BULLETIN N°12 V3
ACCEPTATION SANS CONTACT SUR AUTOMATE ET PAIEMENT DE PROXIMITE

DATE D'APPLICATION
1er Juillet 2012

CLASSIFICATION SECURITAIRE

DIFFUSION RESTREINTE		
Création		Sur poste de travail à accès contrôlé
Transmission	*Télécopie*	Oui
	Messagerie interne	Oui
	Messagerie Internet	Chiffrement ou Mot de passe recommandé
	Courrier	Enveloppe simple et nominative
Diffusion		Liste de diffusion gérée par l'émetteur
Impression		Ne doit pas séjourner durablement sur l'imprimante
Reproduction		Nombre minimal de reproductions pour action
Stockage magnétique		Support à accès contrôlé
Stockage papier		Recommandation : Dans un local à accès contrôlé
Destruction		Electronique : effacement simple

FEUILLE DE MODIFICATION

DATE DE MISE A JOUR	PARTIE MODIFIEE (*chap. et page*)	NOUVEL INDICE DE REVISION	DESCRIPTION DES MODIFICATIONS
Décembre 2008		1.1	Version
Novembre 2009		2.0	Intégration de • Payez Mobile • Gestion des BIN, opposition et cumul des transactions après les échanges carte/Terminal • Paramétrage des événements (RTT) • Adaptation de l'édition du Ticket • Sélection de l'application selon la priorité du terminal
Août 2011		3.0	Version EMV sans contacte

Sommaire

ILLUSTRATIONS

1 REFERENCES

1.1 Références documentaires

[MPE52]	MPE version 5.2.2 et bulletins
[MPA52]	MPA version 5.2.2 et bulletins
[VCPS202]	Visa Contactless Payment Specification Version 2.0.2 du 07/2006 including Additions and clarifications Version 3.0 d'Août 2007
[VCPS21]	Visa Contactless Payment Specification Version 2.1.1 du 07/2011
[VCPS14]	VMCPS 1.4
[VSGU12]	Visa Europe Contactless Terminal Guide v1.2 de Mars 2010
[MCPP21]	PayPass - MChip Reader Card Application Interface Specification version 2.1
[MCGU11]	PayPass - Terminal requirements and Implementation guide version 1.1 de février 2007
[MCMb10]	Mobile MasterCard Paypass M/CHIP 4 version 1.0 D'avril 2010
[CB2AA]	Autorisation - CB2A : versions 1.1.2, 1.13, 1.1.4, 1.1.5, 1.1.A et Addendum Paiement en mode sans contact (PSC)
[CB2AT]	CB2A TLC-TLP-GR : versions 1.1.3, 1.1.4, 1.1.5, 1.1.A, 1.1.6, 1.1.B et Addendum Paiement en mode sans contact (PSC) à définir
[CB01]	Spécification générale de la carte « CB dual interface » pour un pré-déploiement 1.0 de 11/2008
[CB02]	Spécification générale de la carte « CB dual interface » pour un pré-déploiement 2.0 de 11/2010
[AEPM01]	Payez Mobile Book 1 – Product definition realease 3.0 d'octobre 2010
[AEPM02]	Payez Mobile Book 2 – Technical Specification realease 3.0 d'octobre 2010
[AEMC30]	Guide d'implémentation Mastercard release 3.0
[[AEVS30]	Guide d'implémentation Visa release 3.0
[AECB30]	Guide d'implémentation pour un mobile CB sur une base EMV (en cours d'étude)
[BOOKA]	Book A – Architecture and generals requirements
[BOOKB]	Book B : Specification Entry Point
[BOOKC2]	Book C-2 : kernel 2 specification (AID Mastercard)
[BOOKC3]	Book C-3 : kernel 3 specification (AID Visa)
[BOOKD]	Book D : Protocole de communication sans contact
[BUL15]	Bulletin 15 : Gestion du multi-commerce (à paraître)

1.2 Références documentaires par produit sans contact

	Acceptation	Emission			
Référence documentaire CB	**Application sans contact**	**Carte ou mobile CB**	**PayPass**	**Payez Mobile**	**PayWave**
Bulletin 12 V3	- Book A : Architecture et exigences générales - Book B : Specification Entry Point - Book C-2 : kernel 2 specification (AID MasterCard) - Book C-3 : kernel 3 specification (AID Visa) - Book D : Protocole de communication sans contact	**Carte** Référentiel « CB dual interface » version 1.0 Référentiel « CB dual interface » version 2.0 **Mobile** Paiement CB sur Mobile V 0.1	**Carte** PayPass M/Chip v1.3 PayPass M/Chip v1.4 M/Chip Advance V1.0 **Mobile** Paypass -Mobile MasterCard M/Chip V1.0	**Mobile** - Payez Mobile Version 2.1 de Juillet 2009 - Payez Mobile V3.0 d'octobre 2010.	Carte • Visa Contactless Payment Specification Version 2.0.2 Visa Contactless Payment Specification Version 2.1.1 Mobile VMCPS Version 1.4

1.3 Terminologie

Combinaison	Désigne le couple {AID – Kernel ID}
Entry Point	Logiciel du terminal permettant le pilotage de la transaction sans contact. Il gère la communication entre le Reader et le terminal pour sélectionner l'application carte, activer les kernels et exploiter les caractéristiques de la transaction sans contact transmises au travers des Résultats.
Kernel	Logiciel applicatif installé dans un système d'acceptation traitant les transactions sans contact. Dans le cadre de cette documentation, deux Kernels sont appelés C-2 (MasterCard) et C-3 (Visa).
Outcome	L'outcome est appelé dans ce document résultat et correspond à des instructions du Kernel précisant la suite des traitements à effectuer pour la transaction en cours
Reader	Le Reader a pour fonction de gérer la communication avec la carte sans contact, et permet la sélection, l'activation, et l'exécution du kernel, la sélection de la CVM et création du résultat final (Outcome) et des paramètres associés. Par ailleurs il assure la gestion des communications avec la carte (pas de réponse carte) durant le déroulement de la transaction.
Résultat du **T**raitement du **T**erminal	Le principe d'analyse des TAC/IAC, quel que soit le kernel, est retenu pour la gestion du sans contact. Les événements identifiés lors du déroulement de la transaction sont enregistrés, dans une donnée appelée **R**ésultat du **T**raitement du **T**erminal (RTT) et utilisé dans l'analyse des TAC/IAC en lieu et place du TVR ou des deux indicateurs du Kernel C-3 (Declined ou online) pour déterminer si la transaction doit être refusée, acceptée ou si une demande d'autorisation doit être transmise.
Terminal	Le terminal gère la saisie du montant par le commerçant et les caractéristiques de la transaction au travers des Résultats (Outcomes) ; il assure le lien avec les autres interfaces et pilote les échanges (autorisation, annulations, télécollecte).

2 PRESENTATION

2.1 Rappel du contexte

Le Groupement des Cartes Bancaires a émis fin 2009 un bulletin 12 v2 afin de prendre en compte le mobile AEPM.
Depuis, les réseaux internationaux ont publié des spécifications Mobile et l'AEPM s'est alignée sur ces spécifications. Dans ce contexte, une mise à niveau du bulletin 12 est nécessaire.

2.2 Objectifs

Ce document propose la liste des exigences minimales devant être respectées par les systèmes d'acceptation CB. Elles concernent

- les caractéristiques des systèmes et points d'acceptation,
- l'architecture des traitements du sans contact,
- le paramétrage des systèmes et points d'acceptation sans contact,
- les échanges entre les systèmes d'acceptation et les acquéreurs
- la mise en œuvre du suivi des incidents.

Le bulletin ne reprend pas les spécifications EMV mais précise le cas échant les options retenues par le système CB ainsi que les aspects fonctionnels non couverts par ces dernières.

Ce bulletin décrit uniquement les aspects qui diffèrent du référentiel contact décrit dans [MPE52] [MPA52].
Il présente le déroulement des transactions de paiement sans contact sur

- des systèmes d'acceptation de paiement de proximité (hors PLBS , Quasi-cash) ;
- des automates de classe 1 CB (CAT 2 et CAT 3) et classe 2.1 ;
- le paiement ;
- ainsi que les fonctions suivantes :
  - les remboursements pour le paiement ;
  - l'affichage du solde carte (permet à certains dispositifs sans contact de proposer le solde sans contact sur un ticket ou à l'écran) ;
  - la gestion des montants dans le Kernel C-3 via la fonction Dynamic Reader limits ;
  - le « Torn Transaction Recovery » (MasterCard) qui permet de redémarrer une transaction interrompue (carte enlevée de la cible au cours de la transaction).

2.3 Champ d'application

Cette version du Bulletin 12 V3 annule et remplace la version V2. Elle s'applique aux systèmes d'acceptation de paiement équipés d'un lecteur :

- Contact/sans contact (cas général),
- Sans contact.

Les systèmes d'acceptation devront être conformes à tous les bulletins CB obligatoires.

Ces points d'acceptation doivent accepter les :

- cartes CB-Visa, CB-MCI (V1, V2), Mastercard et Visa à double interface : contact et sans contact ;
- cartes agréées CB (Visa et MasterCard) à interface sans contact uniquement ;
- Mobile AEPM R1 ;
- Mobile AEPM R3 ;
- Mobile CB;
- Mobile Visa, MCI.

Les fonctions suivantes ne sont pas dans le périmètre de ce bulletin :
Pour Visa [VSGU12] § 4.3.2.

- L'authentification Offline pour autorisation online,
- Cash-back,
- Cash,
- L'issuer Update Processing
- Status check
- Zero value Transaction

Pour MasterCard

- **Data Storage** : Cette fonction sera étudiée dans le cadre d'un projet pilote concernant la billettique ;

3 CARACTERISTIQUES DES SYSTEMES ET POINTS D'ACCEPTATION

3.1 Architecture des systèmes d'acceptation paiement

L'architecture des systèmes d'acceptation paiement s'articule autour de deux applicatifs de paiement étanches

- Contact : application existante dédiée au contact,
- Sans contact : application dédiée au sans contact conforme au présent bulletin.

L'étanchéité des applications impliquera pour toute transaction refusée ou abandonnée, l'enregistrement d'une transaction non aboutie, même lorsqu'il sera proposé au porteur d'insérer sa carte en contact. Le montant de la transaction, en cas d'abandon ou de refus, peut être réutilisé sans ressaisi pour le paiement en cours.

3.2 Adaptations des fonctions du contact au sans contact.

Les fonctions suivantes sont supportées en contact mais doivent être adaptées ou précisées afin qu'elles répondent aux besoins du sans contact.

3.2.1 La gestion des multi-devises

La gestion des devises s'appuiera sur un paramétrage spécifique pour la monnaie concernée. Dans ce cadre, la demande d'autorisation est systématique quel que soit le paramétrage. On appelle devise, toute monnaie différente de l'Euro (Yen, Franc CFA,..).

3.2.2 Multi-commerce / Multi applicatif

Le multi-commerce est une option qui concerne les terminaux autonomes. Elle est applicable en sans contact et son activation s'effectue avant la lecture de la carte. Pour les informations complémentaires il est nécessaire de se reporter au [B15]

3.2.3 Le différé de recouvrement

En sans contact, il n'est pas possible de proposer le débit différé avant d'avoir identifié l'applicatif. L'impossibilité d'interrompre les traitements cartes après la sélection nécessite la finalisation des échanges carte /terminal avant de proposer le différé de recouvrement. La cinématique à appliquer est la suivante :

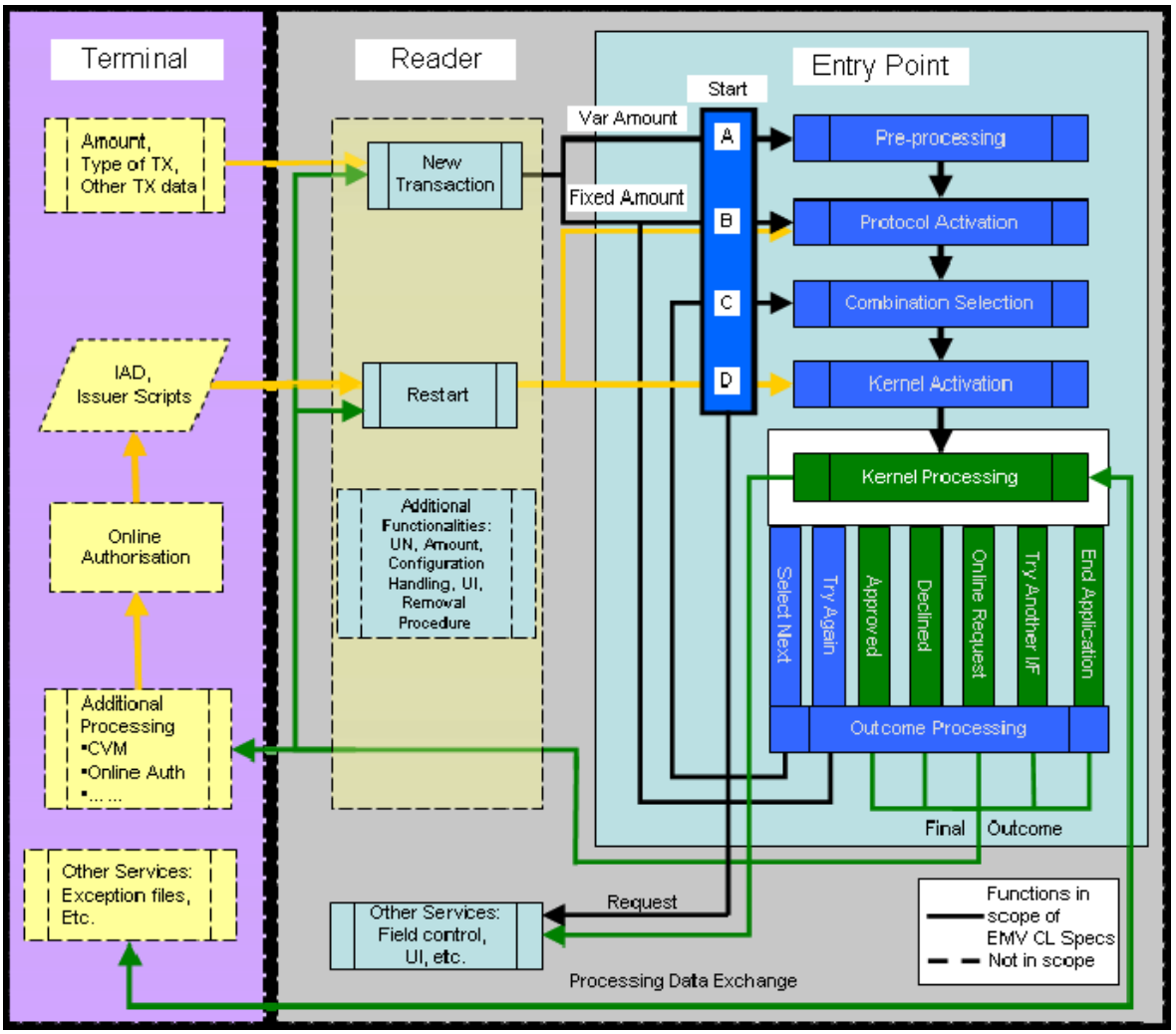
1 Lire la carte sans contact à partir d'un kernel sans contact
2 La transaction sans contact est exécutée et la carte est enlevée du champ,
3 Il est proposé au porteur le différé de recouvrement s'il est activé ;

4 Effectuer tous les traitements cartes fonctionnels du CB 5.2 : Authentification, Gestion risque, finalisation de la transaction.

4 TRANSACTION SANS CONTACT

4.1 Architecture sans contact EMV

Ce schéma, extrait de la documentation EMV, présente l'architecture logique d'une application sans contact EMV (Book A § 5.3)



4.2 Saisie du montant

Le commerçant saisit le montant de la transaction qui sera affiché sur le terminal et le Reader. Le montant de la transaction doit être compris entre le montant minimum et le montant maximum paramétrés par la banque acquéreur dans la table « risque acquéreur » (montant maximum, montant minimum).

- Si le montant est inférieur au montant minimum ou supérieur au montant maximum, il sera proposé au porteur d'effectuer uniquement la transaction

en contact. En introduisant la carte dans le lecteur contact, l'interface sans contact du terminal (qui permet l'activation de l'application sans contact de la carte) doit être désactivée avant la RAZ contact.

- Si le montant est supérieur au montant minimum et inférieur au montant maximum, il sera proposé au porteur d'effectuer la transaction en sans contact. Dans ce dernier cas, le porteur pourra s'il le désire effectuer sa transaction en contact ; pour cela les deux interfaces seront activées.

Le message à afficher est le suivant et concerne l'interface contact et sans contact.

Information	LIBELLE	Commerçant	Porteur
Demande de présenter sa carte pour un montant (« xxx ») dans la monnaie (« yyy »)	PRESENTEZ CARTE xxx « yyy »	X	X

- Si le porteur décide de l'exécution de la transaction en « sans-contact » en présentant sa carte à l'interface sans contact, l'interface contact du terminal sera désactivée ;
- Si le porteur décide de l'exécution de la transaction en « contact » en présentant sa carte au lecteur piste ou puce, l'interface sans contact sera désactivée.

4.3 Le forçage de l'autorisation par le commerçant

Après la saisie du montant, le commerçant a la possibilité de provoquer une demande d'autorisation. Cette fonction est commune au contact et au sans contact et se traduira par l'intervention du commerçant sur une touche de fonction ou par un choix dans un menu.

Pour le sans contact, le bit [4-4] du RTT « Merchant forced transaction online» est positionné à 1.

4.4 Entry Point

Lorsque le montant est saisi et visualisé par le porteur, le traitement de la transaction sans contact débute par l'exécution d'Entry Point [BOOKB] qui assure le pilotage de la transaction.

Les schémas (§4.5, 4.6,4.7)) décrivent l'architecture de l'application sans contact et mettent en évidence les traitements et la position de la carte lors du traitement d'une transaction.

Le fonctionnement d'Entry Point s'organise autour de 4 étapes qui présentent les points de démarrage ou redémarrage de la transaction selon certains critères.

- A : Traitement du pré-processing (Sélectionne les combinaisons {AID et Kernel ID} susceptibles d'effectuer la transaction avant la lecture de la carte selon le montant saisi.
- B : Activation du protocole
- C : Sélection de la combinaison
- D : Activation du Kernel

4.4.1 Représentation graphique Entry Point et appel aux Kernels.

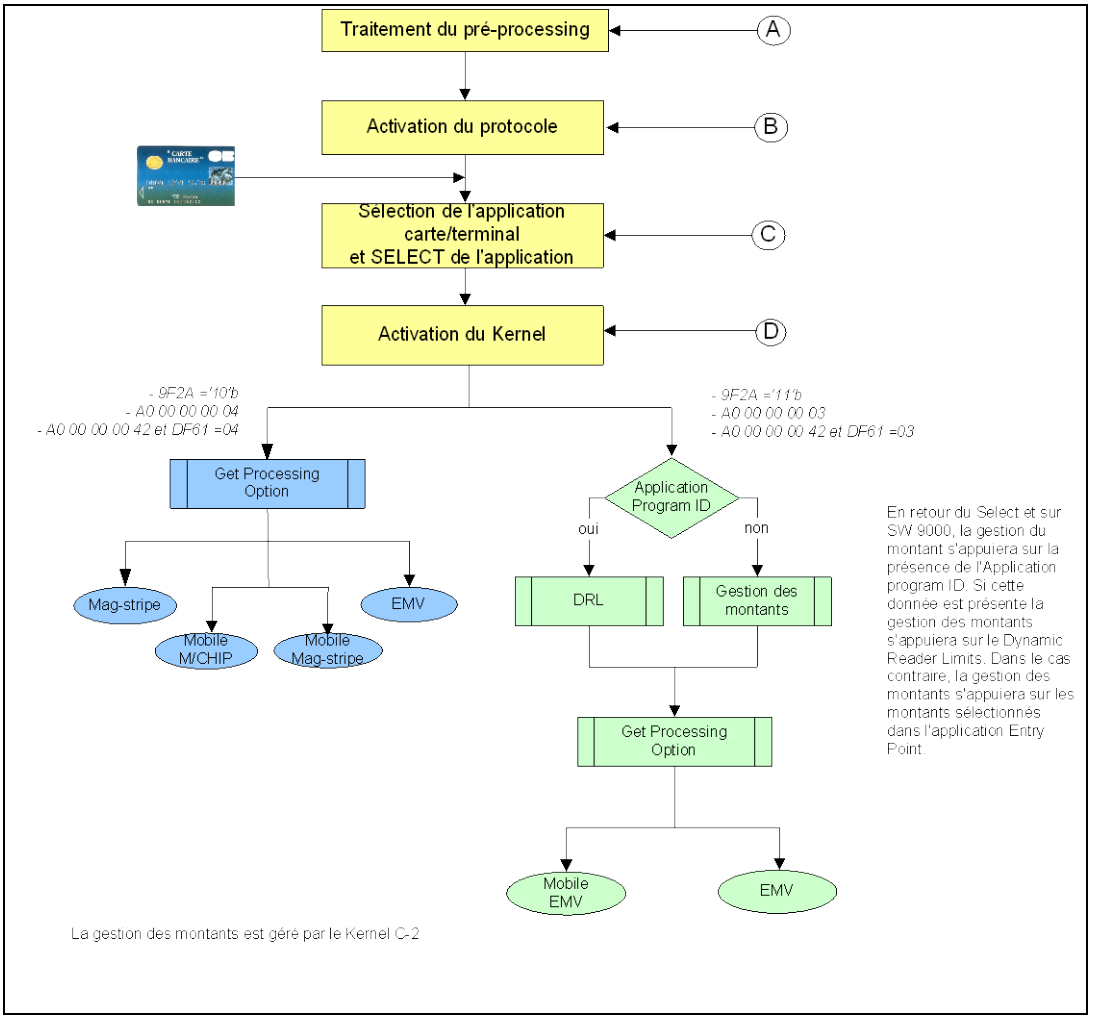


Figure 1 : Entry Point

4.4.2 Traitement du pré-processing (Start A)

Le traitement du pré-processing sélectionne les Combinaisons terminal {AID et Kernel-ID} et positionne les indicateurs de traitement en comparant le montant de la transaction aux données référencées dans le chapitre 6.5.

Si aucune combinaison ne répond aux critères, le résultat est positionné à '**Try Another Interface**' (se reporter à la liste des Résultats [BOOKB].

Pour les combinaisons sélectionnées, le TTQ est valorisé pour chaque combinaison (cf. 6.6) et les bits [2-8 (Online cryptogram required)] et [2-7 (CVM required)] sont valorisées selon les caractéristiques de la transaction.

Chaque contrôle positionnera des indicateurs de traitement qui seront exploités dans les Kernels appelés.

Cette étape est préalable à l'activation de l'interface sans contact. Pour le paramétrage se reporter au 6.4 et pour le détail du traitement se reporter au [BOOKB] EMV § 3.1.

Si le montant est fixe cette étape n'est pas effectuée.

Spécificité Kernel 2 :
Le Kernel 2 n'utilise pas les résultats du pré-processing décrits ci-dessus. Le contrôle du montant est délégué au Kernel. Par conséquent les points suivants sont à noter :

- Le Kernel 2 n'utilisera pas les résultats du pré-processing comme décrit dans le chapitre 3 du [BOOKB] car le contrôle des montants est délégué à ce Kernel ; Ceci induit que les AID traités par le Kernel 2 doivent être inclus systématiquement à la candidate List ;
- Le TTQ n'est pas utilisé par le Kernel 2.

Spécificité Kernel 3 :
Le TTQ est une donnée utilisée uniquement dans le Kernel 3.

4.4.3 Activation du protocole (Start B)

Cette étape est exécutée

- pour débuter une nouvelle transaction avec un montant fixe ;
- pour reprendre une transaction après une demande d'autorisation ou si une carte ou un mobile doit être représenté.

Pour obtenir le détail des traitements se reporter au [BOOKB] EMV § 3.2)

L'activation des échanges se fait lorsque la carte rentre dans le champ électromagnétique du lecteur coupleur. Ces échanges sont conformes au [BOOKD].

Dans ce cadre, la vérification de l'anticollision (présentation de plusieurs cartes simultanément) est assurée par l'interface. Selon l'événement rencontré, des messages seront affichés selon les caractéristiques présentées dans le tableau des résultats [BOOKA] et [BOOKB].

4.4.4 Sélection de la combinaison (Start C)

La sélection de la combinaison est soit, l'étape suivant l'activation du protocole, soit un point d'entrée d'Entry Point (selon le résultat d'un traitement).
L'objet de cette étape est la construction de la candidate List qui identifie les combinaisons communes entre la carte et le Reader. Pour obtenir le détail des traitements se reporter au Book B EMV § 3.3.

4.4.4.1 Structure carte attendue

Les applications carte sans contact possèdent obligatoirement un PPSE (Proximity Payment Systems Environment). C'est à partir du PPSE que débutera la sélection de l'application par le point d'acceptation. Les données du PPSE sont les suivantes :

'6F'	FCI Template			M
	'84'	DF Name ('2PAY.SYS.DDF01')		O
	'A5'	FCI Proprietary Template		M
		'BF0C'	FCI Issuer Discretionary Data	M
			'61' Directory Entry	M
			'4F' ADF Name	M
			'50' Application Label	O
			'87' Application Priority Indicator	C
			'9F2A' Kernel Identifier	C
			'9F29' Extended Selection	C
			'61' Directory Entry	O
			'4F' ADF Name	M
			'50' Application Label	O
			'87' Application Priority Indicator	C
			'9F2A' Kernel Identifier	C
			'9F29' Extended Selection	C
			'61' Directory Entry	O
			'4F' ADF Name	M
			'50' Application Label	O
			'87' Application Priority Indicator	C
			'9F2A' Kernel Identifier	C
			'9F29' Extended Selection	C

Figure 2 : Réponse au SELECT

Un Kernel Identifier (9F2A) est structuré comme suit :

b8	b7	b6	b5	b4	b3	b2	b1	Informations
x	x							Type of kernel
0	0							An international kernel, with a Kernel Identifier assigned by EMVCo and coded in the Short Kernel ID
0	1							RFU
1	0							A domestic kernel, with Kernel Identifier in EMVCo format, coded by the concatenation of the Short Kernel ID and the Extended Kernel ID
1	1							A domestic kernel, with the Kernel Identifier in proprietary format, coded by the concatenation of the Short Kernel ID and the Extended Kernel ID
		x	x	x	x	x	x	Short Kernel ID
		0	0	0	0	0	0	The kernel is associated with the corresponding ADF Name
		0	0	0	0	0	1	Kernel 1
		0	0	0	0	1	0	Kernel 2
		0	0	0	0	1	1	Kernel 3
		0	0	0	1	0	0	Kernel 4
		0	0	0	1	0	1	5th kernel
		–	–	–	–	–	–	
		1	1	1	1	1	1	63rd kernel

Figure 3 : Format du Kernel Identifier – Octet 1

Octet	Informations
2	Extended Kernel ID : • Pour les Kernels Internationaux (Legacy) : RFU • Pour les kernels International (Legacy) : Code monnaie défini dans l'ISO 4217 • Pour les kernels domestiques (Legacy) utilisant un format propriétaire : Propriétaire
3	
4-8	RFU

Figure 4 : Format du Kernel Identifier – Octet 2

4.4.4.2 Sélection de la combinaison

Le système d'acceptation sélectionne les combinaisons supportées à la fois par la carte et le terminal et crée la candidate list avec les éléments suivants qui seront utilisés dans la sélection.

- ADF name
- Kernel ID
- Application Priority Indicator (si présente)
- Extented Selection (si présente)

Un traitement particulier présenté dans le § 4.4.4.4 et concernant les AID CB sera à mettre en œuvre.

Si la liste est vide le Résultat est positionné à « ***End Application*** » Se reporter à la liste des Résultats [BOOKB].

4.4.4.3 Sélection finale de la combinaison

Les AID sélectionnés seront triés selon la priorité de la table des AID. La suite du traitement de cette étape s'appuie sur les règles définies dans le [BOOKB] § 3.3.3.

La sélection s'effectuera comme suit

- Si la liste commune (carte et terminal) ne contient qu'une seule application, l'application sera sélectionnée ;
- Si la liste contient de multiples applications, le terminal sélectionnera
  - L'application de plus haute priorité du terminal ;
  - Si plusieurs applications du terminal ont la même priorité, l'application carte de plus haute priorité (0 ou pas de priorité sont considérées comme les plus basses priorités) ;
  - Si plusieurs applications du terminal ont la même priorité et que les applications carte sont de mêmes priorités, l'application sélectionnée sera l'application carte qui apparaît la première dans le PPSE.

Le SELECT AID prend en compte l' « Extended Selection » si cette donnée fait partie de la candidate List.

La sélection se termine par la commande SELECT AID, puis passage à l'étape suivante §4.4.5.

4.4.4.4 Sélection pour un AID CB

Pour un AID CB, en cas d'absence du TAG 9F2A, la base applicative sera identifiée selon le contenu du TAG propriétaire « DF61 » contenu dans le FCI Issuer Discretionary Data :

- '03' : CB-qVSDC application
- '04' : CB-Paypass M/Chip application

Le Requested Kernel ID par défaut est positionné selon le DF61 aux valeurs suivantes :

Matching AID	Valeur par défaut du Requested Kernel ID
AID CB - Base applicative MasterCard	00000010b
AID CB - Base applicative Visa	00000011b

Figure 5 : Valeur par défaut du Requested Kernel ID pour carte CB

4.4.5 Activation du Kernel (Start D)

L'entry Point active le Kernel selon les résultats de la sélection. Pour obtenir le détail des traitements se reporter au Book B EMV § 3.4.

Cette étape correspond au traitement après la sélection de l'application mais aussi au point de reprise après le résultat émis par un Kernel autre que le Kernel 2 (ce point de reprise n'étant pas utilisé par le Kernel 2)

4.5 Kernel 2 (Mastercard) Mode EMV

Le schéma suivant représente les traitements du Kernel C-2. L'alimentation du RTT identifie les événements rencontrés dans le déroulement du Kernel mais aussi sur les traitements complémentaires qui sont effectués sur le terminal. Ce RTT est positionné comme la TVR mais prend en compte des traitements CB (Bin, Oppositions,..) qui seront rapprochés des TAC/IAC après l'exécution du Kernel pour la finalisation de la transaction.

Informations sur la saisie du code activation sur le Mobile de base applicative MasterCard

La saisie du code peut être demandée par l'application du terminal ou par le mobile.

- Si le montant de la transaction est supérieur au reader CVM required limit, l'application sans contact du terminal transmettra au GEN AC la CVM result [octet 3] valorisée à « Successful ». A la réception de cette valeur l'application mobile répondra avec un statut '9000' et un AAC et transmettra la donnée « **P**OS **C**ardholder **I**nteraction **I**nformation-DF4B » [2-1] positionnée à 1 (Pin required) pour demander la saisie du code au pont d'acceptation.

- Si la gestion du risque du mobile nécessite une saisie de code (quel que soit le montant de la transaction et quel que soit la valorisation du CVM result), le terminal recevra en réponse un AAC, et un SW '9000' et le « **P**OS **C**ardholder **I**nteraction **I**nformation - DF4B » [2-1] positionnée à 1 (Pin required).

La réception de ces éléments provoquera systématiquement la valorisation du résultat '**Try Again**'.

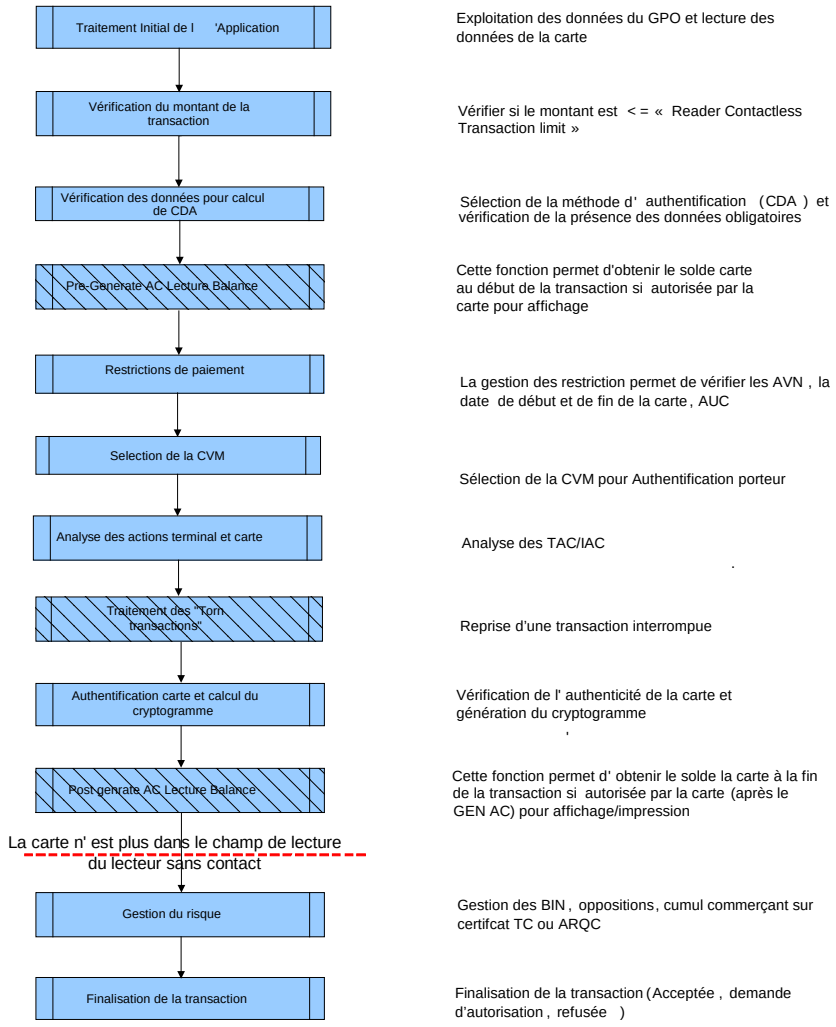


Figure 6 : Kernel 2 – Traitement EMV sans contact

Les blocs optionnels sont hachurés

4.5.1 Traitement initial de l'application

Durant cette étape, le kernel récupère l'AIP et l'AFL de la carte avec la commande GPO. En fonction de l'AFL, les données de la carte seront lues via les commandes Read Record et Get Data.
Durant cette étape, l'application vérifie si le dispositif permet l'authentification du porteur et si la carte supporte le CDA comme méthode d'authentification. En cas d'absence de l'AIP et de l'AFL, le bit [4-4] du TVR/RTT « ICC data Missing » est positionné à 1.

Remarque : la gestion des montants est assurée par le Kernel 2 et non pas par Entry Point.

4.5.2 Vérification du montant de la transaction

Le kernel vérifie si le montant de la transaction est inférieur ou égal au « Reader Contactless Transaction Limit ». Si ce n'est pas le cas, le résultat rendu par le kernel (Résultat) est « Select Next » et le reader revient au Start C.

4.5.3 Vérification des données cartes pour calcul de CDA

Le kernel vérifie si la carte possède bien les données nécessaires au calcul du CDA .Si des données nécessaires au calcul du CDA sont identifiées comme manquantes par le terminal le bit [1-6] « ICC data Missing » et le bit [1-3] « Combined dynamic authentication failed »des TVR/RTT seront positionnés à 1.
Ces données sont les suivantes :

- CA Public Key Index (Card)
- Issuer Public Key Certificate
- Issuer Public Key Exponent
- ICC Public Key Certificate
- ICC Public Key Exponent
- Static Data Authentication Tag List

Si la zone de donnée[1] ne permet pas l'enregistrement des données pour l'authentification offline**,** le bit [1-3] « Combined dynamic authentication failed »des TVR/RTT sera positionné à 1.
Si la méthode d'authentification supportée par la carte n'est pas le CDA, le bit [1-8] « offline Data Authentication was not performed » est positionné à 1 dans la TVR/RTT.

[1] [1] Cette donnée est appelée "Static Data To Be Authenticated".

A la fin de cette étape, le kernel vérifie si une authentification porteur est nécessaire en comparant le montant de la transaction au « Reader CVM Required Limit » :
Si le montant de la transaction est inférieur ou égal au « Reader CVM Required Limit » alors pas d'authentification porteur, sinon une authentification porteur est requise.

4.5.4 Pré-Generate AC lecture Balance (optionnel)

Cette fonction permet d'obtenir le solde offline de la carte au début de la transaction (avant d'exécuter la commande Generate AC). L'information est obtenue par commande GET DATA. Ce traitement est systématique si l'information « Application Capabilities Information [2-2] » précise que cette fonction est supportée.

4.5.5 Restrictions de Paiement

Les contrôles des données suivantes s'appuient sur les règles décrites dans la documentation EMV Book 3, section 10.4 et décrit dans les documents [MPE52] [MPE52] [MPE52] [BOOKC2] [BOOKC3]

- Application Version Number (AVN)
- Date de début d'application
- Application Usage Control
- Date d'expiration

- si la version est différente des applications terminal (bit [2-8] « ICC and terminal have different application versions») est positionné à 1 dans le TVR/RTT.
- si la date de début de validité n'est pas atteinte (bit [2-6] « Application not yet effective») est positionné à 1 dans le TVR/RTT
- Si le service de paiement n'est pas autorisé pour ce dispositif le bit [2-5] « Requested service not allowed for card product » est positionné à 1 dans le TVR/RTT
- si la date de fin de validité est expirée (bit [2-7] « Expired application») est positionné à 1 dans le TVR/RTT

4.5.6 Sélection de la CVM

Lors de cette étape, le kernel authentifie le porteur si besoin et renseigne la CVM results en conséquence.
Les informations déterminantes sont :

- Le montant de la transaction (si supérieur « Reader CVM Required Limit »),
- Le bit [1-5] de l'AIP « Cardholder verification is supported »,

- Le bit [1-2] de l'AIP « On device cardholder verification is supported» ; si ce bit est positionné le traitement de la CVM list n'est pas effectué

Si la CVM est traitée, les RTT/TVR sont mises à jour comme suit :

- Si la CVM list est absente, le bit [1-6] « ICC Data Missing » est positionné à 1 dans RTT/TVR.
- Si un problème a été rencontré dans le traitement de la CVM le bit [3-8] « Cardholder verification was not successful » est positionné à 1 dans RTT/TVR.
- Si le CVM Code n'est pas reconnu, le bit [3-7] « Unrecognised CVM » est positionné à 1 dans RTT/TVR.
- Si la CVM n'est pas connue de l'application du terminal le bit [3-8] « Unrecognised CVM » est positionné à 1 dans RTT/TVR et le bit [3-8] « Cardholder verification was not successful » est positionné à 1.
- Si il n'y a plus de CVR dans la CVM list, le bit [3-8] « Cardholder verification was not successful » est positionné à 1.

Avant de commencer l'analyse des TAC/IAC le kernel compare le montant de la transaction au « Reader Contactless Floor Limit ». S'il est supérieur, il positionne à 1 le bit TVR/RTT RTT « Transaction exceeds floor limit »

4.5.7 Analyse des actions carte/terminal

Le Velocity Checking est non applicable en sans contact. Les bits [2-4], [4-6] et [4-7] du RTT ne sont donc jamais positionnés.

Le traitement offline ou l'émission d'une demande d'autorisation s'appuie sur la valorisation des TAC/IAC par comparaison au RTT. Les règles à appliquer sont les suivantes :

- Si le cryptogramme transmis par la carte est un AAC, la transaction est abandonnée le résultat est positionné à '**Declined**'
- Si le cryptogramme transmis par la carte est un TC, une analyse des TAC/IAC en comparaison au RTT sera effectuée. Cette comparaison autorisera soit un accord, une demande d'autorisation ou un refus le résultat est positionné à '**Approved**'.
- Si le cryptogramme transmis par la carte est un ARQC, une analyse des TAC/IAC en comparaison au RTT sera effectuée. Cette comparaison autorisera la transmission d'une demande d'autorisation ou un refus le résultat est positionné à '**Online Request**'.

La valorisation des TAC pour les AID CB sont présentées au § 9.5 et 9.6.

4.5.8 Recouvrement des « Torn transactions » (optionnel)

Le traitement permet de récupérer les données d'un GENERATE AC et s'effectue par la commande RECOVER AC.
Si la carte n'a pas décrémenté ses compteurs, une nouvelle transaction devra débuter. Dans le cas contraire, la transaction débutera à la commande GENERATE AC. Pour cette fonction le Kernel C-2 gère

- un log de transaction,
- un nombre de transactions loguées pour cette fonction,
- des paramètres.

Pour ce traitement, il est nécessaire de s'appuyer notamment sur le § 3.7.et 4.5 du [BOOKC2]

4.5.9 Authentification carte et calcul du cryptogramme

L'application carte ''CB'' sur base applicative Mastercard supportera obligatoirement la méthode d'authentification de l'application carte offline CDA.

Le terminal supporte uniquement la méthode CDA. Ce contrôle ne s'effectue pas avec un cryptogramme AAC de la carte. En cas d'échec sur le CDA, le bit [1-3] de la RTT « Combined dynamic authentication failed » est positionné à 1.

4.5.10 Post-Generate AC lecture Balance (optionnel)

Cette fonction permet d'afficher le solde offline de la carte à la fin de la transaction (après la commande Generate AC). La donnée est récupérée par la commande GET DATA.

4.5.11 Gestion du risque

Les contrôles suivants sont effectués par l'application du terminal après la décision carte et l'envoi du cryptogramme. Ces traitements peuvent contredire la décision carte, c'est-à-dire qu'un TC (carte) peut être transmis en lieu et place d'un ARQC dans une demande d'autorisation (exemple Bin inconnu).

La TVR transmise dans la demande d'autorisation sera la même que celle transmise à la carte. Les contrôles suivants ne provoquent pas la valorisation de la TVR mais uniquement celle du RTT.

4.5.11.1 Contrôle d'opposition

Le système d'acceptation supporte le contrôle d'opposition par rapport à la liste téléparamétrée par l'acquéreur. Il est effectué après les échanges carte/terminal et ne tient pas compte de l'existence de la carte en transaction non aboutie.

Si la carte est en opposition, le bit [1-5] du RTT « Card appears on terminal exception file» est positionné à 1.

4.5.11.2 Gestion des seuils

L'application sans contact contrôle

- les utilisations successives en montant d'une carte (FE 30.3.3) selon la valorisation du seuil d'appel.
- pour le montant cumulé, c'est le minimum du montant paramétré dans la table de paramétrage du sans contact et des seuils (table 08).

Sur réponse d'un cryptogramme TC ou d'un ARQC, si le seuil est dépassé, le bit [4-8] « Transaction exceeds floor limit » est positionné dans le RTT.

4.5.11.3 Contrôle du BIN en table

Le système d'acceptation contrôle la présence du BIN dans la table des BIN. Le tableau suivant présente les actions selon la valorisation du code niveau.

Mode	Code niveau	Action
EMV	Accepté	Poursuite de la transaction
	Surveillé	Positionne le bit [4-8] du RTT « Transaction exceeds floor limit » à 1
	Interdit ou refusé	Positionne bit [1-5] du RTT « Card appears on terminal exception file» à 1
	Bin inconnu	Positionne le bit [4-8] du RTT « Transaction exceeds floor limit » à 1

A l'exception de la valorisation « Carte de test », le code traitement particulier est ignoré.

Quand le code traitement indique carte de test, la mention « Carte de Test » doit être imprimée lors de l'édition du ticket et visualisée par l'accepteur.

4.5.12 Finalisation de la transaction

La finalisation de la transaction est à mettre en œuvre si le résultat transmis est '**approved'** ou '**Online request**'. Pour ces deux résultats, une analyse des TAC/IAC en comparaison au RTT sera effectuée sur les événements de la gestion du risque. Selon le paramétrage des TAC/IAC le résultat final pourra être positionné à '**Approved'**, '**Online request**' ou '**declined'**.

A la fin de la transaction, le kernel peut afficher ou imprimer le solde offline de la carte. Si la donnée « *Balance Read After Gen AC*» est fournie, le résultat est « **Approved (balance)** ».

4.6 Kernel 2 (MasterCard) Mode MagStripe

Une demande d'autorisation sera transmise systématiquement pour une transaction en Mode Magstripe. Elle sera complétée d'une raison de demande d'autorisation spécifique. Pour la saisie du code se reporter à 0.

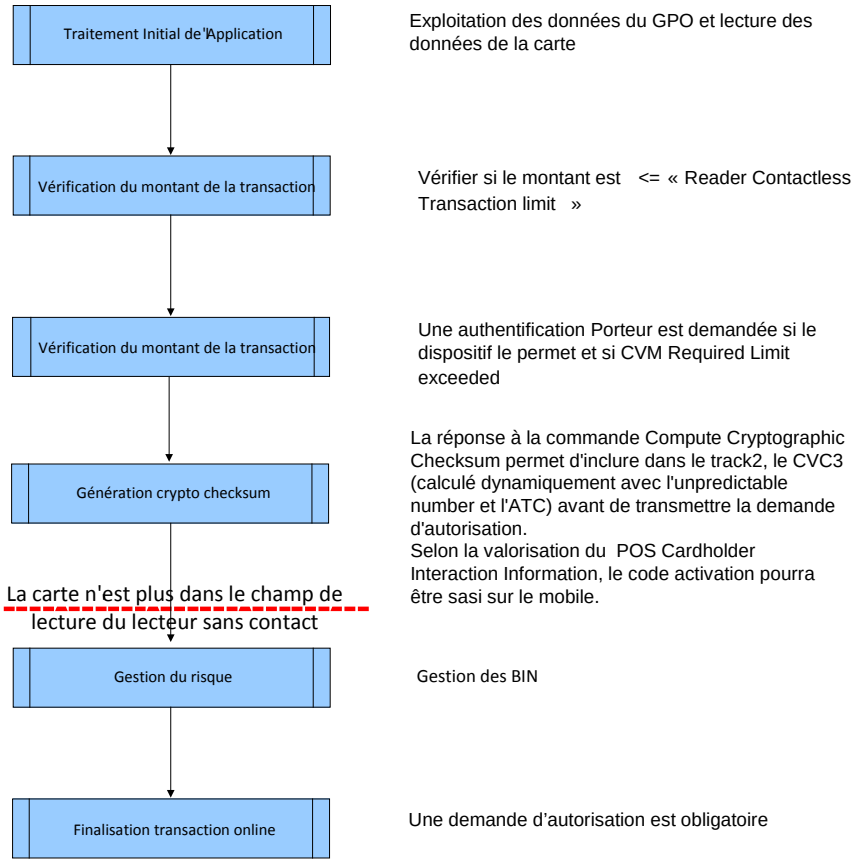


Figure 7 : Kernel -2 – Traitement Magstripe Sans contact

Les blocs conditionnels sont de hachurés

Les blocs fonctionnels « Traitement initial de la transaction » et « vérification du montant de la transaction » sont les mêmes que dans le traitement EMV. Se reporter aux §0 et 4.5.2.

4.6.1 Génération du crypto checksum

La commande Compute Cryptographic Checksum génère un CVC3 permettant à l'émetteur d'authentifier la carte en effectuant un calcul à partir des données transmises par le Reader et selon le contenu de l'UDOL (Unpredictable Number, ,….). La Track2 sera transmise dans la demande d'autorisation et le CVC3 positionné selon les caractéristiques de la carte (position et longueur) contenues dans les enregistrements de l'AFL..

Lorsque la carte ne possède pas d'UDOL, la valorisation par Défaut est la suivante :

Données	**Tag**	**Longueur**	**Valeur**
Unpredictable number	9F6A	4	
Mobile Support Indicator	9F55	1	[1-2] :1b : Offline Pin required by reader [1-2] 1b : Reader supports Mobile
Amount , Authorized	9F02	6	
Transaction currency Code	5F2A	2	
Terminal Country Code	9F1A	2	

4.6.2 Gestion du risque

Le système d'acceptation contrôle la présence du BIN dans la table des BIN. Le tableau suivant présente les actions selon la valorisation du code niveau.

Mode	**Code niveau**	**Action**
Magstripe	Accepté	Une demande d'autorisation doit être transmise.
	Surveillé	Une demande d'autorisation doit être transmise.
	Bin inconnu	Une demande d'autorisation doit être transmise.
	Interdit ou refusé	La transaction est abandonnée

A l'exception de la valorisation « Carte de test », le code traitement particulier est ignoré.

Quand le code traitement indique carte de test, la mention « Carte de Test » doit être imprimée lors de l'édition du ticket et visualisée par l'accepteur.

Si la carte est en opposition, la transaction est abandonnée.

4.6.3 Finalisation de la transaction

Selon les traitements de la gestion du risque, le résultat sera positionné à '**Online request**' ou '**declined'**.

4.7 C-3 [Kernel Visa],

Afin d'obtenir des informations sur les événements de la transaction, ceux-ci sont enregistrés, dans une donnée appelée **R**ésultat du **T**raitement du **T**erminal (RTT). La finalisation de la transaction s'appuiera sur les valorisations du RTT et des TAC ce qui provoquera un accord, un refus ou une demande d'autorisation. La valorisation des TAC reprendra les actions spécifiées dans les spécifications du C3.

4.7.1 Informations sur la saisie du code activation sur le Mobile de base applicative Visa

La saisie du code activation sur le mobile s'effectue par la transmission au mobile d'un TTQ[3-7] précisant que le terminal supporte le contrôle de code sur un dispositif sans contact et [2-8] indiquant qu'une authentification porteur est nécessaire. Si Le mobile répond un SW '6986' l'application du terminal valorisera le résultat à '**Try Again**' (se reporter à 5.2.2.2 du [BOOKC3]°.

4.7.2 Dynamic reader Limits (DRL)

Cette étape permet d'accéder à des paramètres spécifiques selon les informations contenues dans la réponse au Select.(se reporter au schéma 4.4.1)

- si le tag « 9F5A - Application Program ID» est présent la gestion du DRL est mise en œuvre pour la suite de la transaction

sinon

- il n'y a pas de gestion particulière des montants (les montants d'Entry Point sont utilisés pour la suite de la transaction).

Octet	Bit(s)	Valorisation
1	8-5	b'0011': Assignment by Visa Europe.
	4-1	b'0001': Application Program ID Format
2	8-5	b'0000'
	4-1	3 caractères numériques code monnaie émetteur, conforme à la norme [ISO 4217] ; exemple € = '978'
3	-	
4	8-5	b'0000'
	4-1	3 caractères numériques code pays de l'émetteur code, conforme à la norme [ISO 3166]. '250' for la France.
5	-	
6-16	-	

Figure 8 : exemple d' application Program ID « 9F5A »

Par ce biais, il sera possible de

- mettre en œuvre des programmes spécifiques à certaines monnaies (octet 1 à 3 seulement) ;
- mettre en œuvre des programmes spécifiques à certaines monnaies et certains pays (octet 1 à 5 seulement) ;
- Appliquer des programmes à certaines cartes dans certains pays ;
- Introduire certains programmes identifiés par certains programmes identifiés par Application Program ID.

Le Reader appliquera les règles de rapprochement selon la description faite dans le [BOOKC3] § 5.1 et [VSGU12] § 4.3.7.Le nombre de paramétrage (Application program IDs et des données associées) est d'un minimum de 4 [VSGU12] § 4.24.

4.7.3 Analyse des capacités du Reader et de la carte (Contactless Path Determination)

L'analyse des capacités s'appuie sur l'AIP et la capacité du terminal à gérer des transactions sans contact EMV (TTQ). Dans le cadre du Kernel C-3, le mode magstripe n'est pas supporté. Si l'AIP est absent de la réponse carte ou que son format est invalide, le résultat est positionné à « **End Application** ».

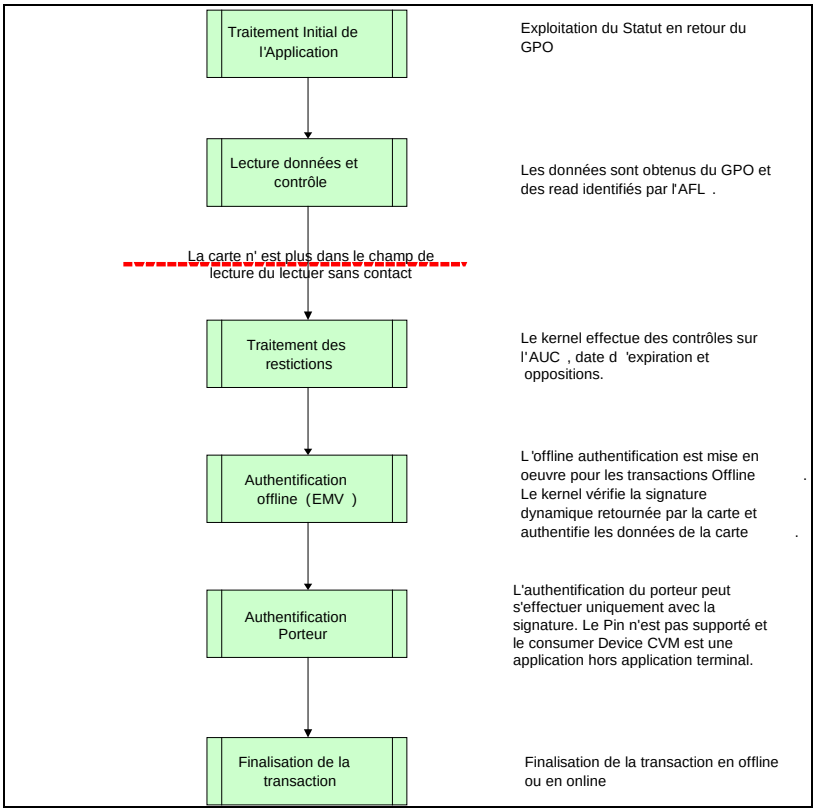


Figure 9 : Kernel C-3 – Traitement EMV sans contact

4.7.4 Traitement initial de la transaction (Initiate Application Processing)

Ce traitement consiste en l'envoi de la commande GPO et à l'analyse du statut en retour

Si le SW du GPO est à '9000' la transaction se poursuit par l'analyse des capacités du Reader de la carte.

Dans le cas contraire

- Si le SW du GPO = '6984'et que le Reader supporte mode EMV, le RÉSULTAT est positionné à « Try Another Interface' ;
- Si le SW du GPO = '6985', le résultat est positionné à 'Select Next' ;
- Si le SW du GPO = '6986' et que le Reader supporte mode EMV, le résultat E est positionné à « Try Again » ;
- Si le SW est valorisé à une autre valeur, le résultat est positionné à « End Application »

4.7.5 Lecture et contrôle des données.

Cette fonction permet de lire et de contrôler la cohérence des données d'une application carte sans contact.

Le kernel possède à ce stade toutes les données nécessaires à l'exécution de la transaction.

Si l'AFL est reçu et concerne la récupération de données complémentaires. Un message est affiché à destination du porteur est affiché afin que la carte soit retirée du champ.

Le Kernel vérifie que les données obligatoires sont présentes et qu'il n'y a pas de redondance de données.

Si des données sont identifiées comme manquantes ou redondantes le bit [1-6] « ICC data Missing » du RTT est positionné à 1et le résultat est positionné à « ***End Application*** ».

- Si le CID (Cryptogram Information Data) n'est pas transmis par le dispositif sans contact, il sera reconstitué à partir des positions 6-5 de l'octet 5 de l'Issuer application Data.
- Si le Cryptogramme reçu de la carte n'est pas interprétable ou ne correspond pas à un TC, ARQC et AAC, le bit [1-8] du RTT « Offline Data authentication was not performed» est positionné à 1 dans le RTT.

4.7.6 Contrôles des restrictions de paiement

Les contrôles suivants ne s'effectuent que si la carte a renvoyé un « TC ».

- *Contrôle sur la date d'expiration de la carte*

  La donnée concernée par ce traitement est le CTQ bit [1-4] « Go online if application expired and Reader is online capable » et ne concerne pas le risque acquéreur.

  Si la date locale est supérieure à la date d'expiration
  Le bit [2-7] « Expired application») est positionné à 1 dans le RTT.
  Si le terminal a la capacité d'aller online (TTQ bit [1-4] = b'0') et si le CTQ bit [1-4] est valorisé à b'1',
  le IAC bit [1-4] est positionné à {0,1,1}
  Sinon
  le IAC [1-4] est positionné {1,0,0} ;

- *Contrôle d'opposition (Terminal Exception File Check)*

  Le système d'acceptation supporte le contrôle d'opposition par rapport à la liste téléparamétrée par l'acquéreur. Il est effectué après les échanges carte/terminal et ne tient pas compte de l'existence de la carte en transaction non aboutie.

  Si la carte est en opposition, le bit [1-5] du RTT « Card appears on terminal exception file» est positionné à 1.

- *Gestion des seuils*

  L'application sans contact contrôle
  - les utilisations successives en montant d'une carte (FE 30.3.3) selon la valorisation du seuil d'appel.
  - pour le montant cumulé, c'est le minimum du montant de la table 08 et de la table des seuils sans contact.

  Si le seuil est dépassé, le bit [4-8] « Transaction exceeds floor limit » est positionné dans le RTT.

- *Contrôle du BIN en table*

  Le système d'acceptation contrôle la présence du BIN dans la table des BIN.
  Le tableau suivant présente les actions selon la valorisation du code niveau.

Mode	Code niveau	Action
EMV	Accepté	Poursuite de la transaction
	Surveillé	Positionne le bit [4-8] du RTT « Transaction exceeds floor limit » à 1
	Interdit ou refusé	Positionne bit [1-5] du RTT « Card appears on terminal exception file» à 1
	Bin inconnu	Positionne le bit [4-8] du RTT « Transaction exceeds floor limit » à 1

A l'exception de la valorisation « Carte de test », le code traitement particulier est ignoré.

Quand le code traitement indique carte de test, la mention « Carte de Test » doit être imprimée lors de l'édition du ticket et visualisée par l'accepteur. Cette information sera paramétrée dans le résultat.

4.7.7 Authentification offline EMV

L'authentification offline est traitée par le Kernel pour vérifier la signature dynamique et l'authentification des données de la carte. Cette fonction est implémentée si les transactions offlines sont supportées (si cryptogramme TC reçu)

Si la signature est erronée, le Kernel positionne le bit [1-4] du RTT « Fast DDA failed» à 1 ; c'est le bit du DDA qui sera utilisé pour Fast DDA.

Par ailleurs et selon les valorisations suivantes une valorisation des IAC sera mise en œuvre

- TTQ bit [1-4] : 0 (Online capable reader)
- CTQ bit [1-6] : 1 : Go online if Offline data authentication fails and reader is online capable ;
- CTQ bit [1-5] : 1 : Switch Interface if Offline Authentication fails and reader support contact Chip

Si Terminal Transaction Qualifiers bit [1-4] est positionné à b'0' (online capable), et si le CTQ bit [1-6] est valorisé à b'1'

Alors

le IAC bit [1-4] est positionné à {0,1,1}

sinon

le IAC [1-4] à {1,0,0} ;

Si Terminal Transaction Qualifiers bit [1-4] est positionné à b'1' (offline only) et si le CTQ [1-5]= '1'

alors le bit [1-4] du RTT « Switch interface if offline data authentication fails and reader supports VIS»[2] est positionné à 1, le résultat est valorisé à « **Try Another Interface** »

4.7.8 Authentification porteur

The Kernel détermine si une méthode d'authentification pour le porteur doit être effectuée.

Les méthodes supportées sont :

- Consumer Device CVM (méthode effectuée sur le mobile et validée par le mobile)
- Signature.

Ce traitement n'est effectué que si le RTT est positionné à zéro (les contrôles précédemment effectués sont positifs).

Pour le déroulement de cette fonction, voir §5.7 du [BOOKC3].

- Si le CTQ n'est pas retourné à l'application du terminal
  - Si le reader supporte la signature, le résultat sera positionné avec signature,
  - Si le reader supporte seulement Consumer Device CVM, le bit [3-8] du RTT « Cardholder verification was not successful » est positionné à 1.

Si le CTQ est retourné (voir §5.7.1.2 et 5.7.1.3. [BOOKC3]. :

- S'il y a une incohérence entre le CTQ octets 1-2 et la Card Authentication Related Data octets 6-7 du RTT bit [3-7] « Unrecognised CVM » est positionné à 1
- Si le Card Authentication Related Data n'est pas retournée et que le cryptogramme n'est pas un ARQC le bit [3-8] du RTT « Cardholder verification was not successful » est positionné à 1.

[2] L'autorisation ou le refus est géré uniquement par les paramètres cartes (CTQ)

4.7.9 Finalisation de la transaction

La finalisation de la transaction se décide dans le Kernel C-3 sur la valorisation de deux indicateurs

- Decline required by reader (0 : approved, 1 : declined)
- Online required by reader (0 : offline, 1: online)

La valorisation du RTT et TAC/IAC reprennent les décisions du Kernel ainsi que les Gestion du risque permettant de finaliser la transaction et peuvent contredire les décisions du kernel.

C'est pourquoi, le traitement offline ou l'émission d'une demande d'autorisation s'appuie sur la valorisation des TAC/IAC par comparaison au RTT. Les règles à appliquer sont les suivantes :

- Si le cryptogramme transmis par la carte est un AAC, la transaction est abandonnée.
- Si le cryptogramme transmis par la carte est un TC ou ARQC, une analyse des TAC/IAC en comparaison au RTT sera effectuée. Le résultat est un accord, une demande d'autorisation ou un refus.

Les valeurs des TAC pour les AID CB sont présentées en annexe.

A la fin de la transaction, le kernel peut afficher ou imprimer le solde offline de la carte. Si la donnée « Available Offline Spending Amount -9F5D » est fournie, le résultat est « **Approved (balance)** ».

4.7.10 Acceptation des mobiles 'Payez mobile' V2.1

Les mobiles « Payez Mobiles » V2.1 devront continuer à être acceptés par les solutions Bulletin 12 V3 par conséquent le TAG DF20 devra être reconnu et traité. Si la valeur de cette donnée est '00 00 00 01'b le traitement est le suivant :

- Sur réception du statut « 6986 » en réponse à la commande Get Processing Option, l'application du terminal désactive le lecteur entre 1s et 1,5 s ; à l'issu de ce délai un timer d'attente est armé pendant 60 secondes.
- Le porteur reçoit une demande de saisie de code activation sur son mobile. Si le délai de 60 secondes du terminal est échu, la transaction est abandonnée.

Après saisie du code, le porteur représente le mobile.

Le système d'acceptation conserve le montant saisi en mémoire (pas de re-saisi du montant par le commerçant) et sur présentation du mobile reprend la transaction au Select AID.

La réception de ce statut pour tout autre dispositif sans contact provoquera l'abandon de la transaction.

Les transactions en mode Magstripe (avec DF20 à '00 00 00 01'b**) sont interdites : la transaction est abandonnée et le résultat est positionné à « Declined ».**

Si le Mobile présente un DF20 différent de la valeur mentionnée ci-dessus, celle-ci est ignorée (il s'agit d'un mobile V3) et le Mobile est traité comme décrit dans le paragraphe 4.

4.8 Forçage d'un transaction

4.8.1 EMV

Le forçage est possible sur « AAC » quel que soit le mode de déclenchement paramétré par l'acquéreur (manuel, automatique) si les conditions de la transaction le permettent (Forçage autorisé pour l'AID, aucune raison d'appel en RPO) et si le paramétrage de l'application autorise le forçage.

Le forçage d'une transaction est autorisé sur ARQC avant ou après une demande d'autorisation. Les règles de forçage dépendent des codes raison identifiés pour la demande d'autorisation.

La liste des codes raison permettant le forçage est présentée en annexe 9.1.

4.8.2 Le mode Magstripe (MasterCard)

La transaction en mode Magstripe est une transaction online. En cas de réponse négative ou de non réponse, la transaction est abandonnée.

Il n'y a pas de forçage en mode Magstripe.

4.9 Réponse à une demande d'autorisation

Le système d'acceptation finalise la transaction selon la valorisation du code réponse de l'autorisation.

Par ailleurs, en cas de non réponse ou de problème technique, toute transaction transmise avec un code raison d'autorisation à 1660 (ARQC demandé par la carte) est refusée par l'application du terminal. La décision étant une décision carte, le forçage est interdit (avant ou après) la demande d'autorisation.

Pour le Kernel C-2, la finalisation de la transaction s'appuiera sur la valorisation des TAC/IAC 'default'.

Certaines réponses peuvent nécessiter des messages complémentaires gérés par le terminal. Dans certains cas la capture de la carte peut être demandée par l'émetteur.

Pour toute autre réponse, les messages affichés correspondront à la réponse transmise par l'émetteur.

Motif	Message affiché sur l'écran commerçant	Message affiché sur cible sans contact pour le porteur
Interdit en autorisation	CARTE INTERDITE Puis CAPTURER CARTE	CARTE REFUSEE
Bin refusé	CARTE REFUSEE	CARTE REFUSEE
Bin interdit	CARTE INTERDITE	CARTE REFUSEE

4.10 Appel Phonie

Sur réception d'un code « 02 » dans la réponse à la demande d'autorisation, le terminal affichera à l'écran les données nécessaires à l'appel Phonie (PAN,..).

Afin de sécuriser les actions du commerçant, ses interventions sont validées explicitement par passage de la carte commerçant.

Lutte contre la fraude : Cette règle est mise en œuvre suite à une réponse « 02 : contacter la banque » et après un appel phonie du commerçant (centre d'appel). Cette fonctionnalité s'applique aussi au crédit commerçant, à l'annulation et au forçage (la **double validation n'est plus acceptée).**

La carte commerçant valide l'ensemble des actions commerçant. Lorsque le point d'acceptation demande son passage, deux actions sont envisageables :

- Valider la transaction par le passage de la carte.
- Appuyer sur la touche 'ANNULATION' pour abandonner la transaction. Cette action peut être utilisée pour tous les problèmes liés à la carte commerçant (carte non trouvée, carte invalide,..).Une TNA sera dans ce cas enregistrée.

4.11 Traitement des Résultats

Chaque Kernel termine son traitement en fournissant le résultat de la transaction. Certains résultats, comme « **Try again** » ou « **Select Next** » indiquent que le traitement de la transaction doit reprendre à un point particulier.

Les résultats comme « **Approved** » et « **Online requested** » sont les résultats finaux du traitement par le kernel et transmis au Reader avec ses paramètres et les données associées.
Quelques exemples sont décrits ci-après :

- Si le résultat est valorisé à « Try again », Entry Point se positionnera en Start B (Book B § 3.3.2.6),
- Si le résultat est valorisé à « Select Next », Entry Point retire de sa liste l'application courante et se positionne en Start B (Book B § 3.3.2.6)
- Si le résultat est différent de « Try Again » ou « Select Next » entry Point fournit au terminal/reader, les informations reçues du kernel par exemple :
  - Si le paramètre « *UI requested on Outcome Present - message à afficher au porteur*» est valorisé à « YES », entry point transmettra à l'interface associé.le message à afficher.
  - Si le paramètre « Field off request » : délai de désactivation du champ est différente de N/A , Entry point transmettra à l'interface associé la valeur « Hold Time » qui correspond au temps pendant lequel le champ devra rester actif.

Pour obtenir le détail des traitements se reporter au Book A EMV .

4.12 Les remboursements ou annulations

Pour la gestion du crédit et des annulations plusieurs types de cryptogrammes peuvent être transmis par la carte selon la base applicative sur laquelle elle s'appuie.

Il n'y a pas de repli en contact pour une annulation ou un crédit.

4.12.1 Les crédits ou annulations sur base applicative Visa

Pour les opérations de remboursement sans contact, quelle que soit la configuration du terminal, la valorisation du TTQ doit être le suivant :

- [1-6 : = 1] EMV mode supported
- [1-8 : = 0] Mag-Stripe mode not supported
- [1-4 : = 0] Online Capable reader
- [2-8 : = 1]Online cryptogramme required
- [2-7 : = 0]CVM not required

Pour les opérations de remboursement sans contact, le montant autorisé transmis à la carte doit être fixé à la valeur du montant du remboursement. Le type de transaction doit être valorisé à « 20 »

La carte selon sa version et le paramétrage ci-dessus l répondra soit un ARQC ou un AAC.

Conformément au [VSGU12] § 4.3.11, il ne sera pas possible d'annuler une transaction sans contact traitée en mode offline. Une transaction 'Crédit' du même montant que la transaction originale sera utilisée.
Le résultat du kernel est positionné à « Approved »

4.12.2 Les crédits ou annulations sur base applicative Mastercard

4.12.2.1 EMV

Type de transaction	20
Montant	Montant à annuler ou créditer *(Nb : La version PayPass 2.1 permet de transférer le montant de la transaction)*
Cryptogramme demandé au mobile ou à la carte	AAC

Le résultat du kernel est positionné à « **Approved** » si aucune anaomlie n'est rencontrée.

4.12.2.2 Magstripe

Pour une transaction magstripe, la commande Compute Cryptographic Checksum est nécessaire. Cette transaction est traitée offline et le résultat est positionné à « Approved » si aucune anomalie n'est rencontrée.

4.13 Les tickets

La mention « sans contact » générique figure sur le ticket carte en dessous du titre « Carte Bancaire » et doit être accompagné du Logo suivant :

Le ticket est conforme aux spécifications 5.2.2 et dépend du résultat et des caractéristiques de la transaction.

Le nom de l'application sur le ticket (« Application Preferred Name» ou «Application Label») est édité selon les spécifications EMV.

L'édition du justificatif porteur et commerçant est systématique quel que soit le montant de la transaction. Le ticket commerçant peut être dématérialisé.

Afin d'éliminer les problèmes d'édition, une vérification de la disponibilité du papier dans l'imprimante du terminal sera faite avant le démarrage de la transaction. Si ce contrôle est négatif, la transaction ne pourra pas débuter.

Les règles suivantes devront être appliquées :

- Si le montant de la transaction est supérieur au montant de double authentification, une signature est demandée au porteur.
- Si l'édition du ticket porteur est incomplète, la transaction est abandonnée avec l'enregistrement d'une transaction non aboutie.
- Si l'édition du ticket commerçant ne s'effectue pas convenablement (problème de papier, bourrage ou édition incomplète), la transaction est finalisée et la transaction financière enregistrée. Le commerçant pourra éditer son ticket sous forme de duplicata après.

Sur un automate, les fonctionnalités du contact s'appliquent (notamment : le manque de papier provoque soit la désactivation de l'automate (parcmètre) ou soit une information du porteur qui peut abandonner la transaction)

Le solde carte est imprimé si disponible.

Les tickets seront édités systématiquement lorsque le Résultat de la transaction sera positionné « **Declined** », « **Approved** » (avec ou sans balance).

4.14 Information complémentaire pour le commerçant

Afin d'aider le commerçant à identifier les problèmes rencontrés pendant la transaction, un numéro d'anomalie sera ajoutée lorsqu'une transaction non aboutie sera enregistrée.

Le code de cette anomalie sera édité sur le ticket commerçant sans contact en cas d'Abandon et une information sera affichée uniquement sur l'écran commerçant après l'édition du ticket pour informer le commerçant du problème.

Code	Libelle Message Commerçant	Informations
1	CARTE INVALIDE	Des données obligatoires de la carte sont absentes ; la transaction sans contact ne peut se poursuivre.
2	CARTE INVALIDE	Des données permettant de vérifier la signature de la carte sont absentes. La transaction sans contact ne peut se poursuivre
3	PROBLEME TECHNIQUE	Une zone de traitement du CDA est inférieure à la taille nécessaire.
4	CARTE INVALIDE	La méthode d'authentification supportée par la carte n'est pas le CDA (base applicative Mastercard)
5	DATE DEBUT INVALIDE	La date de début de validité de l'application carte n'est pas atteinte et ne peut dans ce cadre être utilisée.
6	CARTE PERIMEE	La carte est périmée et ne peut être utilisée.
7	CARTE DE TEST	La carte présentée est une carte de tests.
8	TYPE DE TRANSACTION REFUSEE	La carte n'est pas paramétrée pour être utilisée sur ce point d'acceptation.
9	CARTE INVALIDE	L'authentification proposée au porteur n'est pas supportée par l'application sans contact de votre terminal.
10	CARTE INVALIDE	Toutes les authentifications disponibles ont échouée.
11	INCIDENT CARTE	Erreur durant le déroulement de l'authentification carte (CDA)
12	CARTE INTERDITE	La carte étant en opposition la transaction n'a pu aboutir

Code	Libelle Message Commerçant	Informations
13	CARTE REFUSE	Le Bin de la carte est refusé ou interdit dans la table des BIN de l'application sans contact
14	PROBLEME TECHNIQUE	Le certificat reçu de la carte n'est pas interprétable
15	CARTE PERIMEE	La date d'expiration est > à la date locale. Le paramétrage de la carte demande le refus de la transaction.
16	INCIDENT CARTE	La carte demande de changer d'interface sur un échec d'authentification (Visa)
17	ANNUL REFUSEE	Abandon de la transaction demandée par le commerçant dans le cadre d'une annulation.
18	PB SAISIE CODE SUR MOBILE	Le délai avant représentation du mobile est échu.
19	REFUS EMETTEUR	Une demande d'autorisation a été transmise et la réponse de la banque émettrice est négative.
20	CARTE INTERDITE	Une demande d'autorisation a été transmise et la réponse de la banque émettrice est de type demande de capture.

5 CONFIGURATION DE L'APPLICATION SANS CONTACT

Les paramètres suivants concernent l'application sans contact EMV. Certains sont initialisés dans l'application dès l'installation, d'autres sont à la charge de l'acquéreur.
Dans ce document, ne seront mentionnées que les nouvelles données, pour les autres se reporter aux référentiels existants. L'application sans contact sera téléparamétrée selon la version fonctionnelle du système d'acceptation.

5.1 Paramètres permanents

5.1.1 Autorun

Autorun est un paramètre de fonctionnement de l'application sans contact qui permet d'activer ou de désactiver le champ NFC.

Il est positionné à 'NO' si un événement permet d'activer le champ (par exemple la saisie du montant) et à 'YES 'si le champ est toujours activé (montant identique pour toutes les transactions (distributeurs de boissons, ticket de transport).

Pour les points d'acceptation (face à face et automate) la valeur sera fonction de l'application et paramétrable localement.

5.1.2 Identification des applications sans contact du système d'acceptation

Les applications doivent être conformes à tous les bulletins CB (à l'exception du bulletin 8 optionnel en 5.2.2). Les deux versions fonctionnelles suivantes sont définies pour le sans contact :

- 535 : Sans contact Bulletin 12 V3 *(si B8 obligatoire)*

Les versions fonctionnelles font partie de l'identification des spécifications de référence du constructeur. Celle-ci est présente dans l'ouverture de dialogue.

5.2 Types de transaction

Les types de transaction acceptés sont pour

- les systèmes d'acceptation de paiement de proximité : le débit, le crédit et l'annulation.
- Pour les automates de classe 1 CB (CAT 2 et CAT 3) et classe 2.1 : le débit

La valorisation du Transaction Type (9C) pour le paiement Face à face est

- Paiement : 00
- Crédit : 20
- Annulation : 20 (pour Visa : effectuée sous la forme d'un Crédit)

La valorisation du Transaction Type (9C) pour le paiement sur automate est

- Paiement : 00

5.3 Methodes d'authentification porteur

Le Consumer Device CVM est une CVM traitée et vérifiée par le dispositif porteur et est indépendante du terminal.

5.3.1 Kernel C2 (MasterCard)

- Les systèmes d'acceptation paiement CB (Face à Face) supportent le consumer device CVM, signature et No CVM (le PIN online n'est pas supporté),
- Les automates supportent uniquement No CVM et Consumer device CVM.

5.3.2 Kernel C3 (Visa)

- Les systèmes d'acceptation paiement CB (Face à Face) supportent le consumer device CVM et signature (le PIN online n'est pas supporté),
- Les automates supportent uniquement Consumer device CVM.

5.4 Table des « Combinaisons » par type de Transaction

Cette table permet de configurer pour le paiement et les crédits, les Kernels qui seront utilisés pour l'exécution de la transaction.

5.4.1 Paiement Face à face

{AID – Kernel ID}	A0000000651010	A0000000421010	A0000000422010	A0000000424010	A0000000425010	A0000000031010	A0000000032010	A0000000041010	A0000000043060
Kernel C1									
Kernel C2		X	X	X	X			X	X
Kernel C3		X	X	X	X	X	X		

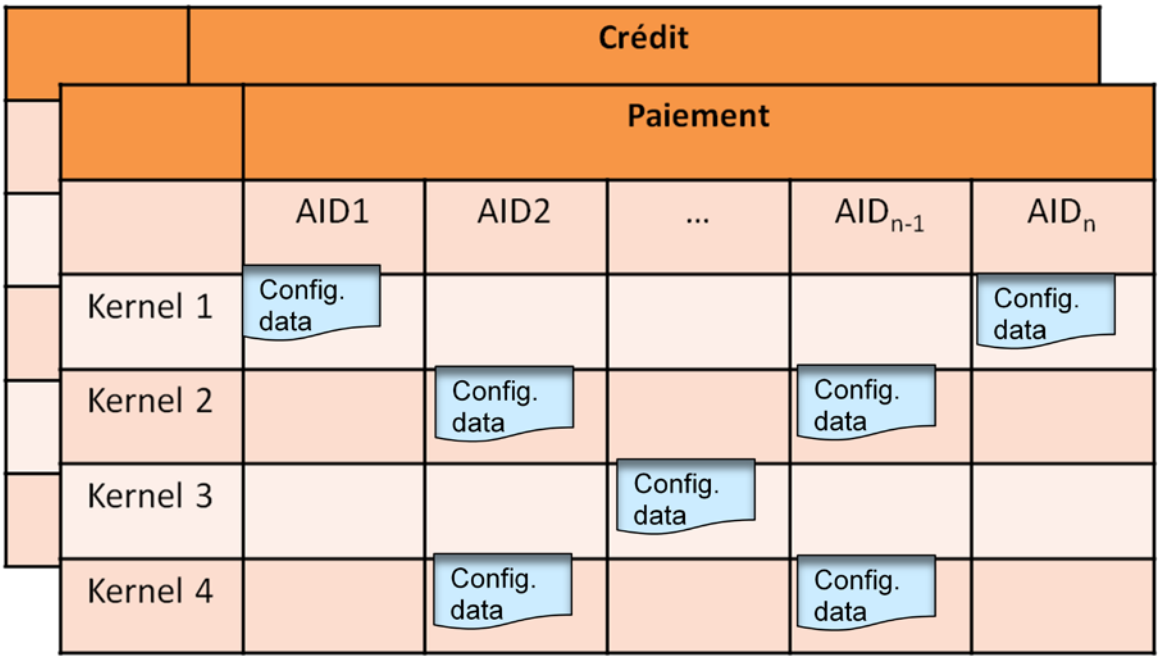
5.4.2 Crédit en Face à face

{AID – Kernel ID}	A0000000651010	A0000000421010	A0000000422010	A0000000424010	A0000000425010	A0000000031010	A0000000032010	A0000000041010	A0000000043060
Kernel C1									
Kernel C2		X	X	X	X			X	?
Kernel C3		X	X	X	X	X	X		

5.4.3 Paiement sur automate

{AID – Kernel ID}	A0000000651010	A0000000421010	A0000000422010	A0000000424010	A0000000425010	A0000000031010	A0000000032010	A0000000041010	A0000000043060
Kernel C1									
Kernel C2		X	X	X	X			X	?
Kernel C3		X	X	X	X	X	X		

5.5 Données à configurer par combinaison et par type de transaction



Pour chaque combinaison (kernel-AID) et par type de transaction les données suivantes sont configurées :

- CVM (Signature, PIN online, No_CVM, consumer Device CVM)
- Capacité du terminal (Offline, Online),
- Les seuils (dans une monnaie donnée) [3] :
  - Reader ContactLess Transaction limit : Montant maximum d'une transaction sans contact (toute transaction dont le montant est supérieur ou égal sera refusée en sans contact) ;
  - Reader ContactLess Floor limit : Seuil au-delà duquel la transaction doit être traitée Online.
  - Reader CVM Required Limit : seuil à partir duquel une authentification du porteur est obligatoire.
- Type de terminal
- TAC

La mise en œuvre du DRL demande une gestion de paramètres spécifiques pour la mise en œuvre de cette fonction. Le paramétrage s'effectue par acquéreur et

[3] Ces données sont contenues dans la table 09 du Bulletin 12 V2

commerçant et est présenté dans le document [VCPS21] *[5.52].* Les données nécessaires à cette fonction sont les suivantes :

- Program ID
- Currency
- Country
    - Reader ContactLess Transaction limit
    - Reader ContactLess Floor limit
    - Reader CVM Required Limit

Exemples de configuration

Type de paiement	Kernel ID	AID	CVM (*)					Capacité Du PA	*Libellé de l'application carte (information)*	Monnaie	RCTL (**)	RCTFL	RCCRL
00 (paiement)	02 (MC)	A0 00 00 00 42 1010	1	3				Online	*CB (paiement retrait)*	Euro	20	20	20
00 (paiement)	03 (Visa)	A0 00 00 00 42 2010	1					Online	*CB (paiement retrait)*	Euro	-	20	20
00 (paiement)	02 (MC)	A0 00 00 00 42 1010	1	3				Online	*CAS*	Euro	20	20	20
00 (paiement)	03 (Visa)	A0 00 00 00 42 2010	1					Online	*CAS*	Euro	-	20	20
00 (paiement)	02 (MC)	A0 00 00 00 42 1010	3					offline	*CB (paiement retrait)*	Euro	20	20	20
00 (paiement)	02 (Visa)	A0 00 00 00 42 1010						offline	*CB (paiement retrait)*	Euro	-	20	20
00 (paiement)	02 (MC)	A0 00 00 00 04 1010	2	3				online	*Mastercard*	Euro	300	100	20
00 (paiement)	02 (Visa)	A0 00 00 00 03 1010	2					online	*Visa*	Euro	-	20	20

RCTL(**R**eader **C**ontactless **T**ransaction **L**imit), RCTFL(**R**eader **C**ontactless **T**ransaction **F**loor **L**imit), RCCRL (**R**eader **C**ontactless **C**VM **R**equired **L**imit)

(*) - : non renseigné

(**) Valeurs CVM : 1 (signature), 2(Consumer device CVM), 3 (NO_CVM) , 4 (Pin online)

"

5.6 Terminal Transaction Qualifiers

Cette table est utilisée dans les échanges avec le Kernel C-3. Ce paramétrage est local et non paramétrable par l'acquéreur. Le contenu de cette table est le suivant :

Octet	Bit	Définition	Valorisation
1	8	1b – Mag-stripe mode supported 0b – Mag-stripe mode not supported	0b – Mag-stripe mode not supported
	7	RFU (0b)	0b
	6	1b – EMV mode supported 0b – EMV mode not supported	1b – EMV mode supported
	5	1b – EMV contact chip supported 0b – EMV contact chip not supported	1b – EMV contact chip supported si l'application contact est active. Dans le cas contraire la valorisation sera positionnée à 0b – EMV contact chip not supported
	4	1b – Offline-only reader 0b – Online capable reader	0b – Online capable reader
	3	1b – Online PIN supported 0b – Online PIN not supported	0b – Online PIN not supported
	2	1b – Signature supported 0b – Signature not supported	1b – Signature supported
	1	RFU (0b)	0b
2	8	1b – Online cryptogram required	
	7	1b – CVM required 0b – CVM not required	Selon la valorisation Reader CVM Required Limit. Si le montant du bien est supérieur, sa valorisation sera 1b – CVM required Sinon 0b – CVM not required
	6	1b – (Contact Chip) Offline PIN supported 0b – (Contact Chip) Offline PIN not supported	0b – (Contact Chip) Offline PIN not supported
	5-1	RFU	00000b
3	8	1b – Issuer Update Processing supported 0b – Issuer Update Processing not supported	0b – Issuer Update Processing not supported
	7	1b – Consumer Device CVM supported 0b – Consumer Device CVM not supported	1b – Consumer Device CVM supported
	6-1	RFU	000000b
4	8-1	RFU	00000000b

5.7 Liste des messages EMV

Dans le cadre de cette mise en œuvre, EMV propose des messages pour les échanges sans contact. Ils sont référencés dans les Résultats (cf. chapitre **Erreur ! Source du renvoi introuvable.**). Par ailleurs, les aspects LED, tonalité et messages sont présentés dans la documentation EMV [BOOKA].

Ces messages seront associés à des données qui permettront par exemple d'afficher le solde sans contact.

Message Identifier	Message	Information complémentaire
3	Paiement sans contact accepté	Transaction acceptée
7	Paiement sans contact refusé	Transaction refusée.
9	Entrer votre code confidentiel, SVP	La demande de saisie du code est demandé (Non supportée chez Cb)
OF	Erreur de traitement	
10	Vous pouvez enlever votre carte	
14	Bienvenue	Message d'accueil (terminal en attente).
15	Présentez carte	Demande au Porteur de présenter une carte au Reader.
16	En cours	Ce message est affiché pendant le déroulement de la transaction
17	Retirez Carte	La carte n'est plus nécessaire à la finalisation de la transaction. Elle doit être retirée du champ.
18	Insérez Carte ou Passez votre carte	Ce message indique que la carte ne peut utiliser l'interface sans contact et qu'il est possible d'utiliser la puce ne mode contact ou la lecture de la piste.
19	Présentez une seule carte	Plusieurs cartes sans contact sont dans le champ du lecteur un message est affiché afin qu'il ne présente qu'une seule carte
1A	Paiement Accepté – Signature	Accepté suite à une autorisation mais une signature est demandée
1B	Autorisation - Patientez	Une demande d'autorisation est en cours
1C	Insérez, passez la carte ou essayez une autre carte	Aucune application commune entre le terminal et la carte sans contact. Le produit sans contact n'est pas géré par le système d'acceptation, son utilisation est donc interdite (Non gérée)
1D	Insérez votre carte SVP	Message informant le porteur que la carte peut être insérée dans le lecteur Contact
1E	Pas de message	Permet de réinitialiser l'écran, aucun message n'est affiché
20	Voir les instructions sur votre téléphone	Ce message est affiché au porteur si une en cours de transaction si des actions spécifiques sont à effectuer sur le dispositif sans contact.

21	Veuillez représenter votre carte	Ce message est affiché après une demande d'autorisation ou la carte doit être représentée ou si une erreur ou si la représentation de la carte permet de corriger une anomalie.

6 LES ECHANGES AVEC LE SYSTEME ACQUEREUR

Les échanges pour le sans contact s'appuient sur les versions CB2A suivantes :

- CB2A Autorisation : 1.1.2, 1.13, 1.1.4, 1.1.5, 1.1.A
- CB2A TLC-TLP-GR : 1.1.3, 1.1.4, 1.1.5, 1.1.A, 1.1.6, 1.1.B
- CB2A Autorisation : Addendum Paiement en mode sans contact (PSC) de décembre 2009
- CB2A TLC-TLP-GR : Addendum Paiement en mode sans contact (PSC) de décembre 2009

Sera mise à jour à partir des travaux du groupe protocole

6.1 Demande d'autorisation

Les informations échangées sont notamment :

- le contexte de réalisation de la transaction (transaction réalisée en mode sans contact),
- les données de la carte spécifiques au sans contact.

Les données RTT (DF85 - Tag et valeur) ainsi que le code raison spécifique à la gestion du mode Magstripe seront diffusés en autorisation.

En outre, les données suivantes seront transmises dans les autorisations :

- TTQ (donnée utilisée par le Kernel C-3)
- Facteur de forme (Visa, CB,..)
- Kernel ID
- Type de terminal
- CVM Result : cette information sera initialisée selon les caractéristiques de la transaction pour le Kernel C-3.

6.2 Télécollectes

Chaque application (contact et sans contact) effectuera une télécollecte avec une ou plusieurs remises par application. La donnée RTT (DF85 - Tag et valeur) sera remontée en télécollecte.

La gestion des crédits et des annulations s'appuient sur la génération d'un cryptogramme au même titre que les transactions de débit. Les éléments de calcul seront eux aussi diffusés.

En outre, les données suivantes seront transmises en télécollecte :

- TTQ (donnée utilisée par le Kernel C-3)
- Facteur de forme (Visa, CB,..)
- Kernel ID
- Type de terminal
- CVM Result : cette information sera initialisée selon les caractéristiques de la transaction pour le Kernel C-3.
- Discretionary Data Tag “FF8106” (donnée utilisée par le Kernel C-2)
- Motif de la transaction non aboutie en sans contact

6.3 Paramétrage

6.3.1 Données à configurer par {Kernel ID/ AID} et type de transaction

La gestion des données dans le cadre du paramétrage demande une gestion de données pour une combinaison (kernel-AID) et par type de transaction les données suivantes sont configurées :

- CVM (Signature, PIN online, No_CVM, consumer Device CVM)
- Capacité du terminal (Offline, Online),
- Les seuils (dans une monnaie donnée) :
  - Reader ContactLess Transaction limit : Montant maximum d’une transaction sans contact (toute transaction dont le montant est supérieur ou égal sera refusée en sans contact) ;
  - Reader ContactLess Floor limit : Seuil au-delà duquel la transaction doit être traitée Online. Le Reader Contactless Transaction Limit (No On-device CVM) (‘DF8124’) et Reader Contactless Transaction Limit (On-device CVM) (‘DF8125’) utilisés dans le Kernel C-2 seront initialisés avec le reader Contactless limit.
  - Reader CVM Required Limit : seuil à partir duquel une authentification du porteur est obligatoire.

Ces données sont complétées par les informations suivantes :

- Type de terminal
- TAC

6.3.2 Données à configurer pour la fonction « Dynamic Reader limits »

La gestion des montants dans le Kernel C-3 via la fonction « Dynamic Reader limits » requiert un paramétrage par acquéreur et commerçant des données suivantes :

- Program ID

- Currency
- Country
  - Reader ContactLess Transaction limit
  - Reader ContactLess Floor limit
  - Reader CVM Required Limit

6.4Etat fonctionnel

L'application du terminal remontera le TTQ dans l'état fonctionnel.

7 DIVERS

7.1 Déclaration du matériel

Les établissements acquéreurs déclareront les applications sans contact selon les modalités et les circuits d'informations SISPE (identique au circuit contact).

L'identification du sans contact s'effectuera selon la valorisation de la version fonctionnelle identifiée dans l'ITP.

7.2 Délai d'attente pour un mobile.

L'application du terminal attendra la présentation du mobile dans un délai maximum de 30 secondes. Si le délai de 30 secondes du terminal est échu, la transaction est abandonnée.

7.3 Logo

Le terminal doit afficher le pictogramme défini par EMVCo suivant :

Il doit être positionné au centre de l'antenne.

7.4 Gestion des incidents

Les événements terrain rencontrés par les commerçants et les porteurs devront être diffusés à l'équipe en charge de la gestion des incidents à l'adresse suivante :

evenements-terrain@cartes-bancaires.com

7.5 Les agréments

Les applications supportées par les points d'acceptation devront avoir reçu de la part de Visa et de MasterCard les « Approval statement » nécessaires à leur mise en exploitation.

Ces « approval statement » des réseaux sont des pré-requis à l'Agrément CB qui sera délivré sous réserve des tests complémentaires suivants :

- non régression de l'application CB5.2 «contact» par rapport aux spécifications CB 5.2 de référence et aux bulletins précédant le présent document,
- Conformité au bulletin 12 V3,
- tests protocolaires nécessaires aux traitements des données (Télécollecte, paramétrage, autorisation,…) ,

Pour les systèmes d'acceptation paiement gérant les modes contact et sans contact, si l'application CB5.2 contact n'est pas modifiée par rapport à sa dernière version agréée « CB », seuls des tests de non régression et de cohabitation avec l'application CB5.2 « Sans Contact » seront effectués. La configuration présentée à l'agrément devra contenir alors, a minima, les deux applications (contact et sans contact).

Le processus d'agrément applicable est similaire à celui existant en mode contact.

7.6 Mise en œuvre du Bulletin dans le cadre de l'Agrément CB

Situation	Mise en œuvre du Bulletin : Obligatoire / Recommandée / Non Date éventuelle (dépôt en laboratoire)
La solution est présentée pour la 1ère fois à l'Agrément CB	30/06/2012
La solution est déjà agréée CB. Elle se représente à l'Agrément CB suite à correction d'anomalie (ET par exemple).	30/06/2012
La solution est déjà agréée CB. Elle se représente à l'Agrément CB car l'Industriel la fait évoluer (de son propre chef ou pour prendre en compte des évolutions CB).	30/06/2012

NB : en cas de combinaison de situations, c'est la situation la plus contraignante qui prévaut.

8 ANNEXES

8.1 Correspondance raisons d'appel et TVR/RTT en SANS CONTACT

Octet	Bit	Terminal Verification Results	RPO	Condition d'émission d'une demande d'autorisation	MCHIP		qVSDC		
					TVR	RTT	TVR	RTT	Raison d'appel
1	8	Offline data authentication was not performed	**Oui**	Authentification des données offline non exécutée	X	X			1508 : "on-line" forcé par le terminal
	7	Offline static data authentication failed	**Oui**	Authentification statique offline des données échouée (SDA)	X	X			1508 : "on-line" forcé par le terminal
	6	ICC data missing		Données facultatives absentes	X	X			1656 : Forcé par l'émetteur (contrôle de flux)
	5	Card appears on terminal exception file	**Oui**	Sur BIN refusé		X		X	1663 : BIN refusé
	5	"	**Oui**	Sur BIN en interdit		X		X	1512 : BIN interdit
	5	"	**Oui**	Sur « carte interdite » en liste de contrôle		X		X	1513 : Carte interdite
	5	"	**Oui**	Sur « carte refusée » en liste de contrôle		X		X	1659 : Carte refusée
			Oui	Sur « carte surveillée » en liste		X		X	1654 : N° surveillé

Octet	Bit	Terminal Verification Results	RPO	Condition d'émission d'une demande d'autorisation	MCHIP		qVSDC		
					TVR	RTT	TVR	RTT	Raison d'appel
				de contrôle					
	4	Offline dynamic data authentication failed	**Oui**	Authentification dynamique offline des données échouée				X	1508 : "on-line" forcé par le terminal
	3	Combined dynamic authentification failed	**Oui**	Authentification en mode CDA échouée	X	X			1508 : "on-line" forcé par le terminal
	2	Switch interface if offline data authentication fails and reader supports VIS						X	
2	8	ICC and terminal have different application versions		Versions application carte et système d'acceptation différent	X	X			1508 : "on-line" forcé par le terminal
	7	Expired application	**Oui**	Application Expirée	X	X		X	1508 : "on-line" forcé par le terminal
	6	Application not yet effective	**Oui**	Application non encore active	X	X			1508 : "on-line" forcé par le terminal
	5	Requested service not allowed for card product	**Oui**	Service non autorisé pour cette carte	X	X			1508 : "on-line" forcé par le terminal
	4	New card							
	8	Cardholder verification was not successful	**Oui**	Authentification du porteur selon CVM a échouée	X	X		X	1508 : "on-line" forcé par le terminal
	7	Unrecognised CVM		CVM non reconnue	X	X			1508 : "on-line" forcé par le terminal
	6	PIN Try Limit exceeded							
	5	PIN entry required and PIN pad							

Octet	Bit	Terminal Verification Results	RPO	Condition d'émission d'une demande d'autorisation	MCHIP		qVSDC		
					TVR	RTT	TVR	RTT	Raison d'appel
3		not present or not working							
	4	PIN entry required, PIN pad present, but PIN was not entered							
	3	Online PIN entered							
4	8	Transaction exceeds floor limit		Sur montant de la transaction supérieur au seuil d'appel	X	X		X	1510 : Dépassement seuil d'appel
	8	"		Sur transaction en devise	X	X		X	1657 : Monnaie étrangère
	8	"	**Oui**	Bin à surveiller		X		X	1652 : BIN surveillé
	8	"	**Oui**	BIN inconnu		X		X	1653 : BIN inconnu
	8	"		Sur cumul des montants des transactions abouties supérieur au seuil d'appel		X		X	1651 : Cumul/porteur/application
	7	Lower consecutive offline limit exceeded		Limite inférieure pour la transaction offline dépassée		X			1656 : Forcé par l'émetteur (contrôle de flux)
	6	Upper consecutive offline limit exceeded		Limite supérieure pour la transaction offline dépassée		X			1656 : Forcé par l'émetteur (contrôle de flux)
	5	Transaction selected randomly for online		Sélection aléatoire d'une transaction		X		X	1503 : Déclenchement aléatoire par terminal
	4	Merchant forced transaction online		Transaction forcée on line par l'accepteur	X	X		X	1506 : "on-line" forcé par l'accepteur de carte

Octet	Bit	Terminal Verification Results	RPO	Condition d'émission d'une demande d'autorisation	MCHIP		qVSDC		
					TVR	RTT	TVR	RTT	Raison d'appel
5	8 7 6 5	Default TDOL used Issuer authentification was unsuccessful Script processing failed before final GENERATE AC Script processing failed after final GENERATE AC							- - - -
		la carte retourne ARQC au premier GENERATE AC							

Le code raison de la demande d'autorisation en mode magstripe est 1671.

8.2 Identification des erreurs dans le Kernel C-2

Le kernel C-2 gère des informations permettant de connaître les caractéristiques de la transaction. Ces éléments sont caractérisés par 3 variables qui peuvent prendre plusieurs valorisations. Ces variables sont appelées L1, L2 et L3 dans la description du Kernel C2.

Ces éléments sont stockés dans le Discretionary *Data* Tag “FF8106” qui seront remontées dans la télécollecte.

La variable L1 est utilisée pour indiquer si les échanges sont valides ou invalides.

Ils peuvent indiquer les événements suivants :

- Collision détectée,
- Erreur - Timeout ;
- Erreur - Protocole ;
- Erreur – Transmission ou toute autre erreur

L1			
Byte 1	b8-1	L1	
			00000000: OK
			00000001: TIME OUT ERROR
			00000010: TRANSMISSION ERROR
			00000011: PROTOCOL ERROR
			Other values: RFU

La variable L2 indique le problème rencontré dans le déroulement de la transaction sans contact

L2			
Byte 1	b8-1	L2	
			00000000: OK
			00000001: Données cartes manquantes
			00000010: Méthode d'authentification carte en erreur
			00000011: Statut de la commande
			00000100: Erreur de syntaxe
			00000101: Montant sans contact dépassé
			00000110: Erreur de données de la carte
			00000111: Mode piste non supporté
			00001000: PPSE absent
			00001001: Erreur de PPSE
			00001010: Pas d'application commune
			00001011: Integrated Data Storage (IDS) READ ERROR
			00001100: Integrated Data Storage (IDS) WRITE ERROR
			00001101: Integrated Data Storage (IDS) DATA ERROR
			00001110: Integrated Data Storage (IDS) NO MATCHING AC
			RFU

Les valeurs grisées sont hors scope

Byte 1	b8-1	L3	
			00000000: OK
			00000001: TIME OUT
			00000010: STOP
			00000011: AMOUNT NOT PRESENT (montant non présent)
			RFU

8.3 Valorisation des TAC (Online Capable Pos) pour AID CB (base applicative Visa)

TVR			TAC Valeur Binaire		
Byte [1]	Bit [2]	Event	Denial	Online	Default
1	8	Offline data authentication was not performed	1	0	0
	7	Offline static data authentication failed	0	0	0
	6	ICC data missing	0	0	0
	5	Card appears on terminal exception file	1	0	0
	4	Offline dynamic data authentication failed	0	0	0
	3	Combined dynamic authentication failed	0	0	0
	2	Switch interface if offline data authentication fails and reader supports VIS	0	0	0
	1	RFU	0	0	0
2	8	ICC and terminal have different application versions	0	0	0
	7	Expired application	0	0	0
	6	Application not yet effective	0	0	0
	5	Requested service not allowed for card product	0	0	0
	4	New card	0	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
3	8	Cardholder verification was not successful	1	0	0
	7	Unrecognised CVM	1	0	0
	6	PIN Try Limit exceeded	0	0	0
	5	PIN entry required and PIN pad not present or not working	0	0	0
	4	PIN entry required, PIN pad present, but PIN was not entered	0	0	0
	3	Online PIN entered	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
4	8	Transaction exceeds floor limit	0	1	1
	7	Lower consecutive offline limit exceeded	0	0	0
	6	Upper consecutive offline limit exceeded	0	0	0
	5	Transaction selected randomly for online processing	0	0	0
	4	Merchant forced transaction online	0	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
5	8	Default TDOL used	0	0	0
	7	Issuer authentication was unsuccessful	0	0	0
	6	Script processing failed before final GENERATE AC	0	0	0
	5	Script processing failed after final GENERATE AC	0	0	0
	4	RFU	0	0	0
	3	RFU	0	0	0

	2	RFU	0	0	0
	1	RFU	0	0	0

Byte 1 is the leftmost byte ; byte 5 is the rightmost byte. – Bit 8 is the most significant bit.

TAC	DENIAL	ONLINE	DEFAULT
Valeur (Hexadécimale)	90 00 C0 00 00	*00 00 00 80 00*	*00 00 00 80 00*

Remarque : Ces TAC seront utilisés pour les AID CB A0000000421010, A0000000422010, A0000000424010, A0000000425010, pour le paiement de proximité et les automates.

Le contrôle sur la date d'expiration et l'authentification offline est à l'initiative de l'émetteur. Le terminal reste neutre quant à la décision, c'est pourquoi les TAC [1-4] et [2-7] seront toujours à {0,0,0}

8.4 Valorisation des TAC (offline only) pour AID CB (base applicative Visa)

Ces TAC sont spécifiques aux systèmes d'acceptation paiement offline only.

TVR			TAC Valeur Binaire		
Byte [1]	Bit [2]	Event	Denial	Online	Default
1	8	Offline data authentication was not performed	1	0	0
	7	Offline static data authentication failed	0	0	0
	6	ICC data missing	0	0	0
	5	Card appears on terminal exception file	1	0	0
	4	Offline dynamic data authentication failed	0	0	0
	3	Combined dynamic authentication failed	0	0	0
	2	Switch interface if offline data authentication fails and reader supports VIS	0	0	0
	1	RFU	0	0	0
2	8	ICC and terminal have different application versions	0	0	0
	7	Expired application	0	0	0
	6	Application not yet effective	0	0	0
	5	Requested service not allowed for card product	0	0	0
	4	New card	0	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
3	8	Cardholder verification was not successful	1	0	0
	7	Unrecognised CVM	1	0	0
	6	PIN Try Limit exceeded	0	0	0
	5	PIN entry required and PIN pad not present or not working	0	0	0
	4	PIN entry required, PIN pad present, but PIN was not entered	0	0	0
	3	Online PIN entered	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
4	8	Transaction exceeds floor limit	1	0	0
	7	Lower consecutive offline limit exceeded	0	0	0
	6	Upper consecutive offline limit exceeded	0	0	0
	5	Transaction selected randomly for online processing	0	0	0
	4	Merchant forced transaction online	0	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
5	8	Default TDOL used	0	0	0
	7	Issuer authentication was unsuccessful	0	0	0
	6	Script processing failed before final GENERATE AC	0	0	0
	5	Script processing failed after final GENERATE AC	0	0	0

	4	RFU	0	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0

Byte 1 is the leftmost byte ; byte 5 is the rightmost byte. – Bit 8 is the most significant bit.

TAC	DENIAL	ONLINE	DEFAULT
Valeur (Hexadécimale)	90 00 C0 80 00	*00 00 00 00 00*	*00 00 00 00 00*

Remarque : Ces TAC seront utilisés pour les AID CB A0000000421010, A0000000422010, A0000000424010, A0000000425010, pour le paiement de proximité et les automates.

Le contrôle sur la date d'expiration et l'authentification offline est à l'initiative de l'émetteur. Le terminal reste neutre quant à la décision, c'est pourquoi les TAC [1-4] et [2-7] seront toujours à {0,0,0}.

8.5 Valorisation des TAC (Online Capable Pos) pour AID CB (base applicative Mastercard)

TVR			TAC Valeur Binaire		
octet[1]	Bit	Event	Denial	Online	Default
1	8	Offline data authentication was not performed	1	0	0
	7	Offline static data authentication failed	0	0	0
	6	ICC data missing	0	1	1
	5	Card appears on terminal exception file	1	0	0
	4	Offline dynamic data authentication failed	0	0	0
	3	Combined dynamic authentication failed	1	0	0
	2	Switch interface if offline data authentication fails and reader supports VIS	0	0	0
	1	RFU	0	0	0
2	8	ICC and terminal have different application versions	0	1	1
	7	Expired application	1	0	0
	6	Application not yet effective	1	0	0
	5	Requested service not allowed for card product	1	0	0
	4	New card	0	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
3	8	Cardholder verification was not successful	1	0	0
	7	Unrecognised CVM	1	0	0
	6	PIN Try Limit exceeded	0	0	0
	5	PIN entry required and PIN pad not present or not working	0	0	0
	4	PIN entry required, PIN pad present, but PIN was not entered	0	1	1
	3	Online PIN entered	0	1	1
	2	RFU	0	0	0
	1	RFU	0	0	0
4	8	Transaction exceeds floor limit	0	1	1
	7	Lower consecutive offline limit exceeded	0	0	0
	6	Upper consecutive offline limit exceeded	0	0	0
	5	Transaction selected randomly for online processing	0	0	0
	4	Merchant forced transaction online	0	1	1
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
5	8	Default TDOL used	0	0	0
	7	Issuer authentication was unsuccessful	0	0	0
	6	Script processing failed before final GENERATE AC	0	0	0
	5	Script processing failed after final GENERATE AC	0	0	0
	4	RFU	0	0	0
	3	RFU	0	0	0

TVR			TAC Valeur Binaire		
octet[1]	Bit	Event	Denial	Online	Default
	2	RFU	0	0	0
	1	RFU	0	0	0

Byte 1 is the leftmost byte ; byte 5 is the rightmost byte. – Bit 8 is the most significant bit.

TAC	DENIAL	ONLINE	DEFAULT
Valeur (Hexadécimale)	*94 70 C0 00 00*	*20 80 0C 88 00*	*20 80 0C 88 00*

Remarque : Ces TAC seront utilisés pour les AID CB A0000000421010, A0000000422010, A0000000424010, A0000000425010, pour le paiement de proximité et les automates.

8.6 Valorisation des TAC (offline only) pour AID CB (base applicative Mastercard)

Ces TAC sont spécifiques aux systèmes d'acceptation paiement offline only.

TVR			TAC Valeur Binaire		
Byte [1]	Bit [2]	Event	Denial	Online	Default
1	8	Offline data authentication was not performed	1	0	0
	7	Offline static data authentication failed	0	0	0
	6	ICC data missing	1	0	0
	5	Card appears on terminal exception file	1	0	0
	4	Offline dynamic data authentication failed	1	0	0
	3	Combined dynamic authentication failed	1	0	0
	2	Switch interface if offline data authentication fails and reader supports VIS	0	0	0
	1	RFU	0	0	0
2	8	ICC and terminal have different application versions	1	0	0
	7	Expired application	1	0	0
	6	Application not yet effective	1	0	0
	5	Requested service not allowed for card product	1	0	0
	4	New card	0	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
3	8	Cardholder verification was not successful	1	0	0
	7	Unrecognised CVM	1	0	0
	6	PIN Try Limit exceeded	0	0	0
	5	PIN entry required and PIN pad not present or not working	0	0	0
	4	PIN entry required, PIN pad present, but PIN was not entered	0	0	0
	3	Online PIN entered	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
4	8	Transaction exceeds floor limit	1	0	0
	7	Lower consecutive offline limit exceeded	0	0	0
	6	Upper consecutive offline limit exceeded	0	0	0
	5	Transaction selected randomly for online processing	0	0	0
	4	Merchant forced transaction online	1	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0
5	8	Default TDOL used	0	0	0
	7	Issuer authentication was unsuccessful	0	0	0
	6	Script processing failed before final GENERATE AC	0	0	0
	5	Script processing failed after final GENERATE AC	0	0	0

	4	RFU	0	0	0
	3	RFU	0	0	0
	2	RFU	0	0	0
	1	RFU	0	0	0

Byte 1 is the leftmost byte ; byte 5 is the rightmost byte. – Bit 8 is the most significant bit.

TAC	DENIAL	ONLINE	DEFAULT
Valeur (Hexadécimale)	*BC F0 C0 88 00*	*00 00 00 00 00*	*00 00 00 00 00*

Remarque : Ces TAC seront utilisés pour les AID CB A0000000421010, A0000000422010, A0000000424010, A0000000425010, pour le paiement de proximité et les automates.