

Spécifications EMV

PARTIE 2 SPÉCIFICATIONS DE LA CARTE

JUIN 2021

Passion for payments



DISCOVER

JCB



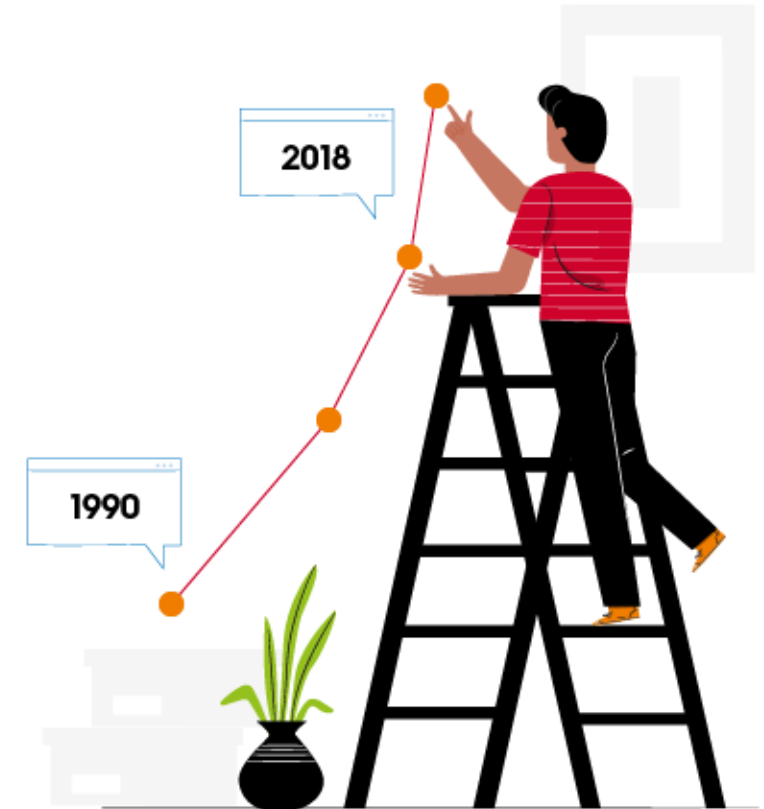
UnionPay 中国银联
China UnionPay

VISA

 **galitt**
a Sopra Steria company

Sommaire spécifications de la carte

- 01 L'interface de communication EMV
- 02 Le contenu d'une carte
- 03 Les profils de cartes
- 04 Exemple d'implémentation



L'interface de communication EMV

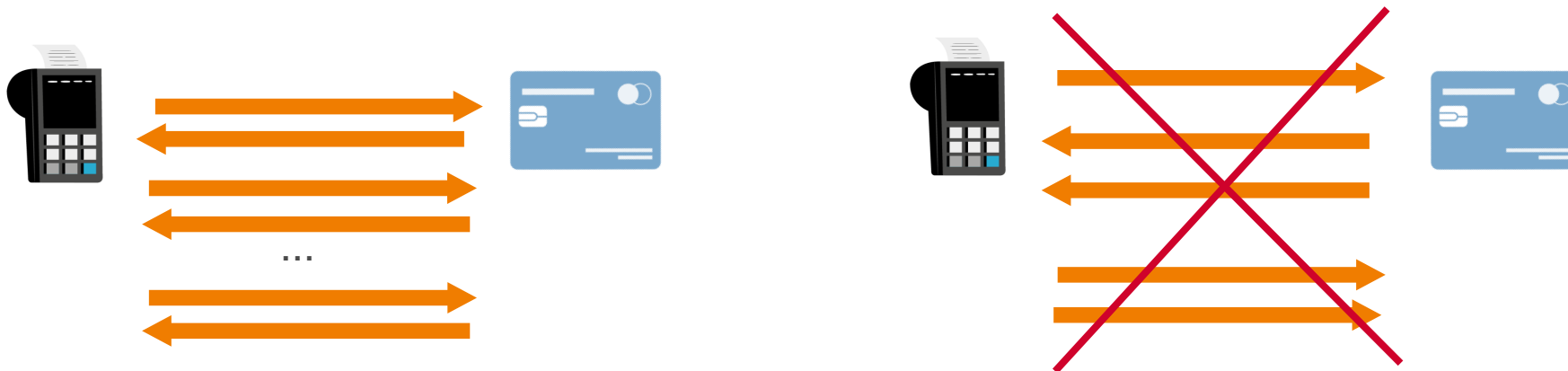
ISO 7816 - Les principes de base



— Echange toujours initié par le terminal

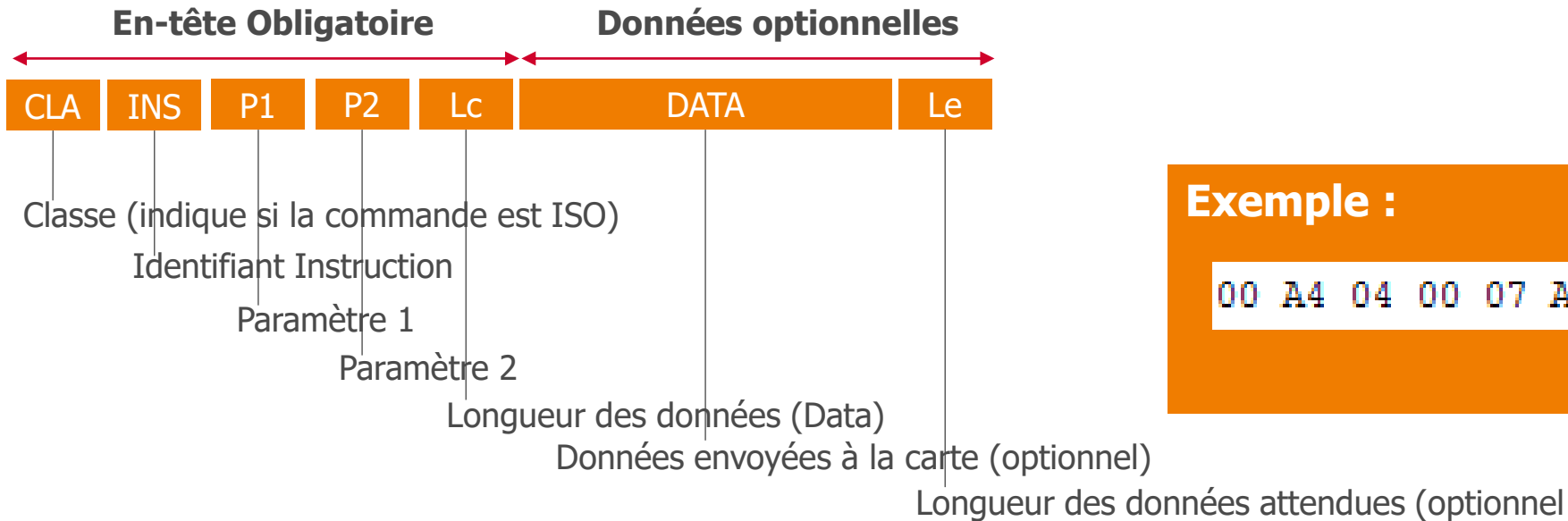


— Séquence



L'interface de communication EMV

ISO 7816 - Commande



Exemple :

00 A4 04 00 07 A0 00 00 00 42 10 10 00

L'interface de communication EMV

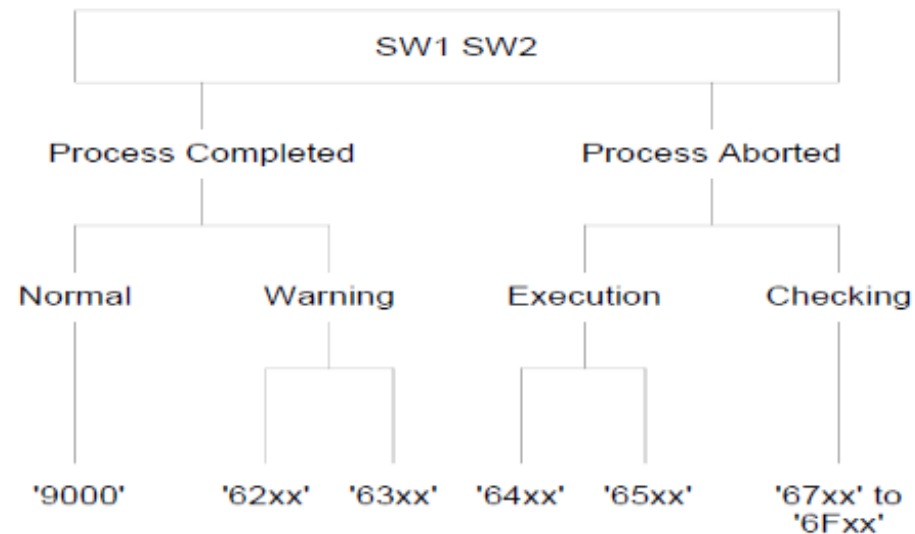
ISO 7816 - Réponse



Exemple :

9F 13 02 01 C2 90 00

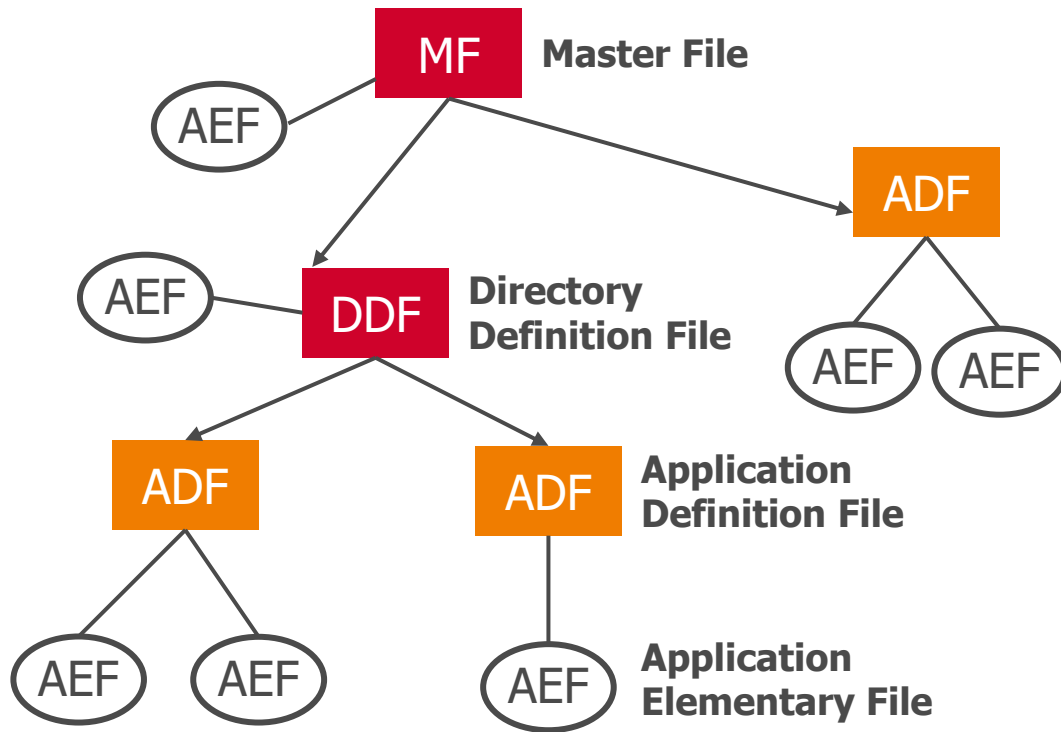
SW1-SW2 compte-rendu du traitement de la commande par la carte



Le contenu d'une carte

Structure des données

— EMV = un exemple d'application de la norme ISO 7816-4



— DDF ou ADF

- ADF identifié par l'**AID** (Application Identifier) conforme à la norme ISO7816-5
longueur 5 à 16 octets
AID = RID (identification fournisseur) + PIX (identification application)
unicité de l'AID pour une carte donnée

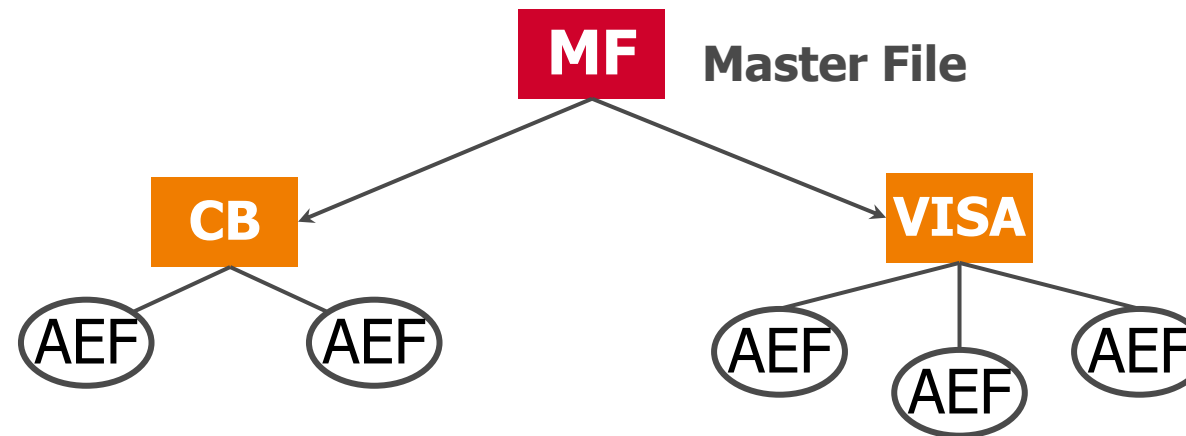
— AEF

- identification par un **SFI** (Short File Identifier)
- longueur 1 octet dont 5 bits de poids forts significatifs
- valeur de 01 à 30
- unicité du SFI pour une application donnée

Le contenu d'une carte

Structure des données

— Exemple



Le contenu d'une carte

Les aids (non exhaustif)

	A0 00 00 00 03
10 10	Visa Debit/Credit
20 10	Electron
20 20	V PAY

	A0 00 00 00 04
10 10	Mastercard Debit/Credit
30 60	Maestro
60 00	Cirrus

	A0 00 00 00 25
01	American Express

	A0 00 00 00 65
10 10	Japan Credit Bureau

	A0 00 00 03 33
01 01 01	Debit
01 01 02	Credit
01 01 03	Quasi Credit

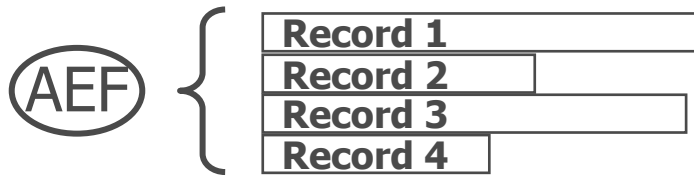
	A0 00 00 01 52
30 10	D-PAS

	A0 00 00 00 42
10 10	CB Debit/Credit
20 10	CB autorisation systématique
30 10	CB retrait

Le contenu d'une carte

Enregistrements et données

- Les fichiers sont constitués d'enregistrements (**records**)

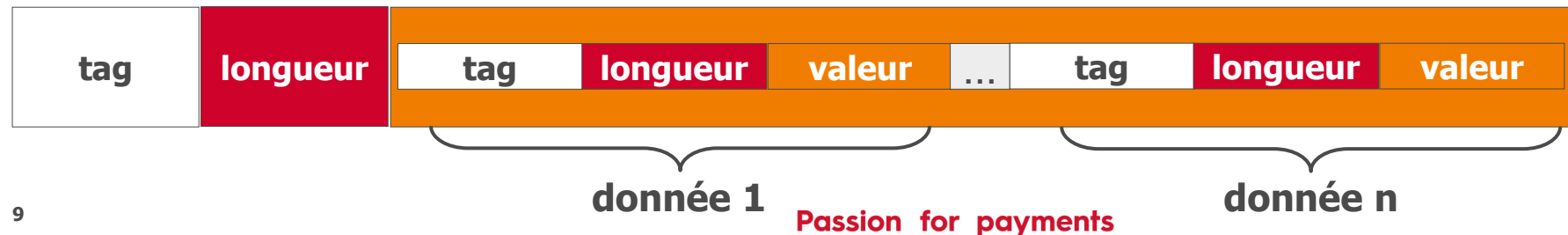


- Les enregistrements sont constitués de données au format **TLV** :

- └ TLV simple (primitive)



- └ TLV complexe (constructed)



Le contenu d'une carte

TLV

— Tag codé sur 1 ou 2 octets

Annex B Rules for BER-TLV Data Objects
B1 Coding of the Tag Field of BER-TLV Data Objects

EMV 4.2 Book 3
Application Specification

B1 Coding of the Tag Field of BER-TLV Data Objects

Table 35 describes the first byte of the tag field of a BER-TLV data object:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	
0	0							Universal class	
0	1							Application class	
1	0							Context-specific class	
1	1							Private class	
		0							Primitive data object
		1							Constructed data object
		1 1 1 1 1						See subsequent bytes	
		Any other value <31						Tag number	

Table 35: Tag Field Structure (First Byte) BER-TLV

— Longueur codée sur 1 ou 2 octets

	1 st byte	2 nd byte	3 rd byte	4 th byte	5 th byte	N
1 byte	'00' to '7F'	-	-	-	-	0 to 127
2 bytes	'81'	'00' to 'FF'	-	-	-	0 to 255
3 bytes	'82'	'0000' to 'FFFF'		-	-	0 to 65 535
4 bytes	'83'	'000000' to 'FFFFFF'			-	0 to 16 777 215
5 bytes	'84'	'00000000' to 'FFFFFFFF'				0 to 4 294 967 295

Le contenu d'une carte

Lecture des données

— Les données sont :

— **Statiques** : ne changent pas durant la vie de la carte

Exemple : numéro du porteur



— **Dynamiques** : évoluent durant la vie de la carte

Exemple : nombre d'essais du code confidentiel



— Leur utilisation peut être :

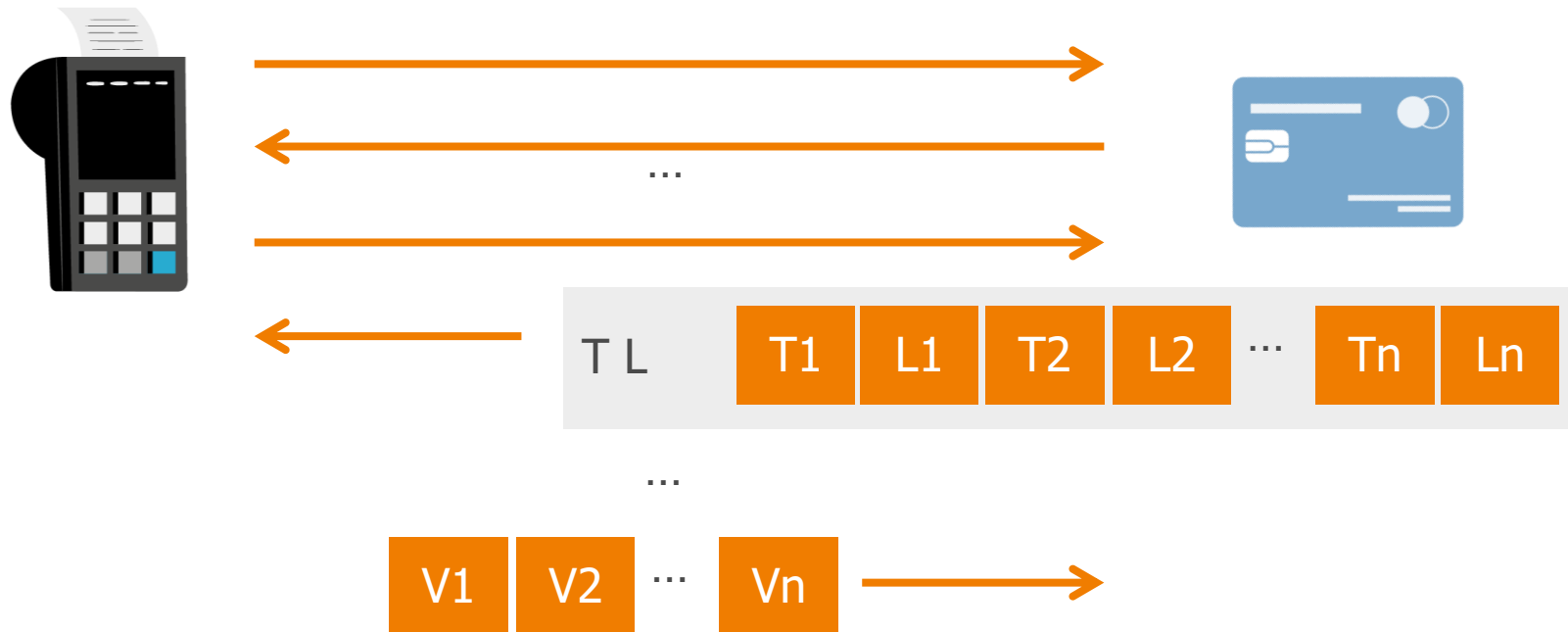
- **Partagée** par plusieurs applications : code confidentiel (choix émetteur)
- **Locale** à une application : AID (norme)

Le contenu d'une carte

DOL (Data Object List)

— Récupération de données par la carte

— "Inversion" du dialogue



Le contenu d'une carte

DOL (Data Object List)

- **CDOL 1 et CDOL 2** (Card Risk Management DOL) **obligatoire**
 - └ Gestion du risque par la carte (finalisation de la transaction)
- **DDOL** (Dynamic DOL) **optionnel**
 - └ Authentification dynamique offline
- **PDOL** (Processing DOL) **optionnel**
 - └ Debut de transaction
 - └ Transmettre le contexte (montant, type de transaction, code pays du terminal)
- **TDOL** (Transaction Certificate Management DOL) **optionnel**
 - └ Scellement de la transaction

Le contenu d'une carte

Exemples de données structurantes

- **AIP** (**A**pplication **I**nterchange **P**rofile)

- └ SDA/DDA/CDA supported
- └ Cardholder Verification supported
- └ ...



Impact sur la cinématique de la transaction

- **CVM List**

- └ Authentification porteur (PIN, signature)



Impact sur l'authentification porteur

- **IAC**

- └ Gestion de risque émetteur (refus, online)



Impact sur l'issue de la transaction

...

Les profils de carte

Maîtrise du comportement de la carte

— Profils types définis par Visa et MasterCard

- └ Profils types définis par Visa et MasterCard

- └ Données obligatoires, optionnelles et "best practices"



Cirrus, Maestro, Debit, Gold,...

— Choix des émetteurs

- └ Paramétrage des données (plafonds, données sécuritaires,...)

- └ Combinaison avec les fonctionnalités du **serveur d'autorisation**

- └ Prise en compte de l'**environnement acquéreur**

Un exemple d'implémentation

