme de la carte à puce privative pétrolière comme étant l'ensemble des serveurs, applications (back office & front office), bases de données, équipements réseaux équipement de sécurité, les TPE, les lignes de communication ainsi que les lieux de traitement de l'information concernant la carte à puce privative que nous présentons dans le schéma suivant :

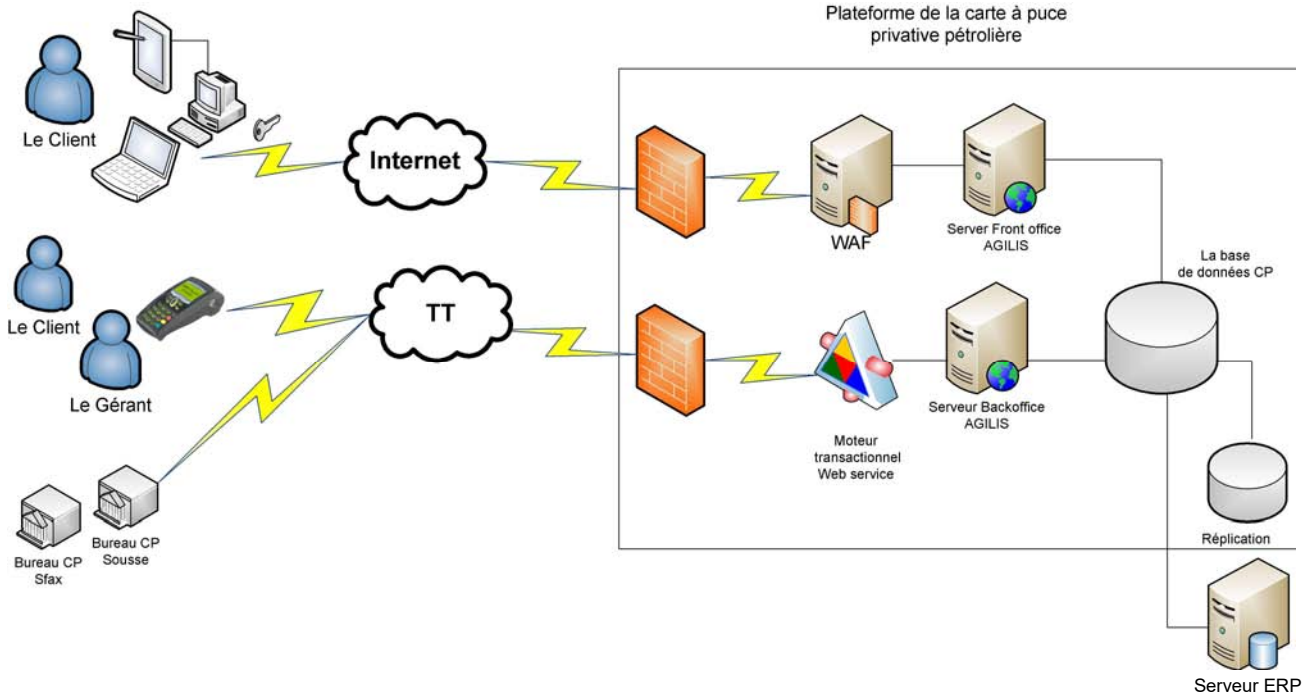


Figure 21 Périmètre de la plateforme

TT : l'opérateur Tunisie Télécom

Serveur Front office : l'application web du site agilis.tn destiné pour le client de la carte

WAF : Web Application Firewall : un dispositif de sécurité pour les applications web

Moteur transactionnel, web service : c'est l'interface pour tout les transactions faites à partir des TPE

Serveur back office : application web en intranet qui est l'application centrale clients, gérant, SNDP

Serveur ERP: le serveur du progiciel de gestion intégré de l'entreprise

Bureaux CP Sousse Sfax et Tunis : les bureaux de vente des cartes à puce privative et réclamations des clients et gérants

5.2 Etablir une politique de sécurité de l'information pour le périmètre de la plateforme de la carte (chapitre 5 de l'ISO 27002)

La politique de sécurité informatique fixe les principes visant à garantir la protection des ressources informatiques et des télécommunications en tenant compte des intérêts de l'organisation et de la protection de la personnalité de l'utilisateur.

La PSSI est un document interne signé par la direction générale. Ce document décrit les objectifs et mesures générales de l'entreprise, en matière de sécurité informatique. La PSSI doit assurer le meilleur compromis entre la souplesse qu'exigent les objectifs stratégiques de l'entreprise et le contrôle requis pour la protection de son système d'information. Elle constitue un document de référence pour tous les acteurs concernés par la sécurité de l'information (Responsables opérationnels, responsables informatiques, responsable sécurité, auditeurs).

La PSSI vise généralement cinq principaux objectifs :

- L'**intégrité** : c'est-à-dire garantir que les données sont bien celles que l'on croit être
- La **confidentialité** : consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées
- La **disponibilité** : permettant de maintenir le bon fonctionnement du système d'information
- Le **non répudiation**, permettant de garantir qu'une transaction ne peut être niée
- L'**authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources

Pour l'établissement d'une politique de sécurité nous recommandons :

- Définir le périmètre de la politique qui est dans notre cas la carte privative
- Suivre les chapitre de la norme ISO 27002 version 2013 (un nouveau chapitre à prendre en compte concernant les fournisseurs et partenaires de la solution)
- Nommer un Responsable de sécurité du système d'information **RSSI** qui doit collaborer avec les deux responsables IT et métier de la carte privative pour l'application des exigences de la politique de sécurité
- Pour le management des risques il faut suivre les chapitres de la norme ISO 27005.
- Mettre l'accent sur la sensibilisation des utilisateurs internes de la plateforme aux problèmes de sécurité qui peuvent toucher la plateforme et surtout éviter les généralités et soyer précis.
- Un des chapitres clé de la politique est le contrôle d'accès logique : on conseillera de documenter une politique de contrôle d'accès pour les accès réseaux filaire et sans fil, les accès OS, les accès des applications Front & back office
- Documenter une politique et une procédure de sauvegarde des données, notamment les bases de données, les applications back & front office ou encore les configurations des équipements de la plateforme.
- La sécurité des télécommunications : technologies réseau, Assurer une connexion continue des TPE avec les serveurs de la plateforme (une ligne principale et une ligne secours), définir les règles d'accès à distance sur la plateforme (les accès VPN).
- La sécurité physique : assurer la sécurité des infrastructures matérielles : salles sécurisées, lieux et espaces communs de l'entreprise, postes de travail des personnels, etc.

5.3 Etablir une charte de bon usage des moyens informatiques pour les utilisateurs et les administrateurs de la carte (chapitre 6 de l'ISO 27002)

La charte informatique est un document juridique à annexer au règlement intérieur de l'entreprise. Elle décrit les règles d'utilisation des moyens informatique et internet dans l'entreprise et détaille les droits et les responsabilités des utilisateurs.

La charte informatique a un rôle double :

- Obtenir l'adhésion des utilisateurs et administrateurs de la plateforme au processus de sécurité informatique
- Assurer à l'entreprise le respect de ses obligations légales vis-à-vis des tiers (clients, fournisseurs et partenaires)

Pour l'établissement d'une charte nous recommandons de mettre les articles suivants :

1. Suivez les règles et procédures de la sécurité de l'information

2. Protégez vos mots de passe **:** Ne révélez jamais vos mots de passe.

3. Sachez garder un secret **:** Ne révélez jamais de données confidentielles.

4. Bloquez l'accès à votre ordinateur **:** Si vous quittez votre bureau, bloquez l'accès à votre ordinateur.

5. Sauvegardez correctement vos données

6. Résister aux méthodes "d'ingénierie sociale" Lors d'une conversation par e-mail ou par téléphone, assurez-vous de l'identité de votre interlocuteur. Soyez prudents à chaque fois que l'on vous demande des informations personnelles, confidentielles, ou importantes au niveau de l'entreprise.

7. Soyez attentifs à vos e-mails

8. Utilisez intelligemment l'Internet

9. Utilisez un antivirus

10. Prenez soin du hardware et du software

11. Signalez les incidents

12. Spécifier des clauses dans la charte pour les administrateurs du système

Nous donnons en **Annexe A** un exemple de charte de bon usage des moyens informatiques et internet

5.4 Validation d'un manuel de procédure de la carte privative : répartition des rôles et des responsabilités (chapitre 6 de l'ISO 27002)

Le manuel de procédures est une documentation descriptive qui doit permettre une meilleure compréhension des systèmes d'informations dans son périmètre de la carte privative et une amélioration de la gestion. C'est un guide opératoire qui indique le circuit de traitement des opérations tout en spécifiant :

- La tâche à faire (quoi)
- Le niveau de responsabilités (qui)
- Les différentes étapes de traitement (quand)
- Les lieux de réalisation (où)
- Le mode d'exécution (comment)

Pour l'établissement des procédures nous recommandons la méthodologie suivante

Section 1 : Analyse de l'existant

Collecte des informations : Il s'agit pour l'auditeur de recueillir le maximum d'informations sur le domaine et le circuit de la carte privative. Plusieurs techniques sont utilisées : entretien et interview, questionnaire, diagramme de circulation de l'information

Description des procédures non formelles : une première description des procédures de traitement de l'information dans l'entreprise.

Diagnostic des procédures existantes : Ces procédures formalisées et validées sont ensuite analysées conformément au référentiel de l'auditeur (ensemble des objectifs de contrôle interne) et aux pratiques d'organisation communément admises.

Section 2 : Rédaction du manuel de procédure

Pour chaque procédure identifiée, le manuel présentera :

- L'introduction
- La description détaillant les étapes de la procédure :
- L'intervenant
- Les tâches et contrôles effectués
- La liste des documents utilisés comme supports

[2] On pourra s'inspirer de ce lien pour l'élaboration d'un manuel de procédure

Nous donnons en **Annexe B** un exemple de procédure de la carte privative

5.5 Désignation de deux responsables IT et métier de la plateforme (chapitre 6 de l'ISO 27002)

5.5.1 Les prérogatives du responsable IT :

- Veille au bon fonctionnement des applications Front & Back office et leurs suivit en MAJ et versionning
- Les sauvegardes des bases de données
- L'interaction entre la plateforme de la carte privative et l'ERP de l'entreprise
- Veille au bon fonctionnement des serveurs : hyperviseur, OS, MAJ, antivirus, ...
- Veille aux différents équipements réseaux et sécurité : Switch, routeur, firewall, antivirus : OS, MAJ et licencing
- L'application des différents politique : générale de sécurité, d'accès, de sauvegarde, ...
- Assurer le contact avec l'operateur pour la déclaration de lignes coupées
- suivit entre la SNDP et le partenaire pour les TPE autonome ou intégrés
- suivit de l'audit de sécurité de l'information de la plateforme de la carte pétrolière

5.5.2 Les prérogatives du responsable métier :

- promotion de la carte privative
- suivit des commandes clients pour les nouvelles cartes et le contact avec le partenaire qui confectionne les nouvelles cartes.
- suivit des réclamations clients (opposition, perte, vol...)
- gérer les bureaux de vente (Tunis, Sousse et Sfax)
- Suivit de la facturation client
- suivit des réclamations gérants des stations services
- suivit des statistiques des ventes et le chiffre d'affaire

5.6 Etablir un inventaire et classification des biens informationnels de la plateforme de la carte (chapitre 8 de l'ISO 27002)

Il s'agit de faire l'inventaire des biens informationnels du périmètre de la carte privative, leur affecter un propriétaire, les classifier; déterminer leur niveau de criticité et de protection et établir les mesures de sécurité à mettre en place selon leur utilisation.

Actif ou bien informationnel : c'est ensemble de données ou d'information, sur tout type de support, base de donnée, équipement informatique ou de télécommunication, logiciel, application informatique, système de courrier électronique, enregistreur d'image, système biométrique de pointage, data center, ligne de communication, locaux techniques.

Afin de respecter les principes de la sécurité de l'information et faciliter la phase d'analyse des risques, on doit fournir pour chaque actif, sa cote en CID (Confidentialité, Intégrité et Disponibilité), ce qui définit sa valeur. On doit aussi, relevé pour chaque actif, le nom de son détenteur ou propriétaire, sa localisation. En ce qui concerne la phase d'analyse de risques, on ne retiendra que les actifs dont la valeur de la disponibilité et/ou l'intégrité et/ou la confidentialité supérieure ou égale à 3. Cette démarche a aidera à se concentrer uniquement sur les actifs les plus critiques. Également, il est à noter que l'étape de catégorisation est un processus continu et par conséquent il doit faire l'objet de réévaluations périodiques, afin de prendre en compte les changements organisationnels et technologiques de l'entreprise ainsi que l'évolution des menaces et des risques inhérents aux actifs informationnels de l'établissement.

Catégorisation : Échelle des valeurs

Principe	**Valeur de l'actif** **1=bas, 2=moyen, 3=élevé, 4=critique**
Confidentialité	**Valeur de 1 à 4**
Intégrité	**Valeur de 1 à 4**
Disponibilité	**Valeur de 1 à 4**

Nous donnons en **Annexe C** des fiches support pour l'opération d'inventaire

5.7 Etablir une politique de sécurité physique et environnementale pour la gestion des cartes et des terminaux (chapitre 11 de la norme ISO 27002)

La sécurité physique concernant la plateforme de la carte est le premier aspect de sécurité à mettre en œuvre. En effet, quel intérêt y a t'il à se protéger avec des mots de passe ou des logiciels compliqués si une personne peut accéder physiquement à une ressource essentielle pour la voler, la modifier ou la détruire ?

Tous les éléments répertoriés comme importants ou vitaux pour « l'organisation » doivent être installés dans des locaux sécurisés. Ces locaux constituent le périmètre de sécurité.

La politique de sécurité physique et environnementale à mettre en place dans le périmètre de la carte peut être composée par les mesures suivantes :

- Protégés contre l'accès de personnes non autorisées et donc a fortiori aux personnes étrangères à l'entreprise. Une seule porte permet d'y accéder avec badgeuse biométrique, et une surveillance vidéo.
- Protégés contre l'incendie. Un système de détection d'incendie relayé par un système d'extincteur automatique. Les portes doivent être coupe-feu et des alarmes incendie doivent être installés.
- Les cartes clients doivent être mises en coffre fort.
- Les clés ne doivent en aucun cas être accessibles au public.
- Les portes et les fenêtres doivent menu de fer forgé, être fermées à clé, en particulier en dehors des heures de bureau.
- Isoler la zone de production de la carte pour avoir seulement le personnel de service
- Les matériaux dangereux ou facilement inflammables (ceci inclut les cartons, papiers, poubelles et produits de nettoyage) ne doivent pas être stockés à proximité des éléments vitaux ou importants.
- Secours et installation électrique : onduleur et un groupe électrogène, un puits de terre pour empêcher le remontée du courant de terre, des disjoncteurs différentiels pour empêcher les défauts d'isolement
- Une climatisation redondante
- un contrôle semestriel électrique et de climatisation sont nécessaires

Nous donnons en **Annexe D** la norme TIA 942 pour les exigences de sécurité d'un Data Center

5.8 Etablir une politique de sécurité des communications : TPE, PC, Serveurs (chapitre 13 de la norme ISO 27002)

On doit établir une politique en vue d'assurer le bon fonctionnement de la sécurité des réseaux de télécommunication, des systèmes d'exploitation et des applications et établir les procédures relatives à toutes les opérations de sauvegarde et d'échange de données à travers les réseaux.

Pour l'établissement de cette politique nous recommandons :

1. Documenter des procédures opérationnelles fixant les responsabilités : mettre en place des procédures pour l'exploitation IT de la plateforme et fixer les responsabilités.
2. Gestion de la prestation de service de partie tierce : déterminer les prérogatives et les responsabilités des partenaires surtout s'il est responsable de la confection des cartes privatives
3. Planification et approbation du système : mise à jour des serveurs avec les patches de sécurité surtout s'ils sont MS-Windows et ceci à l'aide du serveur WSUS détaillé dans le chapitre suivant. Gérer le versionning des applications et l'ensemble des correctifs.
4. Expérimenter les nouvelles versions et patches de sécurité sur la plateforme de test et non sur l'environnement de production.
5. Protection contre les programmes malicieux : mettre en place une solution antivirale de type serveur, la gérer et veillez à la mise à jour de sa licence
6. Sauvegarde : mettre en place une politique et une procédure de sauvegarde pour la plateforme : base de données, applications, des OS des serveurs et configuration des équipements réseau.
7. Gestion de la sécurité réseau : mettre en place les dispositifs nécessaires pour la protection du réseau de la plateforme : Firewall, IPS et IDS
8. Manipulation des Medias : désactivé les autoruns des CD/DVD, clés USB et des disques durs externes
9. Échange d'Informations : sécuriser les communications par des certificats SSL et des liaisons avec le partenaire avec du VPN.
10. Services de commerce électronique : appliquer la norme PCI DSS mentionné dans le chapitre précédent
11. Supervision, Monitoring : mettre en place une solution de monitoring et d'agrégation de log

Nous donnons en **Annexe E** un exemple de politique et procédure de sauvegarde.

5.9 Etablir une procédure de gestions des incidents liés à la sécurité de l'information de la plateforme (chapitre 16 de la norme ISO 27002)

Un incident sur le système d'information est un ou plusieurs événements intéressant la sécurité de l'information indésirable ou inattendue présentant une probabilité forte de compromettre ou de menacer la sécurité du système d'information.

Quelle que soit l'approche, la gestion des incidents, a pour objectif la détection et le traitement des incidents. Le processus de gestion des incidents inclut en général la détection de l'incident, les analyses et diagnostics, la résolution de l'incident et/ou le rétablissement du service affecté. Un des aspects important de la gestion des incidents est le suivi (reporting) de ce processus et la capitalisation sur l'expérience acquise dans ce domaine.

La mise en œuvre d'un processus de gestion des incidents de sécurité nécessite la définition :

- Du Périmètre de sécurité : la plateforme de la carte privative
- Des objectifs (politique de gestion des incidents)
- Des mesures (processus, bonnes pratiques, etc.)
- Des moyens associés (organisation des ressources matérielles/humaines/budgétaires)

5.9.1 Le périmètre de sécurité

C'est tous le périmètre du Système d'Information : périmètre organisationnelle, procédurale, physique et technique et des périmètres particuliers notamment le system de la carte privatif pétrolière « AGILIS »

5.9.2 Les objectifs

- Etude et analyse des incidents : statistique et reporting
- Etude des solutions nécessaires et leur budget
- Soumettre ces solutions au comité de sécurité du système d'information
- Prendre les mesures nécessaires pour résoudre le problème causé par l'incident
- La capitalisation sur la résolution et le traitement des incidents de sécurité du S.I

Nous donnons en **Annexe F** un exemple de politique gestion des incidents.

5.10 Etablir une procédure de reprise informatique de la plateforme : site de secours de la carte (Chapitre 17 de la norme ISO 27002)

Un plan de reprise informatique (PRI) permet à une entreprise de se prémunir d'un arrêt informatique pouvant être préjudiciable à son activité. Il fixe un temps de reprise acceptable pour les utilisateurs. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise.

Comme toutes les entreprises ne sont pas impactées de la même manière lors d'un sinistre, implémenter un plan de reprise efficace suppose une analyse détaillée et structurée des risques liés à entreprise suivi d'un plan adapté et des moyens efficaces pour parer à ces risques.

Pour le cas de carte privative pétrolière, la SNDP va adopter pour une solution de replie basé sur le Cloud tunisien. Cette solution prend en considération les points suivant :

- l'organisation de la gouvernance en cas de sinistre : désigner les personnes à contacter et les responsables pour mettre en route le PRI.
- duplication des serveurs de la plateforme sur des serveurs virtuels avec un fournisseur de Cloud tunisien
- Gestion de la synchronisation de données entre la production et l'architecture de PRI
- la mise en place de liaison avec les TPE des stations services en cas de basculement sur la solution de repli sur le Cloud
- prévoir des connexions VPN aux administrateurs de la plateforme.
- faire un exercice annuel à blanc d'un sinistre pour expérimenter le basculement entre la plateforme chez la SNDP et la plateforme de replie sur le Cloud

5.11 Mise en place d'un SMSI pour le périmètre de la carte et certification ISO 27001 (Chapitre 19 de la norme 27002)

Pour réussir la certification ISO/IEC 27001, nous proposons la démarche suivante :

- Interview et collecte d'informations relatives au périmètre de la carte, son environnement et son système de management
- Réalisation de l'audit de certification
- Etape 1 : analyse préalable des éléments essentiels au système de management de la carte,
- Etape 2 : audit des activités et des pratiques par la conduite d'entretiens, de revue d'indicateurs, etc.
- Rédaction d'un rapport d'audit
- Prise de décision de certification
- Réalisation d'audits de surveillance annuels ou semestriels

Bénéfices :

A court terme, la certification ISO/IEC 27001 permet :

- d'identifier les menaces et dangers pesant sur système de la carte,
- de garantir la conformité aux législations nationales et internationales,
- d'accroître la confiance des clients,
- de se différencier par rapport à la concurrence,
- de responsabiliser les collaborateurs,

A moyen et long terme, elle permet de pérenniser la maîtrise des coûts liés à la sécurité.

Pour la mise en place d'un SMSI nous recommandons :

- de mettre en place le maximum d'action de sécurité de l'information selon les chapitres de la norme ISO 27002
- faire une analyse des risques concernant la sécurité du système d'information selon la norme ISO 27005
- faire un audit sécurité (conformité et technique)
- répondre aux recommandations de l'audit

Chapitre 6 : les exigences techniques de sécurité informatique de la plateforme de la carte à puce privative selon la norme ISO 27002

Introduction

Nous présentons dans ce chapitre les différentes exigences de sécurité de l'information techniques pour le périmètre de la plateforme de la carte à puce privative en se basant sur la norme ISO/CEI 27002 :2013.

6.1 Politique d'accès des clients sur le front office : PCI/DSS (chapitre 9 de la norme ISO 27002)

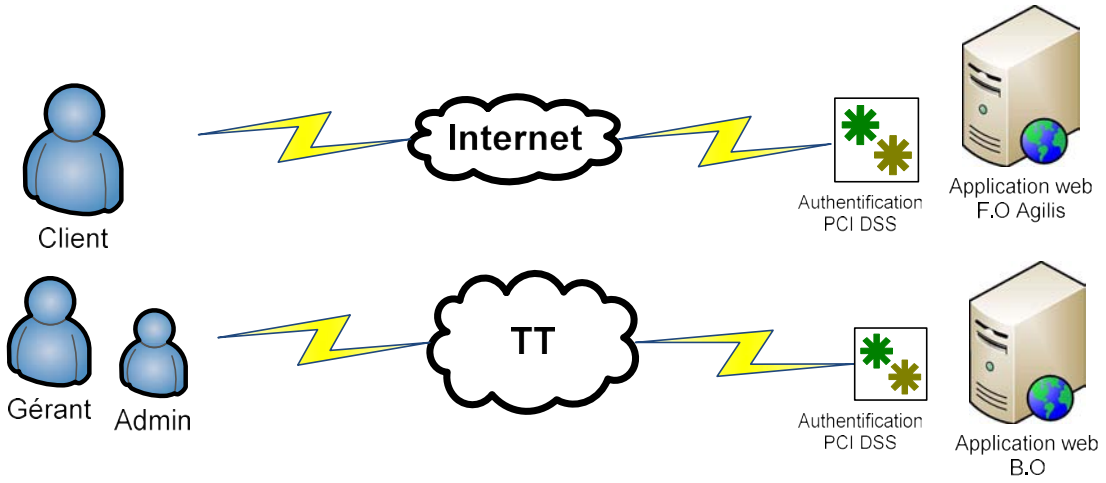


Figure 22 Authentification sur FO, BO avec PCI DSS

La Norme de sécurité de l'industrie des cartes de paiement PCI DSS (Payment Card Industry Data Security Standard) a été développée dans le but d'encourager et de renforcer la sécurité des données du titulaire de la carte ainsi que pour faciliter l'adoption de mesures de sécurité uniformes à l'échelle mondiale. La norme PCI DSS s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, acquéreurs, émetteurs et prestataires de services, ainsi qu'à toutes les autres entités qui stockent, traitent ou transmettent des données du titulaire et/ou des données d'identification sensibles.

Les 12 clauses de la norme PCI DSS sont détaillées ci-dessous.

Création et gestion d'un réseau et d'un système sécurisé	**1. installer et gérer une configuration de par feu pour protéger les donnés du titulaire** **2. ne pas utiliser les mots de passe système et autre paramètres de sécurité par défaut définis par le fournisseur**
Protection des données du titulaire	**3. Protéger les données du titulaire** **4. crypter la transmission des données du titulaire sur le**
Gestion d'un programme de gestion de vulnérabilités	**5. Utiliser des logiciels ou de logiciels anti-virus et les mettre à jour régulièrement** **6. développer et gérer des systèmes et des applications sécurisés**
Mise en œuvre de mesures de contrôle d'accès strictes	**7. restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaitre** **8. Identifier et authentifier l'accès aux composants du système** **9. Restreindre l'accès physique aux données du titulaire**
Surveillance et test réguliers des réseaux	**10. Effectuer le suivi et surveiller tout les accès aux ressources et aux données du titulaire** **11. Tester régulièrement les processus et les systèmes de sécurité**
Gestion d'un politique de sécurité des informations	**12. Maintenir une politique qui adresse les informations de sécurité pour l'ensemble du personnel**

Nous recommandons :

Dans le cadre de la mise en œuvre de mesures de contrôle d'accès strictes et parmi les bonnes pratiques concernant l'authentification des clients de la carte sur le site front office :

- le mot de passe doit être sur 8 caractères au minimum
- le mot de passe doit contenir des caractères alphabétiques, numériques et caractères spéciaux
- le mot de passe doit être changé tout les 3 mois
- le nouveau mot de passe ne doit pas être similaire aux 3 derniers mot de passe

Dans le cas du site Agilis le client reçois un code pin en SMS pour l'introduire dans un troisième champ.

[5] Nous donnons le lien vers le site de la norme PCI DSS

6.2 Le déploiement de deux certificats de chiffrement pour les deux applications web front & back office (chapitre 10 de la norme ISO 27002)

Nous présentons ici le schéma de la partie à protéger par ces certificats :

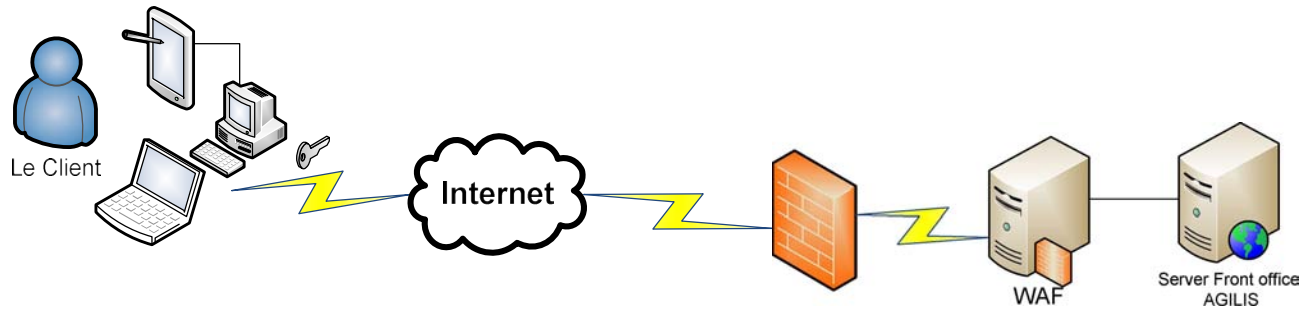


Figure 23 Deux certificats électroniques pour FO, BO

Un certificat électronique (aussi appelé certificat numérique ou certificat de clé publique) peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges.

Il est signé par un tiers de confiance dans notre cas c'est l'ANCE (Agence Nationale de Certification Electronique) qui atteste du lien entre l'identité physique et l'entité numérique (Virtuel).

Deux certificat ont été acquises l'un **serveur** pour le site web de la carte AGILIS.tn et l'autre de **domaine** pour le portail interne du backoffice qui est sous le domaine Agil.com.tn (atoil.agil.com.tn) donc ces deux sites sont accessible qu'en mode **https** ce qui permet d'établir une liaison chiffrée entre un serveur WEB et un client Web SSL.

Nous recommandons :

- Eviter que l'analyse de l'état de certificat SSL montre l'Identification de la version et le type du serveur web (IIS ou Apache).
- Désactiver le support SSL inferieur à la version 3 en raison de ses failles de sécurité.
- Activer des versions plus récentes du protocole TLS (Transport Layer Security « antécédent de SSL TLS v1.1 2006, TLSv1.2 en 2008 »)
- Consolider la sécurité du service SSL de l'application pour éviter le risque de Réalisation d'attaques de : bruts forcing, déni de service, Keylogger

[3] Nous donnons deux liens pour l'installation des certificats électroniques sur les serveurs Web (IIS7, Apache 2).

6.3 Le chiffrement des communications entre le TPE et la plateforme (Chapitre 10 de la norme ISO 27002)

Les certificats SSL (Secure Socket Layer) sont couramment utilisés pour sécuriser et authentifier les communications sur Internet et au sein des intranets d'entreprise. L'utilisation de certificats SSL sur les serveurs Web d'entreprise permet de recueillir en toute sécurité des informations sensibles transmises en ligne afin de garantir aux clients et utilisateurs la protection de leurs communications.

De nombreuses applications transmettent des données confidentielles sur des réseaux, entre différents utilisateurs finaux et entre des nœuds d'applications intermédiaires. Il peut s'agir, entre autres, d'informations d'identification utilisées pour l'authentification, de données telles que des numéros de carte de crédit ou d'informations liées à des transactions bancaires. Pour éviter la divulgation involontaire des informations et pour empêcher une modification non autorisée des données durant leur transit, le canal entre les points de terminaison de la communication doit être sécurisé. La communication sécurisée offre les deux fonctionnalités suivantes :

Confidentialité. La confidentialité consiste à garantir le caractère privé et confidentiel des données et à empêcher des personnes susceptibles d'être équipées de logiciels de surveillance du réseau de consulter ces données. La confidentialité est généralement assurée au moyen du cryptage.

Intégrité. Les canaux de communication sécurisés doivent également garantir que les données sont protégées contre toute modification accidentelle ou délibérée (malveillante) lors de leur transit.

Les technologies de communication sécurisée sont les suivantes :

- **SSL (Secure Sockets Layer) / TLS (Transport Layer Security)**. Ces technologies sont le plus souvent utilisées pour sécuriser le canal entre un navigateur et un serveur Web. Cependant, elles permettent aussi de sécuriser les communications et les messages des services Web échangés en provenance et à destination d'un serveur de base de données qui exécute Microsoft® SQL Server™ 2000.
- **IP Sec (Internet Protocol Security)**. Le protocole IP Sec offre une solution de communication sécurisée au niveau du transport et peut être utilisé pour sécuriser les données transmises entre deux ordinateurs, un serveur d'applications et un serveur de base de données, par exemple.
- **Cryptage RPC (Remote Procedure Call)**. Le protocole RPC utilisé par DCOM (Distributed COM) offre un niveau d'authentification (confidentialité des paquets) qui entraîne le cryptage de chaque paquet de données envoyé entre le client et le serveur.

Recommandation :

- la communication des transactions entre le TPE et les services web qui eux même contacte la base de données doivent être du type SSL3.
- vérifier la communication entre le TPE et la Base de données par une capture réseau lors d'une transaction de vente.
- vérifier les TPE pour qu'il embarque du SSL 3 au minimum
- s'assurer de la validité d'un certificat SSL et la renouveler auprès de l'Autorité de Certification (ANCE)

6.4 Le cryptage des login, mot de passe dans la Base de Données (Chapitre 10 de la norme ISO 27002)

Par sécurité, il est de bonne pratique de crypter les mots de passe stockés dans une table de la base de données. Ainsi, dans le cas ou une personne malveillante arriverait à consulter votre table, elle ne pourrait pas voir le mot de passe, mais une suite de caractères dépourvue de sens.

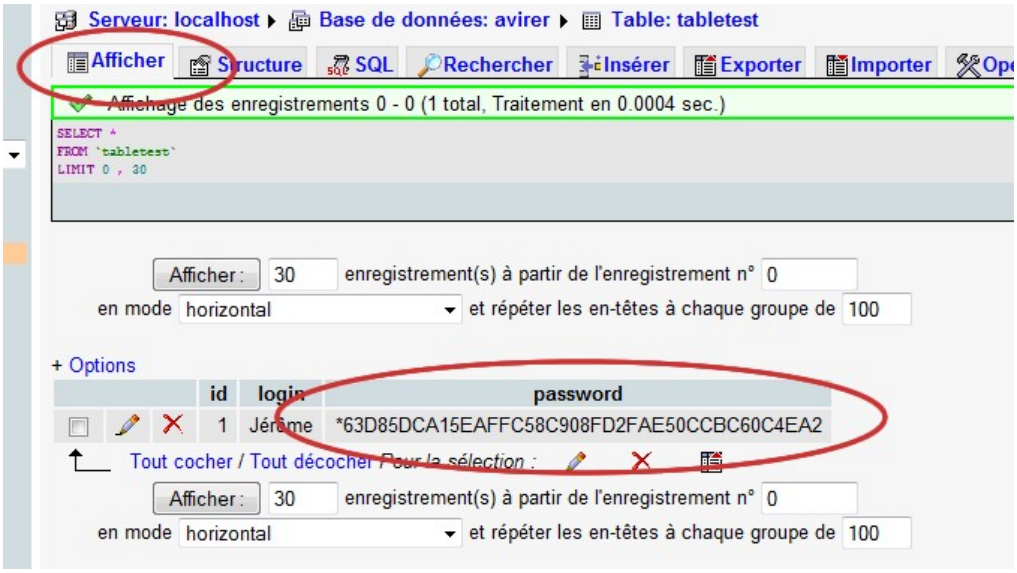


Figure 24 Illustration de cryptage des mots de passe dans une B.D

Nous recommandons :

[6] On pourra adopter des techniques pour crypter les mots de passe dans une base de données et nous donnons ce lien qui explique comment crypter les mots de passe dans une base de données

6.5 Séparation de l'environnement de test et de production (Chapitre 12.1.4 de la norme ISO 27002)

En informatique, un environnement désigne, pour une application, l'ensemble des matériels et des logiciels système, dont le système d'exploitation, sur lesquels sont exécutés les programmes de l'application.

On précise dans ce qui suit les types environnements par ordre d'apparition dans le cycle de vie d'une application informatique :

- L'environnement de développement, sur lequel sont développés les programmes de l'application,
- L'environnement de qualification, sur lequel sont testés les programmes de l'application,
- L'environnement de formation, sur lequel les utilisateurs sont formés à l'application,
- L'environnement de production, sur lequel sont exécutés les programmes opérationnellement.

Un environnement est le plus souvent implanté sur un seul serveur, mais il peut y avoir des exceptions (cas de l'informatique distribuée). Il peut y avoir plusieurs environnements hébergés sur un même serveur (l'environnement de qualification et l'environnement de formation par exemple).

L'environnement de production nécessite tout particulièrement une surveillance continue, car tout dysfonctionnement peut interrompre l'utilisation opérationnelle de l'application, ce qui peut avoir des conséquences graves.

Nous recommandons :

- Mettre en place un serveur de versionning pour faire les différences entre les versions des applications Front & Back office
- La duplication des serveurs de la plateforme Front & Back office pour ainsi créer un environnement de test des modifications faites sur les applications et ne pas perturber la production.
- la formation des utilisateurs se feront sur ces serveurs de test
- les patchs Windows seront testés aussi sur cet environnement

6.6 Mettre en place une solution antivirale (Chapitre 12.2 de la norme ISO 27002)

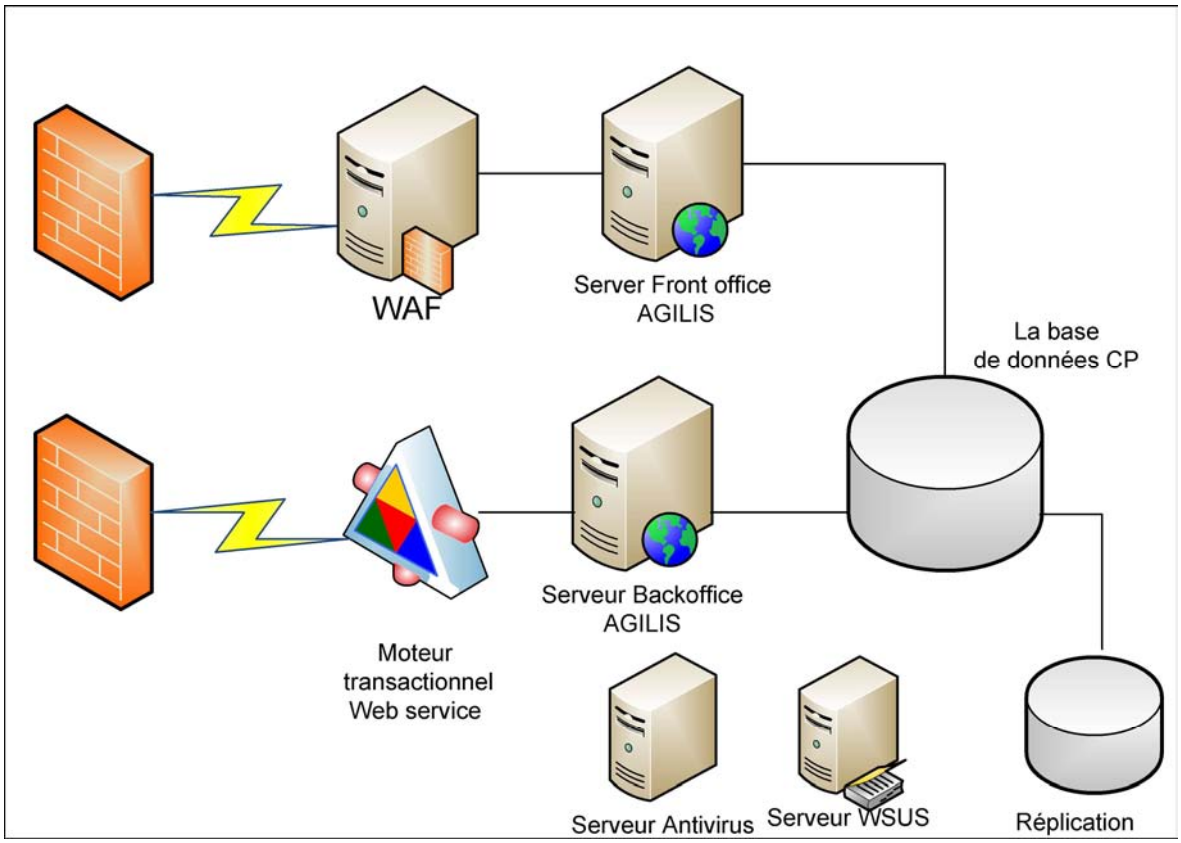


Figure 25 Mise en place d'un serveur antivirus & WSUS

Un antivirus est un logiciel conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

Fonctionnement d'un antivirus

L'antivirus analyse les fichiers entrants (fichiers téléchargés ou courriers électroniques) et, périodiquement, la mémoire vive de l'ordinateur et les périphériques de stockage comme les disques durs, internes ou externes, les clés USB et les cartes à mémoire Flash.

La détection d'un logiciel malveillant peut reposer sur trois méthodes :

- reconnaissance d'un code déjà connu (appelé signature) et mémorisé dans une base de données ;
- analyse du comportement d'un logiciel (méthode heuristique) ;
- reconnaissance d'un code typique d'un virus.

Nous recommandons :

- Une solution antivirale centralisé de type serveur
- Mettre à jour la base de signatures du serveur (en générale la MAJ est automatique)
- Le déploiement des signatures vers les clients antivirus se fera de préférence pendant les heures de travail
- L'une des options qui doivent exister dans un antivirus la fonction appelé : Outbreak Prevention qui ralentie une épidémie virale
- Mettre le serveur antivirus derrières un Firewall
- Veiller à mettre à jour la licence de l'antivirus
- Désactiver les autoruns des clés USB, CD/DVD et Disque dur externe
- configurer un reporting sur l'état global du Park serveur de la plateforme et des potes de travail infectés

6.7 Mise en place d'une solution technique de sauvegarde & restauration (Chapitre 12.3 de la norme ISO 27002)

La perte de données stockées sur l'un des serveurs de la plateforme carte privative peut avoir des conséquences dramatiques pour l'entreprise. Vols, sinistres, défaillance informatique, piratage : l'origine des pertes est multiple. C'est pourquoi les solutions de sauvegardes de données sont indispensables.

Installer un serveur d'entreprise (utile au-delà de 5 PC) limite considérablement les risques de pertes de fichiers. Le serveur est doté d'un lecteur de bandes magnétiques qui effectue une sauvegarde quotidienne.

Nous recommandons pour le choix d'une solution de sauvegarde de prendre en considération les éléments suivants :

- Un environnement avec plusieurs systèmes d'exploitation (Linux, AS 400, Novell, Windows…)
- Exploitant des bases de données complexes et volumineuses (SQL Server, Oracle…)
- Protéger les applications critiques (Back et front office, ERP, CRM, emails...)
- Un environnement hétérogène (VMware, Hyper-V, Citrix…)
- la sauvegarde des configurations des différents équipements (Image des OS serveurs, configuration des équipements réseau et sécurité

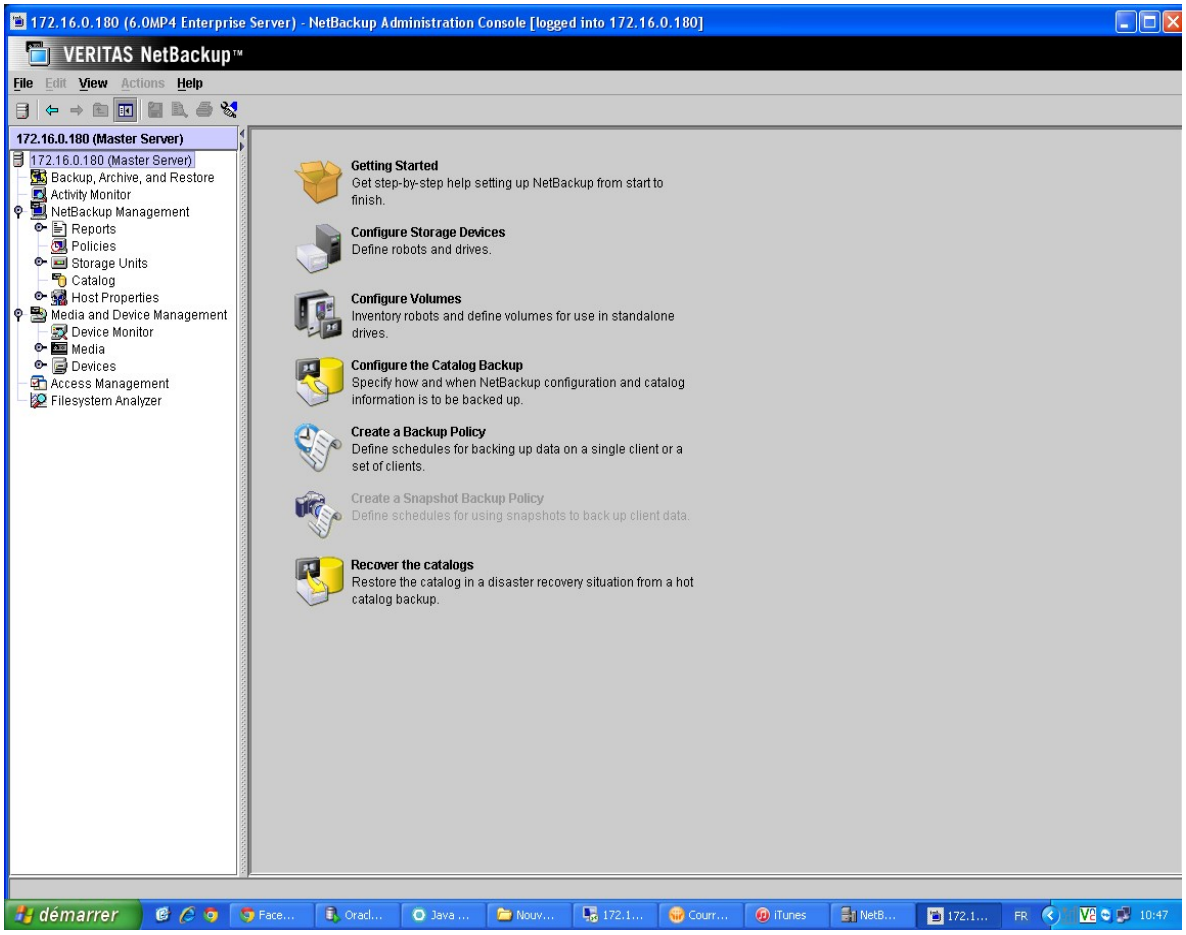


Figure 26 Console de l'application de backup

La SNDP a fait le choix d'une solution de sauvegarde de type serveur centralisé VERITAS NetBackup

6.8 Mise en place d'un outil de monitoring (Chapitre 12.4 de la norme ISO 27002)

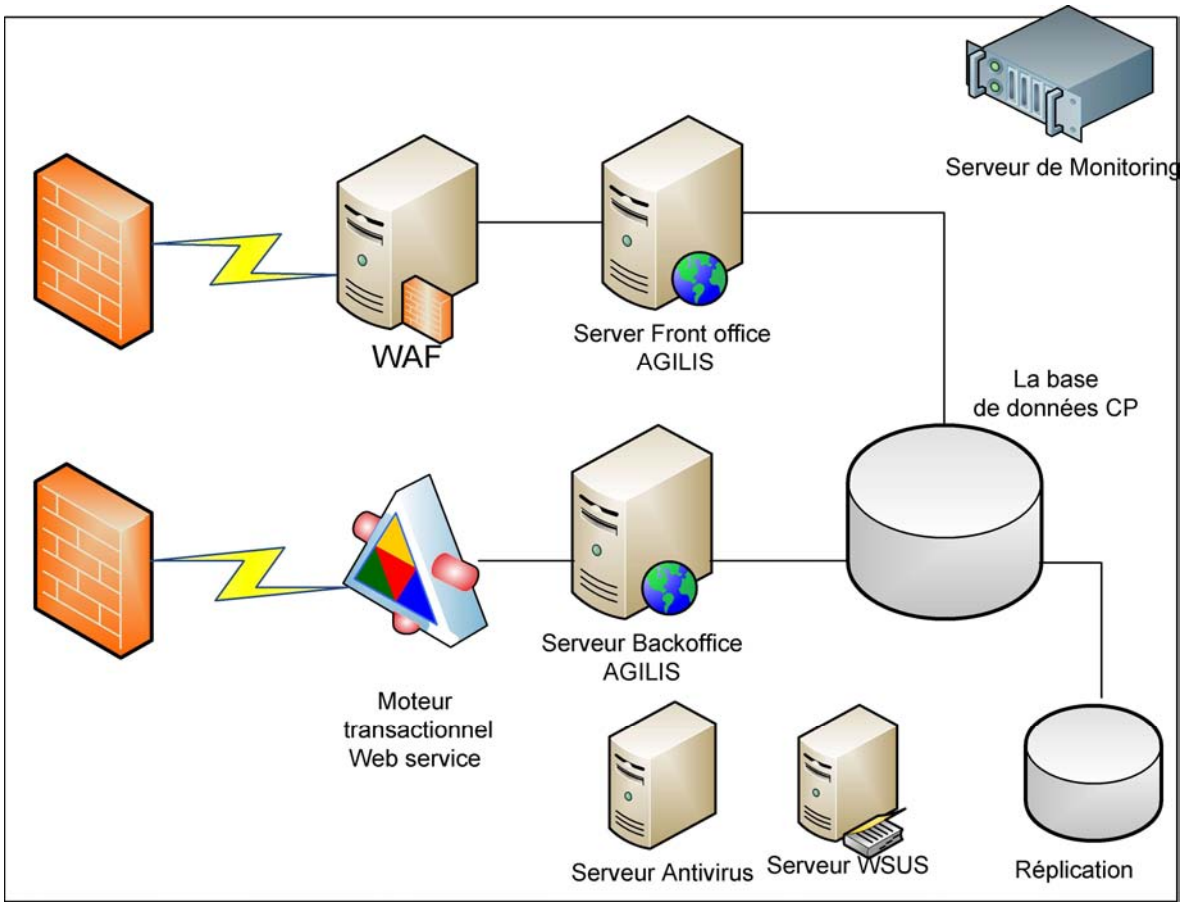


Figure 27 Mise en place d'un serveur de monitoring

La supervision vise à faire remonter les informations cachées du système d'information telles que le taux d'occupation des serveurs, la congestion du réseau ou la disponibilité des applications distantes. Ces données s'accompagnent souvent d'une démarche de garantie du niveau de service. La supervision est alors au service d'une gestion globale des performances, elle-même au service des clients du système d'information.

La supervision fournit également la direction informatique en indicateurs objectifs, remontant les données qualitatives ou quantitatives relatives à la gestion des ressources informatiques. Ces données permettent également de mesurer les effets de l'application de nouvelles mesures comme le changement d'un logiciel, la priorisation de flux IP ou l'optimisation de code. Enfin, dans le cadre de contrats de prestation de services, la supervision s'avère indispensable pour mesurer l'efficacité du prestataire et remonter d'éventuels problèmes.

La supervision est réalisé à plusieurs niveaux d'un parc de machines : Au niveau interconnexions (Réseau), au niveau de la machine elle-même (Système) et au niveau des services offerts par cette machine (Applications).

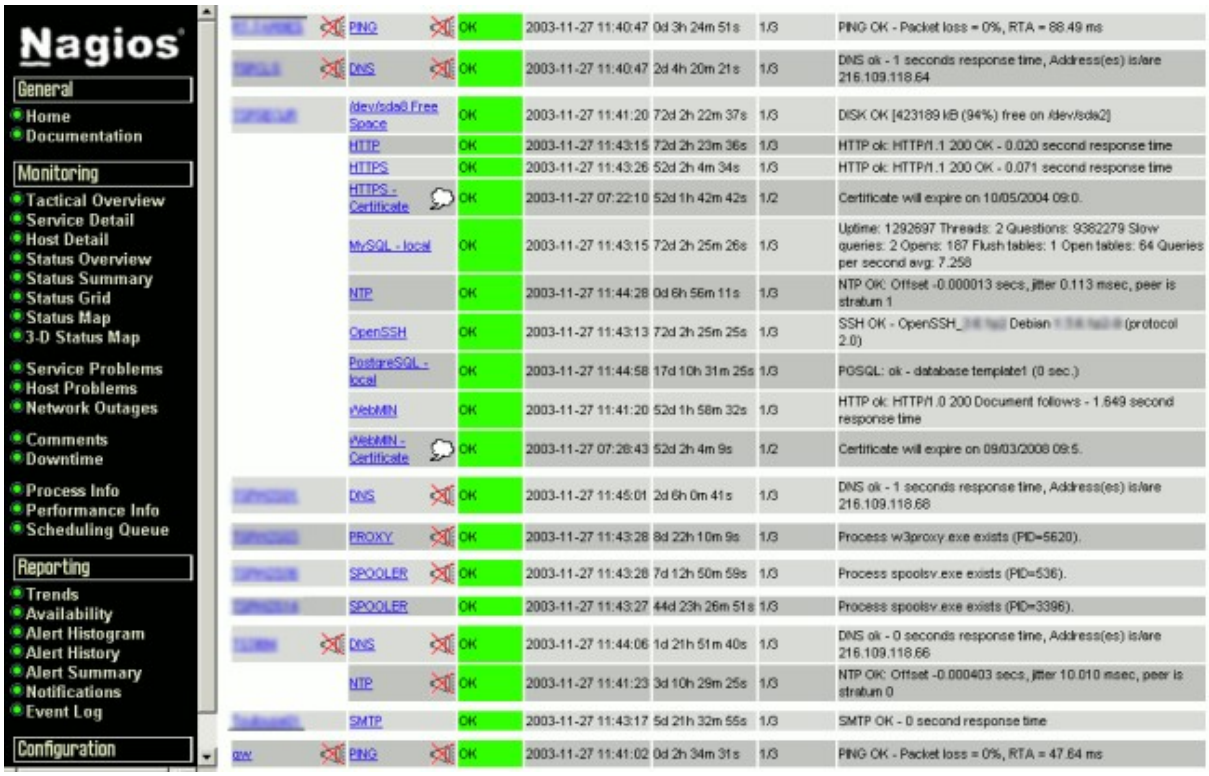


Figure 28 Application Open source Nagios de supervision réseau

La SNDP a fait un choix de logiciel open source Nagios pour la surveillance du réseau de la plateforme de carte à puce

6.9 Mettre en place un serveur des mises à jour de sécurité Microsoft WSUS (Chapitre 12.6.1 de la norme ISO 27002)

Windows Server Update Services (WSUS) permet aux administrateurs des technologies de l'information de déployer les dernières mises à jour de produits Microsoft sur les ordinateurs qui exécutent le système d'exploitation Windows. En utilisant WSUS, les administrateurs peuvent gérer entièrement la distribution des mises à jour publiées via Microsoft Update sur les ordinateurs de leur réseau.

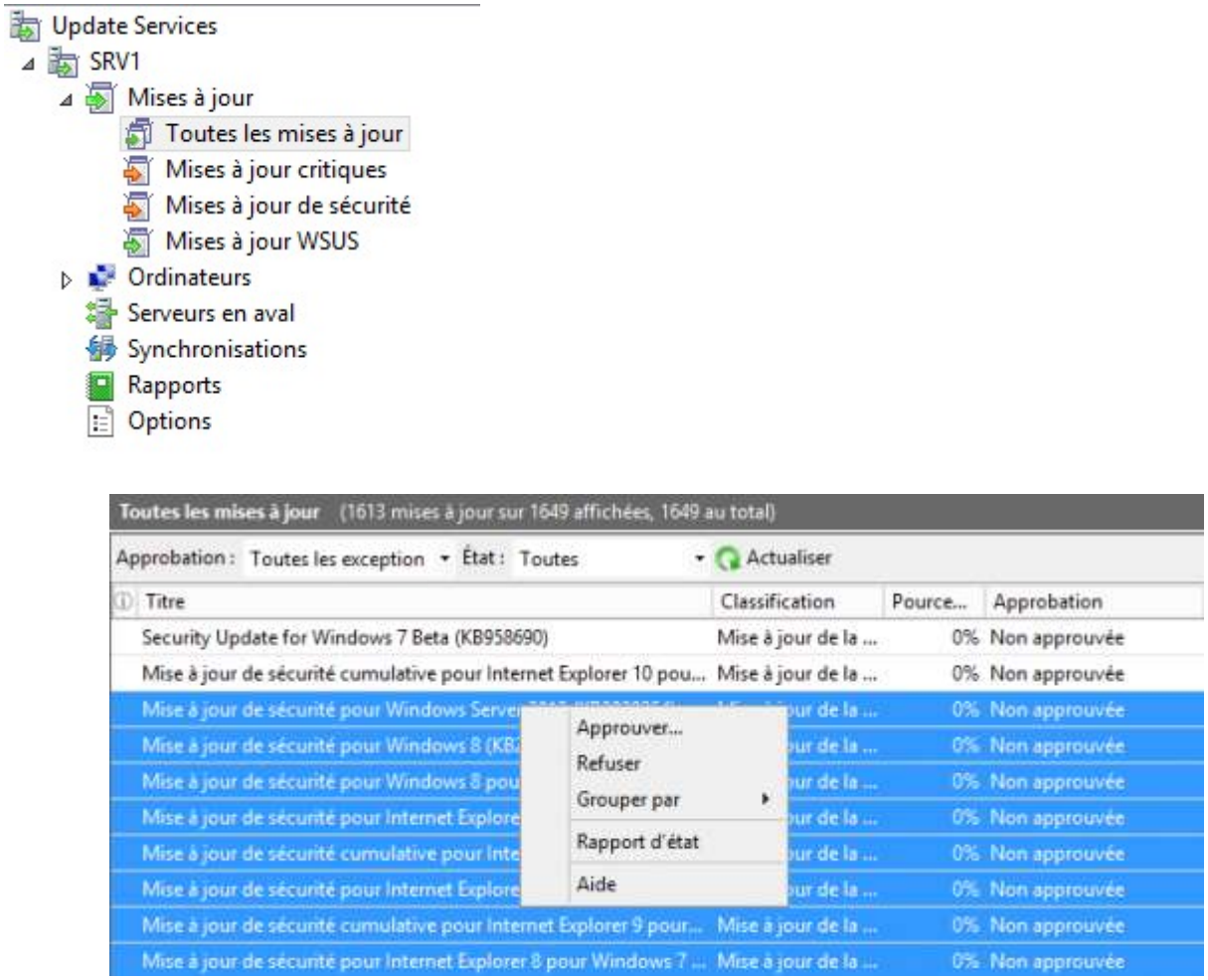


Figure 29 serveur WSUS

Nous recommandons :

- la distribution des mises à jour vers les clients du serveur WSUS par un GPO qui se lance pendant les heures de travail (à 16 h par exemple)
- les mises à jour critiques et de sécurité doivent être approuvées automatiquement
- la synchronisation entre le serveur WSUS et les serveurs de Microsoft doivent se faire la nuit
  Nous présentons en Netographie les liens concernant le serveur WSUS **[8]**

6.10 Établissement d'une matrice de flux (chapitre 13.1.3 de la norme ISO 27002)

Les échanges de données ou de messages entre les acteurs du système d'information sont résumés dans une matrice ou un diagramme des flux (aussi appelé modèle conceptuel de communications).

On élimine notamment les flux internes informant, qui ne font que transférer une information sans entraîner le déclenchement d'un traitement et nous présentons ci-après une matrice de flux d'une entreprise :

	**VLAN Compus**	**VLAN Serveur**	**Firewall IPS Proxy**	**Internet**	**Accès ATI**	**Accès TTN**	**Accès Branches**
VLAN Compus	Oui	Oui	Administrateur	Oui	Administrateur & web master	Non	Oui
VLAN Serveur	Oui		Non	Oui	S24	Serveur TTN	Oui
Firewall/Ips Proxy	Oui	Oui		Oui	Oui	Oui	Oui
Internet	Non	Non	Non		Non	Non	Non
Accès ATI	Non	S24	Non	Non		Non	Non
Accès TTN	Non	Serveur TTN	Non	Non	Non		Oui
Accès Branches (dépôts)	Oui	Oui	Non	Oui	Web master	Oui	

Figure 30 Exemple de matrice de flux

Nous recommandons :

- S'inspirer de ce model de tableau pour la représentation d'une matrice de flux qui définit les différents compartiments du système d'information et ces interactions dans le périmètre de la carte.
- On pourra aussi décliner ces relations sous forme de règles sur les firewalls de la plateforme carte privative
- il faut toujours mettre à jour cette matrice.

6.11 La mise en place d'un Web Application Firewall (WAF) (Chapitre 14.1.3 de la norme ISO 27002)

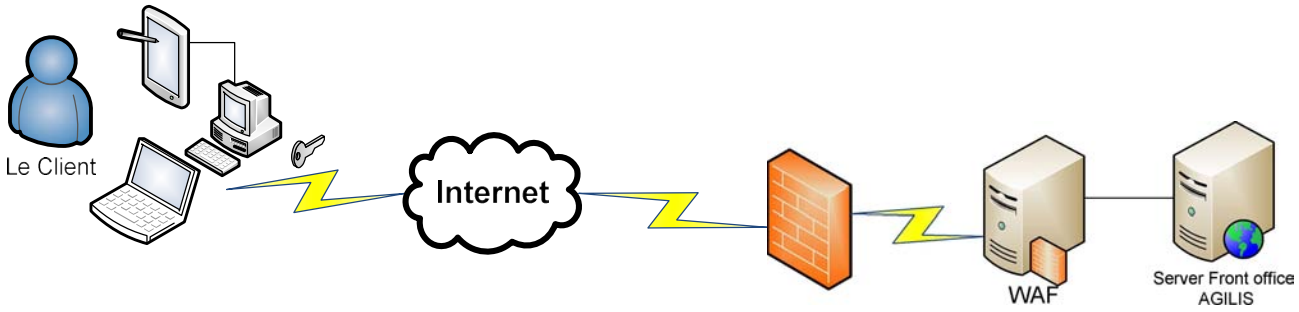


Figure 31 Mise en place d'un WAF

Un WAF protège les serveurs web contre le trafic malicieux et bloque les tentatives de compromission du système, c'est un dispositif matériel ou logiciel qui prévient contre les attaques mentionnées ci-après : SQL injection et Cross Site Scripting, cookies posoning,

Les fonctionnalités majeures d'un WAF :

Prévention :

- Cartographie des applications et identification des ressources
- Evaluation des risques potentiels

Protection :

- Interception et filtrage du trafic applicatif
- Identification des menaces et détection des comportements anormaux
- Génération automatisée de politiques de sécurité granulaire

Investigation :

- Compréhension de l'historique des attaques
- Possibilité de rejeux du trafic

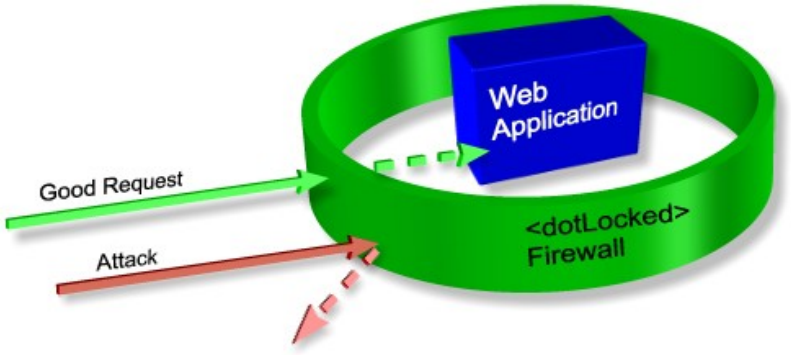


Figure 32 Le Fonctionnement d'un WAF

Nous recommandons :

- De mettre en place des WAF open source et on donnera les liens de leurs site **[7]**
- l'administrateur IT de la plateforme doit suivre quotidiennement la console principale du WAF
- Configurer une remontée d'alerte par mail peut être configuré pour des attaques récurrentes
- Configurer un reporting mensuelle doit être configuré

6.12 Eliminer les vulnérabilités des applications web : SQL injection et XSS cross scripting (Chapitre 14.1.3 de la norme ISO 27002)

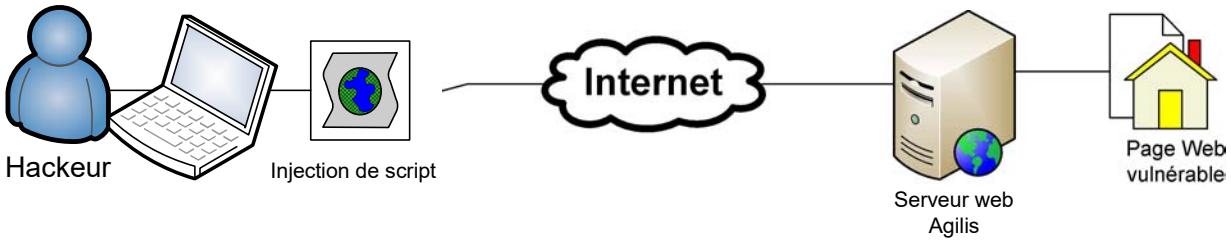


Figure 33 Schéma d'une attaque par injection SQL

SQL injection:

Les vulnérabilités de type SQL injection sont très répondues sur le web, elles sont exploitable très facilement et peuvent avoir des répercutions désastreuses sur le site web, la base de donnée et même le serveur lui même.

Le principe de cette attaque consiste à détourner l'exécution d'un script en modifiant une requête SQL lancer par ce script afin de voler des données, affiché les mots de passe du site, effacer une base de donnée ou contourner une authentification.

Cross Site Scripting ou XSS:

La faille XSS, a l'origine CSS (Cross Site Scripting) changé pour ne pas confondre avec le CSS des feuilles de style (Cascading Style Sheet), est un type de faille de sécurité des sites Web, que l'on trouve dans les applications Web mal sécurisé.

Le principe de cette faille est d'injecter un code malveillant en langage de script dans un site web vulnérable, par exemple en déposant un message dans un forum qui redirige l'internaute vers un faux site (phishing) ou qui vole des informations (cookies).

La faille XSS permet d'exécuter des scripts du coté client. Ceci signifie que vous ne pouvez exécuter que du JAVASCRIPT, HTML et d'autres langages qui ne vont s'exécuter que chez celui qui lance le script et pas sur le serveur directement.

Pour éviter cette faille il y a plusieurs techniques :

- Utiliser la fonction htmlspecialchars(), il convertit les caractères spéciaux en entités HTML.
- Utiliser la fonction htmlentities() qui est identique à htmlspecialchars() sauf qu'elle filtre tout les caractères équivalents au codage html ou javascript.
- Utiliser strip_tags(), cette fonction supprime toutes les balises.

[4] Nous donnons des liens pour deux scripts PHP pour se prémunir de ces deux attaques.

6.13 Mise en place d'un plan de reprise informatique (Chapitre 17 de la norme ISO 27002)

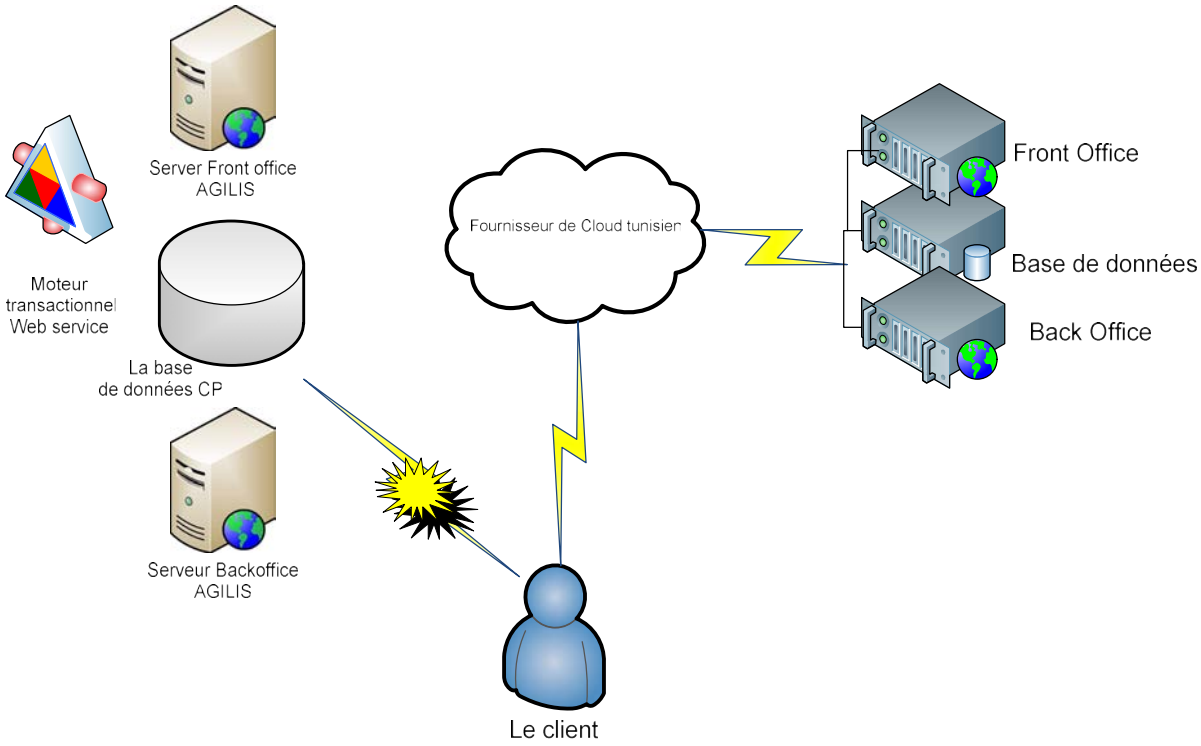


Figure 34 Plan de Reprise informatique de la plateforme

Un plan de reprise informatique (PRI) permet à une entreprise de se prémunir d'un arrêt informatique pouvant être préjudiciable à son activité. Il fixe un temps de reprise acceptable pour les utilisateurs. Comme toutes les entreprises ne sont pas impactées de la même manière lors d'un sinistre, implémenter un plan de reprise efficace suppose une analyse détaillée et structurée des risques liés à l'entreprise suivi d'un plan adapté et des moyens efficaces pour parer à ces risques.

Un point capital de la mise en place d'un PRI concerne la gouvernance du risque. "Qui fait quoi en cas de problème ? Quelle est la responsabilité définie de chacun ?

Les personnes seront sélectionnées dans l'entreprise au préalable et cela permettra généralement un gain de temps appréciable en cas de problème.

Chaque module applicatif doit être évalué pour en déterminer sa criticité en cas de crise, et le traitement dont il doit faire l'objet pour le préparer aux incidents. On procède au mapping des applications, on descend au niveau des bases de données et des systèmes d'exploitation.

Enfin, l'inventaire des applications et des environnements applicatifs ouvrira sur un travail de définition de la criticité de ceux-ci, et du besoin de sauvegarde et de restauration. Il faut prioriser en fonction de ce qui est plus ou moins critique pour le business de l'entreprise.

Nous recommandons :

- Louer des serveurs identiques aux serveurs de la plateforme dans le Cloud National : Tunisie Télécom, Gnet, Ooredoo.
- préparer les scripts de l'alimentation des bases en temps réel
- faite les tests nécessaires de continuité

Conclusion

La carte à puce fait partie intégrante de notre vie quotidienne. Paiement, téléphonie, sécurité, bancaire, TV satellite, elle est omniprésente dans notre environnement. Pas moins de deux milliards de cartes à puce circulent actuellement à la surface du globe. Ces petites cartes plastifiées mesurant quelques dizaines de millimètres renferment tout un système électronique sophistiqué, capable d'emmagasiner et de traiter un nombre impressionnant de données quand il rentre en interaction avec une plateforme constituée d'applications, de serveurs et de base de données. Pour sécuriser ce périmètre, de la carte à puce, il faut mettre en place un certains nombre de mesures de sécurité informatiques organisationnelles et techniques mais encore beaucoup de bon sens.

Parmi les objectifs escomptés par ce travail c'est de partager et essayer d'aider tout organisme désirant de lancer sa carte à puce privative car elle offre la sécurité, la proximité et la souplesse de paiement que le client et l'entreprise cherchent. J'aurais souhaité développer beaucoup plus d'autre aspect de management de la carte à puce comme les aspects fonctionnels de ces applications Front et Back office, le management de changement inhérent à sa production et biens d'autres facettes seulement chaque aspect pourra être traité comme étant un sujet de mémoire de mastère à part entière.

Bibliographie

- Emmanuel Vinatier - HACKING édition Micro Application
  Code 4343 ISBN 2-7429-3343-3 : L'auteur énumère tous les d'attaques des pirates expliquées par la pratique et les méthodes pour mieux les contrer

- Danièle Linhart – La Modernisation des Entreprises
  Code ISBN : 9782707166661
  Édition : La Découverte

Netographie

[1] source : http://www.cartesapuce.fr

[2] Un lien pour l'élaboration d'un manuel de procédure

http://www.memoireonline.com/10/12/6356/elaboration-de-la-procedure-de-gestion-de-cartes-Cas-de-la-Banque-Atlantique-Cte-dIvoire.html

[3] Un tutorial pour l'installation de votre certificat sur IIS7 en français

https://www.globalsign.fr/assistance-technique/iis7/installer-certificat-ssl.html

[3] Un excellent tutorial pour l'installation de votre certificat sur le serveur Apache en français

https://www.globalsign.fr/assistance-technique/apache/installer-certificat-ssl.html

[4] SQL injection:

http://sql.sh/1025-securite-injection-sql

[4] Cross Site Scripting ou XSS :

http://www.funinformatique.com/faille-xss-comment-lexploiter-et-sen-proteger/

http://blog.clever-age.com/fr/2014/02/10/owasp-xss-cross-site-scripting/

[5] Le lien vers le site officiel de la norme PCI DSS.

https://fr.pcisecuritystandards.org/minisite/en/

[6] Un lien pour les techniques de cryptage des mots de passe dans une base de données

http://www.webmaster-freelance.com/2010/10/crypter-les-mots-de-passe-dans-une-base-de-donnees/

[7] Deux liens pour des WAF open source.

https://www.modsecurity.org/
https://www.ironbee.com/

[8] Deux liens concernant le serveur WSUS

https://technet.microsoft.com/fr-fr/technet-techcenter-windows-server-update-services.aspx
http://www.it-connect.fr/cours-tutoriels/administration-systemes/windows-server/wsus/

Annexes

ANNEXE A : Charte de sécurité informatique

Charte du bon usage des moyens Informatiques, de la messagerie et de l'internet à la SNDP

Article 1 Objet

La présente charte de sécurité informatique a pour objet de définir les conditions d'utilisation des moyens informatiques et qui a pour but de faire prendre conscience du problème de la sécurité et de responsabiliser les usagers de l'informatique au sein de la **SNDP**.
Les règles et obligations définies par cette charte s'appliquent à tous les utilisateurs ou administrateur des moyens informatiques de la **SNDP**.
Une personne est considérée comme un utilisateur, quel que soit son statut, à partir du moment où elle est appelée à utiliser des ressources informatiques au sein de la **SNDP**.

Article 2 Règle de non Divulgation - Responsabilité de l'Utilisateur.

L'accès aux ressources du réseau interne **SNDP** est soumis à la délivrance par l'administrateur du réseau & sécurité d'un nom d'utilisateur auquel l'utilisateur associe un mot de passe (Domaine local de la **SNDP**). Tout couple login/mot de passe est personnel et incessible. Il ne doit en aucun cas être divulgué à un tiers, même pour un prêt temporaire. Il est à rappeler que tout utilisateur est responsable de la pérennité de ses fichiers et de l'intégrité de son espace de travail.

Article 3 Engagement de Vigilance.

Tout utilisateur s'engage à signaler au **RSSI** ou à l'administrateur toute tentative de violation de son compte dès qu'il en aura connaissance.
L'abandon du poste de travail sans "fermer la session" constitue une négligence de la part de son auteur et peut entraîner sa responsabilité en cas d'usage frauduleux; il convient donc que tout utilisateur ferme, dès qu'il cesse de travailler, la session qu'il avait ouverte.
Cette pratique constitue une mesure de sécurité d'accès pour l'utilisateur et évitera à autrui d'utiliser votre poste de travail.

Article 4 Règles d'Utilisation, de Sécurité et de Bon Usage

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès (LAN interne de la SNDP et/ou accès WAN ou Internet). Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de son entité.
L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

En particulier:

1. Chaque utilisateur doit :
   - Appliquer les recommandations de sécurité de la Direction et/ou du Service de la **SNDP** à laquelle il appartient,
   - Assurer la protection de ses informations , il est aussi responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition (procédures de sauvegarde interne),
   - Signaler toute tentative de violation de cette charte et, de façon générale, toute anomalie qu'il peut constater,
   - Suivre les règles en vigueur au sein de l'entité pour toute installation de logiciel, par défaut aucune installation n'est autorisée,
   - Choisir des mots de passe sûrs, les garder secrets et ne les communiquer, en aucun cas, à des tiers,
   - S'engager à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage,
   - En cas d'absence ou de congé, désigner un intérim reconnu par son chef hiérarchique. Cette désignation doit être communiquée par note de service interne, notamment aux administrateurs des systèmes. L'intérimaire aura alors, si besoin est, les mêmes droits et devoirs que celui qu'il remplace et il lui sera attribué par l'administrateur réseau et responsable de l'application un nouveau compte temporaire qui expirera à la fin de la période fixée par la note de service.
2. Chaque utilisateur ne doit pas:
   - Utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité,
   - Tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier le ou les fichiers contenant des informations confidentielles ou d'identification,
   - Quitter son poste de travail ni ceux en libre-service sans se déconnecter en laissant des ressources ou services accessibles.
   - Utiliser des supports amovibles (clé USB, disque dur externe, Clé 3G) sans autorisation préalable. (l'utilisation des clés 3G est strictement interdit dans les réseaux informatiques de la SNDP, les cas particuliers seront traités au cas par cas)
3. De plus,
   - Nul ne peut céder ses droits à autrui. Les autorisations d'accès aux ressources informatiques du SI-SNDP sont strictement personnelles, et ne peuvent être cédées, temporairement ou définitivement, à quiconque (collègues, amis et membres de la famille inclus) quelle que soit la confiance vis à vis de ces personnes.
   - Nul ne peut modifier un équipement, tant du point de vue matériel que logiciel système, ni connecter une machine au réseau local sans l'accord explicite de l'administrateur réseau et le RSSI-SNDP.

- Nul ne peut connecter un équipement qui n'est pas propriété de la SNDP sur le réseau local de la SNDP sans l'accord des responsables par Département/Direction et/ou administrateurs réseau et le RSSI-SNDP, qui a autorité pour requérir alors les moyens de l'administrer sans restriction. La présente charte s'applique alors à cet équipement, et son propriétaire en devient utilisateur au titre de la charte.

Article 5 Conditions de Confidentialité

L'accès aux informations conservées sur les systèmes informatiques utilisables doit être limité aux fichiers personnels et publics (sur serveur de fichiers **SNDP**). En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Article 6 Accès aux Ressources Partagées

Certaines ressources (serveurs de données et d'application, serveurs de sécurité, équipements d'interconnexion réseau, etc.…) accessibles par le réseau sont privées même si elles ne sont pas physiquement protégées. Toute utilisation de ces ressources nécessite une autorisation du propriétaire de la ressource.

Article 7 Respect de la ¨Législation Concernant les Logiciels

Il est strictement interdit à l'utilisateur d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit. Les copies de sauvegarde autorisées par la loi ne peuvent être effectuées que par la personne habilitée à cette fin qui est un responsable informatique.

Article 8 Usage des Services Internet

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect des principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

En particulier, il ne doit pas:

- Se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède,
- Usurper l'identité d'une autre personne,
- Intercepter des communications entre tiers,
- Utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,
- Déposer des documents sur un serveur sauf si celui-ci le permet et sans y être autorisé par les responsables habilités.
- Se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités.

De plus,

- Il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions….

- Il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste ….
- Il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à la SNDP.

Article 9

Droits et Devoirs Spécifiques des Administrateurs Systèmes et/ou Réseaux

Sur de nombreux systèmes (Messagerie, serveurs de données et d'applications, serveurs de fichiers), l'administrateur et/ou certains responsables hiérarchiques au sein de l'organisation de la **SNDP** possèdent techniquement des pouvoirs étendus, ils ont de ce fait des devoirs importants, en particulier celui de ne pas abuser de ces pouvoirs. L'administrateur est responsable de la sécurité de la machine et/ou du réseau dont il a la charge. Le **RSSI** au sein de la **SNDP** appartient implicitement à cette catégorie.

Tout administrateur Système et/ou Réseau au sein de la SNDP a le droit :

- D'être informé des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible,
- D'accéder, sur les systèmes qu'il administre, aux informations privatives à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations, en s'efforçant tant que la situation ne l'exige pas de ne pas les altérer,
- D'établir des procédures de surveillance de toutes les tâches exécutées sur la machine, afin de déceler les violations ou les tentatives de violation de la présente charte, sous l'autorité de son responsable fonctionnel et en relation avec le correspondant sécurité informatique,
- De prendre des mesures conservatoires si l'urgence l'impose, sans préjuger des sanctions.

Tout administrateur système, base de données, réseau et applicatif a le devoir:

- D'informer les utilisateurs sur l'étendue des pouvoirs dont lui-même dispose techniquement de par sa fonction,
- D'informer les utilisateurs et les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître, aidé par le correspondant sécurité, les règles de sécurité à respecter,
- De respecter les règles générales d'accès au réseau local et aux réseaux externes accessibles depuis le réseau local de la SNDP (cas de la navigation Internet, accès aux dépôts distants, accès CNI),
- De respecter les règles de confidentialité, en limitant l'accès à l'information confidentielle au strict nécessaire et en respectant un "secret professionnel" sur ce point,
- De respecter, s'il est lui-même utilisateur du système, les règles qu'il est amené à imposer aux autres utilisateurs,

- De configurer et administrer le système dans le sens d'une meilleure sécurité, dans l'intérêt des utilisateurs,
- D'informer le RSSI de la SNDP de la mise en œuvre de procédures exceptionnelles de surveillance ou d'investigations,
- D'informer immédiatement son responsable hiérarchique et le RSSI de toute tentative (fructueuse ou non) d'intrusion sur son système ou de tout comportement dangereux d'un utilisateur,
- De coopérer avec le RSSI de la SNDP en cas d'incident de sécurité impliquant une machine qu'il administre.

Article 10 Sanctions Prévues.

Suivant la gravité de l'infraction à cette charte, la Direction Générale de la **SNDP** pourra engager toute sanction qu'elle jugera nécessaire.

Ces sanctions peuvent aller du simple avertissement jusqu'à des sanctions prononcées par le Conseil de Discipline.

Article 11 Engagement Personnel.

Tout utilisateur doit se conformer à la charte ci-dessus et pour ce faire, signe l'engagement suivant:

Je soussigné : …….. , Déclare avoir pris connaissance de la présente Charte de Sécurité Informatique et m'engage à la respecter.

……, le.....
Lu et approuvé *(manuscrit)*
Signature

ANNEXE B Un modèle de présentation d'une procédure de la carte privative

Libellé	SNDP-AGIL	Projet Carte à Puce
I / La carte pétrolière AGILIS, généralités description et types		
1. Généralités	Le présent manuel de procédures est une documentation descriptive des différentes étapes (processus) de traitement et de gestion de la carte pétrolière AGILIS. Il est destiné à tout acteur de l'entreprise.	
2. Description	La carte pétrolière AGILIS est une carte en plastique souple, d'une forme rectangulaire et d'une épaisseur d' 1 mm. Elle est dotée d'une puce qui porte un circuit intégré capable de mémoriser de façon sécurisée une série d'informations.	

3. Types	Deux types de cartes pétrolières sont disponibles à la SNDP – AGIL : **La carte pétrolière client** La carte client **prépayée** qui est pré chargée d'un certain montant ou d'un certain litrage. Elle est facturée avant consommation. Le paiement est immédiat. La carte client **pré-facturée** qui est pré-chargée en litrage valorisé, facturée le jour du chargement et payée à échéance. La carte client **post-payée,** dont le paiement et la facturation se ferra en post-consommation. Cette carte est soit à crédit soit à solde cumulable. Carte **anonyme** qui, comme son nom l'indique ne sera pas personnalisée. Elle sera prépayée. Le chargement de cette carte se fera lors du paiement avec un montant minimum de 50 dinars. **Carte pétrolière gérant** pour la consultation et le paiement des livraisons

ANNEXE C Modèle de fiches inventaire de la plateforme

Fiche Inventaire – Actif type application

Désignation :
Description fonctionnelle :
Responsable :
Bénéficiaire :
Développement : ☐terne Acq☐

INFORMATIONS :

Criticité	Haute	
	Moyenne	
	Basse	
Disponibilité		
Nature		
Environnement		
Installation		
Utilisateurs finaux / Nb users supportés		
Technologie		
Canal d'accès		
Délai maximum d'interruption admissible pour l'application (DMIA)		
interactivité avec d'autres applications		
Contrat / Maintenance Applicative		

INFORMATIONS DE GESTION :

Mode d'administration		
Documentation	Procédure Document de Politique d'autorisation / Gestion des accès utilisateurs Procédure de sauvegarde des fichiers (fichiers d'installation, code source, fichiers de configuration)	
	Manuel	
	Autre	

INTERACTION AVEC D'AUTRES Applications :

Application	Adresse IP	Protocole/Port	Moyen de communication

Fiche Inventaire – Actif type Fiche équipement sécurité réseau

Désignation :
Responsable :
Catégorie : S☐vice publique Serv☐e Interne

INFORMATIONS RESEAU :

Criticité	Haute	
	Moyenne	
	Basse	
Disponibilité		
Emplacement réseau	LAN	
	DMZ privée	
	DMZ publique	
	Liaison avec le routeur autre actif frontal	
Hébergement physique		
Adresse IP publique		
Adresse IP interne		

INFORMATIONS SYSTEME :

Environnement				
Version du logiciel				
Modules installés	Maximum Physical Interfaces		IDS/IPS	
	VLAN/DMZ		Passerelle AV	
	Filtrage/Policy		Filtrage URL	
	Haute Disponibilité		Gestion logs	
	VPN		Administration	
	Gestion bande passante		Autres	

INFORMATIONS DE GESTION :

Mode d'administration		
Documentation	Procédure	
	Manuel	
	Autre	
Console de monitoring dédiée		

INTERACTION AVEC D'AUTRES Equipements et/ou Serveur:

Equipements/Serveur	Adresse IP	Protocole/Port	Moyen de communication

ANNEXE D La norme ANSI/TIA-942 Data Center

Télécommunications Infrastructure Standard for Datacenter (TIA) a pour objectif de proposer les exigences propres à la spécification, la réalisation et l'équipement des Datacenter garantissant ainsi les meilleurs niveaux de conformité et de disponibilité.
Ses avantages :

- On dispose d'un document reconnu par la communauté internationale sur lequel s'appuyer et définissant de manière très précise les normes à appliquer et les moyens dont il faut s'équiper pour obtenir un bon niveau de disponibilité des données dans les Datacenter.

Ses inconvénients :

- Elle est orientée télécom.
- Elle n'est pas assez aigüe sur la sécurité des informations.
- Elle est limitée en termes de sécurité physique.

Généralité :

La norme ANSI/TIA 942-2005 prévoit plusieurs recommandations dans différents domaines pour la construction d'un Datacenter fiable. Les domaines sont les suivants :

Le local technique :

Pour le choix du local technique, la norme ANSI/TIA 942-2005 énumère plusieurs conditions à respecter :

- Le bâtiment ne doit pas être construit sur une zone en dessous du niveau de crue centennale (le fait qu'un cours d'eau déborde de son lit mineur en moyenne chaque 100ans), ni sur une faille sismique, ni au débouché de masses d'eaux, ni à proximité de constructions susceptibles de s'effondrer en cas de séismes.
- Le site ne doit pas se trouver sous les routes aériennes d'aéroports proches.
- Le local technique ne doit pas être construit à moins de 800m d'une autoroute, d'un axe majeur routier, d'une base militaire, ni à moins de 1,6 km d'un site nucléaire, d'un dépôt de munitions de sites de défense.
- Le site ne doit pas se trouver à moins de 400m d'un aéroport, d'un barrage, de la côte, d'une rivière, d'une usine chimique.
- Le bâtiment doit être construit avec des matériaux solides capables de résister à l'incendie pendant au moins deux heures.
- Les planchers, les murs et le plafond doivent être scellés, peints avec des matériaux capables de minimiser la poussière.

Accès au local technique

- L'accès au Datacenter doit être hautement sécurisé. Il faudrait, pour ce faire, prévoir des mesures qui alertent des personnes en cas d'intrusion, définir des codes d'accès ou des accès par carte magnétique. L'accès au Datacenter pourrait également être protégé par des gardes de sécurité vérifiant à l'entrée l'identité des personnes.
- **Les portes :** La largeur minimale des portes conseillée est de 1m alors que la longueur minimale est de 2 ,13m. Les portes, pouvant être ouvertes vers l'extérieur (code le permet), être glissées d'un côté à l'autre, ou être amovibles, doivent être munies de serrures infalsifiables.

Au niveau architectural

Pour l'architecture du Datacenter, la norme prévoit des prescriptions à certains niveaux :

- **Hauteur au plafond :**

  La hauteur minimale du sol au plafond est de 2,6m. Une augmentation de cette hauteur peut être due à une hauteur élevée des appareils de climatisation et des racks.
- **Faux plancher :**

  Le faux plancher doit être capable de supporter les différentes charges qui lui sont soumises avec des câbles souterrains et des medias. La capacité minimale pour les charges est de 1KPA c'est-à-dire 1t/m².
- **Eclairage :**

  L'éclairage doit être un minimum de 500 lux (unité d'éclairement. 1 **lux** est l'éclairement d'une surface placée à 1 m d'une source de lumière dont l'intensité est de 1 candela : 1 **lux** = 1 lumen/m²) dans le plan horizontal et 200 lux dans le plan vertical, mesuré à 1 m au-dessus du plancher et au milieu des allées entre les armoires.

- **Les murs :**

  Les murs du Datacenter doivent être construits avec des matériaux capables d'éviter au maximum les échanges d'air avec l'extérieur.

Au niveau environnemental

La température et l'humidité dans les Datacenter doivent être sujettes à un contrôle strict. Pour cela, la norme a prévu un tableau récapitulatif des différentes limites à respecter.

Libellé	**Plage**
Température	Entre 20°C et 25°C
Taux d'humidité relative	Entre 40% et 55%
Vitesse maximale de fluctuation	5°C par heure
Température maximum au point de rosée	21°C

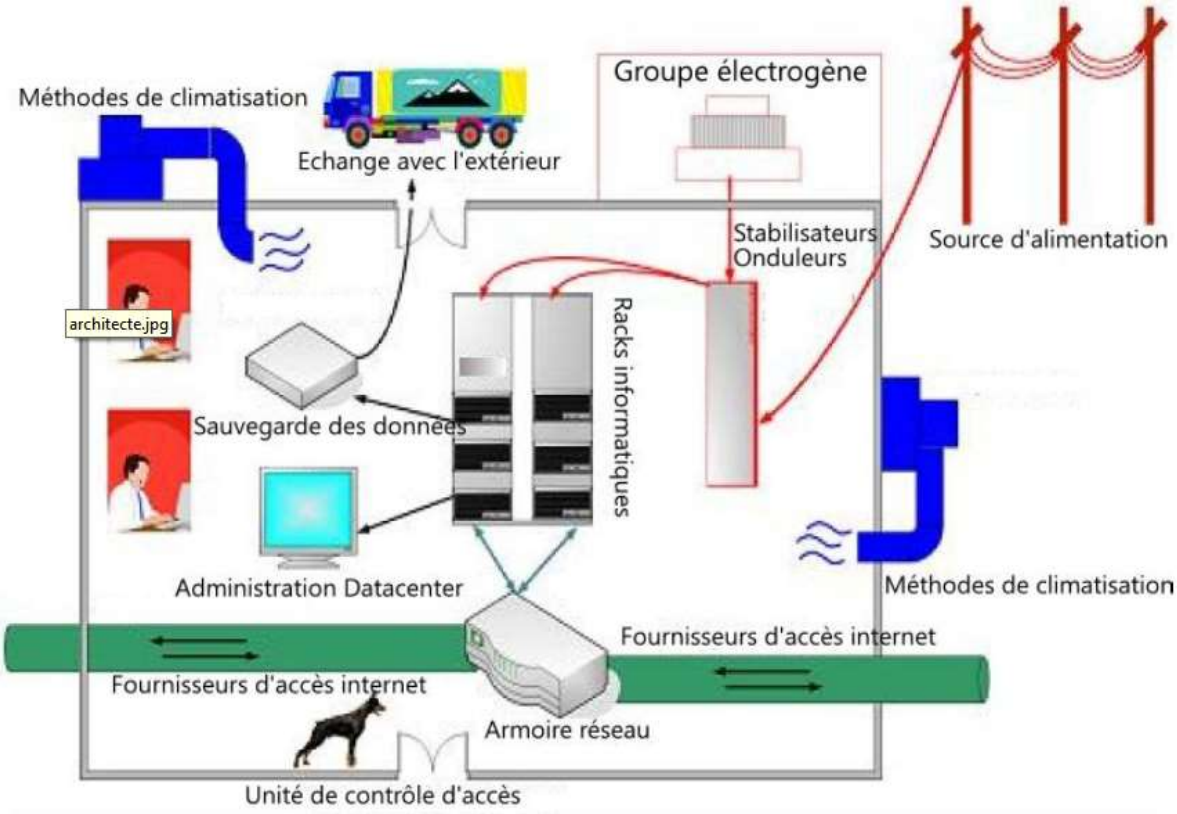
Tableau 1 : conditions environnementales requises

L'on a souvent recours à l'humidification ou à la déshumidification selon les contraintes environnementales du local technique. Aussi, La norme conseille que la température ambiante et l'humidité soient mesurées après que les différents appareils soient mis sous tension. Les mesures doivent être faites à une distance de 1,5 m au-dessus du niveau du sol et tous les 3 à 6 m le long de la ligne centrale des allées froides et à tout endroit dans la prise d'air de l'exploitation des équipements.

Au niveau électrique

Le Datacenter doit être raccordé à un réseau électrique ayant une tension en courant alternatif comprise entre 220v et 240v et une tension de 48V en courant continu. La norme prévoit également une fréquence égale à 60Hz pour les différents équipements.
Pour l'électricité, la norme prévoit trois niveaux ; il y a d'abord les sources d'alimentation, ensuite viennent les régulateurs de tension puis les onduleurs. Il faut, par ailleurs, prévoir des sources alternatives d'alimentation (groupes électrogènes, …) en cas de coupure ou de baisse de la tension afin d'assurer la continuité du service jusqu'au rétablissement du courant électrique.

Architecture générale d'un Datacenter



ANNEXE E Politique et procédure de sauvegarde

SNDP – AGIL
Cellule de sécurité

Politique de sauvegarde

1 - Définitions

Les données et les applications informatiques qui doivent être disponibles doivent être conservées (sauvegardées) afin de pouvoir être récupérées (restauration) le moment voulu. Il s'agit de mettre en œuvre une politique et une procédure de sauvegarde des données et des applications

2 Risques

- La sauvegarde doit aider à se prémunir des pannes matérielles, des compromissions de données, des erreurs de manipulation (utilisateur/administrateur), du vol, des incendies ou dégâts des eaux etc.…

- Les données sauvegardées à un instant donné peuvent ne plus pouvoir être lues, les applications ou versions d'applications utilisées à l'origine n'étant plus disponibles

3 - Les différentes méthodes de sauvegarde

- **Sauvegarde complète** : C'est une méthode de type « annule » et « remplace ». On écrase le contenu de sauvegarde par la nouvelle information. Méthode très sûre mais longue si le volume est important (par ex : la sauvegarde de gros volumes peut être supérieure à la durée de la nuit et empêcher le travail des utilisateurs le lendemain matin).

- **Sauvegarde différentielle** : C'est une méthode qui sauvegarde toutes les informations qui ont été modifiées depuis la dernière sauvegarde complète

- **Sauvegarde incrémentale**: C'est une méthode qui ne sauvegarde que les informations qui ont été modifiées depuis la dernière sauvegarde enregistrée sur le support

- **Synchronisation d'équipements**: C'est une première méthode à mettre en place entre des équipements nomades et des postes fixes d'un utilisateur donné. Elle peut inclure autant les données d'agenda, de carnets d'adresses que de simples fichiers (fonction porte document) et s'active souvent manuellement

4 - Périmètres à sauvegarder

- Les serveurs
- Les Bases de données
- Les applications
- Les commutateurs
- Les équipements d'interconnexion (les routeurs)
- Les équipements de sécurité (Firewall, proxy, IDs, IPS)
- Certains postes de travail

5 - Le type de données à sauvegarder

- Les bases de données
- Active directory
- Les e-mails
- Les codes sources des applications
- Les images des systèmes d'exploitation installées sur les serveurs
- Les configurations des switchs, routeurs, access point, les équipements de sécurité

6 - Fréquence et périodicité des sauvegardes

- Une sauvegarde différentielle journalière (lundi, mardi, mercredi, jeudi) des bases de donnés
- Une sauvegarde totale le vendredi pour les bases de données
- Une sauvegarde tout les mois des équipements de sécurité
- Une sauvegarde tout les quatre mois pour les configurations d'équipement réseaux et les images du système d'exploitation des serveurs.
- Une sauvegarde annuelle des commutateurs et routeurs
- Ces sauvegardes seront faites en double exemplaire.

7 - Emplacement des sauvegardes

- Un exemplaire sera placé dans une armoire ignifuge au Datacenter de la SNDP
- L'autre exemplaire sera placé dans un lieu distant du siège (au magasin principal de la SNDP)
- Une sauvegarde sur disque dur externe placé sur le réseau étendu de la SNDP (au dépôt Skhira)

8 - Vérification des sauvegardes

La procédure avec cette politique précisera le contrôle régulier d'un journal de sauvegarde afin de vérifier qu'aucune anomalie n'ait perturbé le bon fonctionnement des sauvegardes

9 - Test des sauvegardes

La procédure doit prévoir, avant de passer en mode de fonctionnement continu, de tester la bonne récupération des données afin de s'assurer du bon fonctionnement des sauvegardes.

10 - L'opérateur de sauvegarde

La procédure doit prévoir la nomination d'un opérateur de sauvegarde et son intérim pour assurer la continuité de l'opération.

11 - L'audit des moyens de sauvegarde

- Auditer annuellement les équipements de sauvegarde (logiciels de sauvegarde, robots de sauvegarde, les bandes, …)
- Faire des statistiques sur les sauvegardes échouées
- Mettre à jour la procédure si nécessaire.

SNDP-AGIL
Cellule de sécurité

Procédure de sauvegarde

1 - Périmètres à sauvegarder

1.1 Les serveurs : une image du système d'exploitation doit être sauvegardée tout les 4 mois.

1.2 Les Bases de données : une sauvegarde totale des bases de données doit être faite tout les vendredis et une sauvegarde différentielle Lundi, Mardi, Mercredi, Jeudi.

1.3 Les applications : une sauvegarde du code source de l'application doit être faite tout les 4 mois.

1.4 Les commutateurs : une sauvegarde des configurations des commutateurs doit être faite annuellement

1.5 Les équipements d'interconnexion (les routeurs) : une sauvegarde des configurations des routeurs propriétés de la SNDP doit être faite annuellement

1.6 Les équipements de sécurité (Firewall, proxy, IDs, IPS) : une sauvegarde des configurations des équipements de sécurité doit être faite tout les 4 mois.

1.7 Les postes de travail : une sauvegarde des fichiers (word, excel, powerpoint, PDF, … etc) et base de données locales sur le poste de travail doit être faite par l'utilisateur du poste selon une fréquence qu'il déterminera selon son exploitation et le degré de criticité de ces données

2 – Recommandations à propos des sauvegardes

- Eviter d'utiliser les clés USB
- Le support principal recommandé est la bande magnétique
- Eviter de laisser les bandes près du serveur
- Faire les sauvegardes en double exemplaire
- Un exemplaire sera placé dans une armoire ignifuge au Datacenter de la SNDP
- L'autre exemplaire sera placé dans notre magasin central Charguia
- Les sauvegardes totales des bases de données ainsi que les sauvegardes trimestrielle, semestrielle, annuelle seront placés sur disque dur externe mis sur le réseau étendu de la SNDP au dépôt Skhira.
- Toutes les bandes seront recopiées sur de nouvelles bandes tous les 5 ans

- Le disque dur externe sera remplacé tout les 3 ans.

3 - Vérification des sauvegardes

Toute opération de sauvegarde doit générer un journal et une remonté de mail vers l'opérateur de sauvegarde pour la vérification de la bonne marche de cette opération en cas d'anomalie l'opérateur fait suivre le mail au responsable d'exploitation, RSSI et au DSI.

Les journaux de sauvegardes seront archivés pour la traçabilité et pour des opérations d'audit ultérieur.

4 - Test des sauvegardes

Les sauvegardes doivent être testées par une opération de restauration sur un environnement de test sur le serveur loin de l'environnement de production et à des heures qui ne perturbe pas le temps de réponse des serveurs. Les rapports générer par cette opération seront archiver.

5 - L'opérateur de sauvegarde

Les opérateurs de la salle serveur de la SNDP seront en charge des opérations de sauvegarde (lancement, remplacement des bandes, mettre les bandes dans l'armoire ignifuge, …etc) en cas d'anomalie les opérateurs mettent au courant le responsable d'exploitation, le RSSI et le DSI.

6 - L'audit des moyens de sauvegarde

- Auditer annuellement les équipements de sauvegarde (logiciels de sauvegarde, robots de sauvegarde, les bandes, …)
- Faire des statistiques sur les sauvegardes échouées
- Mettre à jour cette procédure si nécessaire.

ANNEXE F Politique de gestion d'incident

Politique de gestion des Incidents de sécurité du S.I

Versions	Rédacteur	Autorité d'approbation	Date d'approbation
V1.0	Amor Mrabet		

Historique des modifications

Date	**Objet de la modification**	**Auteur(s)**	**Statut**

Introduction

Un incident sur le système d'information est un ou plusieurs événements intéressant la sécurité de l'information indésirable ou inattendue présentant une probabilité de compromettre ou de menacer la sécurité du système d'information.
Quelle que soit l'approche, la gestion des incidents, a pour objectif la détection et le traitement des incidents. Le processus de gestion des incidents inclut en général la détection de l'incident, les analyses et diagnostics, la résolution de l'incident et/ou le rétablissement du service affecté.
Un aspect important de la gestion des incidents est le suivi (reporting) de ce processus et la capitalisation.
La mise en œuvre d'un processus de gestion des incidents de sécurité nécessite la définition :

- D'une démarche pour le traitement de l'incident
- Du Périmètre de sécurité
- Des objectifs (politique de gestion des incidents)
- Des mesures (processus, bonnes pratiques, etc.)
- Des moyens associés (organisation des ressources matérielles/humaines/budgétaires)

Démarche pour le traitement des incidents

- Constat de l'incident
- Informer le RSSI (voir ces coordonnées en Annexe)
- Le RSSI informe la cellule de sécurité du S.I
- Faire l'analyse et le diagnostic nécessaire
- Déclarer l'incident sur l'application Gestion des Incidents
- La cellule informe la DG
- La capitalisation sur la résolution et le traitement des incidents de sécurité du S.I

Le périmètre de sécurité

C'est tous le périmètre du Système d'Information : périmètre organisationnelle, procédurale, physique et technique et des périmètres particuliers notamment le system de la carte privative pétrolière « AGILIS »

Les objectifs

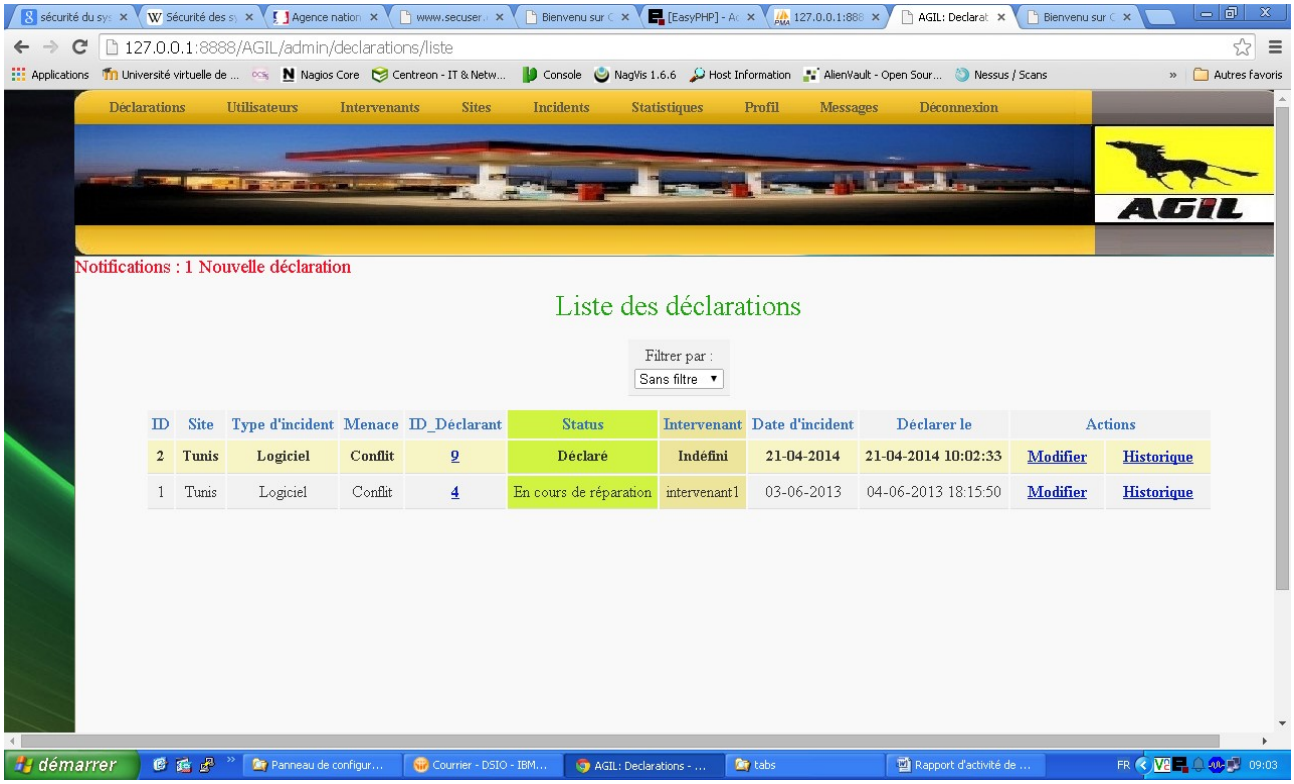
- Etude et analyse des incidents : statistique et reporting
- Etude des solutions nécessaires et leur budget
- Soumettre ces solutions au comité de sécurité du système d'information
- Entreprendre les actions adéquates
- La capitalisation sur la résolution et le traitement des incidents de sécurité du S.I

Les mesures

Les mesures à prendre pour parer aux incidents de sécurité doivent être conforme aux exigences des normes de sécurité ISO 27002 des bonnes pratiques, la norme ISO 27005 l'analyse des risques, les lois en vigueur.

Les moyens associés

L'un des composants essentiels de la gestion des incidents c'est l'organisation et la coordination des ressources matérielles, humaines et budgétaires ainsi que l'utilisation de l'application gestion des incidents de sécurité du système d'information



Qualification et typologie des incidents

Thème(1) : Organisation de la sécurité de l'information

Cause : Attribution des responsabilités en matière de sécurité de l'information ainsi que le système d'autorisation concernant les moyens de traitement de l'information

- Engagement divulgation d'information
- Incident provenant des tiers
- Incident provenant des clients

Thème (2): Gestion des actifs

- Incident sur l'actif (logiciel, matériel,….)
- Utilisation Incorrecte des actifs
- Incident sur le marquage et la manipulation de l'information

Thème (3): Sécurité liée aux ressources humaines

Les risques humains sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

- Incident causé par une ressource en période d'approbation
- Incident causé par un processus d'ingénierie sociale
- Incident causé par un processus d'espionnage
- Incident par la responsabilité directe des ressources Humaines
- Incident au départ d'une ressource

Thème (4): Sécurité physique et environnementale

- Incident sur les accès physiques
- Incident environnementale
- Incident de servitude essentielle
- Incident sur matériel et équipement du traitement de l'information
- Incident sur actifs sortis

Thème (5): Gestion de l'exploitation et des télécommunications

- Incident sur les équipements de développement d'essai et d'exploitation
- Incident provenant d'un service tiers
- Incident provenant d'un code malveillant
- Sauvegarde et restauration

- Incidents sur les services réseaux
- Incident sur les échanges d'information
- Incident sur la messagerie électronique
- Incident sur commerce électronique
- Incident sur transaction en ligne
- Incident sur les journaux administrateurs et opérations
- Incident sur supports d'échange d'information : ligne de télécommunications

Thème (6): Contrôle d'accès

- Incident sur les accès utilisateurs
- Incident de responsabilité de l'utilisation matériel laissé sans surveillance
- Incident sur ports réseaux
- Incident sur connexions réseaux
- Incident sur routages
- Incident sur Active Directory
- Incident sur solution antivirale
- Incident sur le Firewall
- Incident sur le proxy
- Incident de connexion à distance au système d'information
- Incident du bon fonctionnement de l'application
- Incident sur l'accès code source des programmes
- Incident sur modification des progicielles
- Incident sur l'externalisation du développement logiciel.

Résumé :

La carte à puce est aujourd'hui omniprésente dans notre environnement : carte SIM, cartes bancaires, cartes de décryptage de télévision par satellite ainsi que toutes les versions de cartes privatives de diverses enseignes commerciales. C'est un outil puissant de conquête et de fidélisation des clients. Une carte personnalisée aux couleurs de l'entreprise augmente la valeur ajoutée de celle-ci et offre à son client un moyen sécurisé, facile d'utilisation et de proximité.

Pour réussir son projet de mise en circulation de sa carte privative une organisation doit disposer entre autre des composants matériels et logiciels nécessaires mais doit prendre en considération une composante fondamentale qui est la sécurité de l'information pour le périmètre de sa plateforme.

Le travail objet de cette mémoire est de présenter un ensemble de mesures de sécurité de l'information organisationnelles et techniques selon la norme ISO/CEI 27002 version 2013 et selon les expériences vécues dans le projet de la carte à puce privative pétrolière AGILIS de la SNDP-AGIL.

Mots clés : carte à puce, carte privative, carte pétrolière, sécurité de l'information, ISO 27002, sécurité de la carte à puce privative

الملخص

البطاقة الذكيّة هي الآن في كلّ مكان في بيئتنا ، بطاقة سيم و البطاقات المصرفية و بطاقات فكّ التشفير التلفزيونية الفضائية و كذلك كافّة إصدارات البطاقات الخاصّة للعلامات التجارية المختلفة ، إنّها وسيلة قويّة للفوز و الاحتفاظ بحر فاءها .

البطاقة الذكيّة الخاصّة بألوان الشركة تزيد من القيمة المضافة لها و توفّر لعملائها وسيلة آمنة و سهلة الاستعمال و مباشرة.

لإنجاح مشروع تعميم البطاقة الخاصّة يجب أن تكون الشركة مزوّدة بمعدّات و برمجيات كما يجب عليها أن تأخذ بعين الاعتبار عنصرا أساسيا ألا وهو السلامة المعلوماتية لمحيط برنامجها.

الهدف من هذا العمل هو تقديم مجموعة من الإجراءات لسلامة المعلومات التنظيميّة و التقنية وفقا لمعيار ISO 27002 في نسخة 2013 و كذلك طبقا للتجارب التي عشناها في مشروع بعث البطاقة الذكيّة الخاصّة البترولية AGILIS للشركة الوطنية لتوزيع البترول عجيل.