



ASSOCIATION DES SOCIÉTÉS FRANÇAISES
D'AUTOROUTES ET D'OUVRAGES À PÉAGE

La monétique sur les Autoroutes

PCI-DSS

Conférence CLUSIF – 7Avril 2011

***L. BEAUSSART – Directeur Adjoint des Systèmes Opérationnels – RSSI
COFIROUTE***

La Démarche ASFA



Association professionnelle qui regroupe tous les acteurs du secteur de la concession et de l'exploitation d'autoroutes et d'ouvrages routiers à péage :

- Représentation et défense des intérêts de la profession,
- Politique de communication sur les thèmes d'intérêt commun,
- Négociations à caractère social concernant la branche professionnelle,
- Développement des relations internationales non commerciales,
- Réalisation d'études, de recherches et d'enquêtes.

Les travaux de l'ASFA sont menés au sein des instances suivantes :

- La Commission sociale
- Les Comités Sectoriels :
 - o Comité Concession et Partenariats,
 - o Comité Réseau, Qualité, Sécurité, et Service,
 - o Comité Patrimoine et Infrastructures,
 - o Comité Technique Interautoroute Péage,
 - o Comité monétique (groupe de travail cartes bancaires).



**9000 km
d'autoroutes
conçédées
en 2010**

**85 milliards
de Km
parcourus**



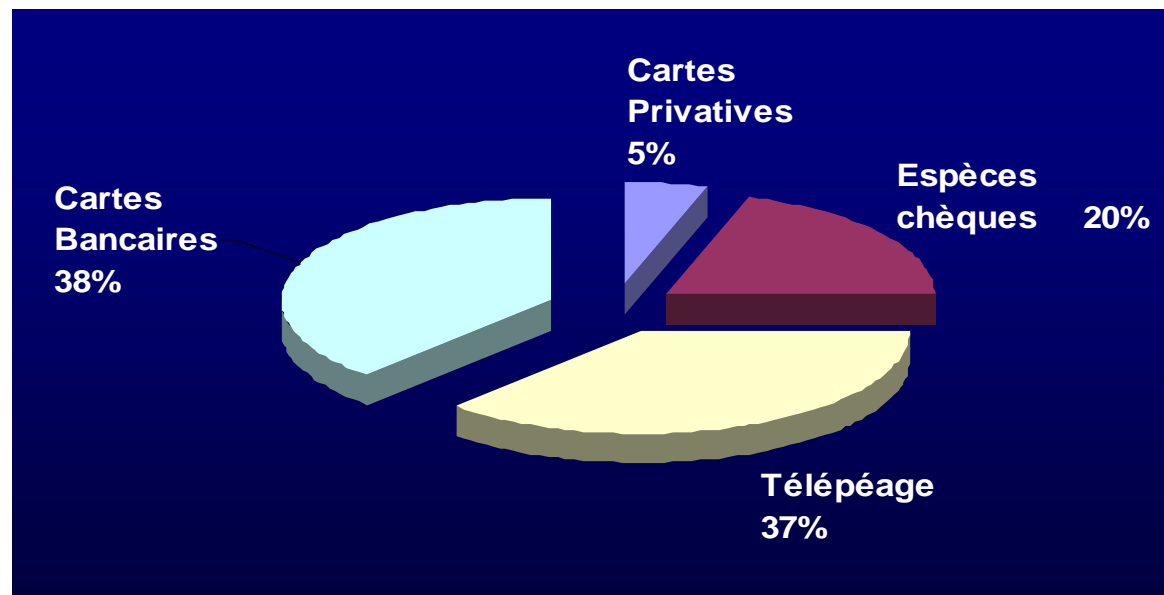
- Un ensemble de concessions qui représente 7,5 milliards d'€ de CA, 1,8 milliard d'Investissement annuel, 28 milliards d'endettement
- Des concessions, filiales des plus grands groupes de travaux publics
- Des partenariats avec :
 - les principaux pétroliers (2,5 milliards de litres de carburant vendus)
 - les fédérations de transporteurs routiers
 - Les chaînes d'hôtels et de restaurants (365.000 nuitées, 326 restaurants)
- Plusieurs sociétés communes avec des banques (AXXES avec le CM, Alis et Adelac avec les CE ...)



1,3 milliard de transactions (tous paiements) traitées par les sociétés de l'ASFA, dont :

- ↪ 490 millions de transactions par cartes bancaires,
- ↪ Des transactions moyennes de 6 €,
- ↪ Un volume d'environ 3 milliards d'euros.

Répartition par moyen de paiement :



- Des contraintes d'exploitation fortes :
 - rapidité de passage en voie pour assurer la fluidité du trafic
 - exploitation 24h/24h, 365 j/an
 - forte variation saisonnière,
 - maintenance et travaux sous circulation
- Une ergonomie très spécifique des lecteurs:
 - cadences élevées,
 - multi épaisseurs,
 - contraintes climatiques ...
- Des chaînes de traitement propres à chaque SCA, et un maillage des réseaux,
- Un parc de matériel > 4 000 lecteurs,
- Une absence d'offre adaptée aux besoins du secteur autoroutier,
- Des coûts d'investissements très élevés (durée d'amortissement des matériels > 10 ans),



■ Différentes menaces

- La compromission :

Aggravée par le nombre et le montant du panier moyen des transactions autoroutières.

- La fraude :

Poursuite de la stratégie sécuritaire et de lutte contre la fraude initiée avec la mise en place de demandes d'autorisation online depuis 2005 :

- Baisse de 25% de la fraude sur les cartes françaises et divisée par 20 pour les cartes étrangères,
- Capture de plus de 20 000 cartes en opposition par an.

- La suspension, voire la radiation de l'adhésion au système CB en cas de non-conformité aux règles imposées par les émetteurs de cartes bancaires et les réseaux.

■ Exposition forte des sociétés d'autoroutes aux multiples risques liés à l'utilisation de la carte bancaire :

- Risque financier : Lié à la perte de recette, au refus de compensation ou aux amendes encourues en cas de non-conformité.
- Risque de perte d'image : Particulièrement sensible dans un secteur autoroutier. Vis-à-vis des clients d'une part mais aussi de son autorité concédante, l'état français.

■ L'organisation

- Lancement du projet en juillet 2006
- Présentation plan d'action à l'acquéreur en juillet 2007
- Coordination des projets des SCA au sein du comité monétique ASFA
- Accompagnement individuel des SCA par Verizon Business depuis 2008.

■ Quatre chantiers menés en parallèle :

- Mise en conformité PCI-DSS
- Migration EMV-MPAA
- Rénovation des systèmes informatiques (obsolescence des serveurs, ...)
- Mise à plat réglementaire et fonctionnelle

■ Solutions métiers retenues (règles communes)

- Troncature des chiffres du PAN non indispensables,
- Règles de stockage qui protègent les clients,
- Mise en œuvre d'une PSSI,
- Chiffrement de bout en bout. Objectif : Réduction du périmètre PCIDSS



Le Projet Cofiroute

Sécurisation spécifique	Création et gestion d'un réseau sécurisé	<ol style="list-style-type: none"> 1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
	Protection des données des titulaires de cartes de crédit	<ol style="list-style-type: none"> 3. Protéger les données des titulaires de cartes stockées 4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts
Sécurité Générale du SI	Gestion d'un programme de gestion des vulnérabilités	<ol style="list-style-type: none"> 5. Utiliser des logiciels antivirus 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	<ol style="list-style-type: none"> 7. Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître 8. Affecter un ID unique à chaque utilisateur d'ordinateur 9. Restreindre l'accès physique aux données des titulaires de cartes
	Surveillance et tests réguliers des réseaux	<ol style="list-style-type: none"> 10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes 11. Tester régulièrement les processus et les systèmes de sécurité
	Gestion d'une politique de sécurité des informations	<ol style="list-style-type: none"> 12. Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants

Les constats

- Un périmètre PCI-DSS trop vaste ce qui implique un faible niveau d'implémentation des exigences du standard
- Un manque de formalisme des processus déjà en place

Le Standard PCI-DSS

Protection des données des
titulaires de cartes de crédit

3. Protéger les données de titulaire de carte stockées
4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts

Différentes solutions

Le Chiffrement : AES, RSA

Basé sur l'utilisation de clés secrètes, de clés publiques et privées, il est symétrique ou asymétrique mais permet toujours déchiffrer la donnée initiale

- ↳ Nécessite la gestion de ces clés, leur stockage, leur mise à jour, conformément aux contraintes sécuritaires

Le Hachage : SHA-2

L'empreinte est unique et ne permet pas de revenir sur l'information initiale.
Les algorithmes sont publics et leur robustesse réside sur le très grand nombre d'itérations nécessaires pour obtenir une collision.

La Troncature

Notre Besoin :

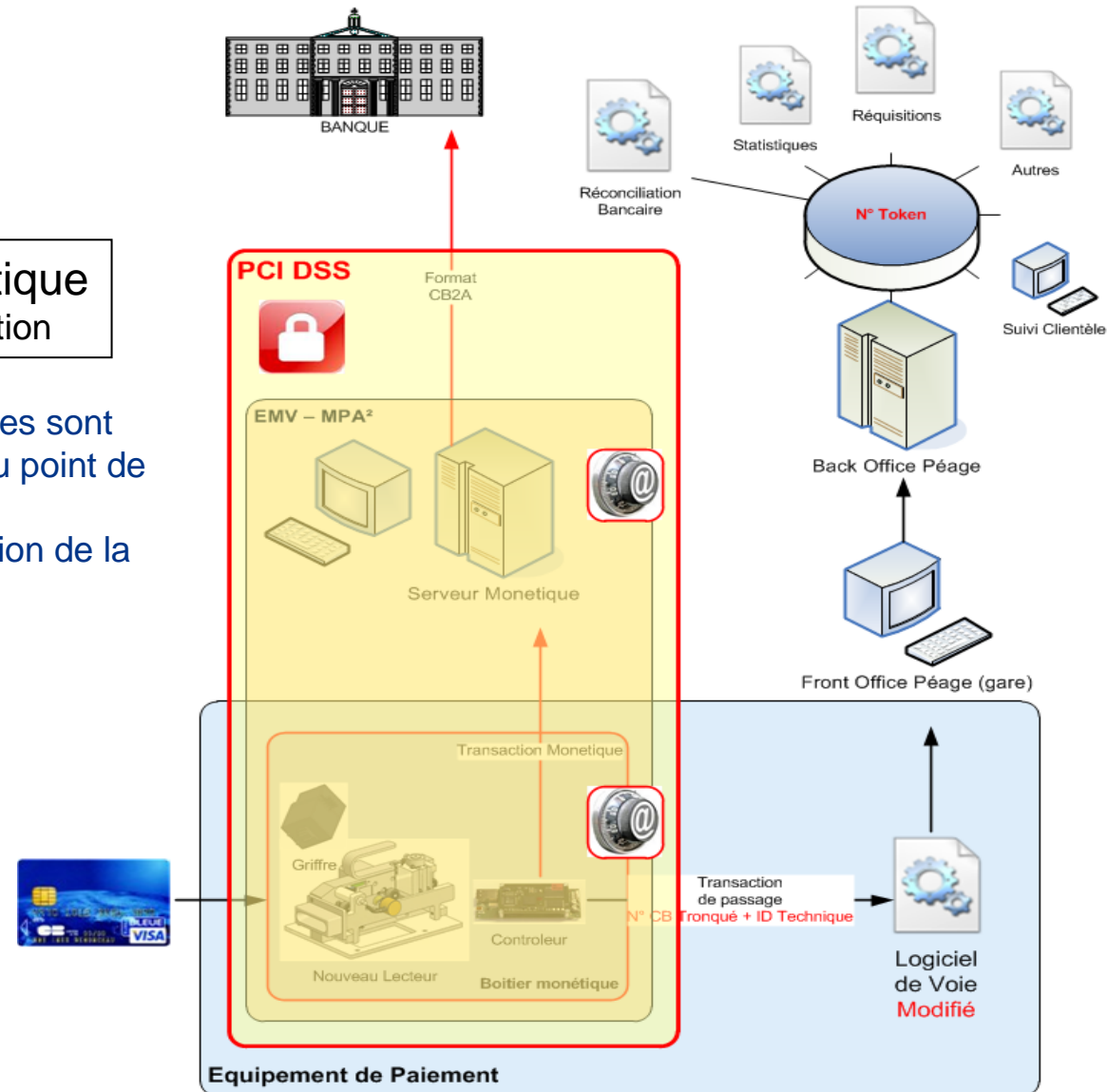
La remise en banque nécessite un déchiffrement de la donnée pour compensation.
Les traitements métiers ont uniquement besoin d'un identifiant porteur unique et de données carte publiques (Code BIN)



Choix de Séparer les Flux

Contrôleur monétique
End To End Encryption

Les informations sensibles sont cryptées au plus proche du point de paiement et l'aiguillage évite l'implication de la chaîne péage.





Statistiques et suivi des Commissions facturées

Réalisés à partir du Code BIN.

On remonte également un identifiant de transaction.

Identifiant porteur

Lutte contre la Fraude

Sur réquisition : Un PAN en clair est fourni.

Le Serveur Monétique fournit le token pour retrouver les transactions porteur dans le Back Office

Fraude identifiée par la SCA : Basée sur des transactions suspectes.

Une procédure est nécessaire pour encadrer la récupération du PAN d'une transaction précise et son décryptage à partir du serveur monétique.

Suivi des Transactions bancaires

Réconciliations opérées par rapprochement des Id de transactions



L'aspect documentaire



- Choix de mise en œuvre d'un Système de Management de la Sécurité du S.I. (SMSI) basé sur ISO 27001
- PCI-DSS est un sous-ensemble du périmètre
- Des niveaux d'exigence spécifiques sont repris pour PCI-DSS au sein des objectifs ISO 27001.
- Le soubassement ISO 27001 facilitera les audits de conformité



ASSOCIATION DES SOCIÉTÉS FRANÇAISES
D'AUTOROUTES ET D'OUVRAGES À PÉAGE

MERCI DE VOTRE ATTENTION