

Le sans contact

PARTIE 7 SANS CONTACT

JUIN 2021

Passion for payments



DISCOVER

JCB



UnionPay 中国银联
China UnionPay

VISA

 **galitt**
a Sopra Steria company

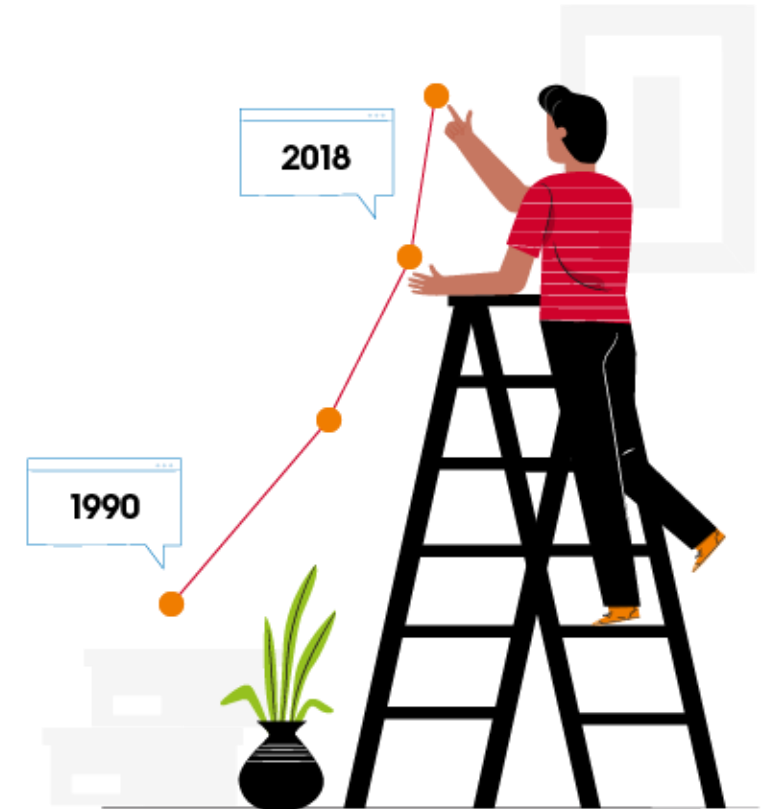
Sommaire le sans contact

01

La technologie

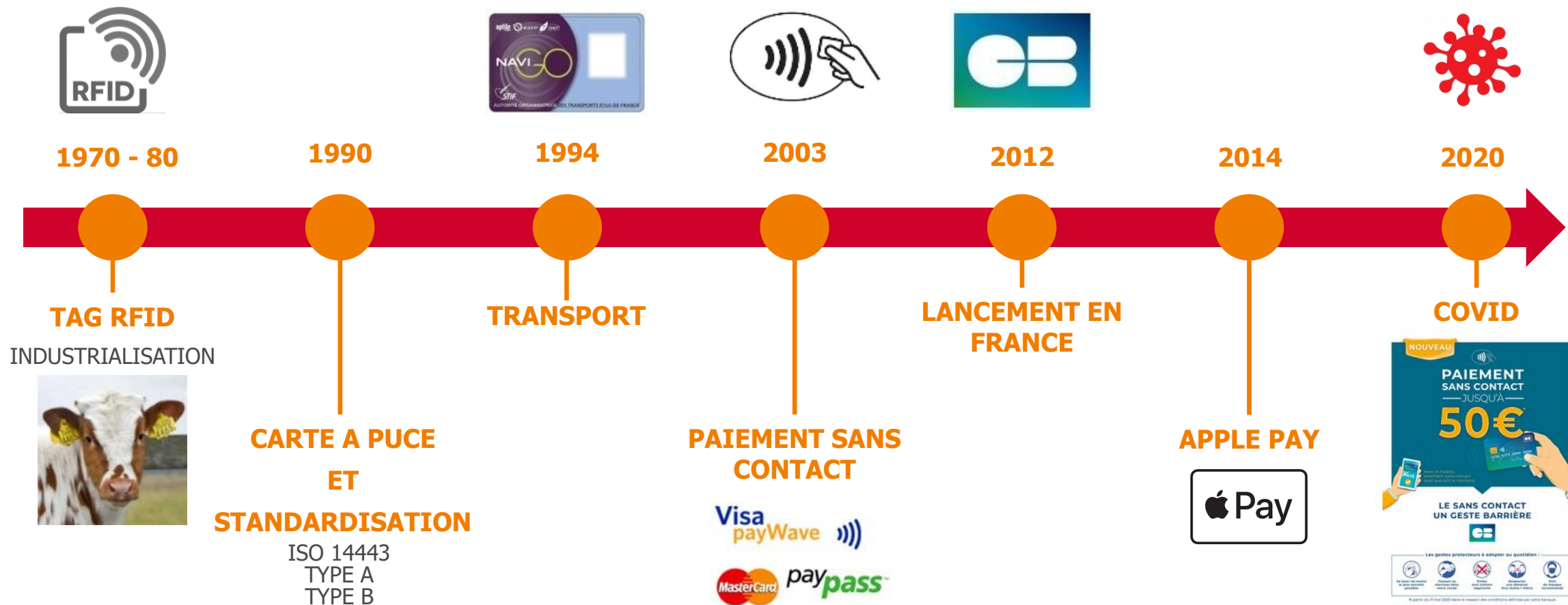
02

La paiement sans contact



Le sans contact

Historique



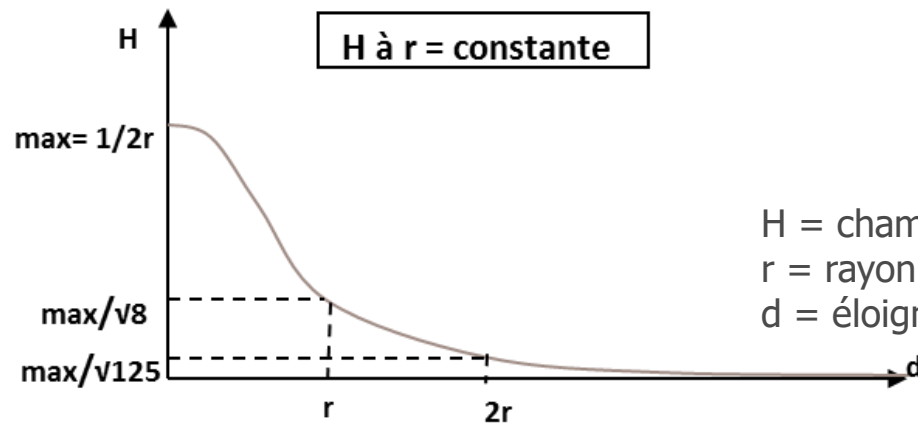
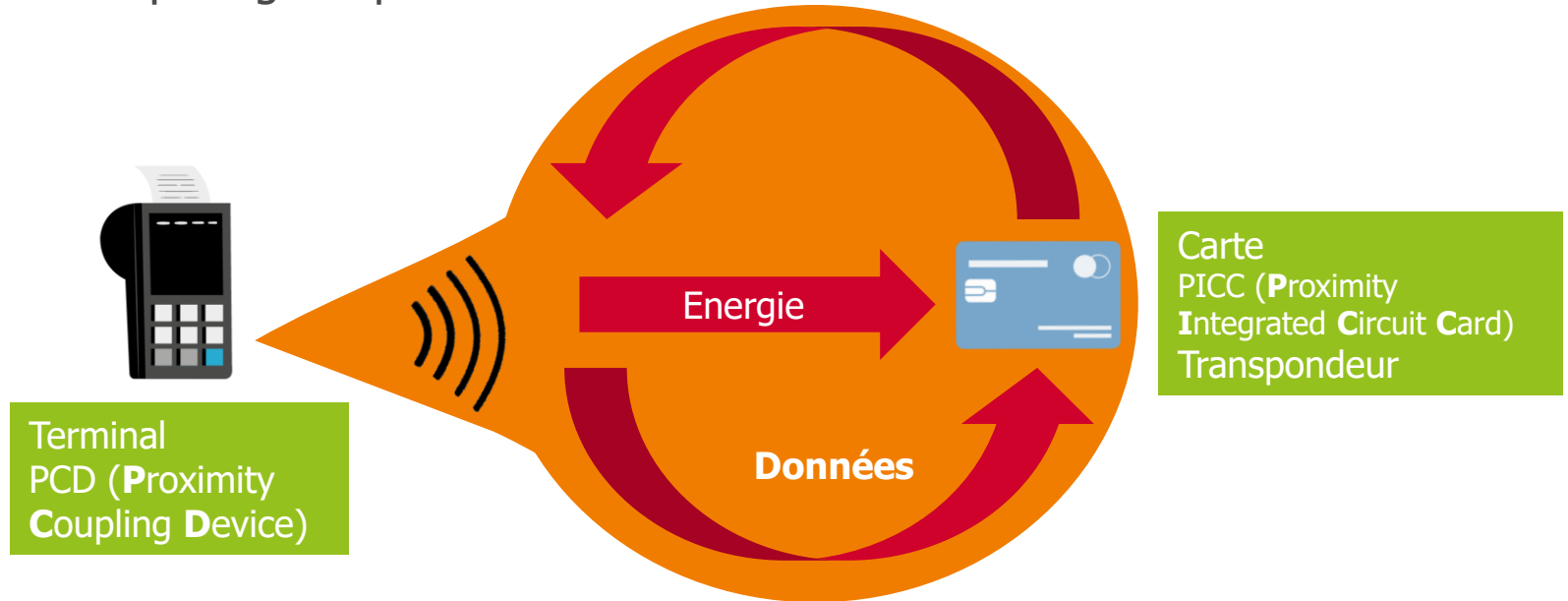
La technologie

La communication sans contact : Le champ magnétique

— La télé-alimentation

- Transmettre l'énergie
- Etablir la **communication**

— Energie émise



H = champ magnétique
 r = rayon de l'antenne émettrice
 d = éloignement par rapport à l'antenne

La technologie

La communication sans contact : ISO 14443

— Caractéristiques physiques

- └ Fréquence de la porteuse : **13,56** MHz $\pm$ 7 kHz
- └ Protocole de communication Type A / Type B

— Vitesse de transmission :

- └ **106kbit/s** (= $f_c/128$)
- └ Possibilité jusqu'à **848 kb/s** ($f_c/16$)

à titre comparatif...

Carte à contact (ISO 7816-3)	$\approx 10\text{kb/s}$
Bluetooth	$\approx 2\text{Mb/s}$
WiFi	$\approx 300\text{ Mb/s} - 10\text{ Gb/s}$

— Gestion de l'anticollision

- └ Pourvoir gérer plusieurs cartes dans le champ
- non géré en bancaire

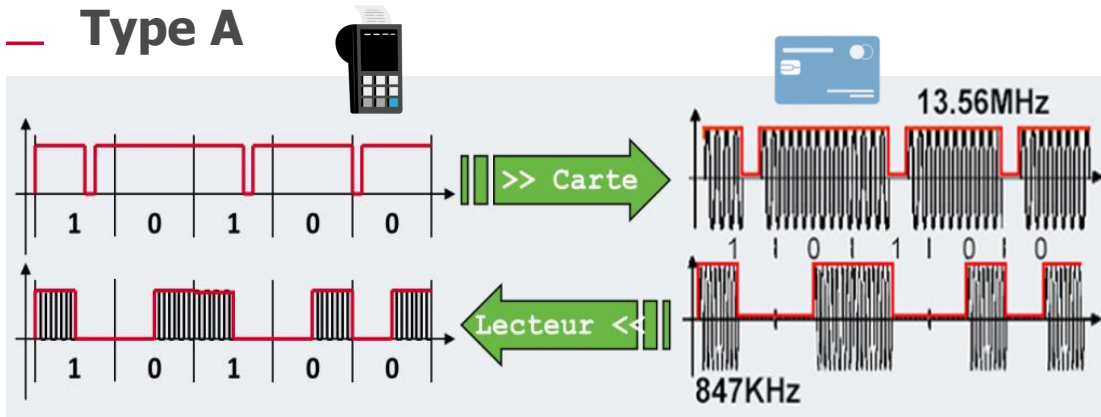
— Format des commandes/réponses

- └ ISO 7816

La technologie

La communication sans contact : ISO 1444

— Type A



Lecteur → Carte

Modulation : Modulation d'amplitude 100% (ASK)

Codage Mode Miller modifié

Débit : 106kbit/s

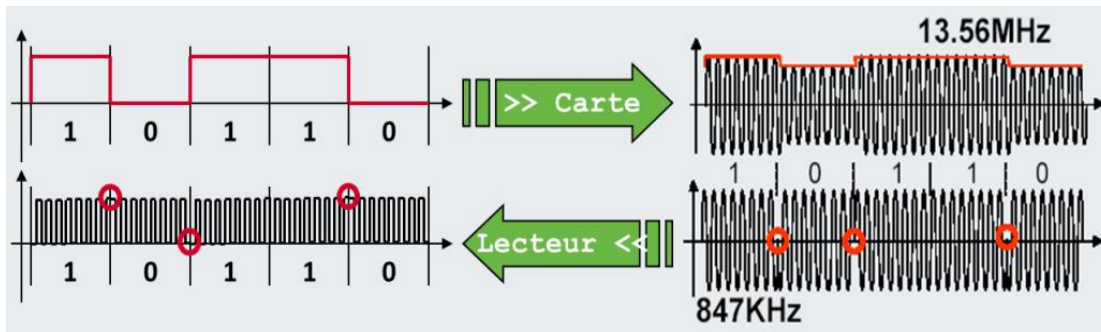
Lecteur ← Carte

Modulation : modulation d'amplitude 100% (ASK)

Codage Mode Manchester en modulation de charge (OOK - On/Off Keying)

Débit : 106kbit/s

— Type B



Lecteur → Carte

Modulation : Modulation d'amplitude 10% (ASK)

Codage Mode NRZ

Débit : 106kbit/s

Lecteur ← Carte

Modulation : Modulation de charge

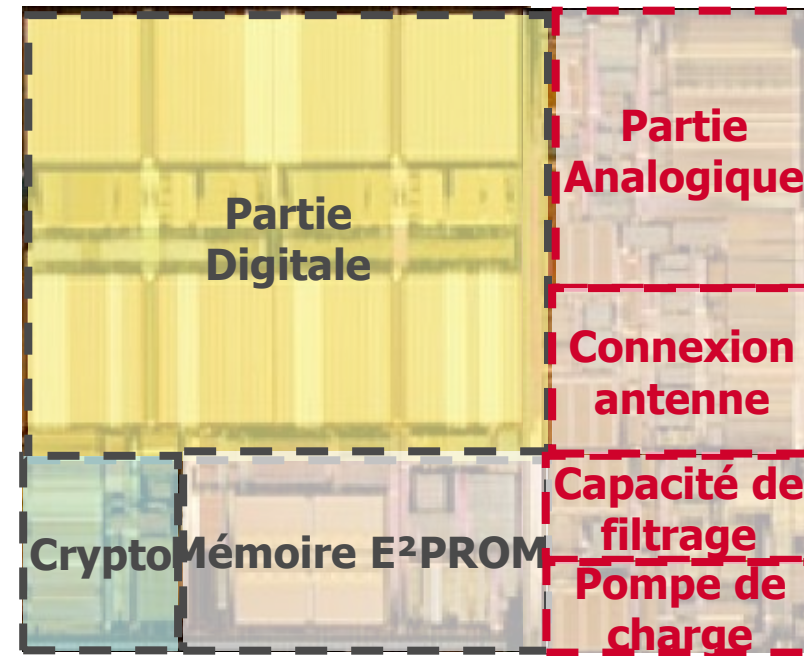
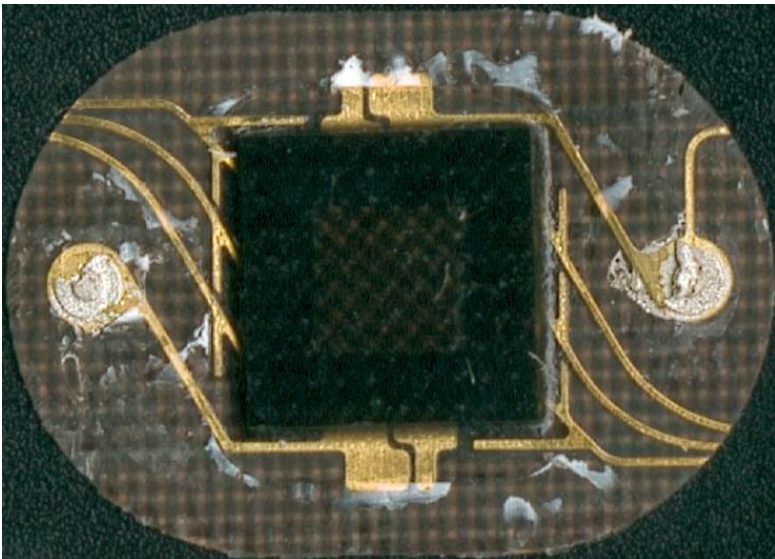
Codage NRZ – L en modulation de phase (Modulation sous porteuse BPSK)

Débit : 106kbit/s

La technologie

La carte sans contact

— Le module



Le paiement sans contact

Généralités

Principaux avantages...

— Paiement plus rapide

Vitesse de transmission des données 10x plus rapide

Manipulations réduites et rapides

— Sécurité

- └ Le marchand ne manipule pas la carte
- └ Peut contenir les mêmes sécurités que les cartes à puce à contact

— Moins de maintenance sur les terminaux

Mais...

— Pour conserver l'ergonomie : concessions sécuritaires

- └ Pas de saisie de PIN (offline)
- └ La carte n'a pas le dernier mot (non EMV)
- └ L'émetteur n'a plus la main sur son support (scripts)

— Peurs sur le Sans-Contact

- └ Eavesdropping
Ecouter, espionner la communication à distance
- └ Pick-pocketing
Engager une transaction avec la carte sans contact

Le paiement sans contact

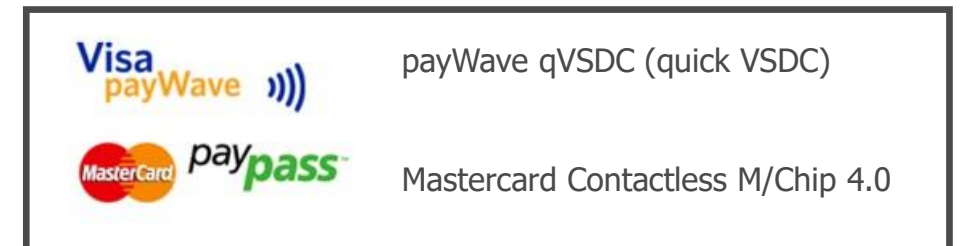
Approches PISTE/PUCE

— Piste

- └ La puce contient : donnée piste, cryptogramme visuel dynamique (CVC3 – dCVV)
- └ **En cours de démantèlement**

— PUCE (EMV mode)

- └ Construit à l'origine pour des **transactions offline**
- └ Terminal est capable de réaliser
 - Gestion de risque (**TRM** - Terminal Risk Management)
 - Authentification offline** (Dynamique)
- └ Carte est capable de réaliser
 - Gestion de risque carte (CRM - Card Risk Management)
- └ Fonctions sécuritaires tirées du contact (sécurité offline)
- └ La carte peut être duale : contact et contactless
 - Pour la France : la carte doit être duale



Le paiement sans contact

La transaction



Pre-Processing

Présentation de la
carte



Échanges sans contact
(< 500ms)

SELECT
GET PROCESSING
OPTIONS
READ RECORD
...

Finalisation Offline

Autre
interface

Acceptée

Refusée

Online

Finalisation Online

Acceptée

Refusée

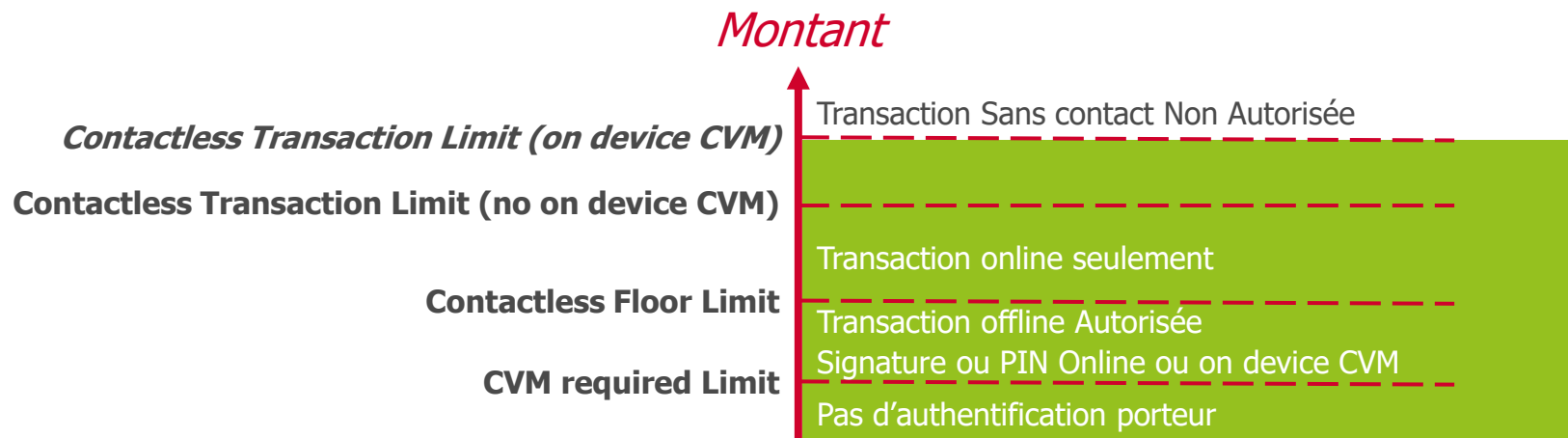
Demande d'autorisation



Le paiement sans contact

La transaction : Traitements préliminaires (pre-processing)

- Des contrôles (**paramètres acquéreurs**) sur le montant permettent au terminal de déterminer, avant d'engager la transaction, si :
 - └ La transaction est **éligible** pour du « sans contact »
 - └ Il doit y avoir une demande d'**autorisation**
 - └ Il doit y avoir **authentification du porteur**



Le paiement sans contact



Les kernels : la problématique

— Contact vs. Sans Contact

CONTACT



SELECT
GPO
READ RECORD
...
READ RECORD
VERIFY
GENERATE AC

Une seule
application

SANS CONTACT



SELECT
GPO
READ RECORD

SELECT
GPO
EXCHANGE RRD
READ RECORD
...
READ RECORD
GENERATE AC

SELECT
GPO
READ RECORD
...
READ RECORD
GENERATE AC

Plusieurs applications
(**KERNEL**)
→ laquelle activer ?
PPSE, Kernel ID

Le paiement sans contact

Le PPSE

— Sélection Application Carte/Terminal

- └ Donnée carte
- └ Identifier le **Kernel** (tag '9F2A')
- └ Application commune et unique
 - Application Priority Indicator
 - Ordre d'apparition dans le PPSE

— Bulletin EMV n°230

- └ Mise à jour du PPSE
- └ Exemple :
 - La carte change la priorité des Applications en fonction du contexte (transport)

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

A000000042 1010
CB
01
03

A000000003 1010
VISA DEBIT
02
03

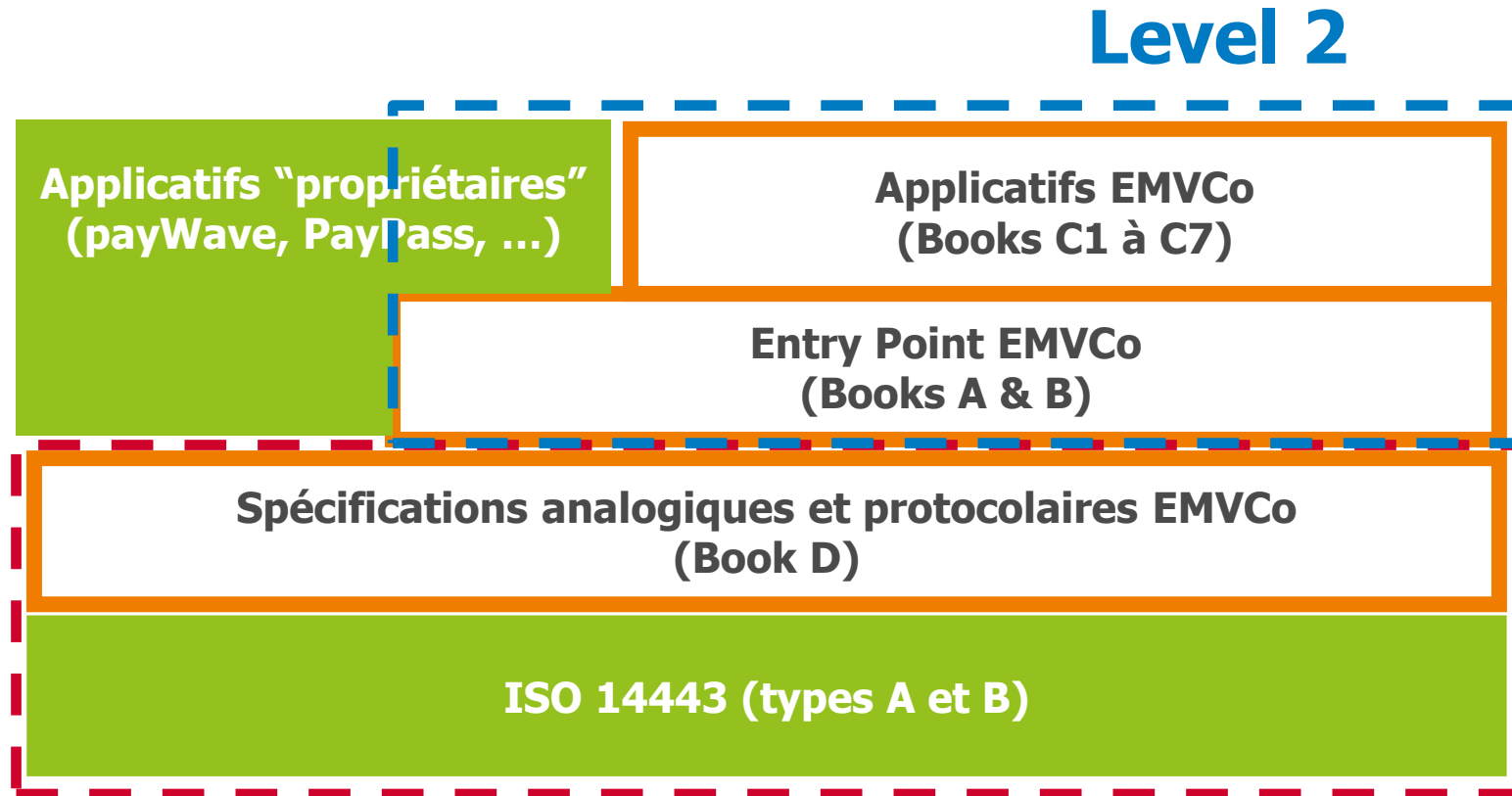


Le paiement sans contact

Le rôle d'EMVCo

- C-1 : Kernel 1 (« JCB » - historique)
- C-2 : Kernel 2 (« MasterCard »)
- C-3 : Kernel 3 (« Visa »)
- C-4 : Kernel 4 (« American Express »)
- C-5 : Kernel 5 (« JCB »)
- C-6 : Kernel 6 (« Discover »)
- C-7 : Kernel 7 (« UP »)

Level 1



Le paiement sans contact

Renforcer la sécurité, à venir...

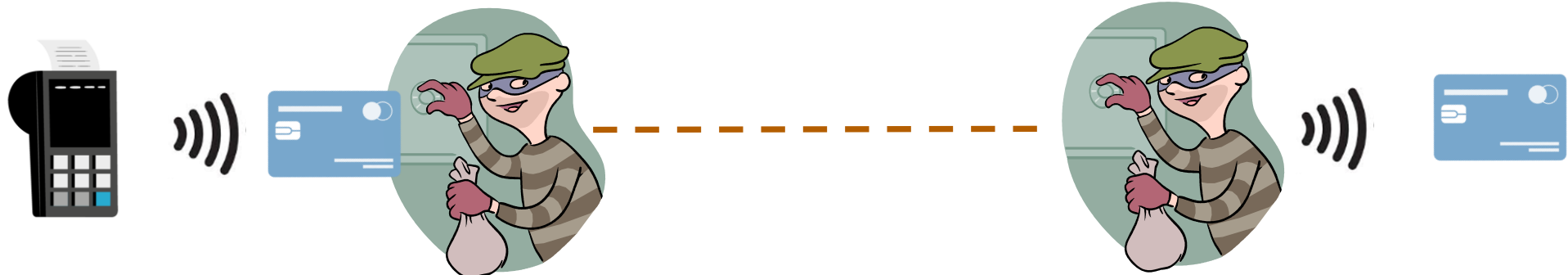
— Eavesdropping

- └ Ecouter, espionner la communication à distance
- └ Chiffrement des données sensibles (PAN, Date d'Expiration,...)
- └ Mécanisme présenté dans les spec EMV 2nd GEN



— Attaque relais

- └ Utilisation d'une carte à l'insu du porteur
- └ Echange de timer en carte et lecteur (RRP - Relay Resistance Protocol)
- └ Mécanisme présenté dans les spec EMV 2nd GEN



Le paiement sans contact

L'acceptation en France : généralités

— Paiement de proximité (MPE v6)

- └ Dispositif sans contact (carte, mobile, montre,...) CB et « non CB »
- └ Acceptation des kernels
 - C2 (Mastercard), C3 (Visa), C4 (AMEX), C5 (JCB), C6 (Discover) et C7 (Union Pay)
 - PURE, WISE et CSPACE

— Transactions

- └ Débit ('00'), crédit ('20'), annulation ('20'), débit différé

— Etanchéité Contact/Sans contact

- └ Transaction Non Aboutie (TNA) en cas de « repli » contact (« try another I/F »)



Le paiement sans contact

L'acceptation en France : transaction

— Gestion du risque

- └ Liste d'opposition, liste de BIN, cumul porteur (seuil spécifique sans contact), appel aléatoire,...

— Ticket

- └ Mention « sans contact »



- └ Logo

— Autorisation / Télécollecte (CB2A)

- └ Facteur de forme (si présent)
- └ Kernel ID
- └ AID
- └ Mode emv

Track2	ATC (Application Transaction Counter)
Application Cryptogram	Issuer Application Data
AID	TVR (Terminal Verification Results) = RTT
	Unpredictable Number

Le paiement sans contact

L'acceptation en France : Limite à 50€

- **Limite pour une transaction par carte**
- **Mise à jour du système**
 - └ Terminal : téléparamétrage



- **Carte : script émetteur**
 - └ Lors d'une transaction online contact
 - └ Maîtrise du SAE
 - Clés SMI
 - Longueur du MAC (4 ou 8 octets)



Exemple :

84DA9F780600000000032009873F2B4

Tag

Valeur à
mettre à jour

MAC (4 octets)

Le paiement sans contact

La DSP2

— Directive UE concernant les services de paiement (janvier 2018)

- └ Authentification forte du porteur (**SCA Strong Customer Authentication**)

Code PIN, empreinte biométrique (CDCVM),...

- └ Exemption pour le sans contact jusqu'à 50€

Soit **limite cumulée de 150€**

Soit **5 transactions consécutives offline**

