

 cetelem**Etudes Monétiques**

Version ✎ 2.0

Date ✎ 14/10/2005

Reference Gemini ✎ PH173334

GUIDE DE MIGRATION A EMV des Filiales Internationales et Nouveaux Partenaires

SIGNATORIES

DIRECTION UTILISATRICE:**IT COORDINATION :****IT DEPARTMENT:**

Révisions

Version	Date	Auteur	Contenu
0.1	31/01/05	Rémi Gitzinger	Création
1.2	26/04/05	“	Validation
1.3	16/05/05		Diffusion Etudes Monétiques
1.31	22/09/05		Précisions compensation
2.0	14/10/05		Document Global

Validation

Intervenant	Date
Olivier Gyorffy	
Mardjan Laroche	
Mohamed Amarti	

© **Cetelem S.A. – Groupe BNP-Paribas**

This document is the property of Cetelem S.A.. The contained information is of technical / informative character and cannot be copied, photocopied, duplicated, translated or subjected to any electronic means without the prior authorization of Cetelem S.A. This one reserving the right to modify the contents and the form of the document without any preliminary notice.

Liste des Acronymes

Acronyme	Définition
3DES	Triple Data Encryption Standard
ADA	Application Data Action
AID	Application Identifier
AIP	Application Interchange Profile
ARQC	Authorization Request Cryptogramm
ATC	Application Transaction Counter
AUC	Application Usage Control
CDA	Combined Data Authentication
CID	Cryptogram Identifier
CVM	Cardholder Verification Method
CVR	Card Verification Result
DDA	Dynamic Data Authentication
EMV	Eurocard Mastercard Visa
HSM	Host Security Module
IAD	Issuer Application Data
MAC	Message Authentication Code
PAN	Personal Account Number
RSA	Rivest Shamir Adleman – algorithme à clé publique
SDA	Static Data Authentication
TVR	Terminal Verification Result

SOMMAIRE

1. Objet du Guide	6
2. Organisation du document	6
3. Champ D'Application	6
4. Migration EMV : Présentation Générale	7
4.1. Schéma Global du Flux Monétique Emetteur.....	7
4.2. Contexte Règlementaire	7
4.2.1. Référencement des documents réglementaires applicables aux émetteurs de cartes Mastercard	7
4.2.2. Référencement des documents réglementaires applicables aux émetteurs de cartes Visa ..	8
4.3. Production des Cartes	8
4.3.1. Choix de produit carte	8
4.3.2. Elaboration de profil carte	8
4.3.3. Mise en œuvre de la personnalisation	9
4.3.4. Gestion des clés	9
4.3.5. Agrément	10
4.4. Gestion des Systèmes Emetteurs.....	11
4.4.1. Serveur d'autorisation	11
4.4.2. Back-office - Base porteur.....	11
4.4.3. Back-office - Compensation.....	11
4.4.4. Gestion administrative des cartes.....	11
4.5. Synthèse des Actions à Entreprendre	12
5. Délivrance Carte : Description Détaillée	13
5.1. Schéma Global de la Production Cartes	13
5.2. Produit Carte	13
5.2.1. Choix d'application	13
5.2.2. Choix technologique.....	15
5.3. Définition du Profil EMV.....	16
5.4. Mise en œuvre de la Personnalisation	18
5.5. Gestion des Clés	20
5.6. Certification et Agrément	21
6. Exploitation Carte : Description Détaillée	22
6.1. Schéma Global de l'Exploitation Cartes	22
6.2. Domaine Front-Office	23
6.2.1. Fonctionnalités sécuritaires et protocolaires	24
6.2.2. Contrôle des données EMV d'autorisation	24
6.2.3. Fonctionnalité de post-modification	25
6.3. Domaine Back-Office	29
6.3.1. Gestion administrative des cartes.....	29

6.3.2.	Compensation – File Clearing	30
6.3.3.	Equipements spécifiques EMV –fonctions complémentaires	30
7.	Annexes	32
7.1.	Annexe A : Migration EMV2000.....	32
7.2.	Annexe B : Exploitation Cartes	32
7.2.1.	Table des contrôles effectués par le serveur de cartes SRVCA	32
7.2.2.	Données EMV en compensation	34
7.2.3.	Identification EMV des données utilisées en autorisation et compensation non-EMV	35

1.OBJET DU GUIDE

L'objectif de ce guide est de fournir toutes les informations nécessaires aux filiales internationales et nouveaux partenaires pour émettre des cartes EMV et en maîtriser l'exploitation.

Il décrit les principales activités qui relèvent de la responsabilité directe ou indirecte de l'émetteur en traitant les aspects fonctionnels, réglementaires ou sécuritaires. Le périmètre d'information s'étend aux 2 réseaux internationaux Visa et Mastercard.

2.ORGANISATION DU DOCUMENT

Ce guide est structuré en trois chapitres :

Une vue générale sur les domaines impactés par la **migration EMV**.

Une description détaillée des actions à entreprendre dans le périmètre de la **délivrance carte**, couvrant les produits carte, la définition des profils EMV, la personnalisation, la gestion des clés ainsi que les différents agréments.

Une description détaillée des actions à entreprendre dans le périmètre de **l'exploitation carte**, couvrant le Front (fonctionnalités sécuritaires et protocolaires, contrôles des données EMV et post-modification) et Back-office (gestion administrative des cartes, compensation, fonctions complémentaires).

3.CHAMP D'APPLICATION

Le présent document est proposé aux nouveaux partenaires France et filiales internationales. Alors que les partenaires suivent les modèles mis en application en France, l'hétérogénéité des contextes des filiales internationales ne permettent pas de définir un modèle unique. La description ci-dessous part de l'hypothèse d'une monétique front et back-office hébergée par les plateformes Cetelem Corporate, et peut selon les spécificités des pays, voir les actions à entreprendre modifiées sur les chaînes de flux présentées (ex : sous-traitance du front-office monétique par un fournisseur, sous-traitance des demandes EMV par un opérateur réseau, etc...).

4. MIGRATION EMV : PRESENTATION GENERALE

4.1. Schéma Global du Flux Monétique Emetteur

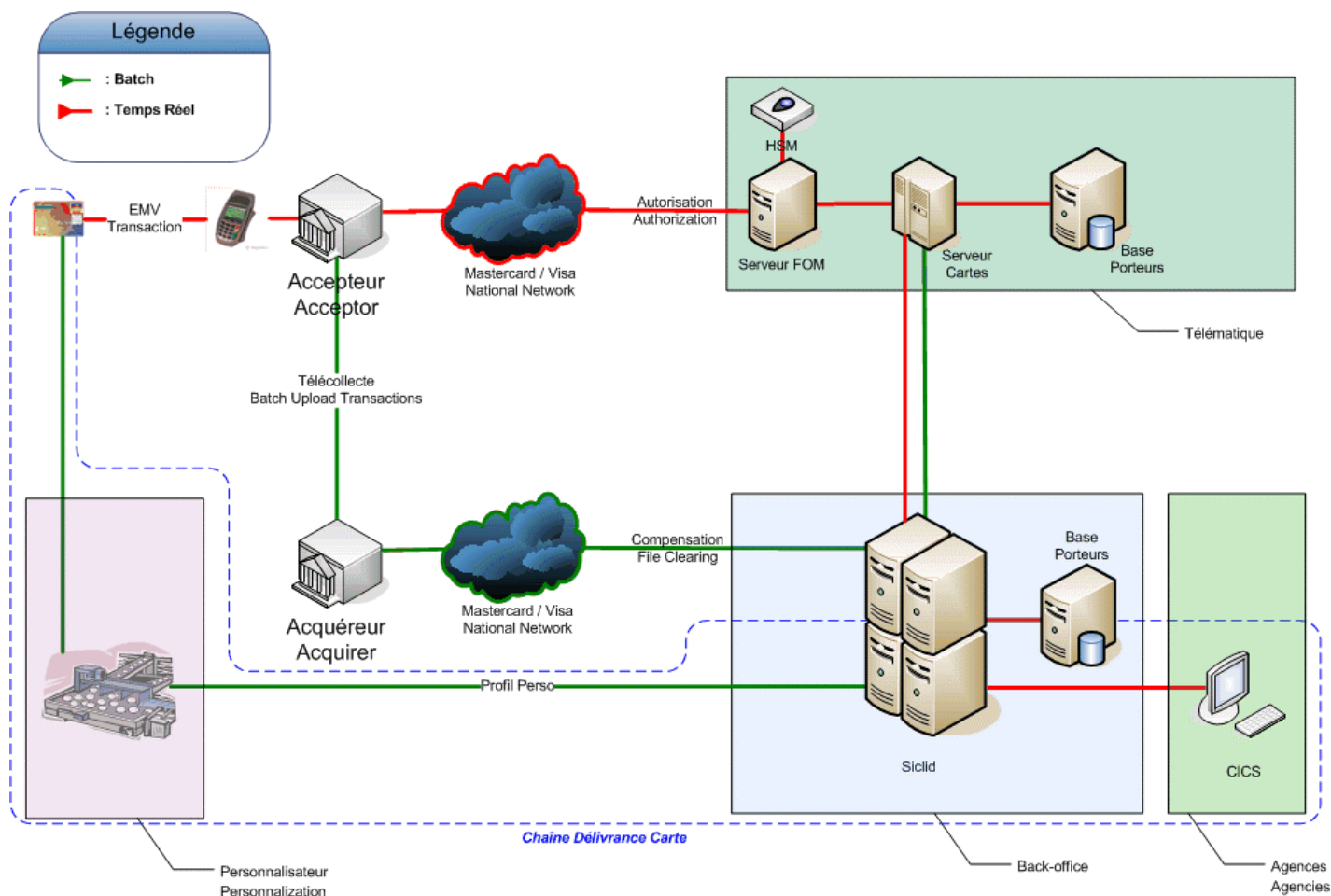


Figure 1: EMV Issuer Overview

Les impacts EMV sont présents sur l'ensemble de la chaîne.

4.2. Contexte Règlementaire

4.2.1. Référencement des documents réglementaires applicables aux émetteurs de cartes Mastercard¹

Tout projet EMV Mastercard doit se conformer aux documents suivants (cf. Annexe sur EMV2000):

- Card Type Approval Personalization Validation Form
- M/Chip 4 Card Applications Specifications for Debit and Credit

¹ Ces documents sont réservés aux membres émetteurs Mastercard. Ils s'appuient sur les normes publiques EMV (cf. <http://www.emvco.com/>)

4.2.2. Référencement des documents réglementaires applicables aux émetteurs de cartes Visa²

Tout projet EMV Visa doit se conformer aux documents suivants (cf. Annexe sur EMV2000) :

- Common Personalization Technical Requirements for Visa Smart Debit and Credit (VSDC)
- Visa Certificate Authority Technical Reference Guide for VSDC
- Visa Integrated Circuit Card Specifications (VIS 1.4)

4.3. Production des Cartes

4.3.1. Choix de produit carte

Le produit carte doit correspondre aux orientations commerciales de la filiale ou nouveau partenaire et aux types de cartes agréés par les réseaux. L'application permettant de mettre en œuvre les services offerts par le produit carte se décline selon :

Services	Mastercard	Visa	Autre Organisme National ³
Paiement et Retrait	Mastercard	Visa	Selon le pays
Retrait	Cirrus	Plus	Selon le pays
Autorisation Systématique	Maestro	Electron	Selon le pays
Autres services

Chaque service correspond à un AID⁴ spécifique.

La filiale peut souhaiter l'ajout d'une application tierce au produit carte. Cette possibilité étant offerte par la technologie, une demande doit être soumise aux réseaux qui détermineront les modalités d'agrément applicables.

De plus, le choix d'un produit carte nécessite la connaissance de critères technologiques en fonction du cahier des charges établi, dont il faut s'assurer qu'ils sont satisfaits auprès des fournisseurs (ex : taille mémoire du composant, cryptoprocasseur, etc. ...).

4.3.2. Elaboration de profil carte

Pour chaque type de carte choisi par la filiale, un profil doit être élaboré pour définir les caractéristiques fonctionnelles et alimenter l'appel d'offre à destination des fabricants. Ce profil doit être construit conformément aux documents référencés précédemment, et être validé par les services de qualification mis en place par les réseaux Mastercard, Visa et réseaux domestiques⁵ (certaines caractéristiques étant obligatoires pour Mastercard et fortement recommandées par Visa).

² Ces documents sont réservés aux membres émetteurs Visa. *Ibid.*

³ Suivant le pays de la filiale, des organismes nationaux communautaires peuvent imposer leur propre application domestique. (ex GCB : application CB pour Paiement/Retrait ou application CB Retrait pour Retrait uniquement, etc...)

⁴ AID : Application Identifier (ex : Mastercard : A000000041010)

⁵ ex : GCB

4.3.3. Mise en œuvre de la personnalisation

La filiale ou nouveau partenaire, fournit au personnalisateur (qui est en charge de la préparation logique des données et peut être également en charge de la préparation physique de la carte) les fichiers contenant les données nécessaires à la personnalisation des applications EMV présentes sur la carte, ces données nécessitant une communication par canal sécurisé garantissant l'intégrité et la confidentialité (jeu de clés administratives propre à chaque acteur (filiale et personnalisateur)).

Le personnalisateur et l'industriel doivent être certifiés par les réseaux Mastercard, Visa et domestiques pour produire des cartes EMV.

4.3.4. Gestion des clés

La sécurité applicable à l'émission de cartes EMV exige une utilisation et maîtrise de nombreux jeux de clés directement liés à la mise en œuvre de la transaction (clés applicatives) ou à la mise en œuvre de mécanismes de protection des données sensibles (clés administratives).

La filiale est tenue de faire certifier l'ensemble de ces jeux de clés émetteur auprès de l'autorité de certification propriétaires de l'application EMV (Mastercard, Visa et réseaux domestiques).

4.3.5. Agrément

L'ensemble de la chaîne émission est soumis à l'agrément des réseaux internationaux. Mastercard et Visa ont mis en place une procédure de qualification des cartes EMV qui porte d'abord sur le profil papier et ensuite sur des cartes spécimen.

L'agrément final conduit à l'ouverture des flux EMV des réseaux sur les BIN déclarés pour bénéficier des conditions particulières (incentives).

Constitution des dossiers	Mastercard	Visa	Autre Organisme National ⁶	GCB (pour nouveau partenaire)
Ouverture projet	Chip Migration Project Questionnaire	Plan de migration	Selon le pays	
Documents	Implementation Plan	Procédure de migration à EMV dont : <ul style="list-style-type: none"> - Key Management Questionnaire - Visa financial institution enrollement form - Questionnaire de personnalisation - Tables des codes actions émetteur - Questions générales - Paramètres STIP 	Selon le pays	Profil EMV (facultatif – service de validation proposé)
Carte Spécimen	Validation de la personnalisation (carte de test) Fourniture carte de production	Fourniture carte de test ou production	Selon le pays	Fourniture carte de test ou production (facultatif)
End to End test	Paielements et retraits avec carte de production	<i>Non requis</i>	Selon le pays	α -tests banque

⁶ Suivant le pays de la filiale, des organismes nationaux communautaires peuvent imposer leur propre agrément et certification (ex : Banksys, APACS, etc...)

4.4. Gestion des Systèmes Emetteurs

Dans ce chapitre, les systèmes monétiques émetteurs mis en œuvre pour l'exploitation des cartes EMV sont présentés sous l'angle d'une gestion opérée par Cetelem Corporate du front et back-office des filiales ou nouveaux partenaires.

4.4.1. Serveur d'autorisation

Le serveur d'autorisation assure pour la filiale ou nouveau partenaire, le contrôle et la réponse d'une demande d'autorisation pour une transaction effectuée par un de ses porteurs. Ce service doit être rendu en tenant compte des facteurs suivants :

- le type de contrat porteur
- les contraintes réglementaires des réseaux Mastercard, Visa et nationaux
- les contraintes sécuritaires liées à la lutte contre la fraude
- le contexte de la transaction (pays, montant, type de terminal...)

Les demandes d'autorisation en provenance des filiales sont transportées par les réseaux Mastercard (EPSnet) et Visa (VisaNet) et réseaux nationaux (e-RSB, etc....)

4.4.2. Back-office - Base porteur

Le système back-office doit gérer une base de données qui identifie chaque porteur de la filiale ou du nouveau partenaire. Ces données doivent permettre le suivi de la carte tant en production (profil EMV) qu'en exploitation (envoi de script de post-modification EMV – vol, perte, abusif, etc....).

De plus, en conformité avec la réglementation Mastercard ou Visa, Cetelem doit pouvoir opposer des critères d'impayés et de rejets techniques aux opérations de compensation qui lui sont présentées.

4.4.3. Back-office - Compensation

Le système back-office doit être en mesure de traiter en compensation les opérations cartes des filiales et nouveaux partenaires présentés par les réseaux d'acquisition Mastercard et Visa via les passerelles internationales ou les réseaux nationaux. Les données échangées comportent le minimum nécessaire aux contrôles et traitement des dossiers de réclamation ou d'impayés (cf. Liability Shift⁷), dont certaines données EMV propres à la transaction de retrait ou paiement.

4.4.4. Gestion administrative des cartes

L'exploitation de cartes EMV en phase d'utilisation peut inclure des deux types de fonctions, soit de réhabilitation, suite à un blocage de code confidentiel ou un blocage d'application, soit d'expertise (lecture des données de la carte et historique des transactions) ou mise à jour des données. Ces fonctions peuvent être exécutées à l'aide de terminaux dédiés à la réhabilitation EMV.

⁷ ou Transfert de Responsabilité : c'est un point essentiel de la migration EMV. Désormais un Emetteur peut émettre un impayé selon que le porteur d'une carte EMV se présente sur un point d'acceptation non-EMV. La banque acquéreur supporte alors le coût de la fraude (puisque non migrée EMV). Ce transfert est opérationnel depuis 01/01/05. (ex : Impayés Visa code 62 et 81 pour respectivement « Transaction Contrefaite » et « Fraude – paiement de proximité »).

4.5. Synthèse des Actions à Entreprendre

Actions	Détail	Commentaires
Domaine Carte		
Choix du produit carte	<ul style="list-style-type: none"> - choix du service offert - choix technologique du composant 	<ul style="list-style-type: none"> - AID correspondant - Taille mémoire, coprocesseur RSA, ...
Elaboration du profil carte	<ul style="list-style-type: none"> - Etude produit & service 	<ul style="list-style-type: none"> - Paramétrage carte, Risk Management, ...
Personnalisation de la carte	<ul style="list-style-type: none"> - constitution des fichiers de personnalisation - transfert sécurisé des fichiers 	<ul style="list-style-type: none"> - en correspondance avec élaboration du profil carte - jeux de clés administratives
Gestion des clés	<ul style="list-style-type: none"> - constitution des jeux de clés 	<ul style="list-style-type: none"> - clés administratives et applicatives
Certification et agrément	<ul style="list-style-type: none"> - constitution des dossiers d'agrément auprès des réseaux 	<ul style="list-style-type: none"> - profil, cartes spécimen, ETED (Mastercard)...
Domaine Systèmes Emetteur		
Front-office	<ul style="list-style-type: none"> - contrôle des données remontées 	<ul style="list-style-type: none"> - contexte transactionnel (TVR, CVR, ...), sécuritaire (cryptogrammes) et réglementaire (code monnaie, CVM, ...)
Back-office – base porteur	<ul style="list-style-type: none"> - gestion back-office – suivi production et exploitation – gestion impayés et rejets techniques 	<ul style="list-style-type: none"> - base des données EMV carte des contrats porteur, post-modification, litiges ...
Back-office - compensation	<ul style="list-style-type: none"> - gestion des échanges de données 	<ul style="list-style-type: none"> - données EMV propres aux transactions
Maintenance carte	<ul style="list-style-type: none"> - gestion administrative des cartes 	<ul style="list-style-type: none"> - réhabilitation carte, expertise (Machines de Banque en France ...)

5. DELIVRANCE CARTE : DESCRIPTION DETAILLEE

5.1. Schéma Global de la Production Cartes

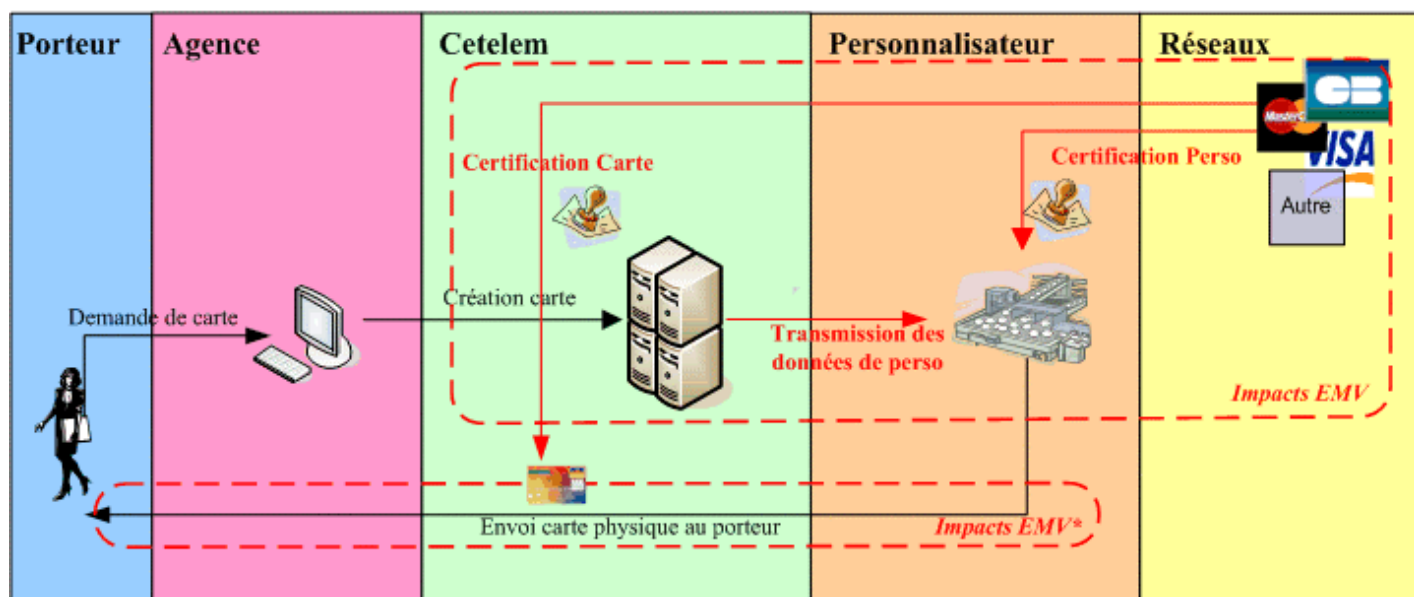


Figure 2 : Impacts EMV et délivrance carte

(*) : l'envoi du code PIN au porteur peut être impactant sur les chaînes d'envoi actuelles pour les filiales internationales.

5.2. Produit Carte

5.2.1. Choix d'application

La sélection du type de carte, et donc des services qu'elle offre, oriente les applications à mettre en œuvre.

Services	Mastercard	Visa	Organisme National ⁸
Paiement et Retrait	Mastercard	Visa	Selon le pays
Retrait	Cirrus	Plus	''
Autorisation Systématique	Maestro	Electron	''

Chaque service correspond à un AID⁹ spécifique.

⁸ Suivant le pays, un organisme national peut imposer ses propres applications domestiques

⁹ AID : Application Identifier (ex : Mastercard : A000000041010 -> PIX : A00000004 = Mastercard; RIX : 1010 = Paiement et Retrait)

De plus, des options peuvent être retenues selon l'expression de besoin de l'émission de la carte. (cf. tableau ci-dessous)

Fonctionnalité EMV optionnelle	Expression du besoin	Paramètres
Fichier d'historisation des transactions	Nécessité de conserver le nombre de transactions réussies ou en échec sur la carte	Taille du fichier cyclique à définir
Base applicative EMV	Dans le cadre d'une carte multi-applicative (ex : carte AID nationale et internationale), la fonctionnalité de blocage application porte sur une ou toutes les (x) applications présentes sur la carte	Indication à fournir au personnalisateur
Longueur du MAC	Choix de la longueur du cryptogramme du Secure Messaging	4 ou 8 octets à indiquer au personnalisateur
Partage des données	Nécessité de rendre commune ou spécifiques les données de (x) applications présentes sur la carte	Cf. § profil EMV

Action EMV – application carte et options

Fonctionnalité EMV	Expression du Besoin	Mise en œuvre
Choix des (x) applications présentes sur la carte	Décision des équipes marketing sur le service rendu par la carte au porteur	Définition de(s) AID(s) de la carte
Choix des fonctionnalités EMV optionnelles	Décision des équipes Gestion du Risque et Lutte contre la Fraude sur les paramètres à mettre en place	Valorisation des paramètres à fournir au(x) personnalisateurs(s)

Mise en application en France :

Le réseau domestique français impose d'utiliser ses propres applications pour les transactions nationales. En conséquence, le choix des applications portera sur les services suivants, Mastercard ou Visa étant utilisés pour les transactions internationales :

Services	Mastercard	Visa	GCB ¹⁰
Paie ment et Retrait	Mastercard	Visa	CB
Retrait	Cirrus	Plus	CB Retrait
Autorisation Système matique	Maestro	Electron	CB CAS

5.2.2. Choix technologique

Le choix technologique doit prendre en compte les besoins nécessaires à l'environnement fonctionnel EMV de la carte :

Action EMV

Fonctionnalité EMV	Expression du besoin	Pré-requis
Authentification dynamique et/ou PIN chiffré offline – bi-clés RSA de longueur > 896 bits	Décision des équipes Gestion du risque et Lutte contre la fraude sur la nécessité de l'authentification dynamique (DDA) et du PIN chiffré offline	Coprocésseur RSA nécessaire aux calculs
Application tierce – environnement multi-applicatif	Décision des équipes marketing produit sur la nécessité d'une carte mutli-applicative	Mémoire de données du produit carte nécessaire aux données EMV, aux nombres de clés (bi-clé par application), à l'historisation des transactions
Partage des données et fichier d'historisation	Décision des équipes Gestion du Risque et Lutte contre la Fraude	Mémoire de données du produit carte nécessaire

Les fournisseurs du produit carte (personnalisateurs) devront satisfaire aux besoins identifiés, et proposer des produits agréés ou certifiés par les réseaux Mastercard, Visa ou réseau domestique (ex : GCB).

Les informations fournies renseignent au minimum les points suivants :

- numéro d'agrément
- standard de référence
- application agréée
- identification du composant et du logiciel de base
- configurations possibles

¹⁰ Dans le cadre de l'intégration d'un nouveau partenaire (réseau domestique français)

Mise en application en France :

Une prérogative de la Banque de France stipule obligatoire l'authentification dynamique de la carte pour toute transaction domestique à compter du 1^{er} janvier 2006¹¹. Tout nouveau projet ouvert en France impliquera :

- soit des cartes à autorisation systématique (authentification dynamique assurée par le front-office)
- soit des cartes DDA, nécessitant la présence d'un crypto-processeur lors du choix technologique du produit

5.3. Définition du Profil EMV

Pour chaque type de carte émis, un profil EMV doit être élaboré pour définir les caractéristiques fonctionnelles de la carte. Ce profil doit être construit à partir des documents de définition proposés par les réseaux Mastercard, Visa, Réseaux nationaux et chef de file des partenaires. Par ailleurs, ces réseaux ont défini des profils type afin de faciliter la constitution du profil.

Action EMV – profil EMV

Fonctionnalité EMV	Expression du Besoin	Mise en œuvre
Choix du profil de base EMV – définition des données fixes	Recommandations et prérogatives des réseaux	Documents de référence des réseaux : <ul style="list-style-type: none"> - Visa Smart Debit and Credit EU Personnalisation Templates - M/Chip 4 Issuer Guide Paramater Management - Autre document de référence selon le pays de la filiale (organisme national)
Choix des données de perso – définition de données sécuritaires de la carte	Choix des équipes Gestion du Risque et Lutte contre la fraude	Valorisation des données : <ul style="list-style-type: none"> - ADA (Risk management carte) - IAC (Risk management carte) - Données SDA à signer (sécurisation carte) - Contrôle de flux (LCOL/UCOL... risk management carte) - CVM List
Choix des données de perso – définition de services cartes	Choix des équipes marketing	Valorisation des données : <ul style="list-style-type: none"> - AUC (type de services associés à la carte)

La valorisation de l'ensemble de ces données constitue le profil EMV complet (profil de base et données personnalisables) propre à tout produit carte EMV. Ces éléments doivent être fournis au(x) sous-traitant(s) pour engager la personnalisation de la carte.

¹¹ sous réserve de modification de la BdF

Mise en application en France :

Fonctionnalité EMV	Expression du Besoin	Mise en œuvre
Choix du profil de base EMV – définition des données fixes	Recommandations et prérogatives du GCB	Document « Personnalisation des données des applications de paiement et retrait de la carte CB EMV »

Le contexte interbancaire français présente la particularité d'avoir sa propre application domestique. Par conséquent, une carte internationale émise par Cetelem comporte 2 applications EMV.

Cetelem a à disposition, des documents type s'appuyant sur les recommandations des réseaux (profil types pour lesquels sont définies des données communes aux X applications de la carte, et des données spécifiques à chaque application). L'objet est de fixer le choix et la valeur de certaines données EMV et de permettre le choix du paramétrage pour les données restantes (dites données personnalisables).

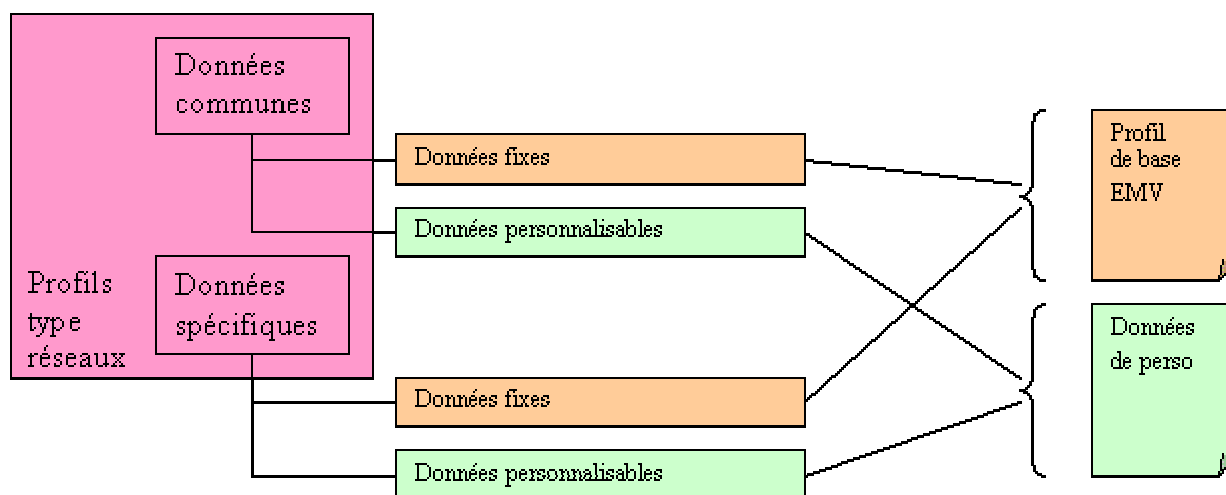


Figure 3: Structure des données EMV – Terminologie Cetelem

5.4. Mise en œuvre de la Personnalisation

Les informations propres à la personnalisation de la carte doivent être fournies aux personnalisateur via des canaux de communications garantissant l'intégrité et la confidentialité des données échangées. Le schéma d'échange entre les différents champs d'action est le suivant :

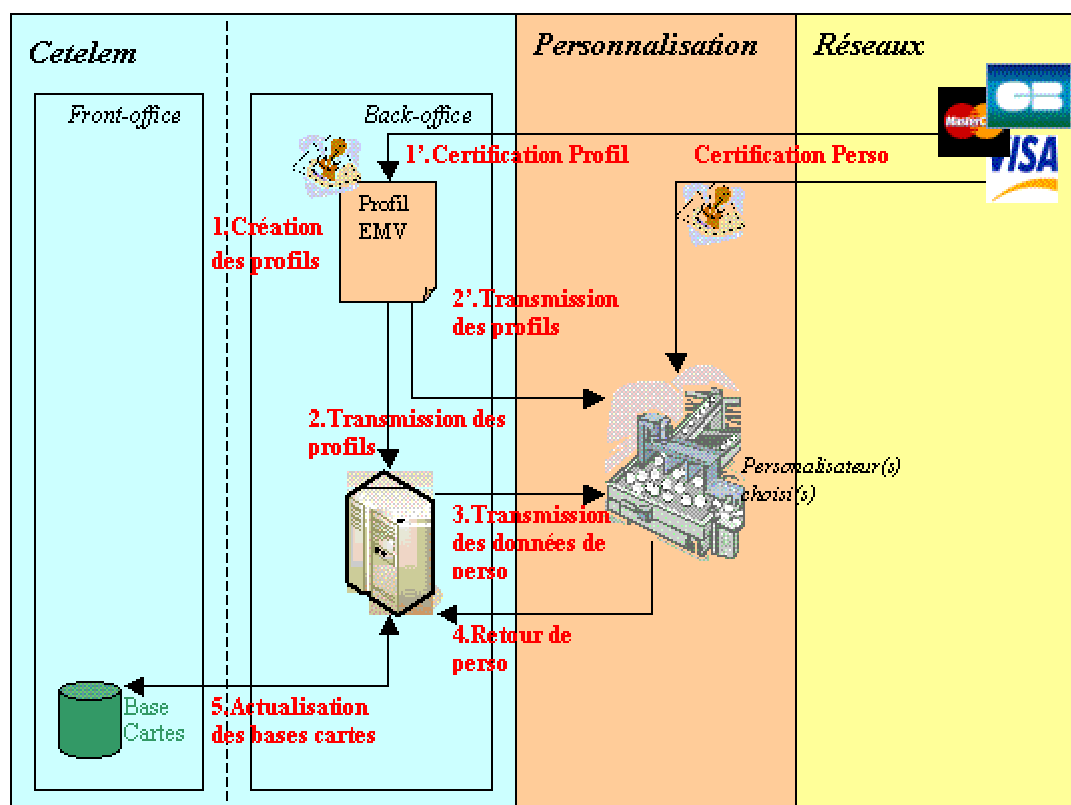


Figure 4: mise en oeuvre de la personnalisation

Action EMV

Fonctionnalité EMV	Mise en œuvre
Création des profils EMV	Prise en compte des profils EMV constitués au préalable (§ précédent)
Certification du profil	Cf. §7
Choix d'un personnalisateur agréé	Contrat de sous-traitance
Transmission des données de personnalisation	Définition des interfaces entre le Back-office et la personnalisation
Contrôle de la personnalisation	Réception et analyse des compte-rendus de fabrication
Actualisation Front et Back-Office	Mise à jour des données base cartes des serveurs Front et Back-office

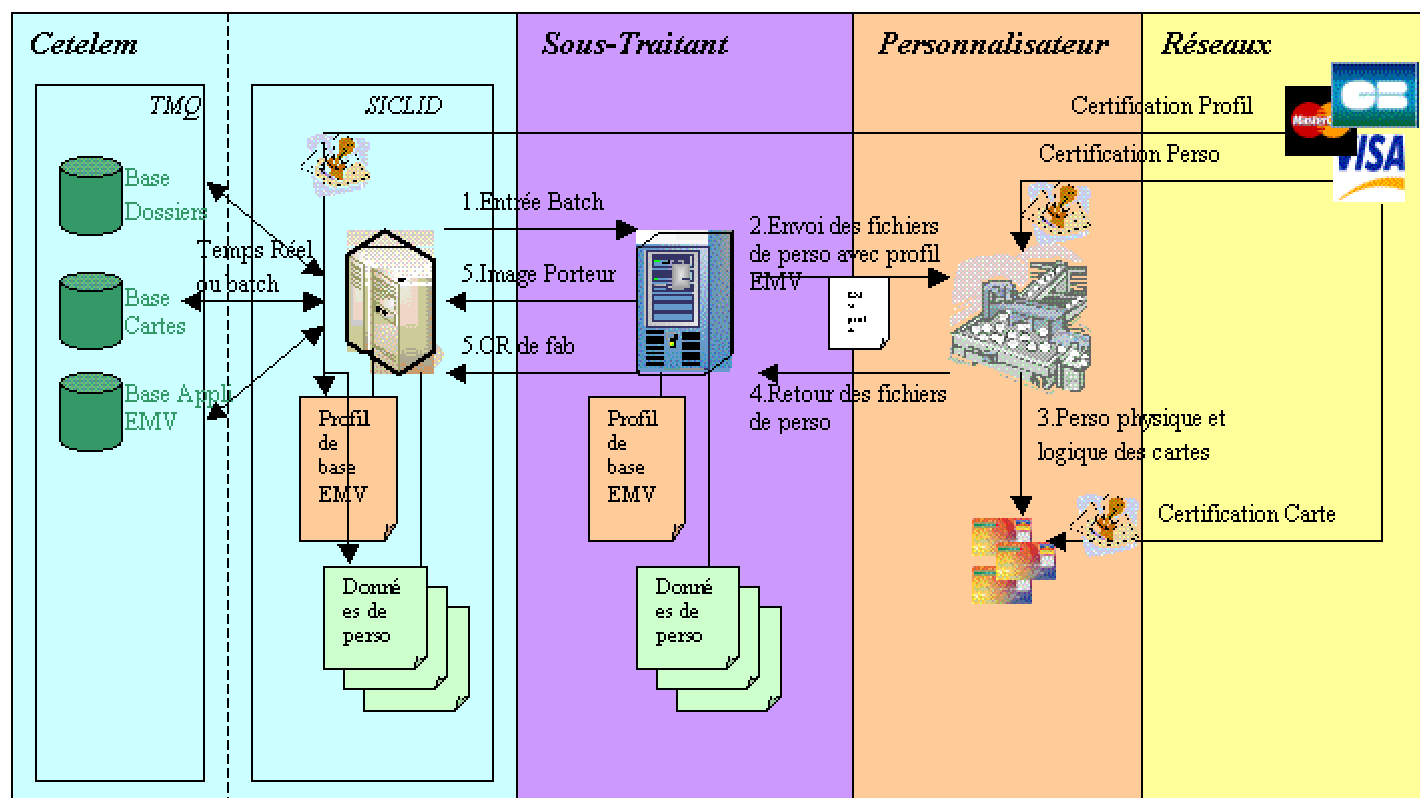
Mise en application en France :

Figure 5: mise en œuvre de la personnalisation Cetelem France

A chaque nouvelle création carte effectuée sur SICLID, un flux batch (ou temps réel) est envoyé au sous-traitant local (Experian ou Atos pour le contexte français) reprenant l'ensemble des éléments nécessaires à la création carte, les éléments propres à la carte issus de la base 'carte', à savoir n° de carte, date expiration, code service..., ainsi que les éléments EMV de personnalisation. Ces éléments constituent le profil EMV défini auparavant avec le profil de base EMV –non modifiable et fourni une seule fois avec le sous-traitant, et les données de personnalisation – modifiables et fournies à chaque modification.

Le sous-traitant reçoit les fichiers, qu'il consolide des données EMV (profil de base), avant de les envoyer au(x) personnalisateur(s) avant la personnalisation physique des cartes.

Un compte-rendu de fabrication est envoyé en retour vers SICLID, reprenant l'ensemble des éléments personnalisés sur la carte afin de contrôler la cohérence des données et stocker dans la base Appli EMV de TMQ (données fixes nécessaires aux contrôles des demandes d'autorisation et les données personnalisables en retour de fabrication).

5.5. Gestion des Clés

La mise en œuvre d'EMV nécessite la mise en place de services de génération, de gestion et de distribution des clés, notamment autour de l'utilisation de bi-clés RSA et de la certification des clés publiques émetteur. Cette gestion implique :

Actions EMV

Fonctionnalité EMV	Mise en oeuvre
Génération de paires de clés RSA émetteur	Prise en charge par la filiale ou le chef de file partenaire
Stockage des clés privées émetteur	Prise en charge par la filiale ou le chef de file partenaire, le personnalisateur, l'équipe monétique et le RSSI
Transmission sécurisée des clés publiques émetteur à l'autorité de certification (Mastercard, Visa ou réseau domestique)	Prise en charge par la filiale ou le chef de file (et RSSI pour les filiales)
Génération de paire de clés RSA carte pour l'authentification dynamique et/ou le chiffrement PIN offline (DDA ou CDA)	Prise en charge par le personnalisateur
Tirage des clés EMV (de test – pour les phases de qualification et certification, et de production)	Prise en charge par la filiale ou le chef de file partenaire, le personnalisateur, l'équipe monétique et le RSSI
Imposition sur le HSM (Host Security Module)	Prise en charge par la filiale ou le chef de file partenaire, le personnalisateur, l'équipe monétique et le RSSI

Mise en application en France :

La certification des clés EMV doit être effectuée auprès de l'autorité de certification AC CB-EMV pour les applications domestiques. L'imposition des clés se fait sur des BNT.

Le GCB met à disposition des services, basés sur l'outil OGDC, permettant de gérer et distribuer les clés nécessaires à la mise en œuvre du projet.

5.6. Certification et Agrément

La production carte est soumise à la certification et agrément EMV des réseaux internationaux. Mastercard et Visa ont mis en place une procédure de qualification des cartes EMV qui porte dans un premier temps sur le profil papier, et ensuite sur des cartes spécimen. L'agrément final conduit à l'ouverture des flux EMV des réseaux sur les BIN déclarés.

Action EMV

Fonctionnalité EMV	Mise en œuvre
Ouverture d'un projet EMV	Contact auprès des interlocuteurs des réseaux Mastercard, Visa, et autre organisme national, puis saisie des dossiers d'ouverture : <ul style="list-style-type: none">- plan de migration- questionnaires de personnalisation- tables des codes actions émetteur- paramètres STIP
Validation des profils EMV de cartes à émettre	Contact auprès des services de qualification des réseaux et chef de file partenaire
Validation des cartes spécimen	Contact auprès des services de qualification des réseaux et chef de file partenaire
Certification et agrément final de l'émission carte	<ul style="list-style-type: none">- Validation bout en bout en production (uniquement Mastercard)- Ouverture des flux EMV des réseaux

6.EXPLOITATION CARTE : DESCRIPTION DETAILLEE

6.1. Schéma Global de l'Exploitation Cartes

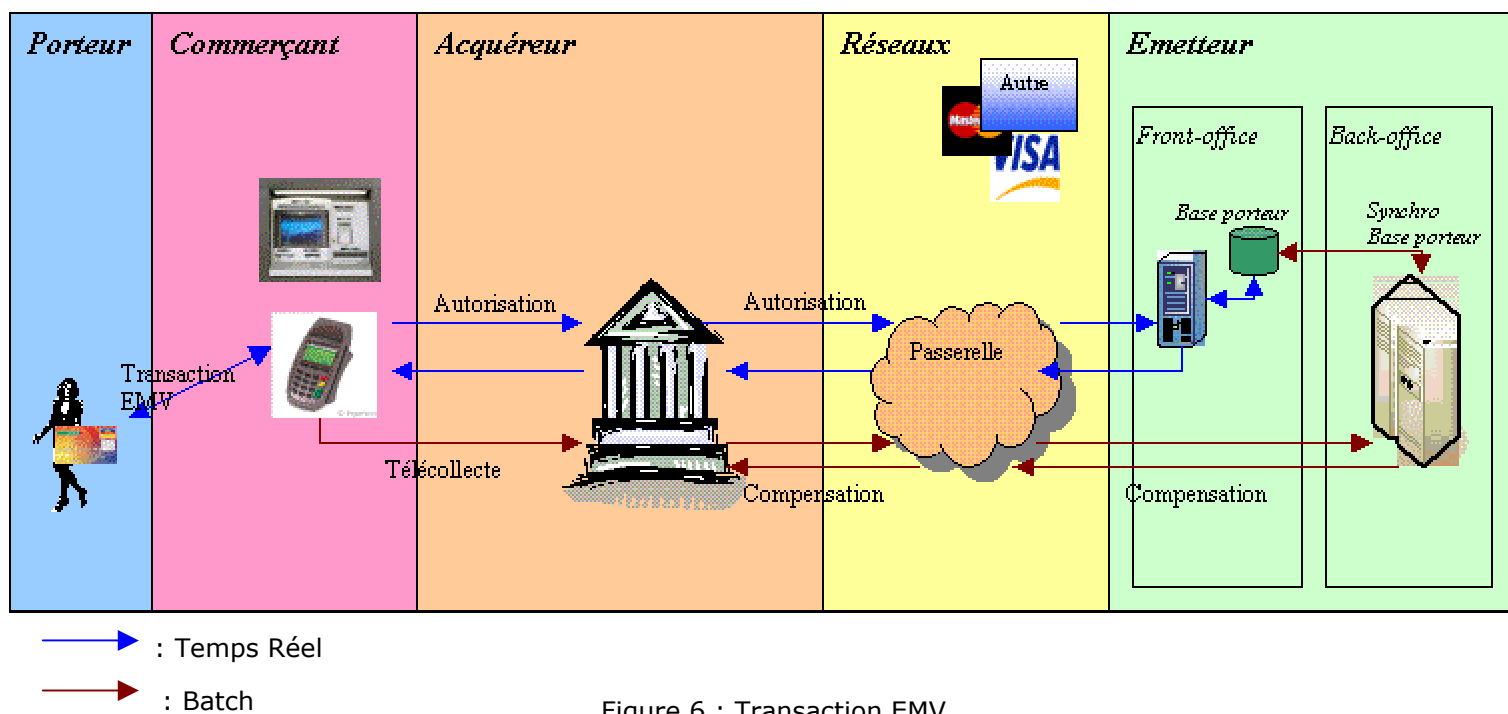


Figure 6 : Transaction EMV

6.2. Domaine Front-Office

Le serveur d'autorisation doit assurer les contrôles et la réponse à une demande d'autorisation. Les données EMV de la transaction remontées permettent le contrôle du contexte de la transaction et les éléments sécuritaires de la transaction.

Le domaine front-office se décompose schématiquement de la façon suivante :

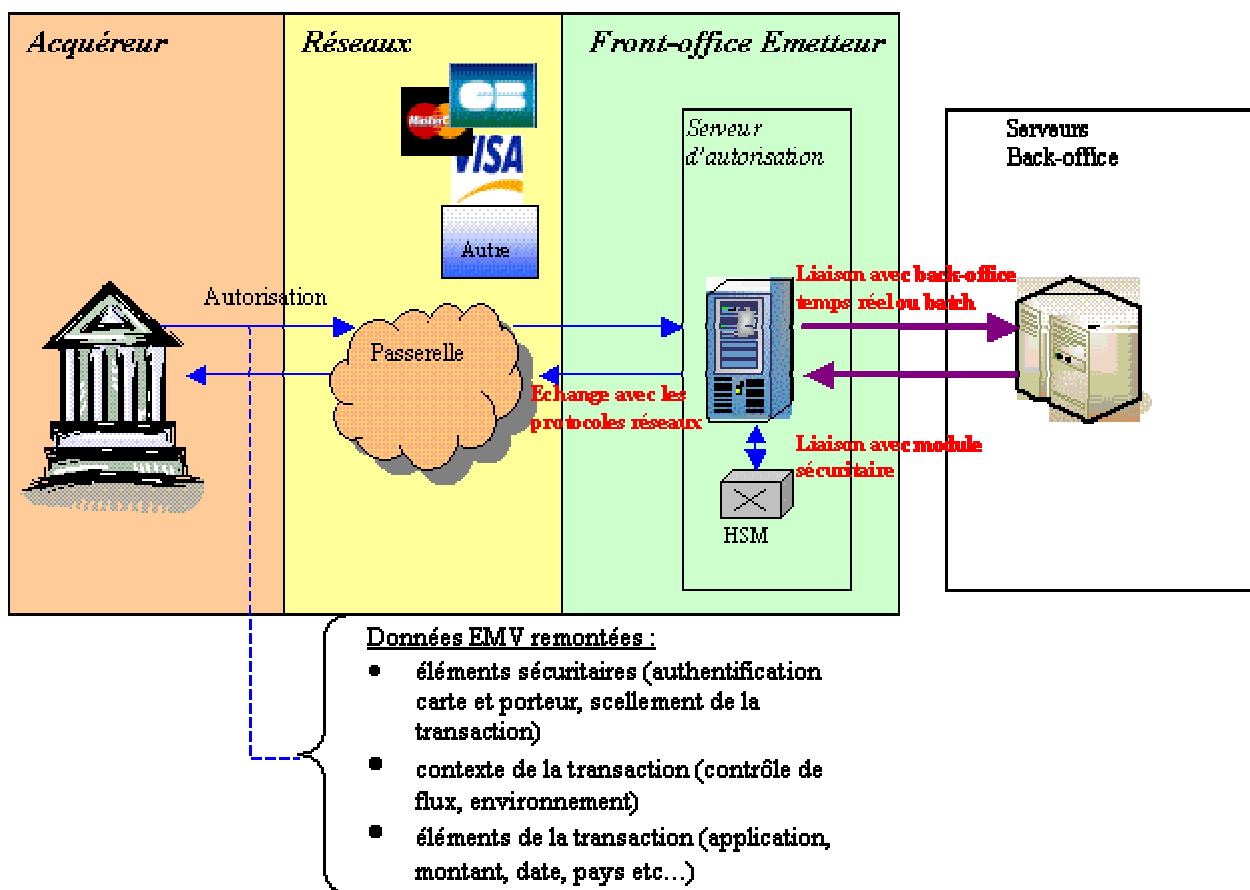


Figure 7: schéma général front-office

6.2.1. Fonctionnalités sécuritaires et protocolaires

Le serveur d'autorisation est en liaison directe avec les réseaux d'acquisition et doit être conforme aux spécifications afin d'interpréter les données EMV remontées dans les demandes d'autorisation.

Il doit permettre les fonctionnalités sécuritaires suivantes :

- Authentification carte : contrôle des cryptogrammes remontés lors des demandes d'autorisation – vérification de l'ARQC – vérification de l'i-CVV
- Authentification émetteur : génération des cryptogrammes en réponse à la demande d'autorisation – ARPC, MAC de post-modification

Ces fonctionnalités sont mises en œuvre à l'aide d'un module sécuritaire (HSM en général).

Action EMV – Front-office – Sécurité et protocoles

Fonctionnalité EMV	Mise en œuvre
Interface avec les passerelles	Conformité de l'interface avec les spécifications propres à chaque réseau
Authentification carte	Algorithme de contrôle 3DES et jeu de clés symétriques chargés sur le HSM
Authentification émetteur	Algorithme de génération 3DES et jeu de clés symétriques chargés sur le HSM
Contrôle des formats	Algorithme de contrôle sur les formats EMV

6.2.2. Contrôle des données EMV d'autorisation

Un ensemble de contrôles propre aux données EMV remontées doit être mis en place afin d'accorder ou non la transaction (et d'octroyer son financement) en concordance avec les données cartes présentes sur la base porteur. A cette fin, une liaison entre le front-office et le back-office doit permettre l'accès à ces données carte (en temps réel ou batch).

Action EMV – Front-office – Contrôle et analyse des données EMV

Fonctionnalité EMV	Mise en œuvre
Contrôle des données EMV de la transaction dont (voir le tableau détaillé ci-dessous) :	Algorithmes de contrôle

Détail des contrôles EMV	Fonctionnalité mise en œuvre
Exploitation AID	- Validité de la sélection de l'application
Exploitation AIP	- Analyse de la conformité de l'environnement transactionnel face aux fonctionnalités cartes disponibles
Cohérence AUC (donnée issue de la base porteur)	- Analyse de la conformité de l'environnement transactionnel face aux services cartes autorisés

Exploitation résultats traitement microcircuit	<ul style="list-style-type: none"> - Contrôle des traitements opérés par le terminal sur la puce
Exploitation de la TVR	<ul style="list-style-type: none"> - Résultat authentification offline carte - Contrôle application (version, date validité/expiration carte, services autorisés, 1^{ère} utilisation) - Information authentification porteur - Contrôle de flux (limite transactions offline autorisées atteinte, LCOL, UCOL) - Information authentification émetteur et script
Exploitation de la CVR	<ul style="list-style-type: none"> - Résultat authentification offline carte - Information authentification porteur - Contrôle de flux - Information authentification carte/émetteur et script lors de la dernière transaction
Exploitation des Résultats des contrôles sécuritaires effectués par le frontal monétique	<ul style="list-style-type: none"> - Authentification Carte (ARQC, i-CVV)

6.2.3. Fonctionnalité de post-modification

La norme EMV autorise la modification de données puce postérieure à la personnalisation (dit post-modification). Plusieurs commandes sont disponibles selon les spécifications (cf. EMVCo), notamment la mise à jour des données, blocage carte, blocage application, déblocage PIN, ..., qui permettent la mise en place de fonctionnalités supplémentaires telles que la gestion des plafonds carte, la maintenance des données carte, la lutte contre la fraude (perte, vol, contrefaçon) ou le risque porteur (abusif, surveillance).

Le contrôle des bases porteurs permet de positionner l'envoi de script en réponse à la demande d'autorisation selon les conditions d'utilisation propres à la politique de gestion risque et de lutte contre la fraude.

Action EMV – Front-office et post-modification

Fonctionnalité EMV	Mise en œuvre
Gestion script de post-modification	Contrôle des bases porteurs back-office ; appel du module d'envoi de script et génération données sécuritaires via HSM

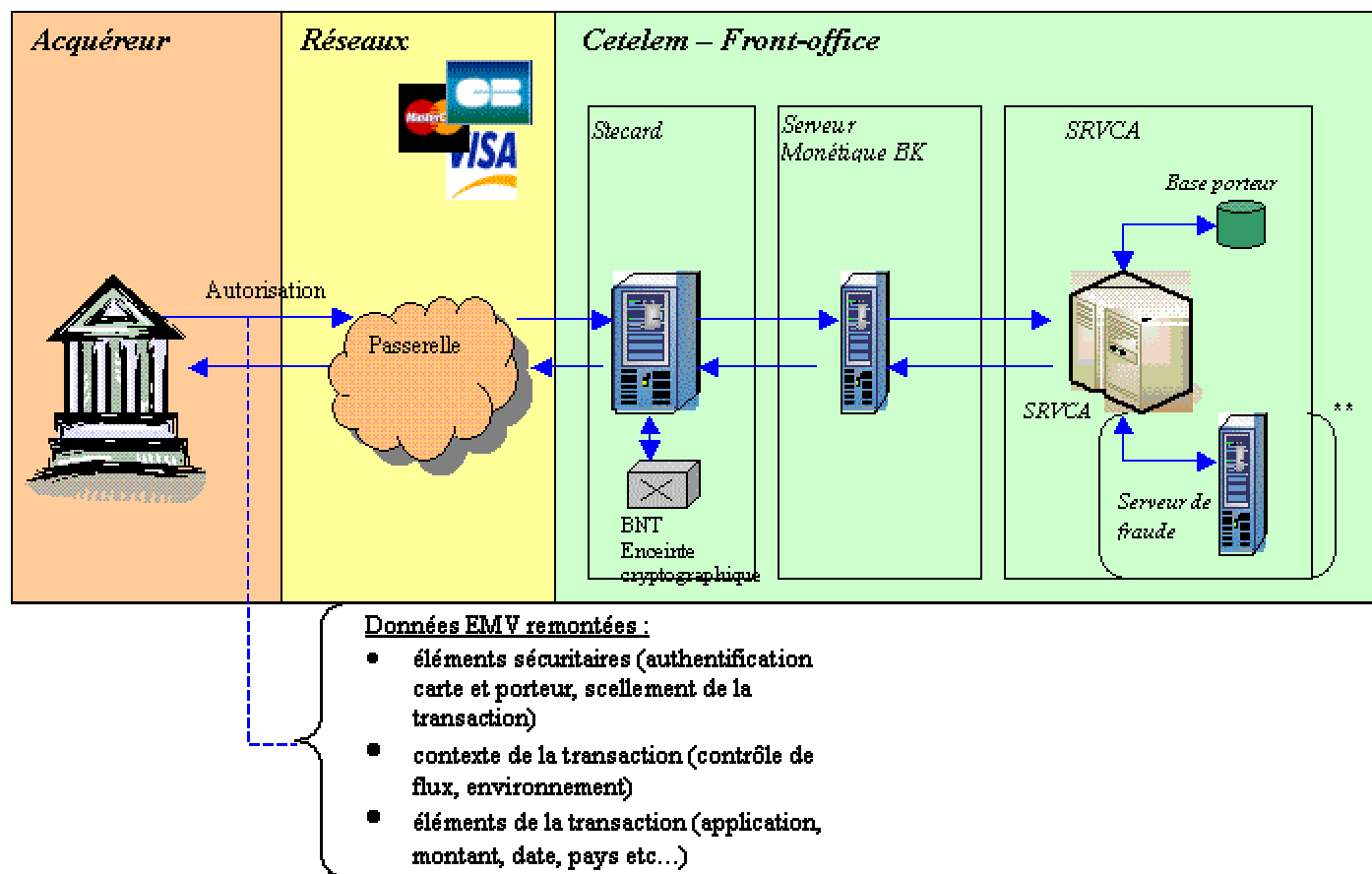
Mise en application en France :

Figure 8 : Front-Office France

(**) : Le serveur de cartes s'appuie également sur un serveur de fraude pour délivrer l'autorisation. Ce serveur est actuellement en place pour CEFI (carte Teoz), et partiellement le Portugal et le Mexique. Cette structure s'inscrit dans le projet de mutualisation front-office.

➤ **Frontal monétique – Stecard**

Stecard assure l'interface entre les réseaux interbancaires (Mastercard via EPSNet, Visa via VisaNet, GCB via RSB) et le serveur d'autorisation.

Les fonctionnalités sécuritaires du frontal monétique sont mises en œuvre à l'aide de BNT. De plus, Stecard contrôle le format des messages entrants et sortants (dont le format des données EMV) et convertit les messages au format supporté par la passerelle (serveur monétique BK).

Action EMV – Frontal monétique – Sécurité et protocoles

Fonctionnalité EMV	Mise en œuvre
Interface avec les protocoles réseaux	Stecard (STUR RSB, spécifications EPSNet et VisaNet)
Authentification carte et émetteur	Stecard + BNT
Conversion champ EMV au format serveur monétique BK	Module de conversion Stecard

➤ **Serveur monétique BK**

Le serveur monétique BK est une passerelle entre le frontal monétique et le serveur d'autorisation, associant à un AID remonté d'une demande d'autorisation un code application EMV Cetelem. Il convertit les messages au format supporté par le serveur de cartes (SRVCA).

Action EMV – Serveur monétique BK

Fonctionnalité EMV	Mise en oeuvre
Passerelle Stecard – SRVCA	Tables des correspondances d'application chargées
Conversion champ EMV au format SRVCA	Algorithme de conversion

➤ **Serveur de cartes SRVCA**

Il assure l'ensemble des contrôles des données transactionnelles EMV (contexte transaction, résultats, etc...) et contrôle les données bases porteurs sur SICLID.

Action EMV – Serveur de cartes SRVCA – base porteur – frontal monétique

Fonctionnalité EMV	Mise en oeuvre
Gestion script de post-modification	Analyse de la table 'décision contrôles réglementaires' et appel du module d'envoi de script. Génération du MAC.

➤ **Serveur de fraude**

Le serveur de fraude exécute un ensemble de contrôle des données EMV selon les règles de détection fraude et filtrage. Les contrôles EMV s'inscrivent dans un système de compteurs d'alertes afin de détecter soit un dysfonctionnement de la carte, soit de la fraude. Ces compteurs concernent les mécanismes sécuritaires de l'authentification de la carte par le terminal et l'authentification de l'émetteur par la carte.

Selon la nature et le contexte du projet, des contrôles supplémentaires peuvent être implémentés sur le serveur de fraude.

Action EMV – Serveur de Fraude

Fonctionnalité EMV	Mise en oeuvre
Contrôle et exploitation des données EMV (voir le tableau détaillé ci-dessous) :	Algorithme de contrôle (détection et filtres)

Détail des contrôles EMV	Fonctionnalité mise en oeuvre
Exploitation de la TVR	<ul style="list-style-type: none"> - Echec authentification carte - Pas de code confidentiel saisi - Données carte manquantes - CVM non reconnu

	- Application carte non valide
Exploitation de la CVR	- Echech authentification émetteur
Exploitation des Résultats des contrôles sécuritaires effectués par le frontal monétique	- Echech contrôle ARQC

6.3. Domaine Back-Office

Le système back-office doit permettre de traiter la compensation, la gestion des litiges (chargesback), le financement, la mise en opposition ainsi que les scripts EMV (ou post-modification).

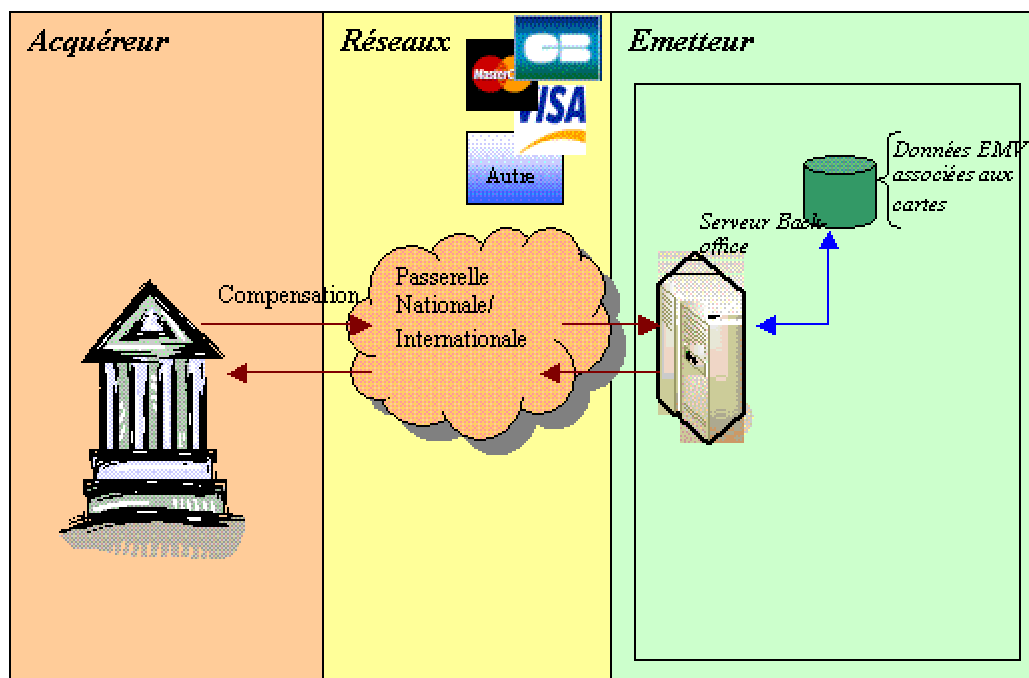


Figure 9: Schéma Back-office

6.3.1. **Gestion administrative des cartes**

L'exploitation des cartes en phase d'utilisation peut inclure des fonctions administratives de réhabilitation (cf. §3.3). Ces fonctions sont mises en œuvre en regard du statut de la carte adossée à un compte. Ces informations sont contenues dans la base porteur Back-office et mises à jour par des circuits propres back-office. Une actualisation régulière des données doit également remonter vers le front-office afin d'assurer une gestion administrative cohérente des cartes.

Cette gestion administrative se traduira par l'envoi de scripts, et optionnellement, par l'utilisation d'équipements dédiés (cf. § 4.3).

Selon la nature et le contexte du projet, des modifications ou évolutions peuvent être apportées dans les échanges entre front et back-office.

6.3.2. Compensation – File Clearing

Les données de l'enregistrement de compensation doivent comporter les éléments EMV (*cf. annexe 5.2*) nécessaires aux fonctionnalités suivantes :

- l'authentification du certificat final de la transaction (fonctionnalité A)
- l'application des règles de transfert de responsabilité (fonctionnalité B) : les règles de Liability Shift s'applique dans la gestion des Chargeback. Le cryptogramme (TC ou AAC) assure l'authenticité de la transaction et permet d'arbitrer les litiges.
- la gestion risque et le suivi porteur (fonctionnalité C) : les informations remontées permettent de suivre l'activité du porteur.

Action EMV – Back-office

Fonctionnalité EMV	Mise en œuvre
Authentification certificat – A	Algorithme de contrôle des données EMV, algorithme de déchiffrement du frontal monétique (authentification carte et intégrité de la transaction) – <i>cf. annexe 5.2</i>
Transfert de responsabilité (Liability Shift) - B	Algorithme de contrôle des données EMV, algorithme de déchiffrement du frontal monétique (authentification carte et intégrité de la transaction) - <i>cf. annexe 5.2</i>
Gestion risque et suivi porteur – C	Algorithme de contrôle et d'exploitation des données EMV - <i>cf. annexe 5.2</i>

6.3.3. Equipements spécifiques EMV –fonctions complémentaires

L'utilisation de terminaux EMV permet d'étendre les fonctionnalités EMV à une gestion administrative carte plus ténue, telles que le déblocage code PIN, l'expertise de la carte, la consultation de l'historiques des transactions, ..., etc.

La mise en œuvre d'une solution nécessite un déploiement de terminaux EMV supportant ce type de fonctionnalités. L'ensemble du parc des terminaux doit être géré en front-office (réponse temps réel des demandes de post-modifications, téléparamétrage) et back-office (déclaration, versioning, base de données, etc.).

Action EMV – Terminaux EMV (optionnel)

Fonctionnalité EMV	Mise en œuvre
<ul style="list-style-type: none">- Réhabilitation carte- Expertise carte- Consultation carte	Déploiement terminaux habilités (Level 1 & 2 EMVCo), gestion front-office des terminaux, évolutions et paramétrage des serveurs.

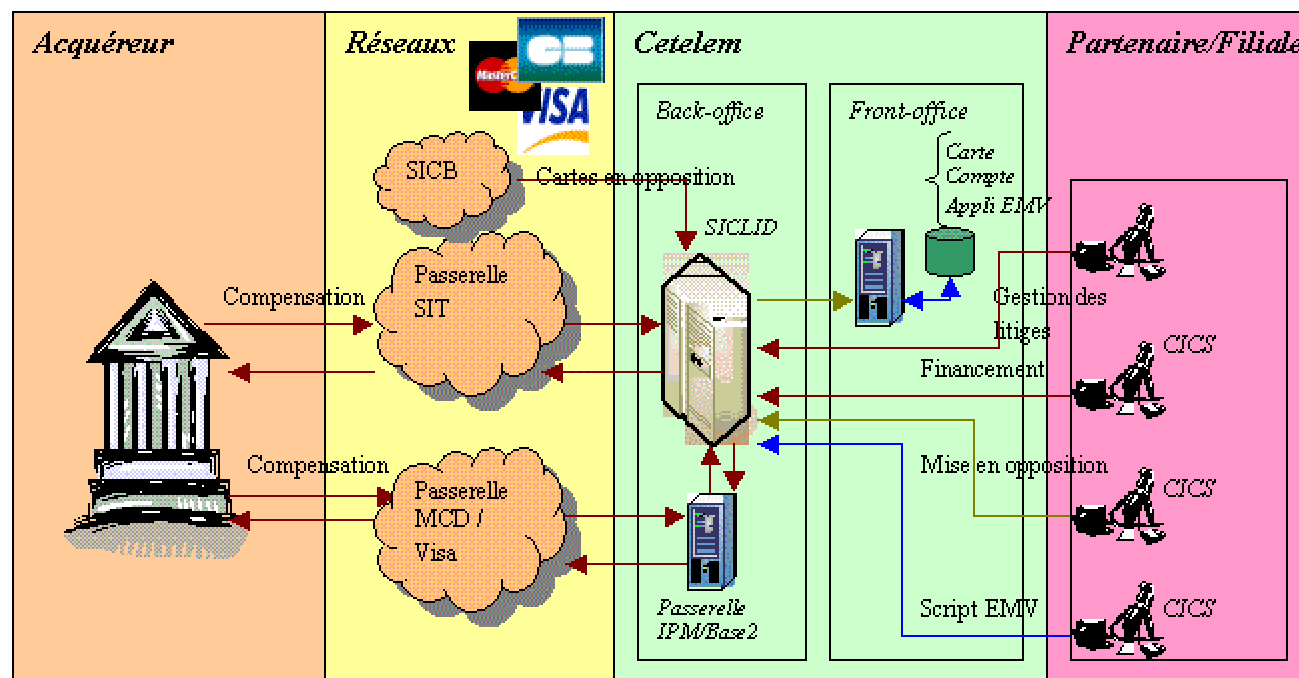
Mise en application en France :

Figure 10: Back-office

A noter que la compensation domestique (transactions en France) utilise le SIT et ne nécessite pas de passerelle entre SICLID et le réseau, contrairement à la compensation pour les transactions à l'international, nécessitant une passerelle entre les réseaux MCD et Visa et SICLID (IPM/Base 2).

Les informations contenues dans la base porteur SICLID sont mises à jour par les circuits CICS des partenaires et filiales, ainsi que le réseau SICB pour les cartes des partenaires (cartes en opposition).

7. ANNEXES


7.1. Annexe A : Migration EMV2000

Tout nouveau projet EMV se doit d'être conforme aux spécifications Mastercard et Visa basées sur la norme EMV2000, à savoir respectivement M/Chip 4 et Vis 1.4. Il est important de noter que ces spécifications, bien que dérivées de la norme EMV2000, diffèrent sur certains points (structure et longueur de CVR, méthode de calcul de clé de session, ...) et impliquent un traitement des données EMV propre aux gammes de cartes Mastercard et Visa.

Par conséquent, l'attention doit être portée aux filiales ou nouveaux partenaires émettant des cartes Visa et Mastercard, pour lesquels une gestion double de la filière technique EMV est obligatoire (distinction sur le front et back-office des cartes Visa et Mastercard)

Cas particulier de la France :

Lors de l'émission des premières cartes EMV, un accord avait été conclu entre Visa et Mastercard pour permettre aux banques françaises d'émettre indifféremment des cartes Visa ou Mastercard sur des spécifications communes dérivées de la norme EMV 96 (MCR 1.3.2 : Minimum Card Requirements, spécifications issues de Vis 1.3.2). Cet accord n'a pas été reconduit pour EMV2000 et contraint les banques duales (émettant des cartes Visa et Mastercard) à gérer la migration d'une base applicative¹² MCR 1.3.2 vers une base Vis 1.4 pour les cartes Visa et vers une base M/Chip 4 pour les cartes Mastercard.

		EMV96 – Specs disponibles		Migration	EMV2000 – specs disponibles
Emetteur	Visa	Vis 1.3.2	MCR 1.3.2		Vis 1.4
	Mastercard	M/Chip 2.1			M/Chip 4

Note :

- la migration entre MCR 1.3.2 et Vis 1.4 est mineure
- la migration entre MCR 1.3.2 et M/Chip 4 implique une évolution front-office et back-office pour le traitement des données EMV

7.2. Annexe B : Exploitation Cartes

7.2.1. Table des contrôles effectués par le serveur de cartes SRVCA

Récapitulatif de l'ensemble des contrôles effectués par le SRVCA

Code des contrôles	Ensemble des contrôles	Contrôle à faire pour type de traitement
« 01 »	contrôle routage	TOUS
« 02 »	cohérence date validité	TOUS
« 03 »	contrôle opposition motif inconnu (I)	BO', EMV, PISTE, EARLY OPTION
« 04 »	contrôle opposition motif non parvenu (X)	BO', EMV, PISTE, EARLY OPTION

¹² base applicative : couche logicielle de la puce implémentée selon les spécifications Visa ou Mastercard

« 05 »	contrôle opposition motif fraude (F) sur DAB interne	B0', EMV, PISTE, EARLY OPTION
« 06 »	contrôle opposition motif 3 codes faux (C) sur DAB interne	B0', EMV, PISTE, EARLY OPTION
« 07 »	contrôle opposition motif perte (P)	B0', EMV, PISTE, EARLY OPTION
« 08 »	contrôle opposition motif vol (V)	B0', EMV, PISTE, EARLY OPTION
« 09 »	contrôle opposition motif abusif (A)	B0', EMV, PISTE, EARLY OPTION
« 10 »	contrôle opposition motif fraude (F) hors DAB interne	B0', EMV, PISTE, EARLY OPTION
« 11 »	contrôle opposition motif 3 codes faux (C) hors DAB interne	B0', EMV, PISTE, EARLY OPTION
« 12 »	contrôle réf support	TOUS
« 13 »	date validité avec avalement	TOUS
« 14 »	date validité sans avalement	TOUS
« 15 »	cohérence code service	B0', EMV, PISTE, EARLY OPTION
« 16 »	code service	B0', EMV, PISTE, EARLY OPTION
« 17 »	contrôle application support	EMV, EARLY OPTION
« 18 »	cohérence AIP	EMV
« 19 »	contrôle AUC	EMV, EARLY OPTION
« 20 »	contrôle ATC	EMV
« 21 »	Contrôle_TVR_IAC_denied	EMV
« 22 »	Contrôle_nombre_script_template_72	EMV
« 23 »	Analyse_TVR_ctl_ octet_1_bit_1	EMV
	...	EMV
« 62 »	Analyse_TVR_ctl_ octet_5_bit_8	EMV
« 63 »	contrôle code confidentiel	B0', EMV, PISTE, EARLY OPTION
« 64 »	contrôle égalité limite du nombre de code faux sur DAB interne	B0', EMV, PISTE, EARLY OPTION
« 65 »	contrôle égalité limite du nombre de code faux hors DAB interne	B0', EMV, PISTE, EARLY OPTION
« 66 »	contrôle stricte limite du nombre de code faux sur DAB interne	B0', EMV, PISTE, EARLY OPTION
« 67 »	contrôle stricte limite du nombre de code faux hors DAB interne	B0', EMV, PISTE, EARLY OPTION
« 68 »	contrôle DAB à puces en France	B0', EMV, PISTE
« 69 »	contrôle authentification puce obligatoire	B0', EMV
« 70 »	contrôle authentification puce	B0', EMV
« 71 »	Contrôle CVV	B0'(si piste présente), EMV, PISTE
« 72 »	Contrôle CVV2	MANUEL
« 73 »	DF80 = 01	B0', EMV, PISTE
« 74 »	DF80 = 10	B0', EMV, PISTE
« 75 »	DF80 = 11	B0', EMV, PISTE
« 76 »	DF80 = 20	B0', EMV, PISTE
« 77 »	DF80 = 21	B0', EMV, PISTE
« 78 »	DF80 = 22	B0', EMV, PISTE

« 79 »	DF80 = 23	B0', EMV, PISTE
« 80 »	DF80 = 24	B0', EMV, PISTE
« 81 »	DF80 = 25	B0', EMV, PISTE
« 82 »	DF80 = 26	B0', EMV, PISTE
« 83 »	DF80 = 27	B0', EMV, PISTE
« 84 »	DF80 = 28	B0', EMV, PISTE
« 85 »	DF80 = 30	B0', EMV, PISTE
« 86 »	DF80 = 31	B0', EMV, PISTE
« 87 »	DF80 = 32	B0', EMV, PISTE
« 88 »	DF80 = 40	B0', EMV, PISTE
« 89 »	DF80 = valeur inconnue	B0', EMV, PISTE
« 90 »	Contrôle B0'V2	Uniquement B0'
« 91 »	plafond élémentaire journalier	TOUS
« 92 »	plafond élémentaire journalier non défini	TOUS
« 93 »	plafond élémentaire glissant	TOUS
« 94 »	plafond élémentaire glissant non défini	TOUS
« 95 »	plafond global journalier	TOUS
« 96 »	plafond global journalier non défini	TOUS
« 97 »	plafond global glissant	TOUS
« 98 »	plafond global glissant non défini	TOUS
« 99 »	Gestion scripts	EMV
« 100 »	Contrôle vendeur	TOUS
« 101 »	Contrôle Quasi cash	TOUS

7.2.2. Données EMV en compensation

La présence et l'exploitation des données suivantes est obligatoire en compensation afin de mettre en œuvre les fonctionnalités EMV détaillées §4.2, outre les données existantes dans les enregistrements de compensation actuels.

Données EMV obligatoires	TAG EMV correspondant	Fonctionnalités EMV mises en œuvre en compensation
AID	9F06	A, B, C
ATC	9F36	A, C
Date fin validité	5F24	A, C
Application Cryptogram	9F26	A, B, C
AIP	82	A, C
PAN	5F34	A, B, C

Unpredictable number	9F37	A
IAD (dont CVR)	9F10	B, C
CID	9F27	A
TVR	95	B, C
Issuer scripts result		C

7.2.3. Identification EMV des données utilisées en autorisation et compensation non-EMV

Equivalence EMV des données existantes en autorisation et compensation .

Données existantes	Equivalence EMV (TAG)
Identifiant Etablissement donneur d'ordre	9F01
Date locale de transaction	9A
Heure locale transaction	9F21
Code traitement	9C
Code monnaie d'origine	5F2A
Code activité accepteur	9F15
Code pays système acceptation	9F1A
Numéro carte porteur	5A
Mode de lecture de la carte	9F39
Numéro autorisation	89
Montant utilisé pour le calcul certificat	9F02