ANNEXES

Volume 4
Version 1.1

SOMMAIRE

1 ANNEXE 1 : TABLES MEDIAA

DESCRIPTION DES TABLES

Table 1	Mode de lecture du numéro porteur
	Lecture piste
	Lecture puce
	Saisie manuelle
	Lecture Puce sans contact
	Lecture mode Magstripe

Table 2	Type d'application carte
	EMV
	Magstripe

Table 3	Code forçage d'une transaction en autorisation et de saisie manuelle d'une autorisation
	Forçage de l'autorisation après réponse de l'émetteur
	Forçage avant la demande d'autorisation
	Saisie manuelle de l'autorisation
	Pas de forçage

Table 4	Type de transaction
	Débit
	Crédit
	Annulation
	Non abouties
	Différé de recouvrement

Table 5	Type de paiement
	Paiement de proximité
	Paiement à distance : non spécifié
	Paiement à distance :Demande par téléphone
	Paiement à distance :Demande par correspondance
	Paiement à distance : Télévision
	Paiement à distance : Demande par réseaux ouverts
	Quasi-cash
	Pré-autorisation
	Clôture
	Facture complémentaire
	Demande de renseignement

Table 6	Mode de validation
	Signature
	Ni code, ni signature

Code confidentiel

Table 9	Code raison de la demande d'autorisation
	Cumul / porteur / Application / jour
	Appel aléatoire
	Monnaie ou devise étrangère de la transaction
	Code Service / carte / porteur
	Contrôle de flux (porteur)
	Bin surveillé
	Bin inconnu
	Transaction forcée on-line par l'accepteur
	Demande de pré-autorisation
	Numéro de carte surveillé
	Carte refusée
	Carte interdite
	BIN interdit
	ARQC demandée par la carte
	On line forcé par le terminal (*)
	Dépassement seuil d'appel
	Code monnaie ou devise de l'application carte
	Demande de pré-autorisation
	Mode magstripe (sans contact)
	SDA selected
	Transaction magstripe
	Transaction Piste

(*) Les codes raison quasi-cash ainsi que les cas d'échec d'authentification sont remontés sous la raison générique 'On line forcé par le terminal'

Table 10	Résultats des vérifications de l'applicatif CB effectués par le système d'acceptation
	Non spécifié
	Carte traitée sans erreur
	Carte bloquée par le point d'acceptation
	Code confidentiel erroné pour la première fois et transaction non aboutie
	Code confidentiel erroné pour la deuxième fois et transaction non aboutie
	Code confidentiel erroné pour la troisième fois et transaction non aboutie
	Valeur d'Authentification erronée
	La carte est grillée au cours de la transaction
	La carte est interdite en liste de contrôle de numéros de porteur
	La carte est refusée en liste de contrôle de numéros de porteur
	La carte est interdite en liste de BINs
	La carte est refusée en liste de BINs
	La carte est interdite en réponse à la demande d'autorisation
	La carte est refusée en réponse à la demande d'autorisation
	Incident de structure lors du contrôle de flux
	Incident technique sur contrôle de flux
	Incident technique lors de l'acquisition des données porteur
	Incident technique lors de l'édition d'un ticket porteur
	Incident sans forçage possible lors d'une demande d'autorisation
	Monnaie ou devise d'une application carte non gérée

Table 11	Type de facture
	Facture No-show
	Facture Pré-autorisée
	Facture Complémentaire

Table 12	Type de fonction
	Télécollecte
	Téléparamètrage
	Téléchargement
	Pas de télécollecte, pas de téléparamètrage, pas de téléchargement, pas d'autorisation

Table 13	Code réponse

Phase « Ouverture de dialogue » : Réponse
Réponse Favorable
• Identification et authentification correctes
• Identification correcte
• Authentification correct
• Mode de facturation non correct - facturation forcée par l'acquéreur
Réponse Défavorable
• Identification et authentification incorrectes
• Identification incorrecte
• Authentification incorrecte
• Application non reconnue
• Type de fonction non reconnu sur le système acquéreur

Phase « Droit de parole » : Réponse
Acceptation
Acceptation avec suivi applicatif
Refus

Phase « Demande d'autorisation » : Réponse
Conforme aux codes réponses définies dans le volume 3 « Autorisation »

Table 14	Code action

Suppression de la remise transmise
Demande de reprise de la remise
Passage à la remise suivante

Table 15	Raison d'appel

Programmé par le système acquéreur (HHMM)
Changement de configuration du logiciel applicatif du système d'acceptation
Changement de configuration matérielle du système d'acceptation
Première initialisation du système d'acceptation
Vidage du fichier de transactions de l'accepteur
Mise à jour de paramètres par l'accepteur de carte
Fichier de transactions plein
Reprise suite à un incident
Appel Acquéreur
Demande d'initialisation suite à une opération de maintenance
Altération de paramètres détectée

Table 16	Code activation impression

afficher
imprimer
afficher / imprimer

Table 17	Code activation appel
	Aucune activation d'appel
	Activer Téléparamètrage
	Activer Télécollecte
	Activer Téléchargement

Table 21	Code activation application
	Désactivé
	Activé

Table 22	Code activation monnaie ou devise
	Monnaie ou devise 1 uniquement
	Monnaie ou devise 1 - Monnaie ou devise 2 simultanément
	Monnaie ou devise 2 uniquement

Table 23	Code activation impression contre valeur
	Pas d'impression de la contre valeur
	Impression de la contre valeur

Table 24	Code niveau d'acceptation associé à une plage

0	Accepté
1	Surveillé
2	Refusé
3	Interdit

Table 25	Code traitement particulier	
	2	• Traitement puce ou piste selon le premier caractère du code service (02) • Si le 1er caractère du code service a pour valeur 1 ou 5 : la technologie de traitement est piste • Si le 1er caractère du code service a pour valeur 2 ou 6 : la technologie de traitement est puce
	8	Traitement obligatoire en mode puce
	10	Carte de test puce
	99	Non significatif

Table 26	Mode de facturation Télécom
	Appelé
	Appelant

Table 27	Niveau d'acceptation d'une carte porteur
	Interdit - Blocage application carte
	Surveillé - Appel autorisation avec réponse positive obligatoire
	Refusé - Rejet de la transaction

Table 28	Identifiant de table référence
	Paramètres de l'état fonctionnel
	Données de référence du système d'acceptation
	Données de référence du point d'acceptation

Table 29	Identifiant de table	
	Monnaie ou Devise	01
	Message porteur	02
	Message accepteur de carte	03
	Paramètres accepteur	04
	Edition ticket porteur	05
	Edition ticket compte rendu	06
	Paramètres applicatifs	07
	Appel	08
	Télécommunications Autorisation	23
	Télécommunications Télécollecte	21
	Télécommunications Téléparamètrage	22
	Télécommunications Téléchargement enveloppe 1	25
	Télécommunications Téléchargement enveloppe 2	26
	Horodatage GMT	18
	Risque acquéreur	12
	Liste de contrôle de numéros de cartes porteur	13
	Liste de BINs	14
	Divers	15
	Autre monnaie ou devise	17
	Liste clés publiques d'authentification EMV	19
	Liste des AID EMV	20
	Appel aléatoire EMV	27
	TCC EMV	09
	TDOLs EMV	11
	DDOLs EMV	11
	TAC EMV	16
	Identifiant pseudo-session étendu du système d'acceptation	32
	Paramétrage du sans contact	34
	Paramétrage sans contact DRL	35
	Libellé réseau	36
	Fonctions	37
	Produits cartes non supportés	38

Table 30	Type de prise en compte
	Avec sceau

Sans sceau

Table 31	Type de transfert
	Liste complète
	Mise à jour
	Suppression

Table 32	Type de mise à jour
	Ajout
	Suppression

Table 33	Code Retour
	Prise en compte correcte
	Dépassement de capacité
	Autres

Table 34	Statut de l'application
	Activé
	Désactivé

Table 35	Code activation autre monnaie ou devise
	Désactivé
	Activé

Table 37	Type d'architecture du système d'acceptation
	Autonome
	Réparti Concentré
	Réparti Grappé

Table 38	Signe du décalage GMT
	Positif
	Négatif

Table 39	Type de liste
	Liste noire normale
	Liste noire de type 2
	Liste noire de type 3

Table 40	Type de sceau
	CRC 16

Table 41	Capacité de capture de carte
	Aucune
	Capture possible

Table 42	Capacité d'affichage et d'impression
	Aucune
	Impression
	Affichage
	Impression et affichage

Table 43	Capacité d'authentification du porteur de carte
	Pas d'authentification électronique
	Authentification par code confidentiel (PIN)

Table 44	Type de transactions acceptées
	Débit
	Crédit
	Débit - Crédit
	Débit - Annulation
	Débit - Crédit - Annulation
	Débit - Différé de recouvrement
	Débit - Crédit- Différé de recouvrement
	Débit - Annulation - Différé de recouvrement
	Débit - Crédit - Annulation - Différé de recouvrement

Table 45	Type de déclenchement de la demande d'autorisation
	Manuel
	Automatique

Table 46	Forçage autorisé
	Activé
	Désactivé

Table 47	Type de raccordement
	PAD EMA
	PAD EBAM
	NON SIGNIFICATIF

Table 48	Code activation impression taux de conversion
	Pas d'impression du taux de conversion
	Impression du taux de conversion

Table 49	Indicateur monnaie ou devise application carte non supportée
	Demande d'autorisation
	Poursuite offline
	Abandon de la transaction

Table 50	Statut de la table
	Valide
	Non valide

Table 51	Kernel ID
	Kernel C2 (MasterCard)
	Kernel C3 (Visa)

Table 53	Etape de la facture
	Initiale - Montant estimé
	Clôture - Montant exact

Table 54	Type de système d'acceptation

Opération sous contrôle de la banque	
11	Commerçant présent et ONLINE seulement (retrait guichet)
12	Commerçant présent et OFFLINE avec capacité ONLINE (retrait guichet)
13	Commerçant présent et OFFLINE (retrait guichet)
Opération sous contrôle du commerçant	
21	Commerçant présent et ONLINE seulement (paiement de proximité)
22	Commerçant présent et OFFLINE avec capacité ONLINE (paiement de proximité) Cette valeur est à retenir pour un système d'acceptation répondant aux spécifications du MPE

Table 55	Identifiant de l'applicatif du système d'acceptation

Paiement de proximité EMV
Pré-autorisation EMV
Quasi-cash EMV
VAD

Table 57	Indicateur de forçage autorisé

Forçage interdit (réponse positive obligatoire)
Forçage permis

Table 58	Libellé du message affiché ou édité Accepteur de carte application EMV

1	TYPE TRANS REFUS
2	MONNAIE REFUSEE
3	CARTE BLOQUEE
4	CARTE ARRACHEE
5	CARTE DE TEST
6	CARTE INTERDITE
7	CAPTURER CARTE
8	CARTE INVALIDE
9	CARTE MUETTE
10	CARTE PERIMEE
11	CARTE REFUSEE
12	VALIDEZ
13	ANNUL REFUSEE
14	CREDIT REFUSE
15	APPEL AUTO ?
17	NUM AUTO ?
18	FORCAGE ?
19	ABANDON
20	APPEL TELECOL
21	APPEL TELECH
22	APPEL TELEPAR
23	APPEL MAINTENEUR
24	TELECOL EN COURS
25	TELEPAR EN COURS
26	TELECH EN COURS
27	AUTOR EN COURS
28	ECHEC TELECOL

29	ECHEC TELECH
30	ECHEC TELEPAR
31	ECHEC AUTOR
32	FICHIER PLEIN
33	FICHIER VIDE
34	LECTURE PUCE
35	INCID TECHNIQUE
36	INCID IMPRESSION
37	PAIEMENT ACCEPTE
38	PAIEMENT REFUSE
39	ENREGIS INCIDENT
40	SIGNATURE
41	IMPRESSION
42	DEBIT DIFFERE ?
44	LECTURE PISTE
45	APPLI DESACTIVEE
46	DOSSIER INCONNU
47	DOSSIER DEJA ATTRIBUE
48	PAIEMENT SANS CONTACT ACCEPTE
49	PAIEMENT SANS CONTACT REFUSE

Table 59	VAD Libellé du message affiché ou édité (Accepteur de la carte)	
	1	TYPE TRANS REFUS
	2	MONNAIE REFUSEE
	3	CARTE DE TEST
	4	CARTE INTERDITE
	5	CARTE PERIMEE
	6	CARTE INVALIDE
	7	CARTE REFUSEE
	8	VALIDEZ
	9	ANNUL REFUSEE
	10	CREDIT REFUSE
	11	APPEL AUTO ?
	13	NUM AUTO ?
	14	FORCAGE ?
	15	ABANDON
	16	APPEL TELECOL
	17	APPEL TELECH
	18	APPEL TELEPAR
	19	APPEL MAINTENEUR
	20	TELECOL EN COURS
	21	TELEPAR EN COURS
	22	TELECH EN COURS
	23	AUTOR EN COURS
	24	ECHEC TELECOL
	25	ECHEC TELECH
	26	ECHEC TELEPAR
	27	ECHEC AUTOR
	28	FICHIER PLEIN
	29	FICHIER VIDE
	30	INCID TECHNIQUE
	31	INCID IMPRESSION
	32	PAIEMENT ACCEPTE
	33	PAIEMENT REFUSE

34	ENREGIS INCIDENT
35	IMPRESSION
36	DATE FIN DE VALIDITE ?
37	FIN DU NUM DANS CADRE SIGNE ?
38	APPLI DESACTIVEE
39	CARTE DE TEST
40	DOSSIER INCONNU
41	DOSSIER DEJA ATTRIBUE

Table 60 Sans Contact Libellé du message affiché ou édité (Accepteur de la carte)

Message Identifier	Message (Français) (*)	Message (English)	Information complémentaire
3	• PAIEMENT SANS CONTACT ACCEPTE • *PAIEMENT ACCEPTE*	APPROVED	Transaction acceptée
7	• PAIEMENT SANS CONTACT REFUSE • *PAIEMENT REFUSE*	NOT AUTHORISED	Transaction refusée par l'émetteur
9	• ENTRER VOTRE CODE CONFIDENTIEL, SVP • *SAISIR CODE ?*	PLEASE ENTER YOUR PIN	La demande de saisie du code est demandée (fonction non supportée sur les terminaux CB)
0F	• ERREUR DE TRAITEMENT • *ERREUR*	PROCESSING ERROR	
10	• VOUS POUVEZ ENLEVER VOTRE CARTE • *RETIREZ CARTE*	REMOVE CARD OR PLEASE REMOVE CARD	
14	BIENVENUE	WELCOME	Message d'accueil (terminal en attente).
15	PRESENTEZ CARTE	PRESENT CARD	Demande au Porteur de présenter une carte au Reader.
16	EN COURS	PROCESSING	Ce message est affiché pendant le déroulement de la transaction
17	RETIREZ CARTE	CARD READ OK REMOVE CARD OR CARD READ OK PLEASE REMOVE CARD	La carte n'est plus nécessaire à la finalisation de la transaction. Elle doit être retirée du champ.
18	• INSEREZ OU PASSEZ VOTRE CARTE • *INSEREZ CARTE*	PLEASE INSERT OR SWIPE CARD '	Ce message indique que la carte ne peut utiliser l'interface sans contact et qu'il est possible en mode contact (puce ou piste)
19	• PRESENTEZ UNE SEULE CARTE • *UNE SEULE CARTE*	PLEASE PRESENT ONE CARD ONLY	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 ACCEPTE – SIGNATURE • ACCEPT/SIGNAT.	APPROVED PLEASE SIGN	Accepté suite à une autorisation mais une signature est demandée
1B	• AUTORISATION– PATIENTEZ • *PATIENTEZ*	AUTHORISING PLEASE WAIT	Une demande d'autorisation est en cours
1C	• INSEREZ, PASSEZ OU ESSAYEZ UNE AUTRE CARTE • *INSEREZ CARTE*	INSERT, SWIPE OR TRY ANOTHER CARD	Le produit sans contact n'est pas géré par le système d'acceptation, son utilisation est donc impossible ; il est proposé au porteur de poursuivre en sans contact par lecteure d'une autre application ou de passer en contact
1D	• INSEREZ VOTRE CARTE SVP • *INSEREZ CARTE*	PLEASE INSERT CARD	Message informant le porteur que la carte peut être insérée dans le lecteur Contact
1E	PAS DE MESSAGE	[NO MESSAGE DISPLAYED]	Permet de réinitialiser l'écran, aucun message n'est affiché

20	• VOIR LES INSTRUCTIONS SUR VOTRE TELEPHONE • *VOIR MOBILE*	SEE PHONE FOR INSTRUCTIONS	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 REPRESENTER VOTRE CARTE • PRESENTEZ CARTE	PRESENT CARD AGAIN	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.

Pour les terminaux CB limité en affichage, il est demandé d'utiliser le message court identifié dans la colonne « Message Français ».

Table 61	Libellé du message multi-langues affiché ou édité pour les porteurs

Numéro MPE	Français fr	Anglais en	Allemand de	Espagnol es	Italien it
1	CARTE BLOQUEE	CARD BLOCKED	KARTE NICHT ZUGELASSEN	TARJETA BLOQUEADA	CARTA BLOCCATA
2	CARTE INVALIDE	NOT ACCEPTED	KARTE UNGULTIG	TARJETA INVALIDA	CARTA NON VALIDA
3	CARTE ARRACHEE	PROCESSING ERROR	KARTE ABGERISSEN	TARJETA EXTRAIDA	CARTA STRAPPATA
4	CARTE MUETTE	CARD ERROR	KARTE ANTWORTLOS	ERROR DE TARJETA	CARTA MUTA
5	CARTE PERIMEE	CARD EXPIRED	KARTE VERFALLEN	TARJETA CADUCADA	CARTA SCADUTA
6	CARTE REFUSEE	CARD DENIED	KARTE ABGELEHNT	TARJETA RECHAZADA	CARTA RIFIUTATA
7	DATE DEBUT INVAL	EFFECTIVE DATE NOT REACHED	ANFANGSDATUM UNGULTIG	FECHA DE INICIO NO VALIDA	DATA INIZIALE NON VALIDA
8	SAISIR CODE	ENTER PIN	GEHEIMZAHL	INTRODUZCA PIN	CODICE SEGRETO
9	DERNIER ESSAI	LAST PIN TRY	LETZTE EINGABE	ULTIMO INTENTO	ULTIMA PROVA
10	CODE BON	PIN OK	GEHEIMZAHL KORREKT	PIN CORRECTO	CODICE VALIDO
11	CODE FAUX	INCORRECT PIN	GEHEIMZAHL FALSCH	ERROR DE PIN	CODICE ERRATO
12	PATIENTEZ	PLEASE WAIT	BITTE WARTEN	ESPERE	ASPETTATE
13	PAIEMENT ACCEPTE	APPROVED	ZAHLUNG ERFOLGT	OPERACION ACEPTADA	PAGAMENTO ACCETTATO
14	PAIEMENT REFUSE	DECLINED	ZAHLUNG ABGELEHNT	OPERACION RECHAZADA	PAGAMENTO RIFIUTATO
15	MONNAIE REFUSEE	CURRENCY DENIED	WAHRUNG ABGELEHNT	DIVISA NO VALIDA	DIVISA NO VALIDA
16	INCIDENT CARTE	CARD ERROR	KARTENFEHLER	ERROR DE TARJETA	ERRORE CARTA
17	ANNUL REFUSEE	CANCEL DENIED	STORNO NICHT MOGLICH	CANCELACION RECHAZADA	CANCELLAZIONE RIFIUTATA
18	CREDIT REFUSE	REFUND DENIED	GUTSCHRIFT NICHT MOGLICH	CREDITO RECHAZADO	CREDITO RIFIUTATO
19	SIGNATURE	SIGNATURE	UNTERSCHRIFT	FIRMA	FIRMA
20	RETIREZ CARTE	REMOVE CARD	BITTE KARTE ENTNEHMEN	RETIRE SU TARJETA	RITIRARE LA CARTA
21	PUCE NON GEREE	CHIP NOT HANDLED	CHIPLESER NICHT MOGLICH	CHIP NO ACEPTADO	CHIP NON GESTITO
22	LECTURE PUCE	USE CHIP READER	CHIPLESER BENUTZEN	LECTURA CHIP	LETTURA CHIP
23	LECTURE PISTE	USE MAG STRIPE	MAGNETSTREIFE BENUTZEN	LECTURA BANDA MAGNETICA	LETTURA BANDA MAGNETICA
	INCIDENT TECHNIQUE	PROCESSING ERROR	TECHNISCHER FEHLER	PROBLEMA TECNICO	INCIDENTE TECNICO
	CARTE CAPTUREE	CARD CAPTURED	KARTE EINBEHALTEN	TARJETA NO DEVUELTA	CARTA RITIRATA
24	VOTRE CHOIX : TICKET SMS	YOUR CHOICE : RECEIPT BY SMS	BITTE WAEHLEN: BELEG PER SMS	SU ELECCION : BILLETE SMS	

25	VOTRE CHOIX : TICKET PAPIER	YOUR CHOICE : PAPER RECEIPT	BITTE WAEHLEN: DRUCKBELEG	SU ELECCION : BILLETE PAPEL	
26	VOTRE CHOIX : RENONCIATION TICKET	YOUR CHOICE : RECEIPT RENUNCIATION	BITTE WAEHLEN :	SU ELECCION : RENUNCIA BILLETE	CODICE SEGRETO
27	VOTRE CHOIX : TICKET MANUSCRIT	YOUR CHOICE : HANDWRITTEN RECEIPT	BITTE WAEHLEN: ANDSCHRIFTLICHER BELEG	SU ELECCION : RENUNCIA BILLETE MANUSCRITO INTRODUZCA PIN	
28	VOTRE CHOIX : TICKET EMAIL	YOUR CHOICE : RECEIPT BY EMAIL	BITTE WAEHLEN: BELEG PER EMAIL	SU ELECCION : BILLETE EMAIL	
29	VOTRE CHOIX : TICKET AUTRE MOYEN	YOUR CHOICE : RECEIPT BY OTHER MEANS	BITTE WAEHLEN: ANDERER BELEG	SU ELECCION : BILLETE OTRO MEDIO	

Les messages relatifs aux choix liés à la dématérialisation du ticket ne sont pas applicables au fonctionnement par défaut avec ticket.
Le libellé « VOTRE CHOIX : TICKET AUTRE MOYEN » peut être adapté aux moyens techniques de l'enseigne

Table 62	Libellé du message affiché ou édité pour les accepteurs à la fin de la transaction en sans contact		
	Numéro	Libelle	Informations
	50	CARTE INVALIDE	Des données obligatoires de la carte (AFL, AIP) sont absentes ; la transaction ne peut se poursuivre.
	51	CARTE INVALIDE	Des données permettant de vérifier la signature de la carte sont absentes. La transaction ne peut se poursuivre
	52	PROBLEME TECHNIQUE	Une zone de traitement du CDA est inférieure à la taille nécessaire.
	53	CARTE INVALIDE	La méthode d'authentification supportée par la carte n'est pas le CDA qui est la seule méthode supportée
	54	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
	55	CARTE PERIMEE	La carte est périmée et ne peut être utilisée. Sa vérification est basée sur les règles EMV.
	56	CARTE DE TEST	La carte présentée est une carte de tests dans le référentiel des listes d'acceptation.
	57	TYPE DE TRANSACTION REFUSEE	La carte n'est pas paramétrée (AUC) pour être utilisée sur ce point d'acceptation.
	58	CARTE INVALIDE	L'authentification proposée au porteur n'est pas supportée par l'application sans contact de votre terminal.
	59	CARTE INVALIDE	La carte ne possède pas de CVM list
	60	CARTE INVALIDE	L'authentification du porteur a échoué ou les authentifications du porteur ne sont pas compatibles avec celles du terminal.
	61	INCIDENT CARTE	Erreur durant le déroulement de l'authentification carte (CDA)
	62	CARTE INTERDITE	La carte étant en opposition pour motif interdit, la transaction n'a pu aboutir.
	63	CARTE REFUSE	Le Bin de la carte est refusé ou interdit dans la table des BIN de l'application.
	64	PROBLEME TECHNIQUE	Le certificat reçu de la carte n'est pas interprétable.
	65	CARTE PERIMEE	La date d'expiration est < à la date locale. Le paramétrage de la carte demande le refus de la transaction. Cette décision est uniquement une décision carte (Visa).
	66	INCIDENT CARTE	La carte demande de changer d'interface sur un échec d'authentification (Visa) Cette décision est uniquement une décision carte (Visa)
	67	ANNUL REFUSEE	Abandon de la transaction demandée par le commerçant dans le cadre d'une annulation. Cette décision concerne tous les kernels.
	68	PB AUTH PORTEUR	Un problème a été rencontré sur le Mobile durant la phase de l'authentification porteur. Ceci peut correspondre à un délai échu avant représentation du Mobile. Cette décision concerne tous les kernels
	69	REFUS EMETTEUR	Une demande d'autorisation a été transmise et la réponse de la banque émettrice est négative.
	70	CARTE INTERDITE	Une demande d'autorisation a été transmise et la réponse de la banque émettrice est de type demande de capture.
	71	PB EDITION TICKET	Erreur lors de l'impression du ticket
	72	ANNULATION REFUSE	La transaction d'annulation n'a pas été acceptée. Ceci est peut-être dû aux éléments contrôlés ou la transaction d'origine non trouvée.
	73	CREDIT REFUSE	La transaction de crédit n'a pas été acceptée.
	80	PROBLEME TECHNIQUE	La transaction n'a pas été transmise pour des problèmes de communication
	81	PROBLEME TECHNIQUE	La réponse n'est pas parvenue
	82	PROBLEME TECHNIQUE	Erreur lors de l'impression du ticket
	83	PROBLEME TECHNIQUE	Structure de la réponse invalide
	84	PROBLEME	Une demande d'autorisation a été transmise et la réponse de la

	TECHNIQUE	banque émettrice est négative.
85	REFUS PORTEUR	L'autorisation partielle a été refusée par le porteur.
86	CARTE INVALIDE	Un code retour a été transmis par la carte avant la connaissance du PAN. Cet événement ne donne pas lieu à un TNA mais à un Ticket d'abandon.
87	DELAI D'ATTENTE ECHU	Un timer est arrivé à échéance à la présentation du dispositif.

S'il y a plusieurs motifs qui ont conduit à une TNA,

- TNA le plus représentatif(voir classification ci-dessous)
- Au maximum, les cinq premiers codes raisons sont édités sur le ticket commerçant ;
- Au maximum, les deux premiers messages informatifs seront affichés à l'écran commerçant.

Le délai d'affichage est identique au délai d'affichage des messages en contact.

Les priorités d'affichage des motifs sont les suivantes :

- Problème d'authentification carte,
- Problème d'authentification porteur et mise en opposition ,
- Problème de structure carte et de validité des données (date de validité, AUC),
- Réponse émetteur

Table 63	Libellé des motifs de transaction non aboutie en contact
01	Donnée carte EMV absente
02	Erreur lors de la lecture des compteurs Carte (*),
03	Données obligatoires de la carte absentes
04	Donnée carte EMV redondante (*)
05	Erreur de format dans les données Carte (*)
06	Erreur lors de l'authentification de la Carte
07	Transaction abandonnée par le porteur lors de la saisie du code
08	Erreur lors de la vérification du code confidentiel offline
09	Erreur lors de la première demande de cryptogramme à la carte
10	Erreur lors de la seconde demande de cryptogramme à la carte
11	Transaction refusée au premier Generate AC
12	Transaction refusée au second Generate AC
13	Validation d'une transaction de crédit incorrecte (Bin non trouvé en table de BIN et mouvement initial non trouvé)
14	Validation d'une transaction d'annulation incorrecte
15	Structure de la carte invalide (Longueur, date de validité ou clé de lühn invalide)
16	Données permettant de vérifier la signature de la carte absentes
17	La carte est périmée et ne peut être utilisée
18	La carte est en opposition
19	La carte est présente en liste de contrôle en « interdit » ou « refusé »
20	La carte est présente dans la liste des BINs en « interdit » ou « refusé
21	Une demande d'autorisation a été transmise et la réponse de la banque émettrice est négative
22	La carte est interdite ou refusée en réponse à une demande d'autorisation ou la réponse de la banque émettrice demande la capture de la carte
23	Erreur lors de l'impression du ticket
24	La transaction d'annulation n'a pas été acceptée (transaction a annulée non trouvée)
25	La transaction de crédit n'a pas été acceptée
26	Problème à l'enregistrement de la transaction
27	Autorisation partielle refusée par le porteur
30	Problème de distribution du bien ou service
31	Produit carte non supporté par le point d'acceptation sur décision commerçant
87	Un timer est arrivé à échéance à la présentation de la carte. Si une TNA est enregistré le problème concerne le délai de saisie du code ou la validation du montant.

(*) Il est possible que certains événements liés à la lecture de la puce puissent être regroupés sous « Erreur lors de la lecture des données carte » si le niveau de détail réclamé est indisponible (impossibilité de différencier les données des compteurs).

Table 64	Codes Produit
	Débit
	Crédit
	Prépayé
	Professionnel

Table 65	Type de sélection
	Choix commerçant (Paramétrage acquéreur)
	Choix Porteur

2 ANNEXE 2 : TYPES DE CONFIGURATION MATERIELLES POUR LA SAISIE DU CODE CONFIDENTIEL

Dans ce type de configuration la saisie et le contrôle du code confidentiel sont réalisés sur le lecteur coupleur carte à microcircuit.

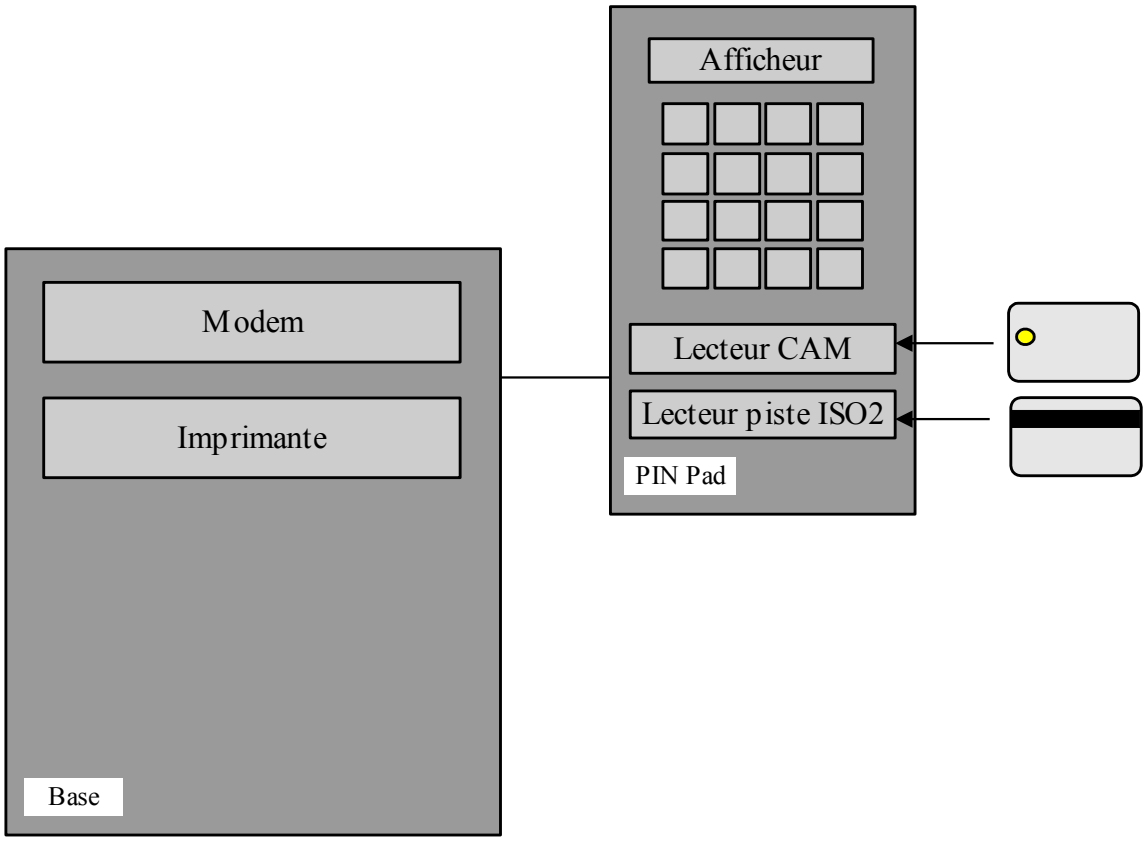


Figure 1

Lecture des cartes à microcircuit sur le PIN Pad
Lecture des cartes à pistes ISO2 sur le PIN Pad
Affichage du montant et saisie du code confidentiel sur le PIN Pad

Dans ce type de configuration la saisie et le contrôle du code confidentiel sont réalisés sur le lecteur coupleur carte à microcircuit.

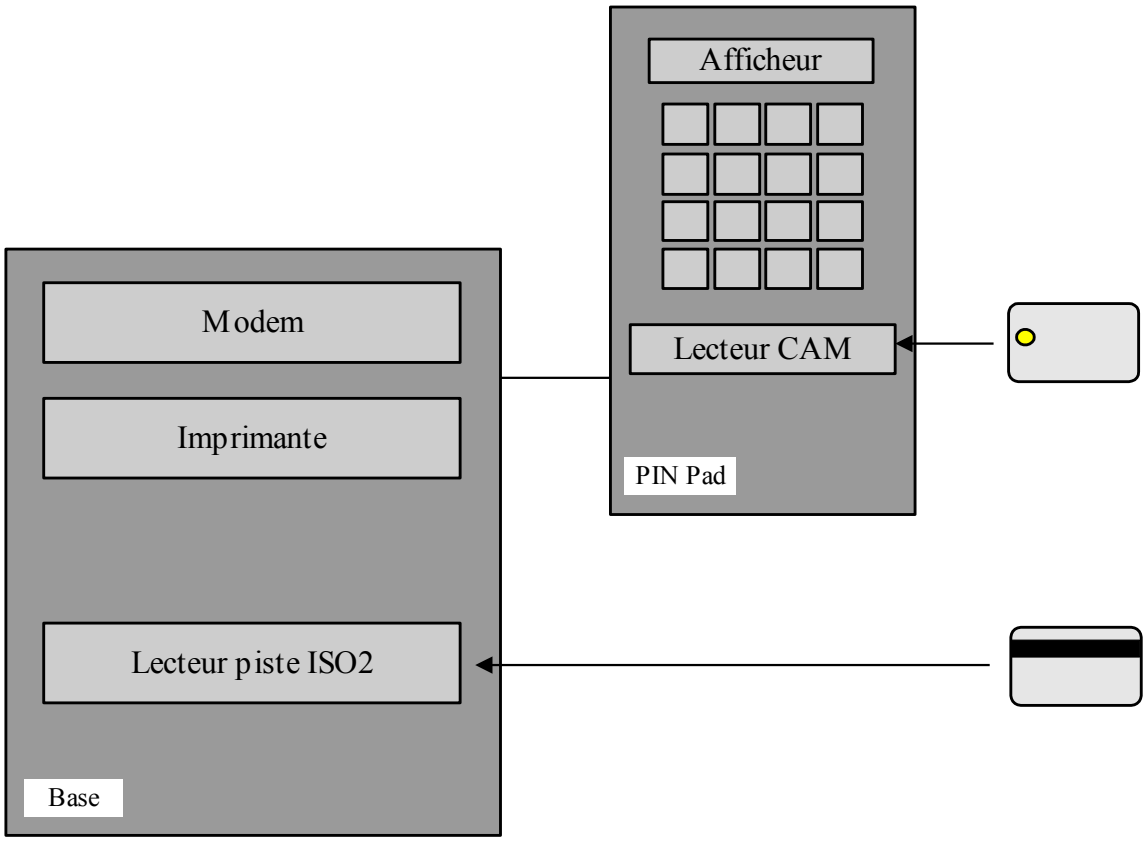


Figure 2

Lecture des cartes à microcircuit sur le PIN Pad
Lecture des cartes à pistes ISO2 sur la base du TPE
Affichage du montant et saisie du code confidentiel sur le PIN Pad

Dans ce type de configuration la saisie du code confidentiel est réalisée sur le pin-pad porteur. Le code confidentiel doit être transmis chiffré à la base du TPE conformément aux exigences sécuritaires définis dans le chapitre 7 et aux spécifications de référence EMV.

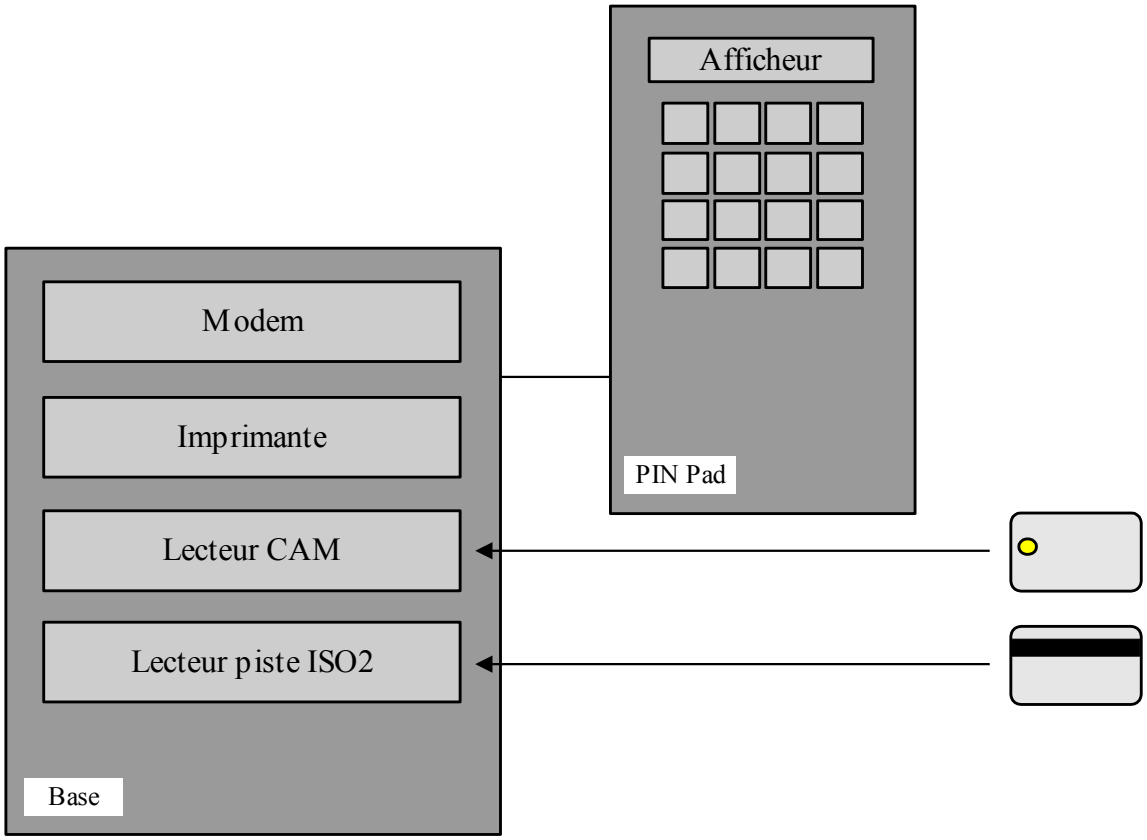


Figure 3

Lecture des cartes à microcircuit sur la base du TPE
Lecture des cartes à pistes ISO2 sur la base du TPE
Affichage du montant et saisie du code confidentiel sur le PIN Pad

3 ANNEXE 3 : ORGANISATION DES CLAVIERS PORTEUR ET COMMERÇANT

Le clavier porteur doit comporter au moins les touches suivantes (systèmes d'acceptation autonomes, répartis avec ou sans Pin-Pad ou Pin-Pad utilisés dans le cadre de la monétique intégrée) :

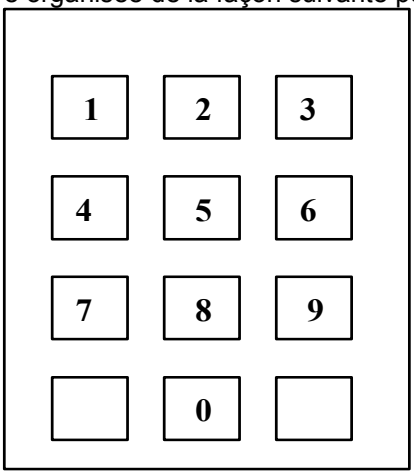
- 10 touches numériques de « 0 » à « 9 »,
- une touche correction qui permet d'annuler les derniers caractères numériques ou alphabétiques saisis par le porteur,
- une touche annulation qui annule la transaction en cours de réalisation,
- une touche validation qui confirme l'action réalisée par le porteur ou l'accepteur,
- des touches alphabétiques, éventuellement.

Les touches de correction, annulation et validation sont respectivement caractérisées par les couleurs et symboles ci-après :

Touche	Couleur	Codification Française	Standard EBS
Correction	jaune	« C »	<
Annulation	rouge	« A »	X
Validation	vert	« V »	O

La disposition des touches numériques et des touches de fonction doit être conforme à la norme prEN1332-3 de décembre 99.

La disposition des touches sur le clavier porteur et le clavier de l'accepteur doit être identique pour les équipements autonomes. Elle doit être organisée de la façon suivante pour les touches numériques :



La touche « 5 » doit pouvoir être identifiée de façon tactile.
En paiement de proximité, l'afficheur de l'accepteur et du porteur doivent pouvoir être dissociés.
L'afficheur destiné au porteur doit disposer d'au moins 2 lignes de 16 caractères.

Dans le cas des systèmes répartis type "Monétique Intégrée" où le clavier commerçant peut être de type "PC" la disposition de celui-ci devra être conforme à la norme ISO 9995-4 et 9995-6

4 ANNEXE 4 : DICTIONNAIRE DES MESSAGES

Les messages définis ci-après constituent une base de référence minimale obligatoire à implémenter sur les systèmes d'acceptation.

Les messages téléparamétrables seront identiques et normalisés quel que soit le système acquéreur concerné.

Pour ne pas perturber l'accepteur, aucun message d'erreur, suite à des contrôles, ne doit être affiché pour une transaction aboutie.

Pour les terminaux qui ne disposent pas d'un écran permettant l'affichage tel que défini, les messages seront proposés dans une présentation déroulante (horizontale ou verticale).

4.1 MESSAGES NOYAU A DESTINATION DU PORTEUR

LIBELLE	DEFINITION	FE / BF
MONTANT xxx « yyy »	affichage du montant dans la monnaie sélectionnée « yyy »	4.1.6
INSEREZ CARTE	affichage consécutif à la validation des données de la transaction / attente d'acquisition d'un moyen de paiement	BF20
CARTE MUETTE	carte à microcircuit muette ou réponse incohérente à la RAZ	26.1.1
CARTE NON LUE	carte à piste mal lue	25.1.2
RETIREZ CARTE	données de la carte (microcircuit ou piste) non acquises	25.2.1 / 26.1.2 / 40.1.3
PATIENTEZ	traitements internes du noyau en cours	11.1.1
ABANDON	abandon des traitements internes du noyau en cours, carte introduite non conforme	25.4.4
PUCE NON GEREE	Carte à puce non gérée par le système d'acceptation (pas d'application commune). Cet événement correspond à un AID non supporté	BF20

4.2 MESSAGES A DESTINATION DU PORTEUR (PROXIMITE / QUASICASH)

LIBELLE	Numéro de message	DEFINITION	FE / BF
CARTE BLOQUEE	1	blocage du microcircuit (toutes applications)	30.2.8
CARTE INVALIDE	2	contrôles d'acceptabilité négatifs (fichiers carte non corrects, données redondantes, lecture incorrecte des fichiers et enregistrements de l'AFL ou des compteurs pour une carte CB EMV) 2nd et 3ème caractère du code service inconnu pour une carte ISO2 Longueur piste ISO2 hors norme ou clé de luhn non valide	30.1.1 / 30.2.1 / 30.1.3 / 30.1.8 / 30.3.9 6.3.1 / 6.3.2 / 6.3.3 6.1.4 / 8.1.1
CARTE ARRACHEE	3	carte arrachée avant la finalisation de la transaction	BF4 / BF5 / BF6
CARTE MUETTE	4	carte muette avant la finalisation de la transaction	30.3.24
CARTE PERIMEE	5	Carte avec date de fin de validité antérieure à date locale ISO2 + EMV si traitements non finalisés	6.4.1 / 30.3.10
CARTE REFUSEE	6	Niveau d'acceptation 'Refusé' dans la table des bins ou liste de contrôle + interdit en fichier transaction (ISO2) + 'Refusé' ou' Interdit' pour transaction EMV non finalisée. Produit carte refusée sur décision commerçant.	9.1.1 / 9.1.2 / 9.1.3 / 30.3.5 / 30.3.7 / 30.3.8 / 30.4.2 30.4.5
DATE DEBUT INVAL	7	Carte à microcircuit avec date de début de validité postérieure à date locale	30.3.10
SAISIR CODE	8	saisie du code confidentiel (tous essais sauf dernier)	30.1.5
DERNIER ESSAI	9	saisie du dernier code confidentiel	30.3.1
CODE BON	10	le code saisi est correct	30.3.1
CODE FAUX	11	le code saisi est faux	30.3.1
PATIENTEZ	12	traitements applicatifs en cours (contrôle SDA, DDA, demande d'autorisation, …)	BF4 / BF5 / BF6 BF(sans contact)
PAIEMENT ACCEPTE	13	transaction acceptée et enregistrée Dans un environnement mPOS, l'équipement affichera "Paiement Accepté" dans la langue du porteur sur le terminal.	14.2.1 / 14.2.2 / 14.2.3/ 30.4.4 / 30.4.6 / 30.4.7
PAIEMENT REFUSE	14	contrôles applicatifs négatifs (montant min, montant max, traitement dégradé EMV étrangère avec transaction non aboutie absente, autorisation refusée ou interdite) type de transaction non activé + tous traitements EMV conduisant à la non acceptation de la transaction	5.3.4 / 5.3.1 / 6.1.2 / 10.2.4 6.4.9 / 30.4.5
MONNAIE REFUSEE	15	contrôle d'acceptabilité de la monnaie négatif	30.3.14
INCIDENT CARTE	16	incidents techniques carte (échec	30.6.3/ 30.3.24

		traitement script, Erreur d'authentification carte (SDA, DDA ou CDA …)	30.2.15, 30.6.4
ANNUL REFUSEE	17	fonctionnalité désactivée par acquéreur ou contrôles négatifs (n° version application, AUC non géré, données carte redondantes). absence de transaction débit initiale validation finale par accepteur incorrecte	6.4.9 / 30.2.1 30.3.9 / 30.3.6 30.3.17 / 11.1.9
CREDIT REFUSE	18	fonctionnalité désactivée par acquéreur ou contrôles négatifs (n° version application, AUC non géré, données carte redondantes). absence de transaction débit initiale si bin inconnu validation finale par accepteur incorrecte	6.4.9 / 30.2.1 30.3.19 / 30.3.6 30.3.9 / 9.1.1 30.3.8 / 30.3.19 11.1.10 / 9.1.3
SIGNATURE	19	transaction à signer par porteur : carte traitée en mode piste avec montant supérieur à la réglementation en vigueur ou CVM list = signature	5.3.5 / 30.1.6
RETIREZ CARTE	20	fin des traitements de la carte porteur ou dépassement de la temporisation de saisie du code confidentiel	14.2.1 / 14.2.2 / 14.2.3 / 30.4.4 / 30.4.5 / 30.4.6 / 30.4.7 / 30.1.5 / 40.1.3
PUCE NON GERE	21	carte à puce EMV à traiter en mode piste	BF20
LECTURE PUCE	22	carte EMV traitée en piste (code service 2xx ou 6xx ou code traitement particulier requiert la lecture puce)	6.3.5 / 30.3.25
TICKET SMS	24	Le porteur opte pour un ticket électronique de la transaction qui lui est remis par SMS.	5.1.3
TICKET PAPIER	25	Le porteur demande le ticket de la transaction sur papier Cette information n'est pas affichée si c'est la seule possibilité du point d'acceptation.	5.1.3
PAS TICKET	26	Le porteur renonce au ticket.	5.1.3
TICKET MANUSCRIT	27	Le commerçant produit un ticket manuscrit.	5.1.3
TICKET EMAIL	28	Le porteur opte pour un ticket électronique de la transaction qui lui est remis par mail.	5.1.3
TICKET AUTRE CANAL	29	Le commerce propose de diffuser les tickets selon les moyens aux moyens techniques adapté à l'enseigne	5.13
Selon les capacités du terminal MONTANT XXXXX,XX RESTE DU : XXXXX,XX Ou MONTANT DU PAIEMENT MONTANT DU COMPLEMENT	32	En autorisation partielle, il est demandé au commerçant de valider le choix du porteur qui peut accepter ou refuser de régler le complément par un autre moyen de paiement. La validation se fera conformément au Volume 4- Ergonomie	30.9.1

Les messages complémentaires pour le sans contact en paiement face à face sont définis dans la table 60 et reposent sur des messages normalisés EMV issus d'Entry Point et des Kernels C2 et C3.

4.3 MESSAGES NOYAU A DESTINATION DE L'ACCEPTEUR

LIBELLE	DEFINITION	FE / BF
DATE (JJ/MM/AA)	saisie date système	1.8.4
HEURE (HH : MM)	saisie heure système	1.8.4
ABANDON	abandon des traitements internes, dépassement de la temporisation de saisie du montant, sélection touche abandon par abandon par accepteur	5.1.1
PATIENTEZ	traitements internes au noyau en cours	
NUM CAISSE	saisie du numéro de caisse	1.8.3
NUM STANDARD	saisie du numéro de standard éventuel	1.8.2
TYPE NUM	saisie du type de numérotation	1.8.2
CARTE COMMERCANT	accès à des fonctions du noyau (menus, maintenance,...)	
CARTE INVALIDE	carte à piste invalide pour l'accès aux menus noyau ou maintenance	
CARTE NON LUE	carte à piste mal lue	25.1.2
IMPRIMANTE HS	imprimante hors service	19.1.1 / 19.1.2
LECTEUR HS	lecteur piste ou puce hors service	
PROGRAMME HS	perte du logiciel applicatif	
APPEL MAINTENEUR	Problème d'intégrité du logiciel noyau ou périphérique HS	
TELECH EN COURS	téléchargement du logiciel en cours	
ECHEC TELECH	échec de téléchargement du logiciel applicatif ou noyau	
TYPE TRANSACTION	sélection explicite du type de transaction utilisé (débit, crédit , annulation)..	4.1.1 / 4.1.3 / 4.1.5 4.2.9
MONTANT ? xxx « yyy »	saisie du montant et sélection de la monnaie	4.1.6 / 5.1.1
INSEREZ CARTE	affichage consécutif à la validation des données de la transaction (montant/monnaie)	
RETIREZ CARTE	données de la carte (microcircuit ou piste) non acquises	25.2.1 / 26.1.2 / 40.1.3
VALIDEZ	montant et monnaie saisis mais non validés	5.1.1
CARTE MUETTE	carte à microcircuit muette ou réponse incohérence à la raz	26.1.1
RETOUR SUR SOCLE	terminaux portables nécessitant d'être reposés sur leur socle lors des transmissions	
NUMERO PORTEUR ?	Saisie manuelle du numéro porteur en VAD	25.1.4

4.4 MESSAGES APPLICATIFS A DESTINATION DE L'ACCEPTEUR

LIBELLE	DEFINITION	FE / BF
INITIALISATION	mise en service d'une application ou mise à jour des paramètres d'une application	BF3/BF30
CARTE COMMERCANT	attente passage carte commerçant (carte accepteur)	25.1.2
NUM LOG SYSTEME	saisie ou mise à jour du numéro logique du système d'acceptation	2.3.3
NUM LOG POINT	saisie ou mise à jour du numéro logique du point d'acceptation (configuration réparti)	2.3.2
ADRES RACCORDEMT	saisie ou mise à jour de l'adresse de raccordement principal pour la communication avec le système acquéreur de téléparamétrage	2.6.3
ADRES APPEL	saisie ou mise à jour de l'adresse d'appel principal pour la communication avec le système acquéreur de téléparamétrage	2.6.3
TYPE RACCORDEMT	saisie ou mise à jour du type de raccordement utilisé par l'adresse de raccordement (EBAM, EMA)	2.6.3
CODE BANQUE	saisie obligatoire lors de la mise en service d'une application du code banque de l'organisme acquéreur	2.5.1
APPEL TELEPAR	déclenchement d'une phase de téléparamétrage ou phase de numérotation du système d'acceptation	BF3
TELEPAR EN COURS	communication en cours avec le serveur acquéreur de téléparamétrage	BF3
ECHEC TELEPAR	communication interrompue (anomalie) avec le serveur acquéreur de téléparamétrage	BF3
MANTENANCE	opération de maintenance effectuée par l'opérateur	
BASCULE SECOURS	Activation manuelle sur le réseau de secours (adressage réseau diffèrent entre le serveur nominal et le serveur de secours)	

4.5 MESSAGES A DESTINATION DE L'ACCEPTEUR (PROXIMITE / QUASI-CASH)

LIBELLE	Numéro de message	DEFINITION	FE / BF
TYPE TRANS REFUS	1	type de transaction refusé par l'application sélectionnée	6.4.9
MONNAIE REFUSEE	2	monnaie sélectionnée par accepteur ou porteur refusée par l'application sélectionnée	30.3.14
CARTE BLOQUEE	3	Blocage du microcircuit à l''initialisation (toutes applications) suite à script émetteur	30.2.8
CARTE ARRACHEE	4	carte à microcircuit arrachée avant la finalisation des traitements	BF4 / BF5 / BF6
CARTE DE TEST	5	traitement d'une carte de test	6.1.5 / 6.3.5
CARTE INTERDITE	6	carte ayant fait l'objet d'une interdiction en liste de BINs; liste de contrôle, code retour en autorisation, présence carte dans fichier transaction avec code retour interdit avec abandon dès détection pour les cartes ISO2 et lors d'abandon à la finalisation de la transaction (1er ou 2nd generate AC)	30.3.5 / 30.3.7 / 30.3.8 30.4.2 / 10.2.4
CAPTURER CARTE	7	carte ayant fait l'objet d'une interdiction en liste de BINs, liste de contrôle, code retour en autorisation, présence carte dans fichier transaction avec code retour interdit (conditions idem au message précédent)	30.3.5 / 30.3.7 / 30.3.8 30.4.2 / 10.2.4
CARTE INVALIDE	8	contrôles d'acceptabilité négatifs (fichiers carte non corrects, données redondantes, lecture incorrecte des fichiers et enregistrements de l'AFL ou des compteurs pour une carte CB EMV 2nd et 3eme caractère du code service inconnu pour une carte ISO2 Longueur piste ISO2 hors norme ou clé de luhn non valide Carte ISO 2 périmée	30.1.1 / 30.2.1 / 30.1.3 / 30.1.8 6.3.1 / 6.3.3 6.1.4 / 8.1.1
CARTE MUETTE	9	carte muette pendant la communication	BF 4 / BF 5 / BF6 BF20
CARTE PERIMEE	10	carte avec date de fin de validité antérieure à date locale pour piste ISO2 + EMV si non finalisation de la transaction	6.4.1 / 30.3.10
CARTE REFUSEE	11	niveau d'acceptation carte « refusée » (table des BINs, liste de contrôle)	9.1.1 / 9.1.2 30.3.7 / 30.3.5 / 6.3.1 / 6.3.2 / 6.3.3

VALIDEZ	12	validation de l'annulation d'une transaction quelconque ou validation d'une transaction de crédit ou traitements divers à valider (édition du 2ème ticket, anomalie, ...)	11.1.9 / 11.1.10 BF 4 / BF 5 / BF6 BF20 BF521SC Kernel C2 / BF522SC Magstripe / BF523SC Kernel C3 / BF621SC Kernel C2 / BF622SC Magstripe / BF623SC Kernel C3
ANNUL REFUSEE	13	fonctionnalité désactivée par acquéreur ou contrôles négatifs (n° version application, AUC non géré, données carte redondantes). absence de transaction débit initiale validation finale par accepteur incorrecte débit initial déjà annulé	6.4.9 / 30.3.17 11.1.9 / 11.1.12 30.1.3 / 30.1.8 / 30.2.1 / 40.3.17
CREDIT REFUSE	14	fonctionnalité désactivée par acquéreur ou contrôles négatifs (n° version application, AUC non géré, données carte redondantes). absence de transaction débit initiale validation finale par accepteur incorrecte Bin inconnu	6.4.9 / 30.3.19 / 11.1.10 / 30.1.3 / 30.2.1 / 30.2.8
APPEL AUTO ?	15	proposition d'appel à autorisation	10.2.5 / 10.2.7
NUM AUTO ?	17	proposition de saisie d'un numéro d'autorisation obtenu en appel phonique	10.2.6
FORCAGE ?	18	Proposition de forçage de la transaction avant ou après la demande d'autorisation si celle-ci ne requiert pas de réponse positive obligatoire (donnée positionné par acquéreur)	11.1.1 / 11.1.2 30.3.18
ABANDON	19	abandon des traitements applicatifs par action explicite de l'accepteur	BF4 / BF5 / BF6 BF20
APPEL TELECOL	20	déclenchement d'une phase de télécollecte ou phase de numérotation du système d'acceptation	16.1.1
APPEL TELECH	21	déclenchement d'une phase de téléchargement logiciel ou phase de numérotation du système d'acceptation	BF1
APPEL TELEPAR	22	déclenchement d'une phase de téléparamétrage ou phase de numérotation du système d'acceptation	BF3
APPEL MAINTENEUR	23	Pb intégrité des données des applications (avec perte de paramètres d'appel) ou du logiciel applicatif ou périphérique HS	
TELECOL EN COURS	24	communication en cours avec le serveur acquéreur de télécollecte	30.6.1 / 30.6.2 / 16.1.1 / 16.1.3 / 16.1.4
TELEPAR EN COURS	25	communication en cours avec le serveur acquéreur de téléparamétrage	BF3
TELECH EN COURS	26	communication en cours avec le serveur acquéreur de téléchargement logiciel	BF1

AUTOR EN COURS	27	communication en cours avec le serveur acquéreur d'autorisation	10.2.1
ECHEC TELECOL	28	communication interrompue (anomalie) avec le serveur acquéreur de télécollecte	16.1.1
ECHEC TELECH	29	communication interrompue (anomalie) avec le serveur acquéreur de téléchargement logiciel	BF1
ECHEC TELEPAR	30	communication interrompue (anomalie) avec le serveur acquéreur de téléparamétrage	BF3
ECHEC AUTOR	31	communication interrompue (anomalie) avec le serveur acquéreur d'autorisation	10.2.1
FICHIER PLEIN	32	fichier transaction plein	14.2.4
FICHIER VIDE	33	information en cas de déclenchement manuel de la télécollecte	16.1.1
LECTURE PUCE	34	carte à microcircuit traitée en piste (code service 2xx ou 6xx) ou code traitement requièrant la lecture puce	6.3.5 / 30.3.25
INCID TECHNIQUE	35	incident technique d'enregistrement de la transaction	14.2.1 / 14.2.2 / 14.2.3 / 14.2.5 30.4.4 / 30.4.6 / 30.4.7 / 30.4.5
INCID IMPRESSION	36	incident d'impression lors de l'édition d'un ticket porteur	19.1.1 / 19.1.2 / 19.1.3 / 30.7.1 / 30.7.3 / 30.7.4 5.1.2
PAIEMENT ACCEPTE	37	Transaction acceptée et enregistrée Après affichage du message porteur, le commerçant validera le message et l'équipement affichera "Paiement accepté" en Français	14.2.1 / 14.2.2 / 14.2.3 / 30.4.4 / 30.4.6 / 30.4.7
PAIEMENT REFUSE	38	contrôles applicatifs négatifs (montant min, montant max, traitement dégradé piste refusé, réponse autorisation refus, ...) + tous traitements conduisant à la non acceptation de la transaction (TAC/IAC, réponse émetteur, ..)	5.3.1 / 5.3.4 / 6.1.2 / 10.2.4 / 30.4.5 / 30.2.7
ENREGIS INCIDENT	39	enregistrement d'une transaction non aboutie	14.2.5 / 30.4.5
SIGNATURE	40	transaction à signer par porteur : carte traitée en mode piste avec montant supérieur à la réglementation en cours ou CVM list = signature	5.3.5 / 30.1.6
IMPRESSION	41	message générique affiché pendant l'impression de tous les tickets (porteur , totalisateur, édition de paramètres, ...)	30.7.1 / 30.7.3 / 30.7.4 / 30.7.6 / 30.7.2 / 30.7.5 / 30.7.7 19.1.1 / 19.1.2 / 19.1.3 / 19.1.4 / 19.1.5 / 19.1.8 / 19.4.3 / 19.5.2 / 19.5.3 / 19.6.1 / 19.7.3 / 19.7.6 /
PUCE NON GEREE	43	carte à puce EMV à traiter en mode piste	BF20

LECTURE PISTE	44	carte EMV muette à la raz à traiter en mode dégradé piste si carte agréée CB (traitement piste-puce-piste)	30.3.24
APPLI DESACTIVEE	45	Application CB désactivée par l'acquéreur et pas de meilleur indice fourni par les autres applications	30.5.15
DOSSIER INCONNU	46	Dans une transaction PLBS (clôture, facture complémentaire), le dossier n'a pas été trouvé.	35.5.8
DOSSIER DEJA ATTRIBUE	47	Dans une transaction PLBS (Demande de renseignement, pré-autorisation), le dossier existe déjà.	
PAIEMENT SANS CONTACT ACCEPTE	48	transaction sans contact acceptée et enregistrée	40.7.1
PAIEMENT SANS CONTACT REFUSE	49	contrôles applicatifs négatifs (montant min, montant max, traitement dégradé piste refusé, réponse autorisation refus, ...) + tous traitements conduisant à la non acceptation de la transaction sans contact (TAC/IAC, réponse émetteur, ..)	40.7.2 40.2.5

Pour les systèmes intégrés, Les messages “APPEL TELEPAR”, “APPEL TELECOL”, TELEPAR EN COURS, TELECOL EN COURS peuvent être substitués par d’autres messages ayant le même sens.

Les messages complémentaires pour le sans contact en paiement face à face sont définis dans la table 60 et reposent sur des messages normalisés EMV issus d’Entry Point et des Kernels C2 et C3

.

4.6 MESSAGES A DESTINATION DE L'ACCEPTEUR (SAISIE MANUELLE)

LIBELLE	Numéro de message	DEFINITION	FE / BF
TYPE TRANS REFUS	1	type de transaction refusé par l'application sélectionnée	6.4.9
MONNAIE REFUSEE	2	monnaie sélectionnée par accepteur ou porteur refusée par l'application sélectionnée	30.3.14
CARTE DE TEST	3	traitement d'une carte de test	6.1.5
CARTE INTERDITE	4	carte ayant fait l'objet d'une interdiction en liste de BINs, liste de contrôle, code retour en autorisation, présence carte dans fichier transaction avec code retour interdit	10.2.4 / 9.1.1 / 9.1.2 / 9.1.3
CARTE PERIMEE	5	carte avec date de fin de validité antérieure à date locale	6.4.4
CARTE INVALIDE	6	contrôles d'acceptabilité négatifs (clé de Luhn, période de validité, ...)	6.1.4 / 6.4.4 / 8.1.1
CARTE REFUSEE	7	niveau d'acceptation carte « refusée » (table des BINs, liste de contrôle)	9.1.1 / 9.1.2 / 9.1.3
VALIDEZ	8	validation de l'annulation d'une transaction quelconque ou validation d'une transaction de crédit ou traitements divers à valider (édition du 2ème ticket, ...)	11.1.9 / 11.1.10
ANNUL REFUSEE	9	fonctionnalité désactivée par acquéreur ou contrôles négatifs	9.1.1/ 11.1.9 / 11.1.12
CREDIT REFUSE	10	fonctionnalité désactivée par acquéreur ou contrôles négatifs	11.1.10 / 9.1.1
APPEL AUTO ?	11	proposition d'appel à autorisation	10.2.5 / 10.2.7
NUM AUTO ?	13	proposition de saisie d'un numéro d'autorisation obtenu en appel phonique	10.2.6
FORCAGE ?	14	Proposition de forçage de la transaction avant ou après la demande d'autorisation dans le cas où celle-ci ne requiert pas de réponse positive obligatoire	11.1.1 / 11.1.2 / 10.2.1
ABANDON	15	abandon des traitements applicatifs par action explicite de l'accepteur	
APPEL TELECOL	16	déclenchement d'une phase de télécollecte ou phase de numérotation du système d'acceptation	16.1.1
APPEL TELECH	17	déclenchement d'une phase de téléchargement logiciel ou phase de numérotation du système d'acceptation	BF1

LIBELLE	Numéro de message	DEFINITION	FE / BF
APPEL TELEPAR	18	déclenchement d'une phase de téléparamétrage ou phase de numérotation du système d'acceptation	BF3
APPEL MAINTENEUR	19	Pb intégrité des données des applications (avec perte de paramètres d'appel) ou du logiciel applicatif ou périphérique HS	
TELECOL EN COURS	20	communication en cours avec le serveur acquéreur de télécollecte	16.1.1
TELEPAR EN COURS	21	communication en cours avec le serveur acquéreur de téléparamétrage	BF3
TELECH EN COURS	22	communication en cours avec le serveur acquéreur de téléchargement logiciel	BF1
AUTOR EN COURS	23	communication en cours avec le serveur acquéreur d'autorisation	10.2.1
ECHEC TELECOL	24	communication interrompue (anomalie) avec le serveur acquéreur de télécollecte	16.1.1
ECHEC TELECH	25	communication interrompue (anomalie) avec le serveur acquéreur de téléchargement logiciel	BF1
ECHEC TELEPAR	26	communication interrompue (anomalie) avec le serveur acquéreur de téléparamétrage	BF3
ECHEC AUTOR	27	communication interrompue (anomalie) avec le serveur acquéreur d'autorisation	10.2.1
FICHIER PLEIN	28	fichier transaction plein	14.2.4
FICHIER VIDE	29	information en cas de déclenchement manuel de la télécollecte	16.1.1
INCID TECHNIQUE	30	incident technique d'enregistrement de la transaction	14.2.1 / 14.2.2 / 14.2.3 / 14.2.5
INCID IMPRESSION	31	incident d'impression lors de l'édition d'un ticket porteur	19.1.7 / 19.1.8 19.1.14 / 19.1.15
PAIEMENT ACCEPTE	32	transaction acceptée et enregistrée	14.2.1 / 14.2.2 / 14.2.3
PAIEMENT REFUSE	33	contrôles applicatifs négatifs (montant min, montant max, réponse autorisation refus, ...)	5.3.1 / 5.3.4 / 10.2.4
ENREGIS INCIDENT	34	enregistrement d'une transaction non aboutie	14.2.5
IMPRESSION	35	message générique affiché pendant l'impression de tous les tickets (porteur , totalisateur, édition de paramètres, ...)	19.1.7 / 19.1.8 / 19.1.14 / 19.1.15 / 19.1.4 / 19.4.3 / 19.5.2 / 19.5.3 / 19.6.1 / 19.7.3 / 19.7.6
DATE FIN DE VALIDITE ?	36	saisie de la date de fin de validité	25.1.5
FIN DU NUM DANS CADRE SIGNE ?	37	Saisie du cryptogramme visuel (CVV2 - CVC2 - CBN2)	25.1.6
APPLI DESACTIVEE	38	Application CB désactivée par l'acquéreur et pas de meilleur indice fourni par les autres applications	4.1.16

5 ANNEXE 5 : LISTE DES BINS

Les listes de BIN sont diffusées par le GIE CB (S.I.C.B) auprès des établissements acquéreurs.

5.1 CALCUL DU SCEAU

Le scellement des données de la table des BIN transmise au système d'acceptation est obligatoire.

Le calcul du sceau doit être réalisé selon l'algorithme « CRC 16 ».
Le polynôme utilisé est x^16 + x^12 + x^5 + 1 (cf norme ISO 3309).

Le SICB (Système Information Cartes Bancaires) transmet la table de BIN au système acquéreur. A la réception, celui-ci calcule un sceau au format ASCII à partir des données intrinsèques reçues.

Lors de la phase de téléparamétrage, à la fin de la réception de la table des BIN, le système d'acceptation fournit au système acquéreur, le sceau qu'il aura calculé. Le système acquéreur vérifie alors l'égalité de ce sceau avec celui mémorisé lors de la réception de la table du SICB.

Les données propres à la table des BIN rentrent dans le calcul :

- Longueur du début de la plage
- Début de plage BIN
- Longueur de la fin de la plage de BIN
- Fin de plage BIN
- Code niveau d'acceptation associé à une plage
- Code traitement particulier

Les éléments liés au transport (bitmap, caractères de contrôle, …) ne sont pas pris en compte, ni le type 'T' et la longueur 'L' des données téléparamétrées.

6 ANNEXE 6 : ERGONOMIES AFFICHAGE - SELECTION

6.1 PRESENTATION

Il s'agit de regrouper dans ce chapitre les spécifications communes à plusieurs traitements portant sur les conditions d'utilisation des touches du clavier et de l'affichage des messages des équipements d'acceptation.

Ces règles s'appliquent aux processus à choix multiples comme notamment:

- La sélection d'une langue lorsque plusieurs langues sont proposées au porteur,
- La procédure de forçage d'une transaction par le commerçant,
- La sélection d'une application par le porteur dans le cadre du multi-applications.

6.2 REGLES COMMUNES DE DEFILEMENT ECRAN ET DE SELECTION

Pour chaque processus dans lequel un choix est proposé au porteur (ou au commerçant), les règles d'ergonomie retenues sont les suivantes :

- Le défilement est cyclique et le déplacement s'effectue par les touches ' **^**' (déplacement vers le haut) et 'v' (déplacement vers le bas).
- L'utilisation de la touche verte (Validation) permet de sélectionner l'option pointée par le caractère '**<**'.
- L'utilisation de la touche rouge (abandon/annulation) permet d'abandonner (ou d'annuler) l'opération en cours.

Le principe du défilement est le suivant :

- Le caractère '<' est positionné sur la ligne courante en dernière position (selon la taille de l'écran),
- La ligne courante est en sur-brillance ou en vidéo inverse,
- Les touches ' ^' et 'v' permettent le défilement vers le haut et vers le bas.

Pour les terminaux qui ne possèdent pas les touches ' ^' et 'v', la touche jaune ou touches de fonction est utilisée à la place de la touche 'v' avec un défilement cyclique vers le bas.

La navigation peut s'effectuer par les touches de fonctions suivantes :

- F3 ou sur la touche '^' (déplacement vers le haut)
- F2 ou sur la touche 'v' (déplacement vers la bas)

6.3 SELECTION DE LA LANGUE PAR LE PORTEUR

Le choix multiple porte sur la langue dans laquelle seront affichés les messages et indications de déroulement d'une transaction lorsque le système d'acceptation propose plusieurs langues au porteur.

La sélection d'une langue se fait suivant les règles précisées au paragraphe '6.2 Règles communes de défilement et de sélection'.

6.4 FORÇAGE D'UNE TRANSACTION PAR LE COMMERÇANT

Le choix multiple est constitué des deux possibilités suivantes (selon le paramétrage acquéreur) :

- APPEL AUTO ?
- FORCAGE ?

La sélection d'une option (action) se fait suivant les règles précisées au paragraphe '6.2 Règles de défilement et de sélection'.

6.5 SELECTION D'UNE APPLICATION DANS LE CADRE DU MULTI-APPLICATIONS

6.5.1 Principes

Le choix multiple est constitué de la liste des applications présentes dans le cadre de l'acceptation des cartes multi-applicatives.

La sélection d'une application parmi celles présentées au porteur se fait suivant les règles précisées au paragraphe 'Règles de défilement et de sélection'.

Le choix de l'application est de la responsabilité exclusive du porteur, seul habilité à choisir une application parmi celles qui lui sont présentées.

Le commerçant ne doit pas avoir la possibilité de choisir une application à la place du client si ce dernier ne sélectionne ou ne valide aucune application.

Lors de la sélection de l'application par le client, sur un terminal avec PIN PAD, le nom de l'application ne doit pas apparaître sur l'écran du commerçant.
De plus, aucune touche accessible au commerçant ne doit être active pendant le choix du client, à l'exception de la touche annulation/abandon qui permet au commerçant uniquement d'abandonner la transaction.

6.5.2 Affichage du nom de l'application

L'affichage du nom de l'application (« Application Preferred Name» ou «Application Label») sur l'écran du dispositif d'acceptation doit être conforme aux spécifications EMV.

6.5.3 Messages

Lors de la sélection par le client :

- le message « Choix Client » sera affiché sur le TPE sans PIN PAD et le message « Choix client en cours » sur le TPE avec PIN PAD afin d'informer le commerçant,
- aucun message ne sera affiché sur le PIN PAD 2 lignes en complément de la liste des applications contrairement aux écrans 4 lignes ou le message «Choix Client» précédera systématiquement la liste des applications,
- l'affichage des applications sur le PIN PAD sera en surbrillance ou en Inverse vidéo.

En ce qui concerne l'enchaînement des messages de la transaction, en vue d'uniformisation, les messages affichés avant et après le traitement de la transaction seront les suivants :

- *« Montant ? » (ce message ne concerne pas le PINPAD des systèmes intégrés).*
- *« Insérer carte »*
- *« Patientez»*

Traitement de la sélection et de la transaction

- *« Abandon » ou « Paiement accepté »*
- *« Retirez carte »*

6.5.4 Cas d'une transaction de crédit

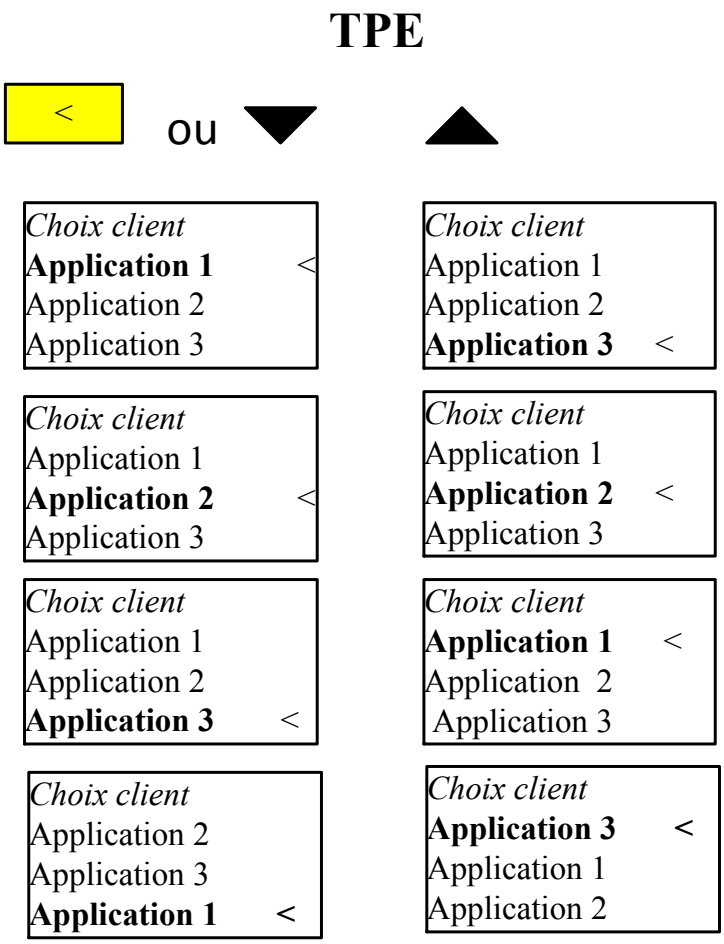
La sélection de l'application pour une transaction de crédit s'effectuera de la même façon que pour la transaction de débit.
La transaction de crédit sera réalisée, comme décrit dans le MPE.

6.5.5 Cas d'une transaction d'annulation

La sélection de l'application pour une transaction d'annulation s'effectuera de la même façon que pour la transaction de débit.
La transaction d'annulation sera réalisée, comme décrit dans le MPE.

6.5.6 Exemples d'affichage d'une sélection d'application

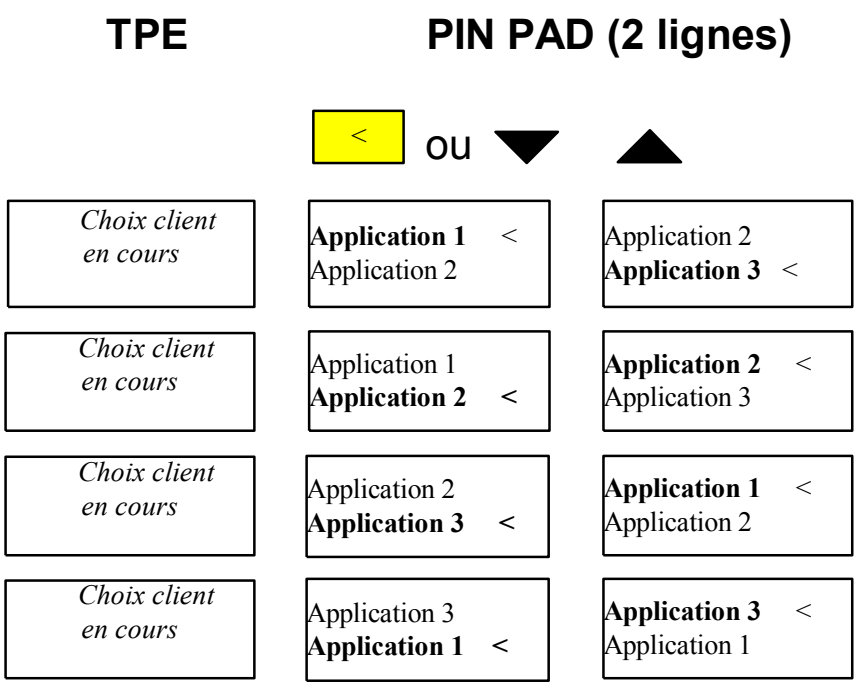
1) l'affichage sur un TPE sans PIN PAD.



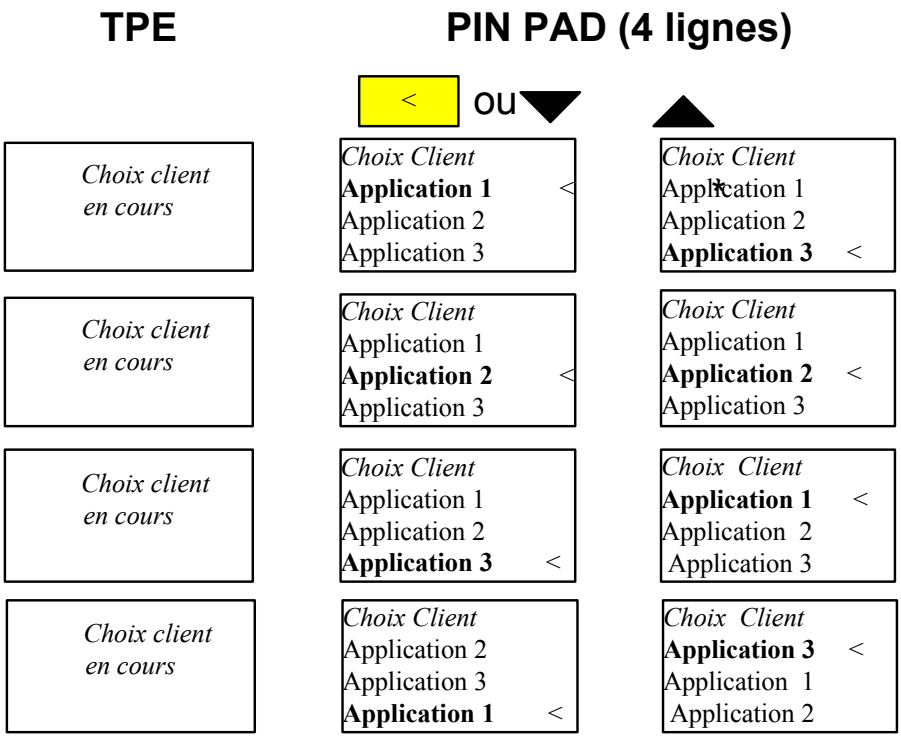
Choix client :

- Le commerçant doit demander à son client d'effectuer un choix dans la liste.
- Le message TPE ne s'efface qu'après le choix du client.

2) l'affichage sur un TPE avec PIN PAD (2 lignes d'affichage).



3) l'affichage sur un TPE avec PIN PAD (4 lignes d'affichage).



Sur le TPE le message affiché doit être : « *Choix client en cours* ».
Le commerçant doit demander à son client de choisir son application sur le PIN PAD. Le message TPE ne s'efface qu'à l'issue de la validation.

6.6 REGLES D'AFFICHAGE SUR UN TERMINAL AVEC UN SEUL ECRAN

Lorsque le terminal (terminal sans PIN-PAD) ne possède qu'un écran pour afficher les messages 'accepteur' et les messages 'porteur', l'affichage des messages se fera selon la règle suivante :

- Si la langue du porteur et celle de l'accepteur sont les mêmes, seul le message accepteur sera affiché à destination du porteur et à destination de l'accepteur. Il pourra être affiché sur deux lignes si nécessaire.

- Si la langue du porteur est différente de celle de l'accepteur, deux messages seront affichés sur deux lignes différentes. Le message à destination de l'accepteur sera affiché sur la ligne du haut, le message à destination du porteur sera affiché sur la ligne du bas (les règles d'affichage sont présentées en annexe 4 du volume 4)

7 ANNEXE 7 : SPECIFICATIONS DU COUPLEUR

7.1 INTRODUCTION

Ce document décrit les spécifications du coupleur Cartes Bancaires « CB ». Ces spécifications viennent en complément des spécifications EMV.

7.2 REFERENCES NORMATIVES

Le coupleur doit être conforme aux spécifications EMV version 4.1 book 1 de mai 2004.

7.3 SPECIFICATIONS COMPLEMENTAIRES

Les spécifications complémentaires concernent les domaines suivants :

- Electrique,
- Mécanique.

7.3.1 Spécificités électriques

7.3.1.1 Contacts électriques

- **CLK**

  Limitation de courant : le terminal ne doit pas générer plus de 70 mA sur ce contact.

- **RST**

  Limitation de courant : le terminal ne doit pas générer plus de 70 mA sur ce contact.

- **VCC**

  Limitation de courant : le terminal ne doit pas générer plus de 200 mA sur ce contact.
  En cas de défaillance du VCC, les autres contacts doivent être désactivés.

7.3.1.2 Spécificités mécaniques

Accessibilité :

- Quand l'équipement avale la CàM, il doit disposer d'un mécanisme qui restitue la CàM à son porteur en cas de panne (par exemple panne d'alimentation). En cas de panne la carte doit être accessible par le porteur.

8 ANNEXE 8 : EXIGENCES SECURITAIRES LIEES AUX COMMUNICATIONS AVEC LES SYSTEMES D'ACCEPTATION PAIEMENT

8.1 CONTEXTE

L'arrivée de nouveaux moyens de communications, de nouveaux terminaux et de nouvelles offres tarifaires modifient considérablement le schéma d'acheminement de la transaction.

Le document présent propose un ensemble d'exigences destinées à ajuster le niveau de sécurité pour tenir compte des nouveaux risques liés aux évolutions des communications avec les systèmes d'acceptation paiement.

L'objectif de ces exigences est de créer un domaine de confiance monétique à l'intérieur duquel les données sont considérées en sécurité.

Les exigences sécuritaires ci-après sont présentées dans leur version 1.7 datée de décembre 2014.

8.2 DEFINITIONS

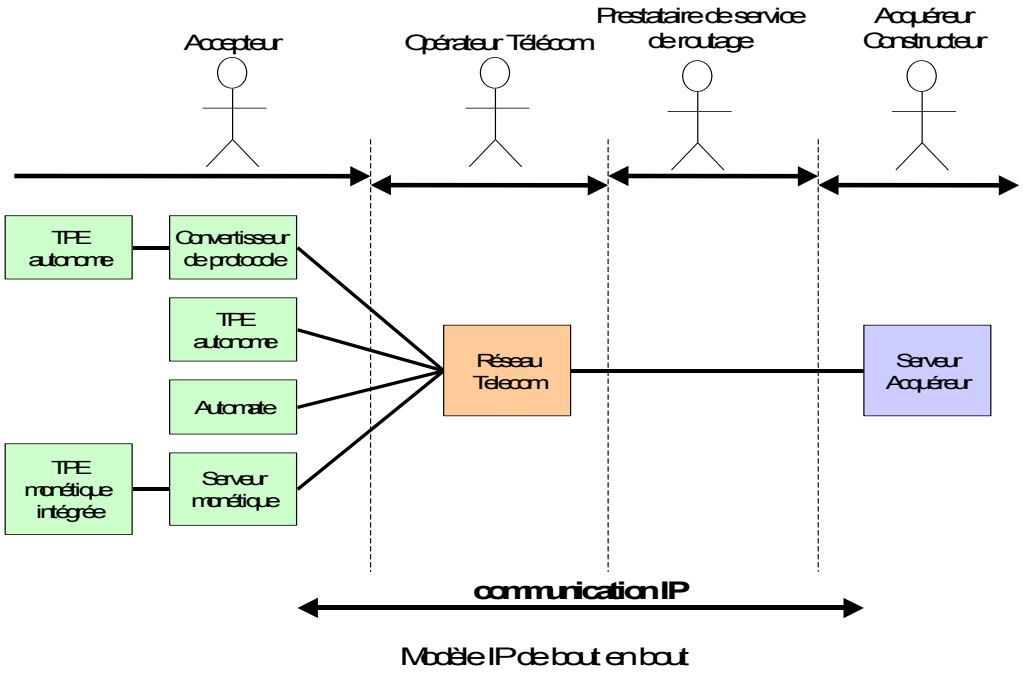
Applications métier	Ensembles d'applications nécessaires au point d'encaissement : acceptation « CB », encaissement, traitement chèque, applications privatives, fidélité
Chiffrement fort	Algorithme symétrique garantissant une force au moins égale à celle de l'AES avec clé de 128 bits. Algorithme asymétrique garantissant une force au moins égale à celle du RSA avec module de longueur 2048 bits. Les valeurs de référence à une date donnée sont données par l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI).
Chiffrement par domaine	Méthode de chiffrement utilisée pour protéger les données à l'intérieur d'un domaine n'est pas nécessairement celle qui est utilisée dans un domaine différent. Il est de la responsabilité des acteurs d'effectuer déchiffrement et chiffrement dans des enceintes cryptographiques
Maintenance monétique	Toute intervention permettant de modifier les caractéristiques, données ou application utilisées dans une opération monétique. Ces interventions nécessitent la présence ou l'assistance d'une personne qualifiée et habilitée à intervenir sur la partie monétique du point de vente.
Prestataire de service de routage	Acteur utilisant les données applicatives monétiques de la transaction pour fournir un service à valeur ajoutée à l'acquéreur et/ou à l'accepteur
Téléchargement	Transfert du noyau ou de l'application vers un système d'acceptation.
Téléparamétrage	Transfert de données de paramétrage vers un système d'acceptation.

8.3 MODELES SIMPLIFIES

Les figures ci-dessous présentent des modèles simplifiés des relations entre les acteurs et les systèmes concernés par les exigences du présent document.

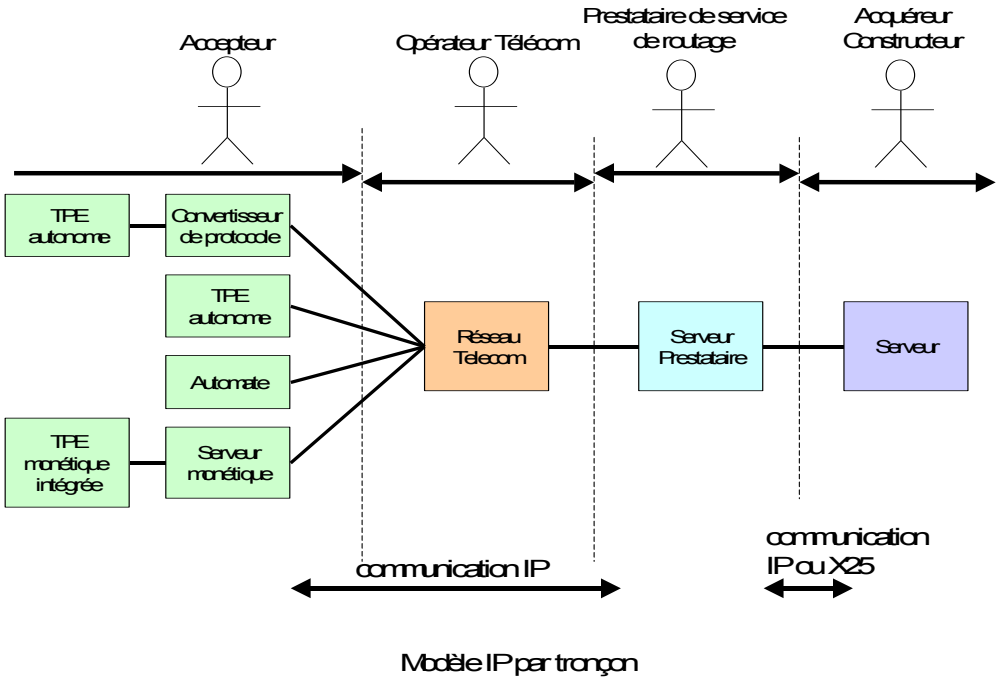
Dans les deux modèles ci-dessous, suivant le type de flux, opérationnel (autorisation, télécollecte, téléparamétrage) ou de maintenance (téléparamétrage / téléchargement), le système d'acceptation est en relation avec l'acquéreur ou le constructeur.

La première figure représente le modèle d'une connexion « IP de bout en bout » établie entre le terminal et le serveur acquéreur.



Modèle IP de bout en bout

La seconde figure représente le modèle d'une communication « IP par tronçon » établie entre des acteurs successifs. L'accès aux données de la transaction est donc possible à chaque serveur reconnu intervenant dans la communication.



Modèle IP par tronçon

8.4 PERIMETRE

Ce document s'applique à l'ensemble des flux échangés par les systèmes d'acceptations « CB » :

- Autorisation
- Téléparamétrage
- Télécollecte
- Téléchargement

Les exigences s'étendent à tous les tronçons utilisant TCP /IP, sur réseaux privés ou publics, depuis les systèmes d'acceptations jusqu'aux systèmes acquéreur ou de téléchargement. Les deux modèles présentés ci-dessus sont concernés par les exigences et sont acceptables dans la mesure où les exigences de sécurité sont respectées.

Les exigences de ce document ont pour but d'accompagner l'utilisation de nouvelles technologies réseau dans le système « CB ». Elles s'appuient donc les couches transport et les couches inférieures. Les couches applicatives sont exclues du périmètre.

Le périmètre de ces exigences exclut le stockage et le traitement des données. Le programme « Payment Card Industry Data Security Standard » (PCI DSS) mis en place par les réseaux internationaux, traite explicitement de ces points.

8.5 EXIGENCES GENERALES

Les exigences ci-dessous sont applicables quelles que soient les évolutions technologiques effectivement déployées dans l'environnement du système d'acceptation.

Chaque exigence est présentée sous la forme suivante.

Exigence N°: Nom

Libellé

Le libellé définit l'exigence en termes de niveau et d'objectif de sécurité. Le libellé est la référence pour l'exigence.

Exemples de solution

Les exemples proposent des axes de solution à titre d'information. Elles donnent des exemples de réalisation mais ne constituent pas l'exigence. Les solutions proposées par les acteurs doivent répondre au libellé de l'exigence.

Application

Le tableau proposé décline pour les acteurs et les types de point d'acceptation, l'applicabilité de l'exigence.

8.5.1 Traçabilité de la maintenance monétique

Libellé

Toute opération de maintenance monétique sur un système d'acceptation doit être tracée, en identifiant au minimum le mainteneur, la date et la nature de l'opération de maintenance effectuée. Cette trace sera consultable a posteriori.

Exemples de solution

Application

TPE autonome	Obligatoire. La journalisation des opérations de maintenance est effectuée par un processus automatique ou manuel.
Automate	Obligatoire. La journalisation des opérations de maintenance est effectuée par un processus automatique.
TPE monétique intégrée	Obligatoire. La journalisation des opérations de maintenance est effectuée par un processus automatique ou manuel.
Serveur monétique intégrée	Obligatoire. La journalisation des opérations de maintenance est effectuée par un processus automatique.

Serveur Opérateur Télécom	Obligatoire. La journalisation des opérations de maintenance est effectuée par un processus automatique.
Serveur Prestataire de service monétique	Obligatoire. La journalisation des opérations de maintenance est effectuée par un processus automatique.
Serveur Acquéreur	Obligatoire. La journalisation des opérations de maintenance est effectuée par un processus automatique.

8.5.2 Intégrité des systèmes monétiques

Libellé

Un contrôle visuel de l'intégrité du système d'acceptation est effectué périodiquement.

Exemples de solution

Application

TPE autonome	Obligatoire Les accepteurs seront sensibilisés aux possibilités de fraude et aux besoins de vérification.
Automate	Obligatoire Le contrôle visuel doit faire partie des procédures de surveillance et d'entretien de base mises en place par l'accepteur.
TPE monétique intégrée	Obligatoire Le contrôle visuel doit faire partie des procédures de surveillance et d'entretien de base mises en place par l'accepteur.
Serveur monétique intégrée	Obligatoire
Serveur Opérateur Télécom	Obligatoire
Serveur Prestataire de service monétique	Obligatoire
Serveur Acquéreur	Obligatoire

8.6 EXIGENCES SPECIFIQUES AUX TECHNOLOGIES IP

Les exigences présentées dans cette section s'appliquent aux évolutions liées à la mise en œuvre et l'usage des technologies IP.

8.6.1 Protection des liens externes à l'accepteur

Libellé

Le réseau de communication entre le système d'acceptation et le serveur d'acquisition de l'acquéreur ou de son prestataire de service doit être protégé en accès, en intégrité et en confidentialité par des algorithmes de chiffrement fort.

L'authentification du serveur externe nécessaire au fonctionnement par le système d'acceptation est obligatoire.

L'authentification mutuelle entre le serveur d'acquisition de l'acquéreur ou de son prestataire de service et le système d'acceptation doit être implémentée dans les capacités du terminal (capability).

Exemples de solution

Les transmissions sur IP peuvent s'appuyer sur un réseau privé virtuel chiffrant (VPN) ou une sécurisation basée sur TLS avec chiffrement fort, avec deux certificats (certificat client et certificat serveur). Lorsque TLS est mis en œuvre, la version minimum du protocole à utiliser pour tous les nouveaux systèmes est 1.2.

Le principe de chiffrement par domaine peut s'appliquer afin d'utiliser des moyens de chiffrement adaptés à chaque étape du transport des informations.

Note

L'authentification d'un système d'acceptation par un système radio (GSM, GPRS, WIMAX) ne répond pas aux exigences ci-dessus.

Application

Flux échangés par le TPE autonome	Obligatoire.
Flux échangés par l'Automate	Obligatoire.
Flux échangés par le TPE monétique intégrée	Obligatoire.
Flux échangés par le Serveur monétique intégrée	Obligatoire.
Flux échangés par le Serveur Opérateur Télécom	Obligatoire.
Flux échangés par le Serveur Prestataire de service de routage	Obligatoire.
Flux échangés par le Serveur Acquéreur	Obligatoire.

8.6.2 Protections des liens internes à l'accepteur

Libellé

Le réseau de communication entre un concentrateur du système d'acceptation et les différents points de vente ou caisses internes doit être protégé en accès, en intégrité et en confidentialité par des algorithmes de chiffrement fort.

L'authentification du concentrateur du système d'acceptation par les différents points de vente ou caisses internes est obligatoire.

L'authentification mutuelle entre le concentrateur du système d'acceptation et les différents points de vente ou caisses internes doit être implémentée dans les capacités du terminal (capability).

Exemples de solution

Les transmissions sur IP peuvent s'appuyer sur un réseau privé virtuel chiffrant (VPN) ou une sécurisation basée sur TLS avec chiffrement fort avec deux certificats (certificat client et certificat serveur). Lorsque TLS est mis en œuvre, la version minimum du protocole à utiliser pour tous les nouveaux systèmes est 1.2.

Le principe de chiffrement par domaine peut s'appliquer afin d'utiliser des moyens de chiffrement adaptés à chaque étape du transport des informations.

Application

Flux échangés par le TPE autonome	Obligatoire.
Flux échangés par l'automate	Obligatoire.
Flux échangés par le TPE monétique intégrée	Obligatoire.
Flux échangés par le Serveur monétique intégrée	Obligatoire.
Flux échangés par le Serveur Opérateur Télécom	Obligatoire.
Flux échangés par le Serveur Prestataire de service de routage	Optionnel.
Flux échangés par le Serveur Acquéreur	Optionnel.

8.6.3 Restriction des communications

Libellé

Des mécanismes de filtrage interdisant toute communication qui n'est pas nécessaire aux « applications métier » du système d'acceptation sont mis en place sur le système d'acceptation.

Exemples de solution

Utiliser un filtrage réseau intégré au système d'exploitation, n'autorisant que les communications à destination de ou provenant de services précis sur des serveurs autorisés.

En cas de télédiagnostic ou télémaintenance, les opérations ne peuvent s'opérer sans autorisation explicite de l'accepteur ou de son représentant.

Note

L'état de l'art recommande que deux mécanismes de filtrage placés en cascade soient de conception différente afin de se prémunir contre des faiblesses communes.

Application

TPE autonome	Obligatoire.
Automate	Obligatoire.
TPE monétique intégrée	Obligatoire.
Serveur monétique intégrée	Obligatoire.
Serveur Opérateur Télécom	Obligatoire.
Serveur Prestataire de service monétique	Obligatoire.
Serveur Acquéreur	Obligatoire.

8.6.4 Durcissement du système d'exploitation

Libellé

Le système d'acceptation doit fonctionner avec un système d'exploitation durci. Un système d'exploitation durci est composé exclusivement des seuls éléments logiciels et matériels nécessaires à son fonctionnement.

Exemples de solution

Le durcissement d'un système d'exploitation consiste au minimum à :

- Supprimer les modules inutilisés (exécutable, librairie, drivers…) ;
- Supprimer les services inutiles (protocoles, services TCP/IP, services systèmes, etc.) ;
- Supprimer les comptes utilisateurs inutilisés et changer les mots de passe par défaut ;
- Mettre à jour le système d'exploitation avec les derniers patchs de sécurité ;
- Désactiver les moyens de démarrage à distance des systèmes (Exemple : télé-démarrage Ethernet PXE) ;
- Respecter les règles de durcissement proposées par les fournisseurs de systèmes d'exploitation commerciaux ou logiciels libres.

Application

TPE autonome	Obligatoire.
Automate	Obligatoire.
TPE monétique intégrée	Obligatoire.
Serveur monétique intégrée	Obligatoire.
Serveur Opérateur Télécom	Obligatoire.
Serveur Prestataire de service monétique	Obligatoire.
Serveur Acquéreur	Obligatoire.

8.7 AUTHENTIFICATION SERVEUR

8.7.1 Génération du certificat serveur

Le certificat serveur doit avoir pour origine une autorité de certification autorisée par Groupement des Cartes Bancaires.

La liste des autorités de certification autorisées est publiée sur le site web du Groupement des Cartes Bancaires dans la rubrique « *Sécuriser les terminaux et les automates* ».

Toute autorité de certification dont les caractéristiques organisationnelles et techniques sont clairement publiées au travers d'une politique de certification qui sera analysée suivant une démarche inspirée de la Politique de certification du Référentiel Général de Sécurité Version 1.0 ou postérieure pourra être ajoutée à cette liste.

Les clés sont fournies au moyen d'un certificat conforme à la norme X509v3.

Ce certificat serveur est généré et signé par l'autorité de certification. Le contenu et le format des champs du certificat sont imposés par cette autorité de certification.

Les certificats utilisés doivent répondre aux caractéristiques minimales suivantes :

Algorithme asymétrique	RSA
Longueur minimale des clés pour algorithmes asymétriques	2048 bits
Algorithme de hachage	SHA-2 (MD5 et SHA-1 exclu)
Durée de vie	2 ans maximum

8.7.2 Installation, renouvellement et traçabilité sur le serveur

L'installation se fait conformément aux modalités prévues par les applications utilisant ces certificats (TLS ou IPSec avec chiffrement fort par exemple).

Il est demandé que la clé privée de la biclé associée au certificat serveur soit conservée dans un module de sécurité cryptographique matériel.

Ce module matériel peut être un accélérateur cryptographique permettant de protéger la clé privée. La clé privée du serveur n'est ni exportable du serveur ni consultable.

Le renouvellement des certificats se fait comme pour l'installation.

Dans un but de traçabilité, les attributs de clé privée tels que l'identifiant, sont signés par la clé privée et vérifiables par l'intermédiaire de la clé publique.

Ces attributs de clé privée sont consultables :

- Obligatoirement par un accès direct à l'équipement,
- Optionnellement par télédiagnostic.

8.7.3 Installation, renouvellement et traçabilité sur le système d'acceptation

Avant toute utilisation du système d'acceptation, un certificat racine d'autorité de certification est chargé :

- soit par le constructeur du système d'acceptation,
- soit dans une phase de personnalisation du système d'acceptation.

Plusieurs certificats racines d'autorité de certification peuvent être installés dans une seule machine. Les certificats pourront être obtenus auprès des autorités de certification correspondantes.

Un procédé organisationnel ou technique défini par le constructeur garantit que les certificats chargés dans le système d'acceptation sont :

- Issus des autorités de certification racine autorisées par le Groupement des Cartes Bancaires
- Authentiques
- Intègres

Si un procédé organisationnel est utilisé, celui-ci est consigné par écrit.

Si nécessaire, le renouvellement des certificats racine peut se faire lors d'un retour en maintenance.

Dans un but de traçabilité, la liste des clés publiques installées est consultable.

8.7.4 Utilisation du certificat serveur sur le système d'acceptation

L'utilisation d'un certificat serveur requiert au préalable la vérification de sa validité avec une vérification :

- Cryptographique de la signature,
- De la date de début de validité,
- De la date de fin de validité,
- Des champs critiques du certificat.

En cas d'échec de la vérification, le certificat n'est pas utilisé et la connexion terminée.

8.8 AUTHENTIFICATION DU SYSTEME D'ACCEPTATION

8.8.1 Génération du certificat du système d'acceptation

Le but de cette authentification est de garantir l'origine de l'équipement ou de la configuration appelant afin d'établir un canal entre machines de confiance.

Le certificat est donc le reflet de la confiance accordée au constructeur sur la base de son agrément. A ce titre, le constructeur a la possibilité de générer des certificats pour chaque machine de la gamme d'équipement ou la configuration agréée.

Le constructeur intervient en tant qu'autorité de certification vis-à-vis de ses propres produits.

Chaque équipement ou configuration dispose d'un numéro de série unique par constructeur.

Les clés publiques sont fournies par un certificat conforme à la norme X509v3. Les certificats sont installés conformément aux moyens prévus dans les logiciels utilisés (TLS ou IPSec avec chiffrement fort par exemple).

Les certificats générés par le constructeur doivent répondre aux caractéristiques minimales suivantes :

Algorithme asymétrique	RSA
Longueur minimale des clés pour algorithmes asymétriques	2048 bits
Algorithme de hachage	SHA-2 (MD5 et SHA-1 exclu)
Durée de vie	4 ans maximum

Pour assurer l'interopérabilité, les champs suivants devront respecter le format spécifié.

Libellé du champ	
C	France
O	Nom du constructeur ou de l'intégrateur
OU	Nom du Produit agréé
CN	Numéro de série unique par constructeur

La politique de certification utilisée peut être référencée par numéro OID dans un champ extension non critique du certificat.

8.8.2 Installation, renouvellement et traçabilité sur le système d'acceptation

La clé privée est installée par le constructeur lors de la fabrication.

Celle-ci peut être générée :

- à l'intérieur de l'équipement et certifiée par une requête auprès de l'autorité de certification du constructeur,
- à l'extérieur de l'équipement, certifiée par une requête auprès de l'autorité de certification du constructeur puis insérée dans l'équipement avec son certificat.

Seules les personnes habilitées par le constructeur peuvent avoir à gérer la clé privée. Celle-ci doit rester confidentielle, notamment vis-à-vis de l'accepteur, des porteurs et de toute personne non habilitée par le constructeur à intervenir sur le système d'acceptation.

Le renouvellement des bi-clés peut se faire :

- Par un retour en maintenance,
- Par une procédure de télémaintenance garantissant l'authenticité de l'appelant et ensuite l'authenticité et l 'intégrité des données installées.

Dans tous les cas, la confidentialité des clés privées doit être assurée. Elles ne sont ni exportables du système d'acceptation ni consultables.

Dans un but de traçabilité, les attributs de clé privée tels que l'identifiant, sont signés par la clé privée et vérifiables par l'intermédiaire de la clé publique.

Ces attributs de clé privée sont consultables,

- Obligatoirement par un accès direct à l'équipement,
- Optionnellement par télédiagnostic.

8.8.3 Installation, renouvellement et traçabilité sur le serveur

Le certificat de l'autorité de certification du constructeur est obtenu auprès de celui-ci.

Les clés publiques sont fournies par un certificat conforme à la norme X509v3. Les certificats sont installés conformément aux moyens prévus dans les logiciels utilisés (TLS ou IPSec avec chiffrement fort par exemple).

Dans un but de traçabilité, la liste des clés publiques installées est consultable,

- Obligatoirement par un accès direct au système d'acceptation,
- Optionnellement par télédiagnostic.

8.8.4 Utilisation du certificat du système d'acceptation sur le système serveur

Si l'authentification du système d'acceptation est requise par le serveur, l'utilisation d'un certificat requiert au préalable la vérification :

- Cryptographique de la signature,
- De la date de début de validité,
- De la date de fin de validité,
- Des champs critiques du certificat.

En cas d'échec de la vérification, le certificat n'est pas utilisé et la connexion terminée.