

Spécifications EMV

PARTIE 3 TRANSACTION EMV

JUIN 2021

Passion for payments



DISCOVER

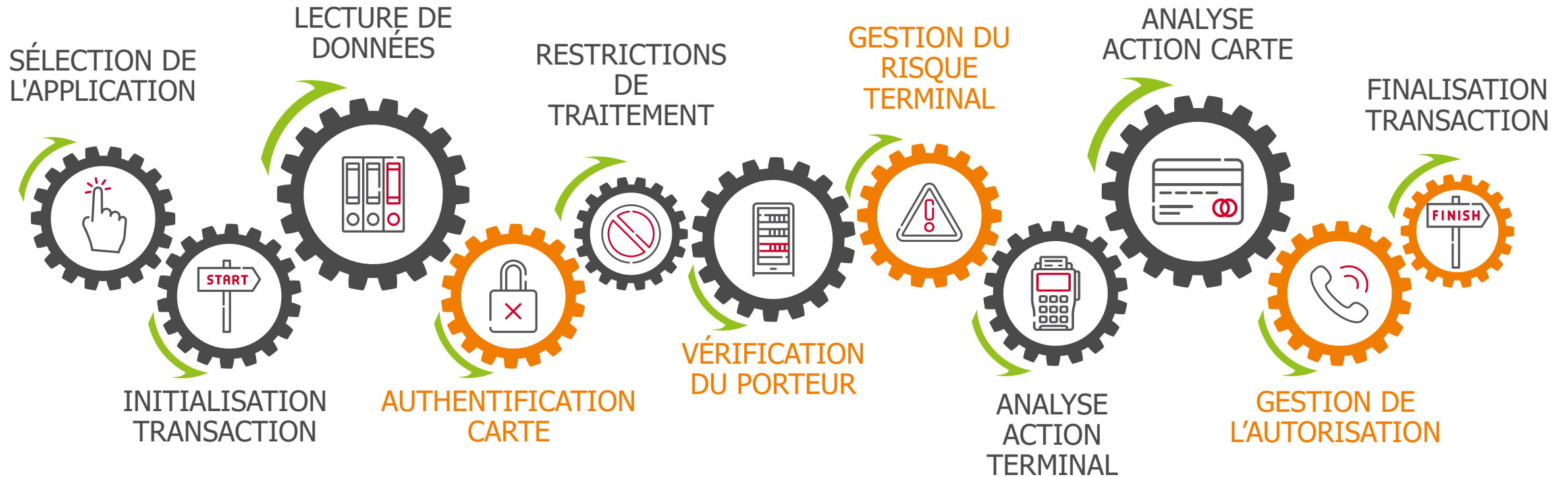
JCB



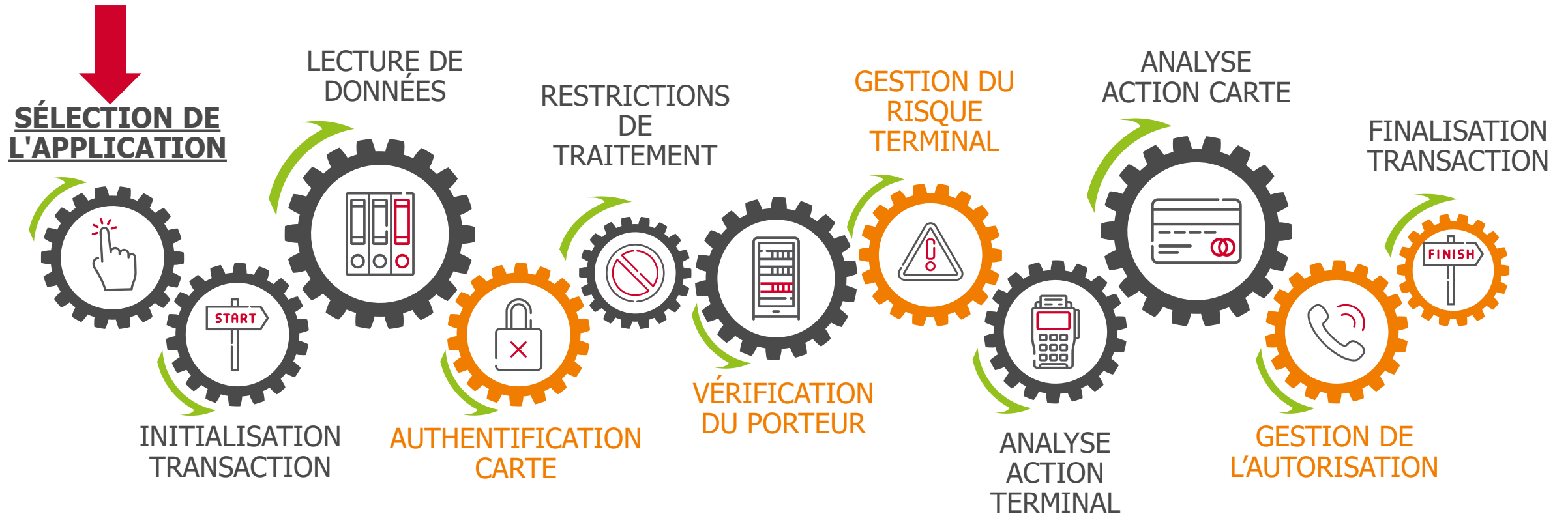
VISA



Synoptique du déroulement de la transaction



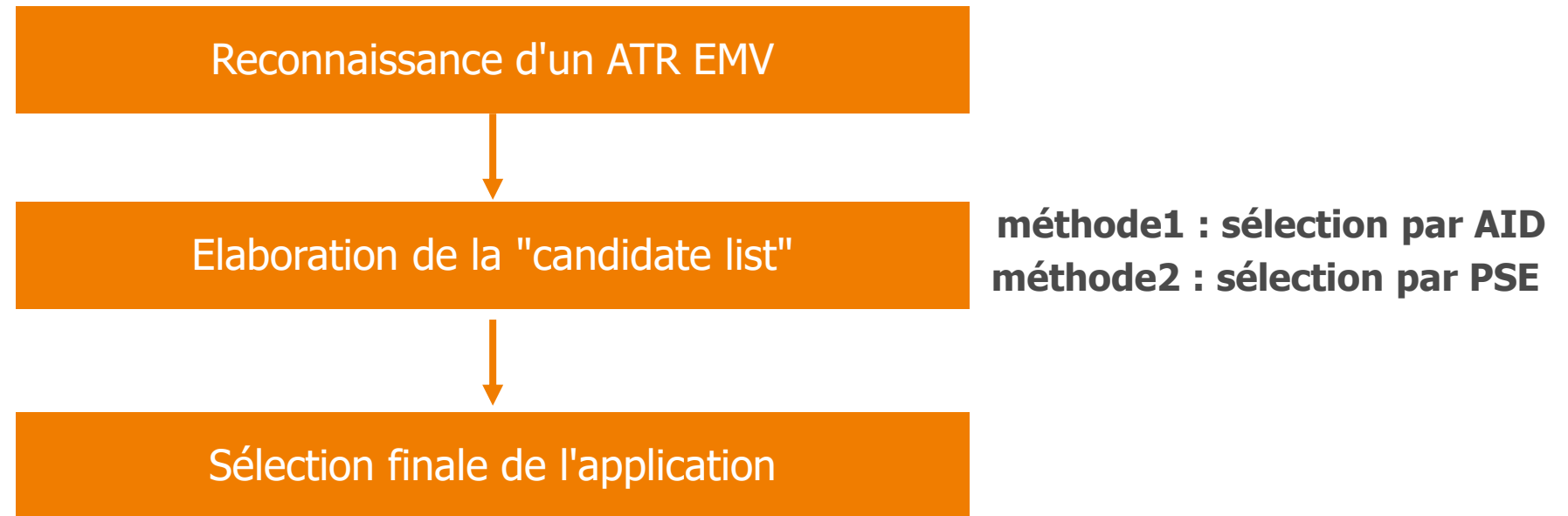
Synoptique du déroulement de la transaction



Sélection de l'application

Objectif

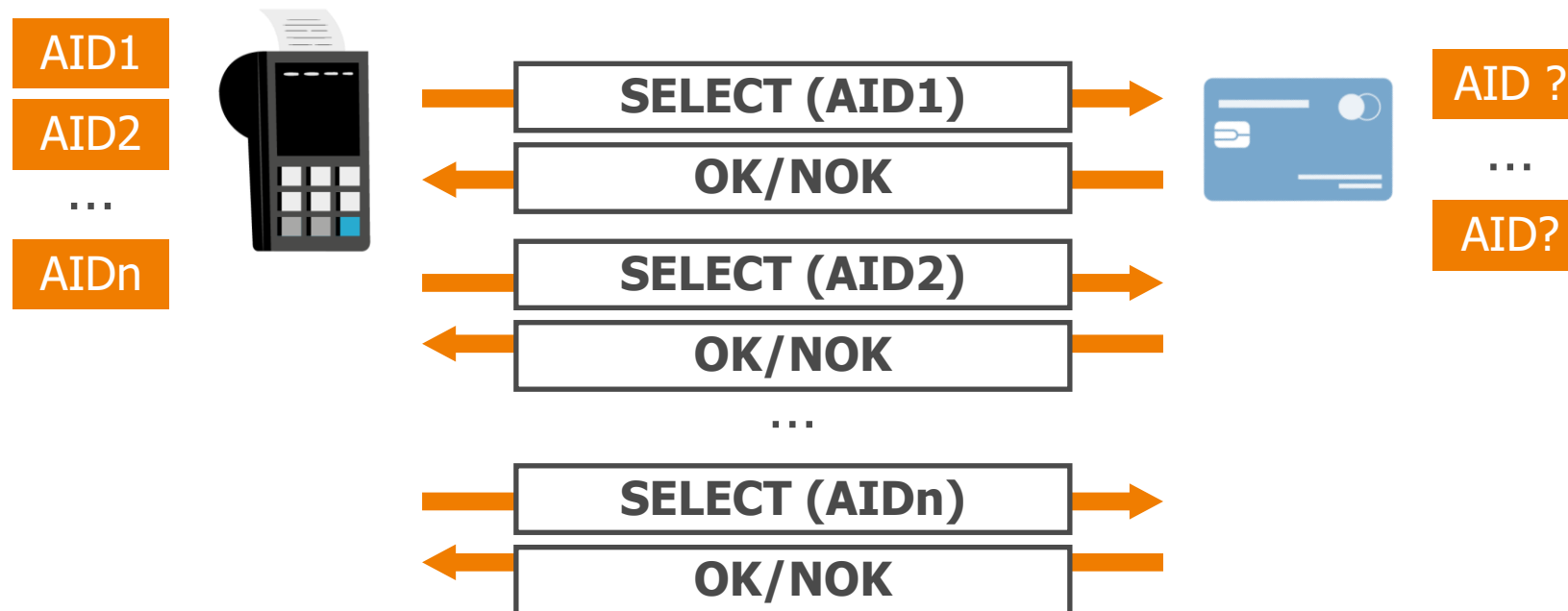
- Sélectionner **une** application **commune**



Sélection de l'application

Elaboration de la "Candidate List" : sélection par AID

— Sélection par liste des AIDs (mécanisme **obligatoire** pour le terminal)



Sélection de l'application

Elaboration de la "Candidate List" : sélection par PSE

- **Sélection** du **PSE** (mécanisme optionnel pour le terminal)



- **Lire** le contenu de PSE : lire du premier au dernier record



- Le terminal met dans sa **candidate list** tous les **AIDs** de la carte qu'il reconnaît (si contrôle ASI* positif lors d'une sélection partielle)

*ASI : Application Selection Indicator

Sélection de l'application

Elaboration de la "Candidate List" : gestion de la réponse



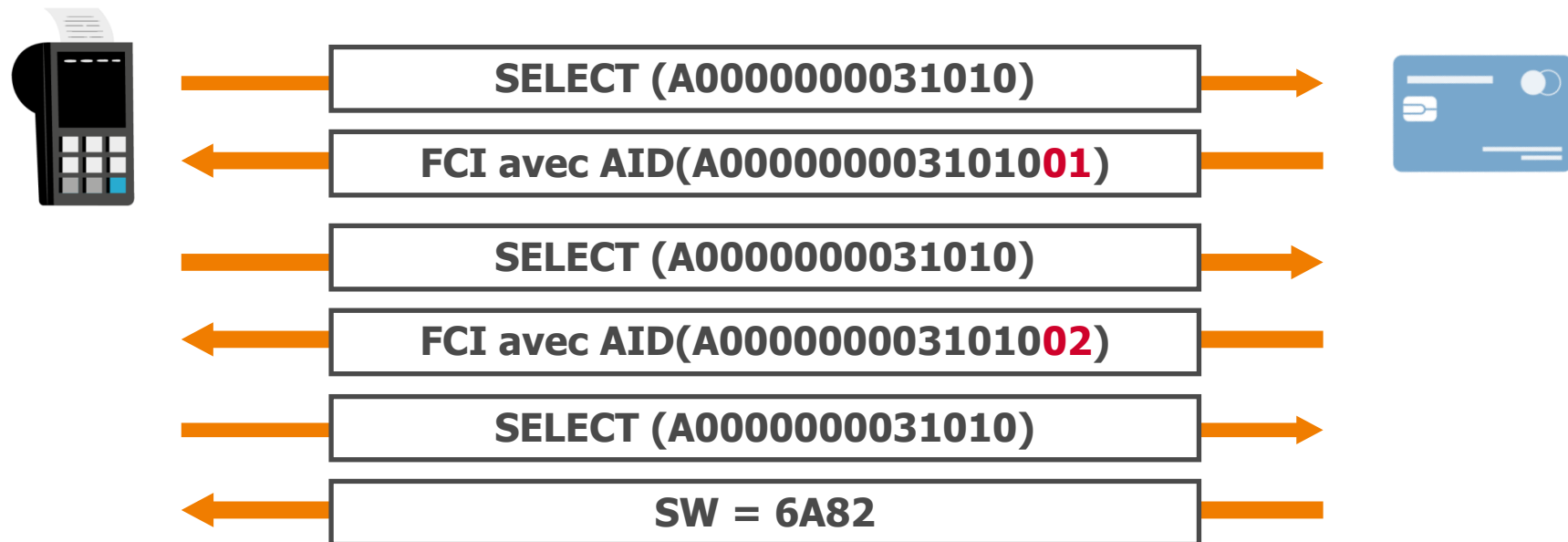
- **AID terminal = AID carte**, le terminal met cet AID dans sa "candidate list" si l'application n'est pas bloquée
- **AID terminal $\subset$ AID carte** **A000000003101001**
 - └ Sélection partielle **permise** par l'ASI*
 - Inclure l'AID dans la "candidate list" si l'application n'est pas bloquée
 - Envoyer une commande SELECT NEXT
 - └ Sélection partielle **non permise** par l'ASI*
 - Ne pas inclure l'AID dans la "candidate list"
 - Retourner au processus de sélection avec un autre AID terminal

*ASI : Application Selection Indicator

Sélection de l'application

Elaboration de la "Candidate List" : select next

— Exemple de sélection partielle



Sélection de l'application

Sélection finale

- "Candidate list" **vide**
 - **Fin** de transaction

- "Candidate list" contient **1 seul AID**
 - └ Vérification de l'**API*** (tag 87, ex: 870101)
 - Si pas de demande de confirmation porteur (Octet 1 - bit 8 à 0) → **sélection implicite**
 - Si demande de confirmation porteur (Octet 1 - bit 8 à 1) → proposer le **choix au porteur**

- "Candidate list" contient **au moins 2 AIDs**
 - └ Sélection par le porteur (méthode recommandée)
 - Le terminal **présente tous les AIDs au porteur**
 - └ Sélection par le terminal
 - L'AID de **plus haute priorité** est sélectionné

*API : Application Priority Indicator

Passion for payments

Sélection finale

Cas d'erreurs

- **Sélection PSE :**

- └ Commande non supportée (PSE inexistant)
- └ "Candidate list" vide
- └ PSE bloqué

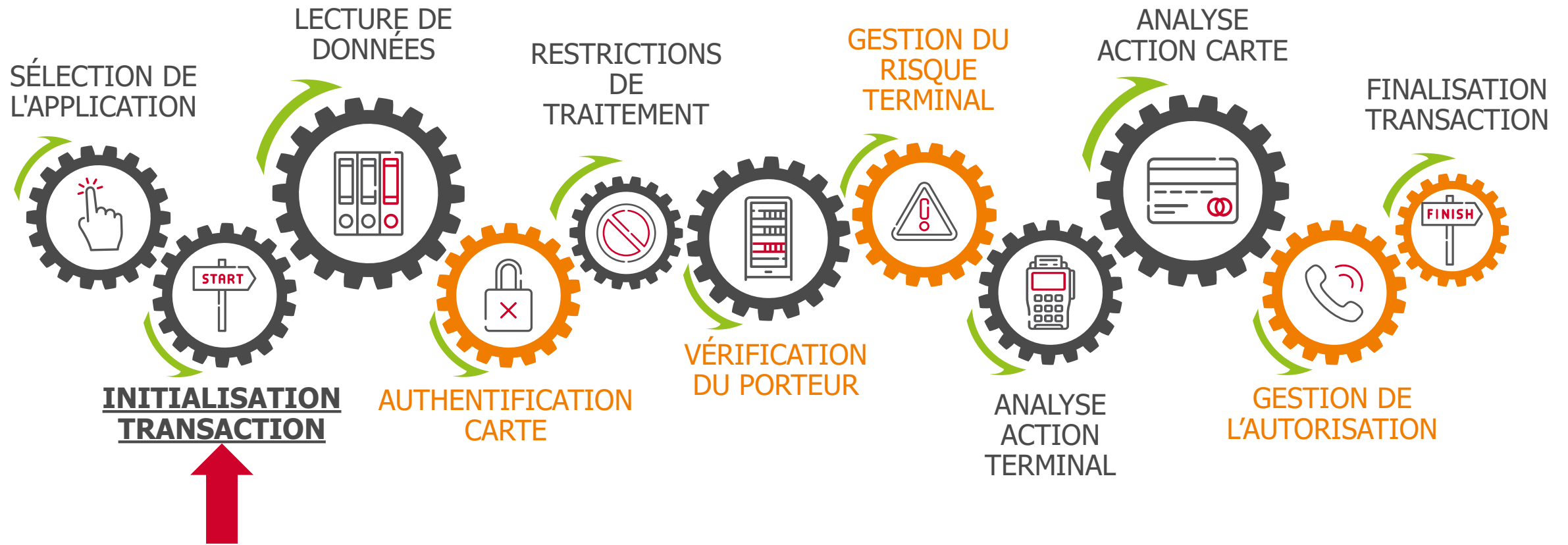
→ **Tenter la sélection par liste d'AIDs**

- **Sélection par AID ou par PSE :**

- └ Carte bloquée

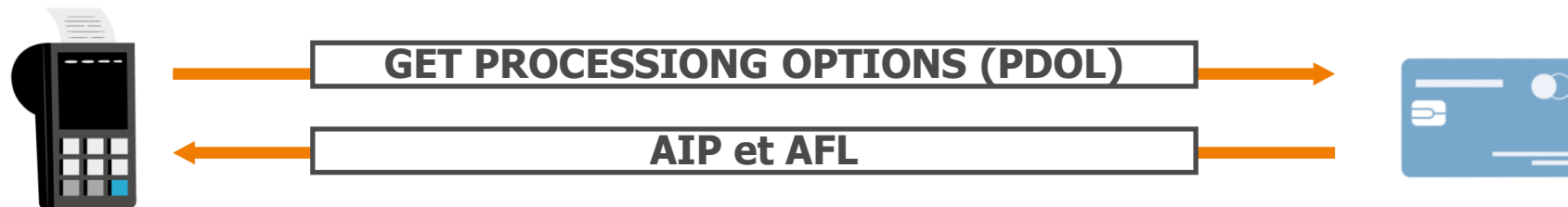
→ **Abandonner la transaction**

Synoptique du déroulement de la transaction



Initialisation transaction

Principe



- **Début** de la transaction
 - └ Récupération de l'**AIP** et l'**AFL**
 - └ Initialisation de la **TVR** et de la **TSI**
 - └ **PDOL** : permet à la carte d'ajuster l'AIP et l'AFL
- Cas d'erreur : si SW =6985 (« conditions d'utilisation non satisfaites »)
 - Retour à l'étape de sélection en supprimant l'AID en cours

Initialisation transaction

Données carte

— AIP (Application Interchange Profile)

AIP Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	1	x	x	x	x	x	x	SDA supported
x	x	1	x	x	x	x	x	DDA supported
x	x	x	1	x	x	x	x	Cardholder verification is supported
x	x	x	x	1	x	x	x	Terminal risk management is to be performed
x	x	x	x	x	1	x	x	Issuer authentication is supported ²⁰
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	1	CDA supported

AIP Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	0	x	x	x	x	x	x	RFU
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Blocs fonctionnels de la transaction à réaliser **par le Terminal**

Authentification carte

Authentification porteur

Gestion du risque terminal

Authentification émetteur

Initialisation transaction

Données carte

- **AFL** (Application File Locator)
 - └ Permet la lecture des **records** de la carte
- **Structure**



- └ **SFI** : référence du **fichier**
- └ **Start Rec** : premier **record** à lire
- └ **End Rec** : dernier record à lire
- └ **Nb Auth** : record participant à **l'authentification de la carte**

Initialisation transaction

Données terminal

- **TVR** (Terminal Verification Results)
- Chaque module fonctionnel va positionner un événement dans la TVR

Octet 1	B8 : authentification non réalisée
	B7 : authentification statique échouée
	B6 : données absentes
	B5 : présence en liste noire
	B4 : authentification dynamique échouée
	B3 : authentification DDA/AC échouée
	B2 : SDA sélectionné
	B1 : RUF

Octet 2	B8 : nos version application différents
	B7 : application périmée
	B6 : application non encore valide
	B5 : service non offert
	B4 : nouvelle carte
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 3	B8 : échec de la Vérification du porteur
	B7 : CVM non reconnue
	B6 : nombre limite d'essais de code atteint
	B5 : pin-pad absent ou hors-service
	B4 : code non saisi
	B3 : contrôle on-line du code
	B2 : Ruf
	B1 : Ruf

Octet 4	B8 : cumul porteur dépassé
	B7 : limite inférieure de tr. off-line dépassée
	B6 : limite supérieure de tr. off-line dépassée
	B5 : transaction sélectionnée aléatoirement
	B4 : transaction forcée online par commerçant
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 5	B8 : TDOL par défaut utilisée
	B7 : Authentification émetteur échouée
	B6 : Echec script avant 2ème Generate AC
	B5 : Echec script après 2ème Generate AC
	B4 : Réserve au contactless
	B3 : Réserve au contactless
	B2 : Réserve au contactless
	B1 : Réserve au contactless

Initialisation transaction

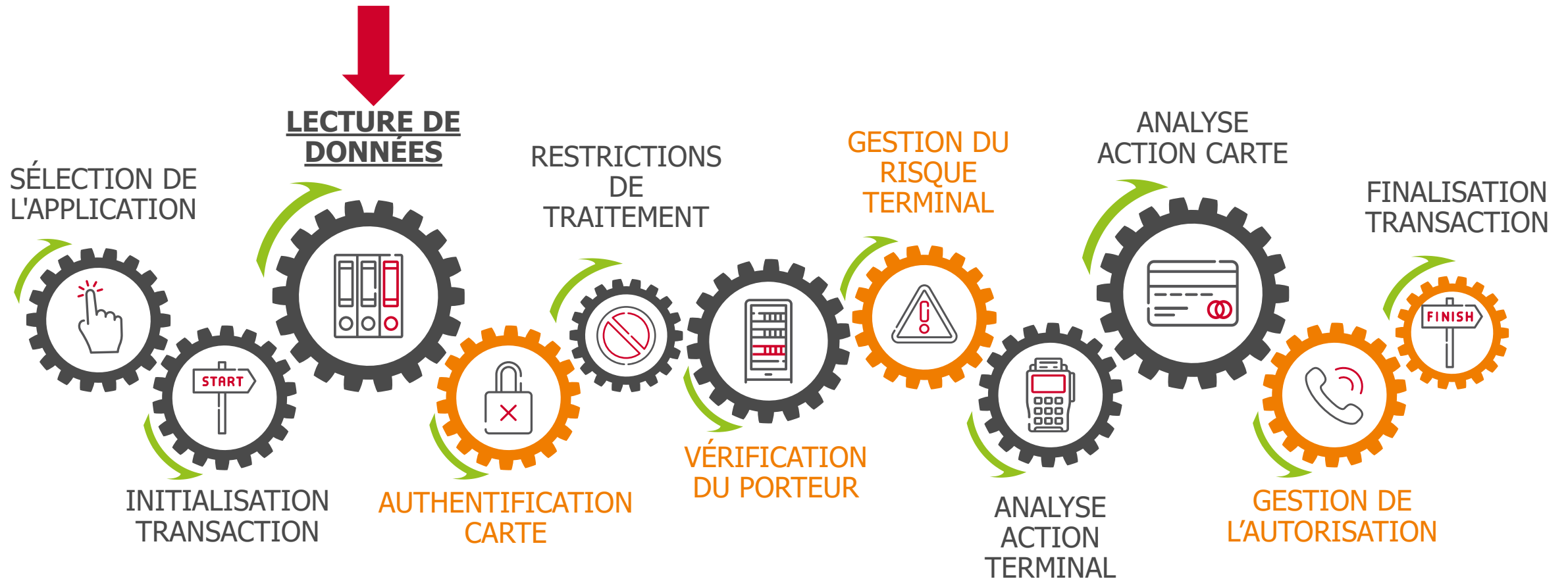
Données terminal

- **TSI** (Transaction Status Information)
- Chaque module fonctionnel va positionner un événement dans la TSI

Octet 1	B8 : authentification réalisée
	B7 : vérification du porteur réalisée
	B6 : gestion du risque carte réalisée
	B5 : authentification émetteur réalisée
	B4 : gestion du risque terminal réalisée
	B3 : traitement des scripts réalisé
	B2 : Ruf
	B1 : Ruf

Octet 2	B8 : Ruf
	B7 : Ruf
	B6 : Ruf
	B5 : Ruf
	B4 : Ruf
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Synoptique du déroulement de la transaction



Lecture des données

Lecture des données de l'application carte



- Utilisation de l'**AFL**
- Une des données obligatoire (expiration date, PAN, CDOL1/CDOL2) est absente :
 - **Abandon de la transaction**
- Données facultatives absente
 - **Mise à jour de la TVR**

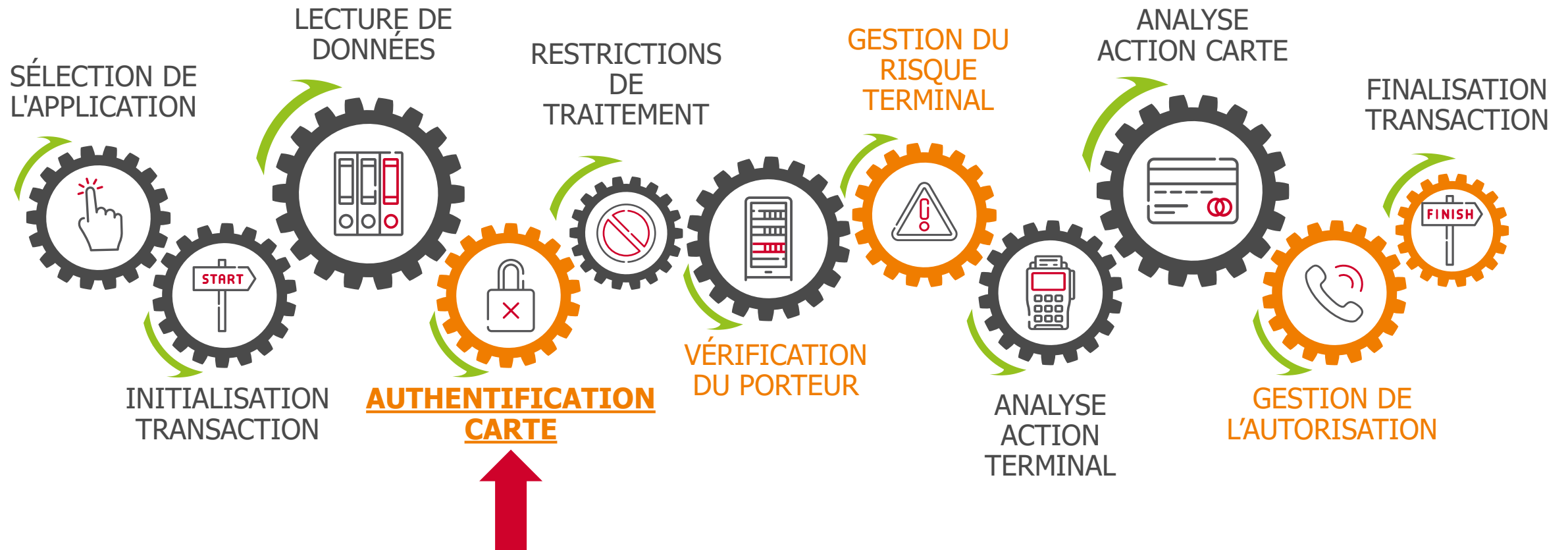
Lecture des données

Mise à jour de l'octet 1 de la TVR

Octet 1	B8 : authentification non réalisée
	B7 : authentification statique échouée
	B6 : données absentes
	B5 : présence en liste noire
	B4 : authentification dynamique échouée
	B3 : authentification DDA/AC échouée
	B2 : SDA sélectionné
Octet 2	B1 : Ruf
	B8 : nos version application différents
	B7 : application périmée
	B6 : application non encore valide
	B5 : service non offert
	B4 : nouvelle carte
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 3	B8 : échec de la Vérification du porteur
	B7 : CVM non reconnue
	B6 : nombre limite d'essais de code atteint
	B5 : pin-pad absent ou hors-service
	B4 : code non saisi
	B3 : contrôle on-line du code
	B2 : Ruf
Octet 4	B1 : Ruf
	B8 : cumul porteur dépassé
	B7 : limite inférieure de tr. off-line dépassée
	B6 : limite supérieure de tr. off-line dépassée
	B5 : transaction sélectionnée aléatoirement
	B4 : transaction forcée online par commerçant
	B3 : Ruf
Octet 4	B2 : Ruf
	B1 : Ruf
	B8 : TDOL par défaut utilisée
	B7 : Authentification émetteur échouée
	B6 : Echec script avant 2ème Generate AC
	B5 : Echec script après 2ème Generate AC
	B4 : Réservé au contactless
	B3 : Réservé au contactless
	B2 : Réservé au contactless
	B1 : Réservé au contactless

Synoptique du déroulement de la transaction



Authentification carte

Cryptographie asymétrique : les principes

— Cryptographie asymétrique (clé publique/clé privée)

— Chiffrer

└ **confidentialité** des échanges

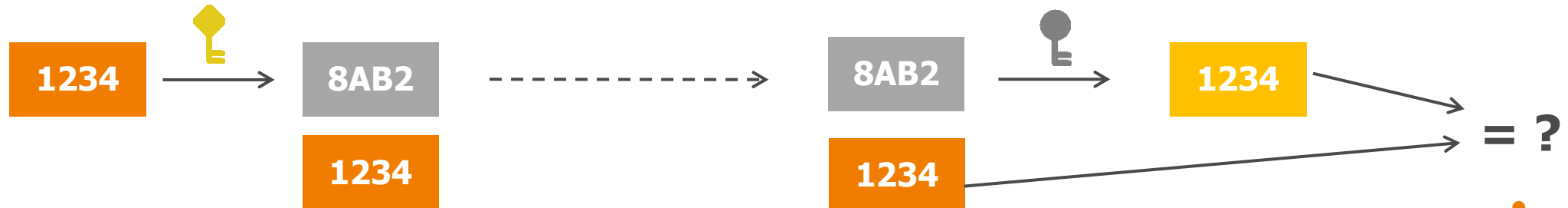
└ avec la clé publique 



— Signer

└ **authentification** de l'émetteur

└ avec la clé privée 



Authentification carte

Cryptographie asymétrique : la signature

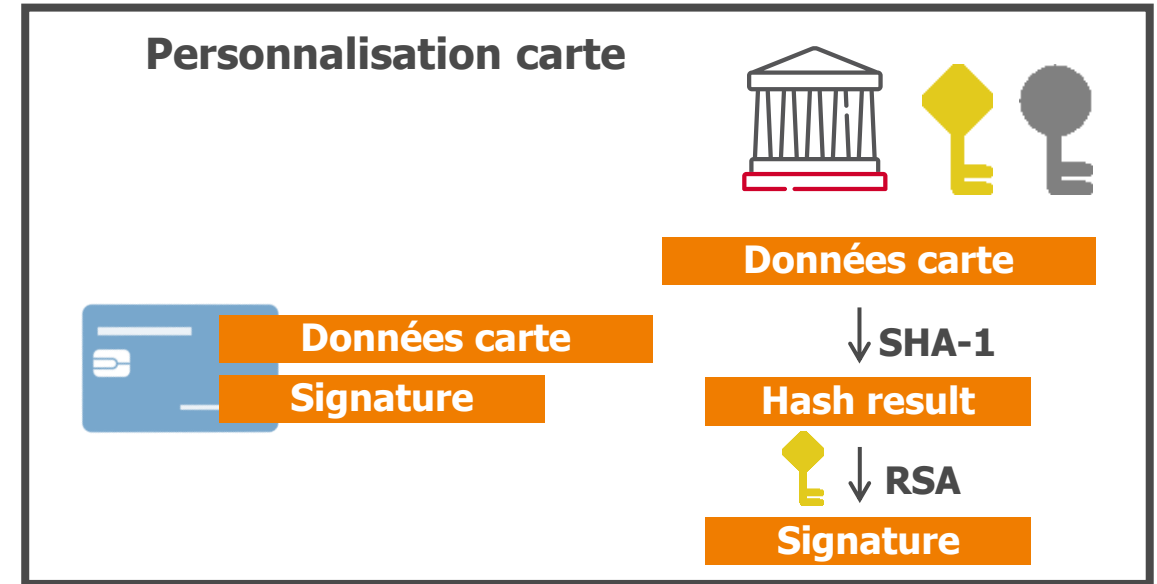
- Les algorithmes : **RSA**, ECC (courbes elliptiques)
- **Contrainte**
 - ▢ Le bloc à chiffrer doit être plus petit que la taille de la clé
 - ▢ Utilisation d'un algorithme de **hachage** (empreinte) : **SHA-1**



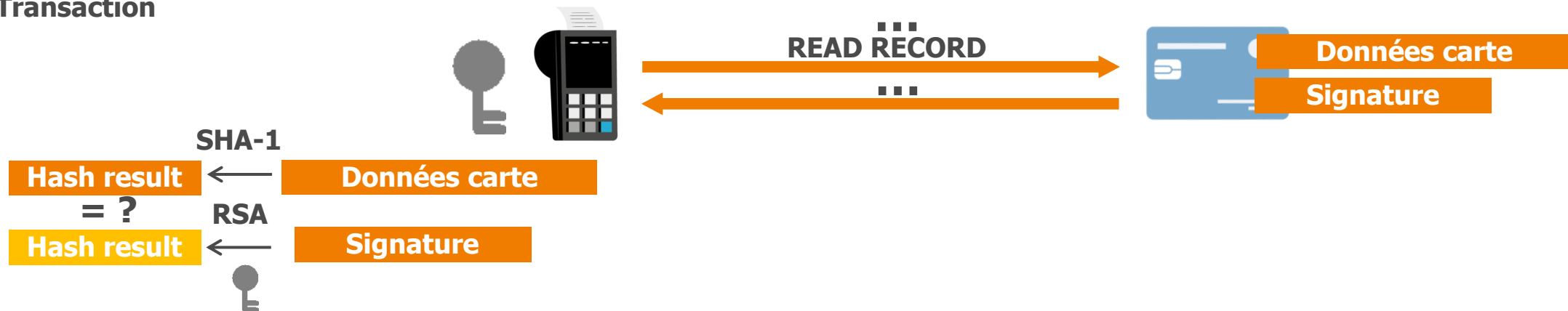
Authentication carte

SDA (Static data authentication)

- Le principe
 - Nécessité d'une architecture **PKI***
- *Public Key Infrastructure

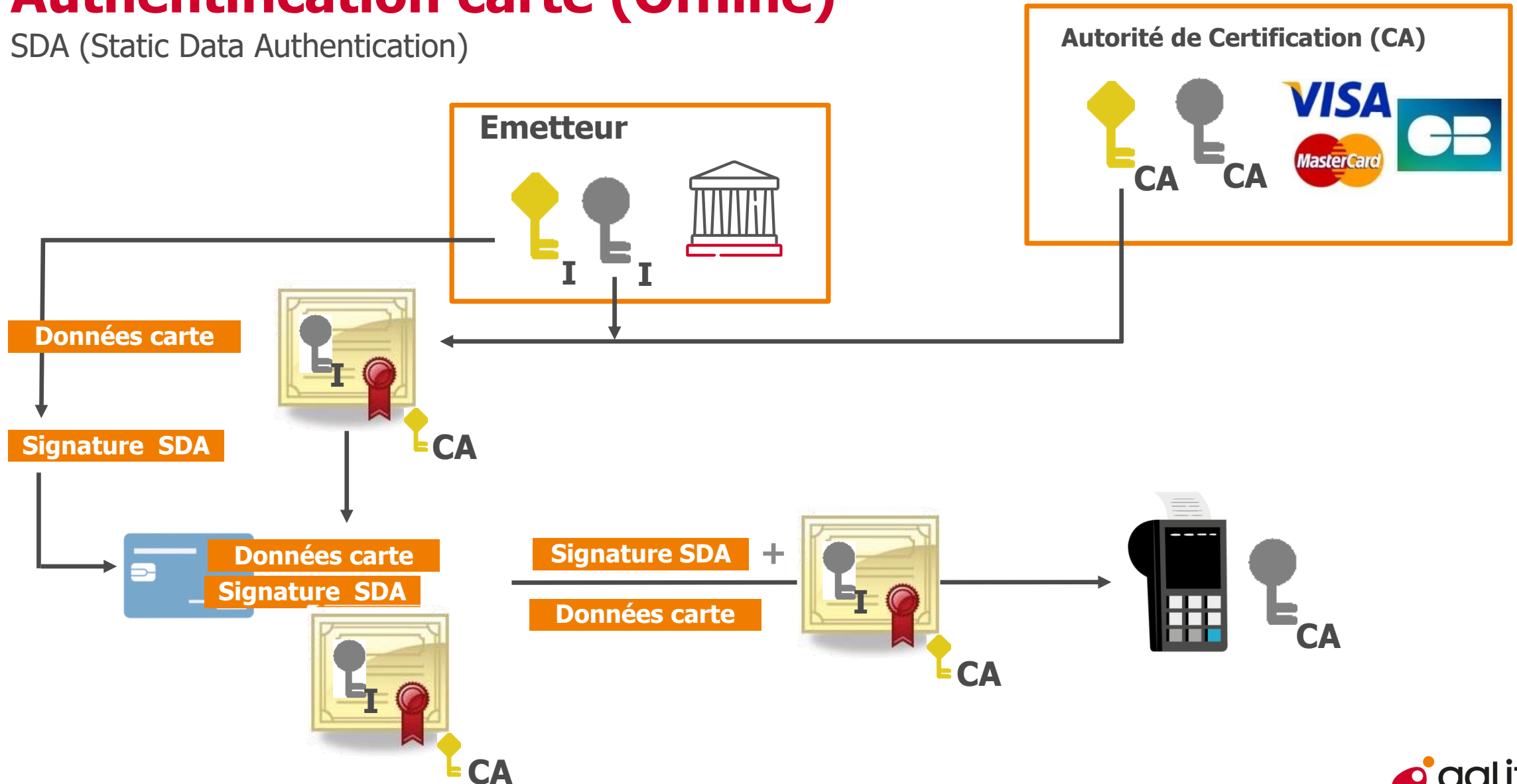


Transaction



Authentification carte (Offline)

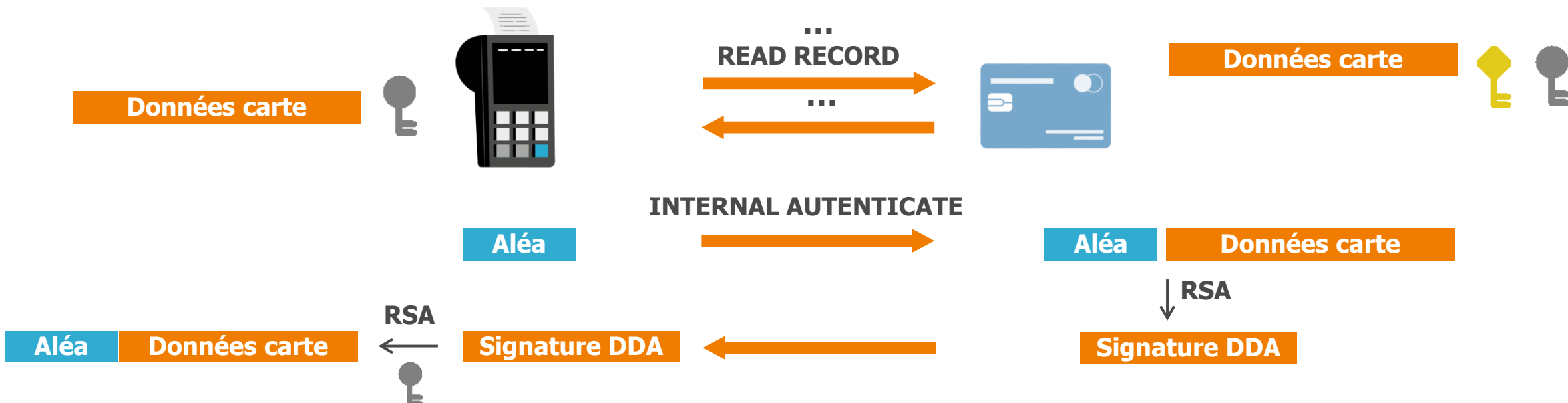
SDA (Static Data Authentication)



Authentification carte

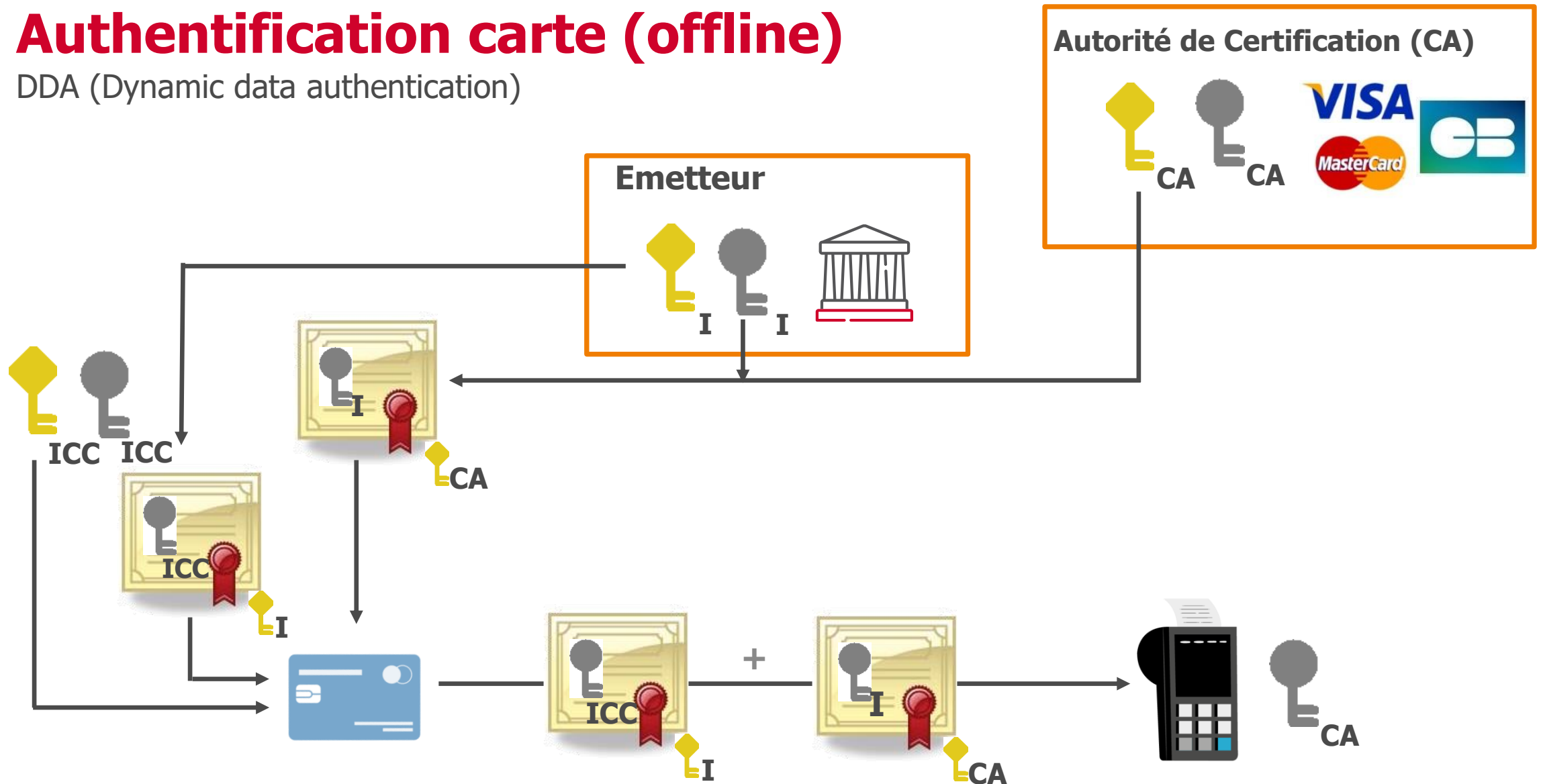
DDA (Dynamic Data Authentication)

- La signature est **différente à chaque transaction**
- Clé secrète présente dans la carte



Authentification carte (offline)

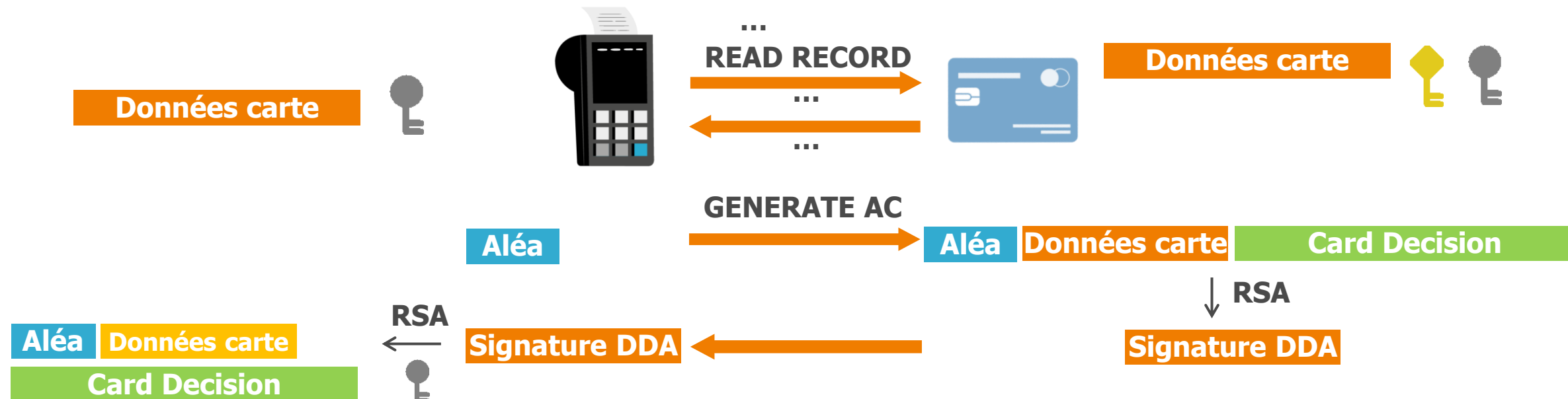
DDA (Dynamic data authentication)



Authentification carte

CDA (Combined Dynamic Data Authentication)

- La signature inclut **la décision de la carte**
- Protège contre **l'échange de carte** pendant la transaction



Authentification carte (offline)

SDA vs DDA vs CDA

— Utilisation des principes cryptographiques de signature

Objectifs	Authenticité des données	Protection de la carte contre le <u>clonage</u>	Protection de la carte contre l'" <u>échange</u> " de <u>carte</u> pendant la transaction
Outils Carte	Signature de données statiques	Secret carte et Crypto processeur Signer des données dynamiques	Secret carte et Crypto processeur Signer des données dynamiques en fin de transaction (≡ décision finale)
Méthodes	SDA DDA CDA	DDA CDA	CDA

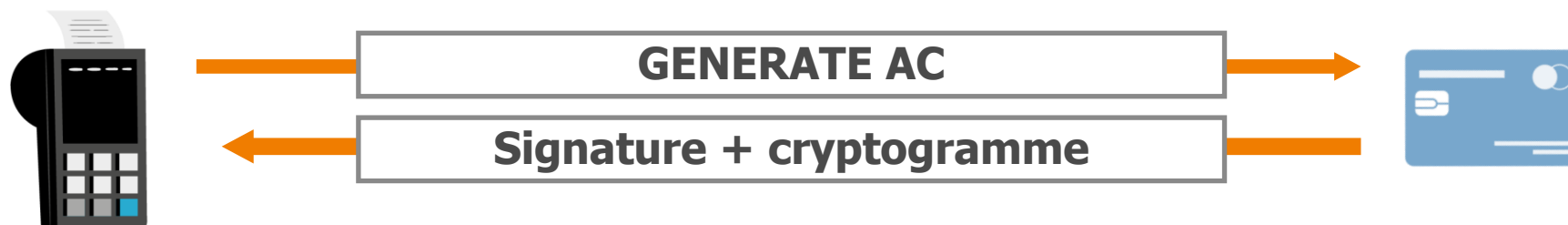
Authentication carte (offline)

Commandes

- Authentification locale de la carte par le terminal
 - └ Authentification statique **SDA** (bit 7 du 1er octet AIP)
Pas de commande
 - └ Authentification dynamique : **prioritaire**
DDA (bit 6 du 1er octet AIP)



CDA Combined DDA/AC (bit 1 du 1er octet AIP)



Authentification carte (offline)

Mise à jour de l'octet 1 de la TVR si échec de l'authentification

Octet 1

B8 : authentification non réalisée
B7 : authentification statique échouée
B6 : données absentes
B5 : présence en liste noire
B4 : authentification dynamique échouée
B3 : authentification DDA/AC échouée
B2 : SDA sélectionné
B1 : Ruf

Octet 2

B8 : nos version application différents
B7 : application périmée
B6 : application non encore valide
B5 : service non offert
B4 : nouvelle carte
B3 : Ruf
B2 : Ruf
B1 : Ruf

Octet 3

B8 : échec de la Vérification du porteur
B7 : CVM non reconnue
B6 : nombre limite d'essais de code atteint
B5 : pin-pad absent ou hors-service
B4 : code non saisi
B3 : contrôle on-line du code
B2 : Ruf
B1 : Ruf

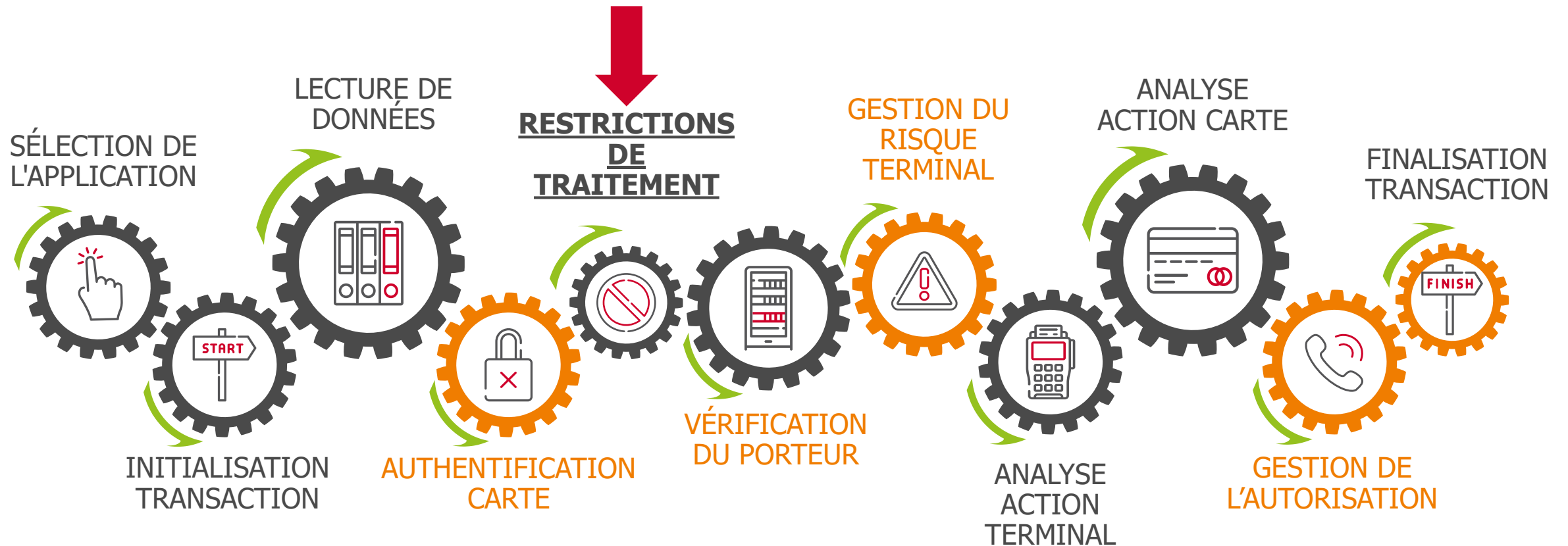
Octet 4

B8 : cumul porteur dépassé
B7 : limite inférieure de tr. off-line dépassée
B6 : limite supérieure de tr. off-line dépassée
B5 : transaction sélectionnée aléatoirement
B4 : transaction forcée online par commerçant
B3 : Ruf
B2 : Ruf
B1 : Ruf

Octet 5

B8 : TDOL par défaut utilisée
B7 : Authentification émetteur échouée
B6 : Echec script avant 2ème Generate AC
B5 : Echec script après 2ème Generate AC
B4 : Réserve au contactless
B3 : Réserve au contactless
B2 : Réserve au contactless
B1 : Réserve au contactless

Synoptique du déroulement de la transaction



Restrictions de traitement

- Les restrictions de traitement contrôlent
 - └ L'adéquation entre les **versions** d'application carte et terminal
 - └ L'adéquation entre l'**AUC*** et les conditions de la transaction
 - └ Les **dates de début** et **fin de validité** de l'application

- Pas de dialogue carte-terminal

*AUC : Application Usage Control

Application Usage Control Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Valid for domestic cash transactions
x	1	x	x	x	x	x	x	Valid for international cash transactions
x	x	1	x	x	x	x	x	Valid for domestic goods
x	x	x	1	x	x	x	x	Valid for international goods
x	x	x	x	1	x	x	x	Valid for domestic services
x	x	x	x	x	1	x	x	Valid for international services
x	x	x	x	x	x	1	x	Valid at ATMs
x	x	x	x	x	x	x	1	Valid at terminals other than ATMs

Application Usage Control Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Domestic cashback allowed
x	1	x	x	x	x	x	x	International cashback allowed
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

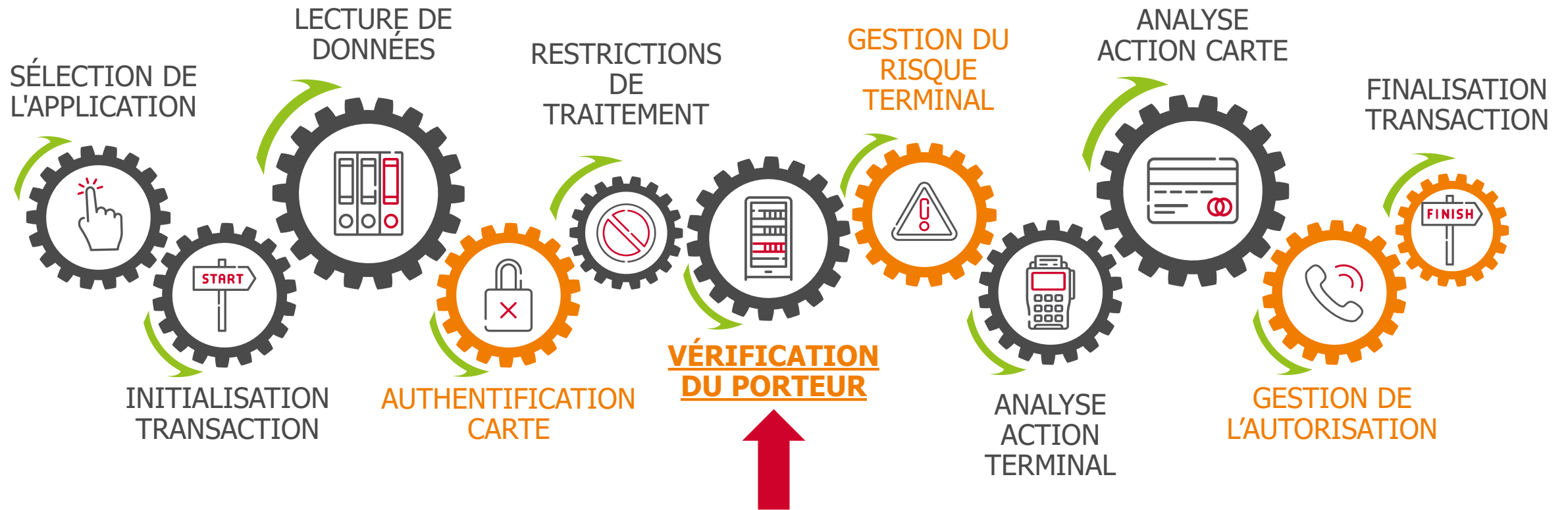
Restrictions de traitement

Mise à jour de l'octet 2 de la TVR si nécessaire

Octet 1	B8 : authentification non réalisée
	B7 : authentification statique échouée
	B6 : données absentes
	B5 : présence en liste noire
	B4 : authentification dynamique échouée
	B3 : authentification DDA/AC échouée
	B2 : SDA sélectionné
Octet 2	B1 : Ruf
	B8 : nos version application différents
	B7 : application périmée
	B6 : application non encore valide
	B5 : service non offert
	B4 : nouvelle carte
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 3	B8 : échec de la Vérification du porteur
	B7 : CVM non reconnue
	B6 : nombre limite d'essais de code atteint
	B5 : pin-pad absent ou hors-service
	B4 : code non saisi
	B3 : contrôle on-line du code
	B2 : Ruf
Octet 4	B1 : Ruf
	B8 : cumul porteur dépassé
	B7 : limite inférieure de tr. off-line dépassée
	B6 : limite supérieure de tr. off-line dépassée
	B5 : transaction sélectionnée aléatoirement
	B4 : transaction forcée online par commerçant
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf
Octet 5	B8 : TDOL par défaut utilisée
	B7 : Authentification émetteur échouée
	B6 : Echec script avant 2ème Generate AC
	B5 : Echec script après 2ème Generate AC
	B4 : Réserve au contactless
	B3 : Réserve au contactless
	B2 : Réserve au contactless
	B1 : Réserve au contactless

Synoptique du déroulement de la transaction



Vérification du porteur

Principe

- Réalisée si supportée par l'AIP
- Le type de vérification du porteur est déterminé par la **CVM List***
 - └ **Méthodes** de vérification
 - └ **Condition** d'application
- Mise à jour de l'octet 3 de la TVR si nécessaire
- Mise à jour de la donnée terminal **CVM Results**

*Cardholder Verification Method List

Vérification du porteur

CVM List : structure



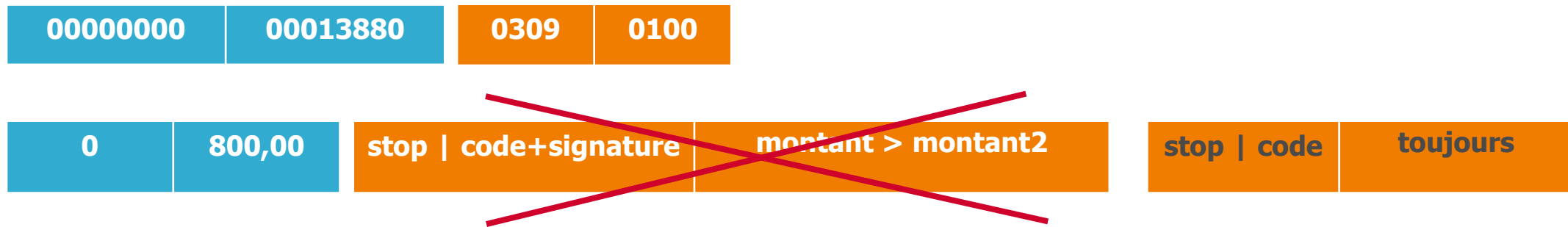
*signature : papier ou
écran électronique

METHODE			CONDITION
b8	b7	b6 ... b1	
0	ind. Poursuite	méthode échouée	toujours
0	ind. Poursuite	code offline en clair	retrait automate
0	ind. Poursuite	code chiffré on-line	paiement
0	ind. Poursuite	code offline en clair + signature*	si supporté par le terminal
0	ind. Poursuite	code offline chiffré	retrait manuel
0	ind. Poursuite	code offline chiffré + signature*	paiement avec cashback
0	ind. Poursuite	signature*	montant < montant1
0	ind. Poursuite	aucune méthode requise	montant > montant1
			montant < montant2
			montant > montant2

Vérification du porteur

CVM List : exemple

- CVM List = 00000000 00013880 0309 0100
- Montant transaction= 50€
- Quelle authentification pendant la transaction?



→ code confidentiel

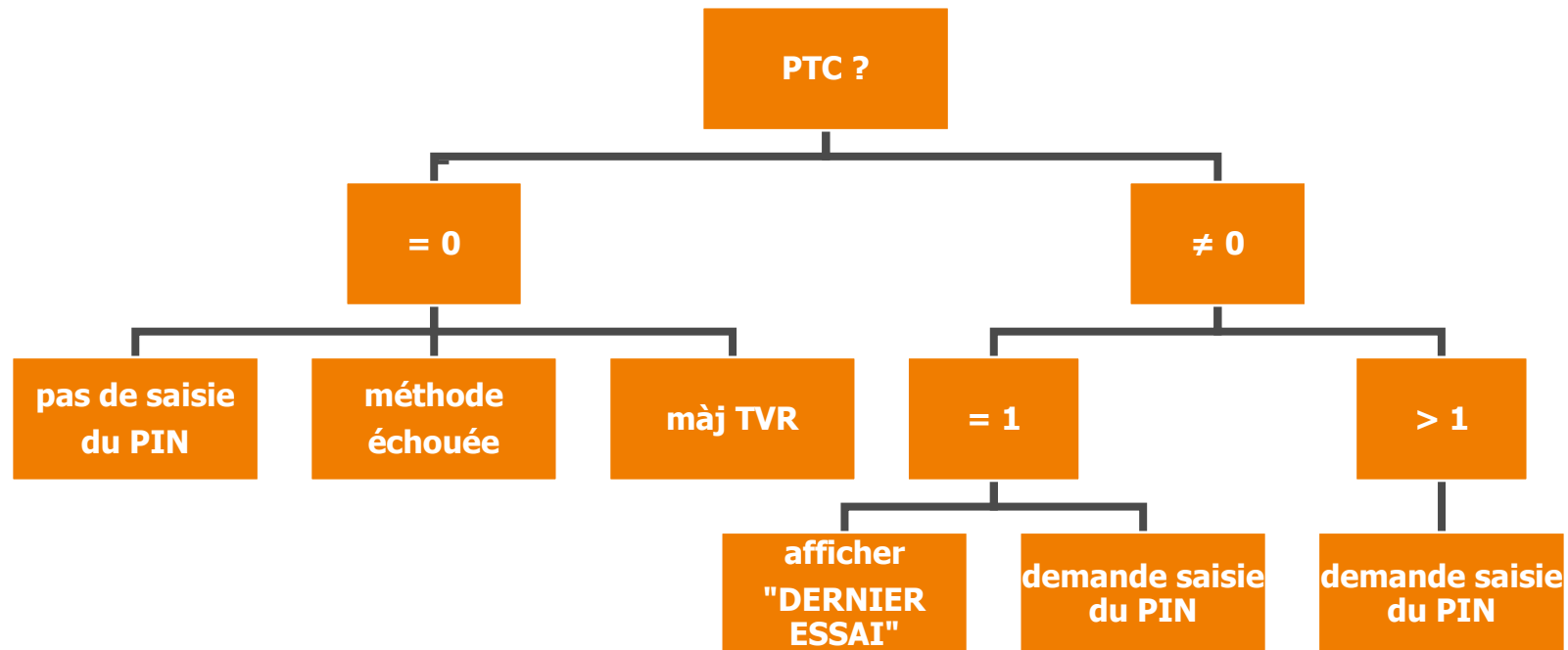
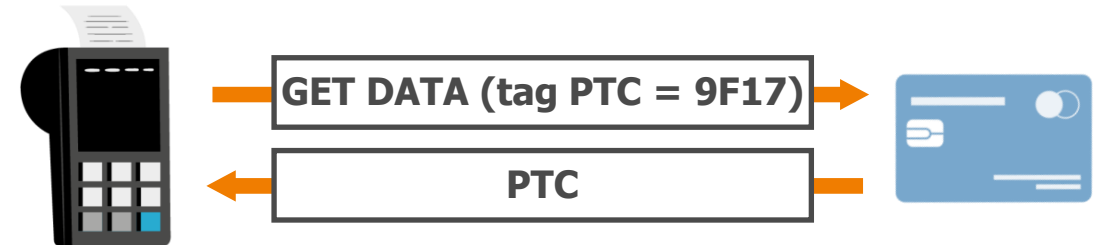
* signature : papier ou écran électronique

Vérification du porteur

Contrôle du PIN : gestion du PTC

- **PTC** (PIN Try Counter)

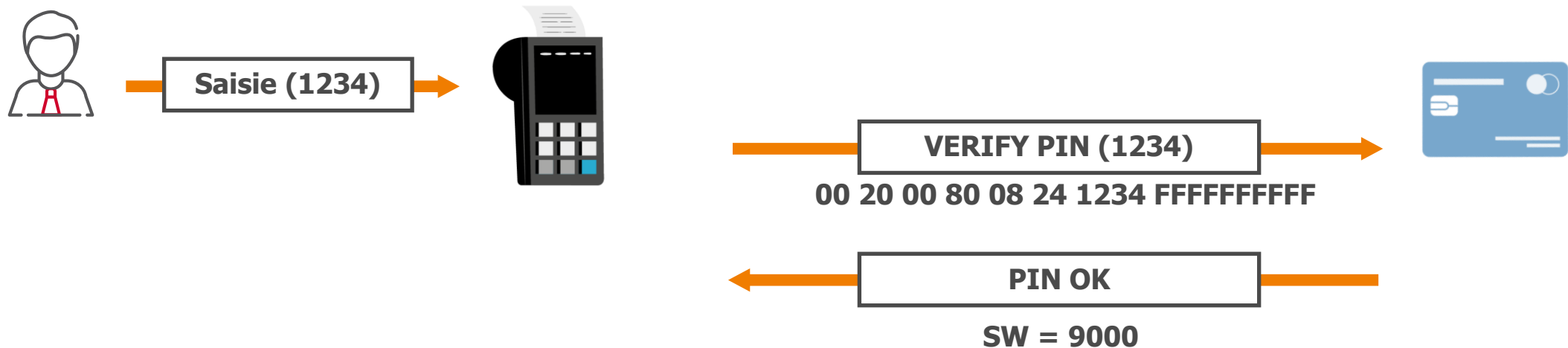
- └ Récupération du nombre d'essai restant
- └ Analyse du PTC



Vérification du porteur

Contrôle du PIN : PIN offline en clair

— Présentation du PIN en clair



— Echec de la vérification porteur :

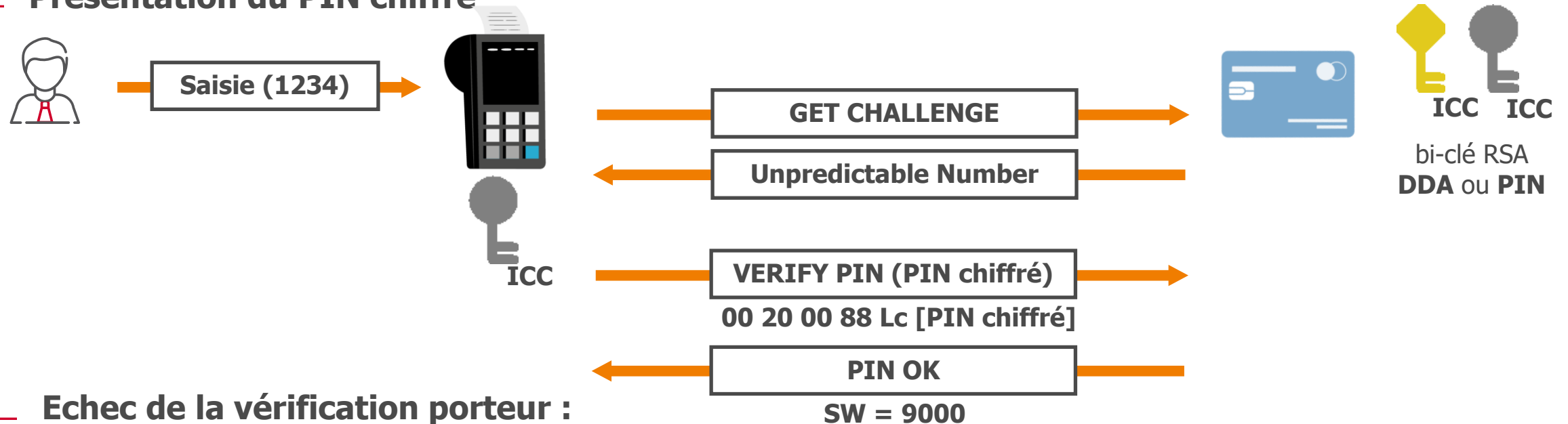
- └ SW1SW2 = 63CX, avec X=nombre d'essai(s) restant(s)
- └ SW1SW2 = 6983, le PIN est bloqué (nombre d'essai atteint)

— Vérification OK → Mise à jour du PTC

Vérification du porteur

Contrôle du PIN : PIN offline chiffré

— Présentation du PIN chiffré



— Echec de la vérification porteur :

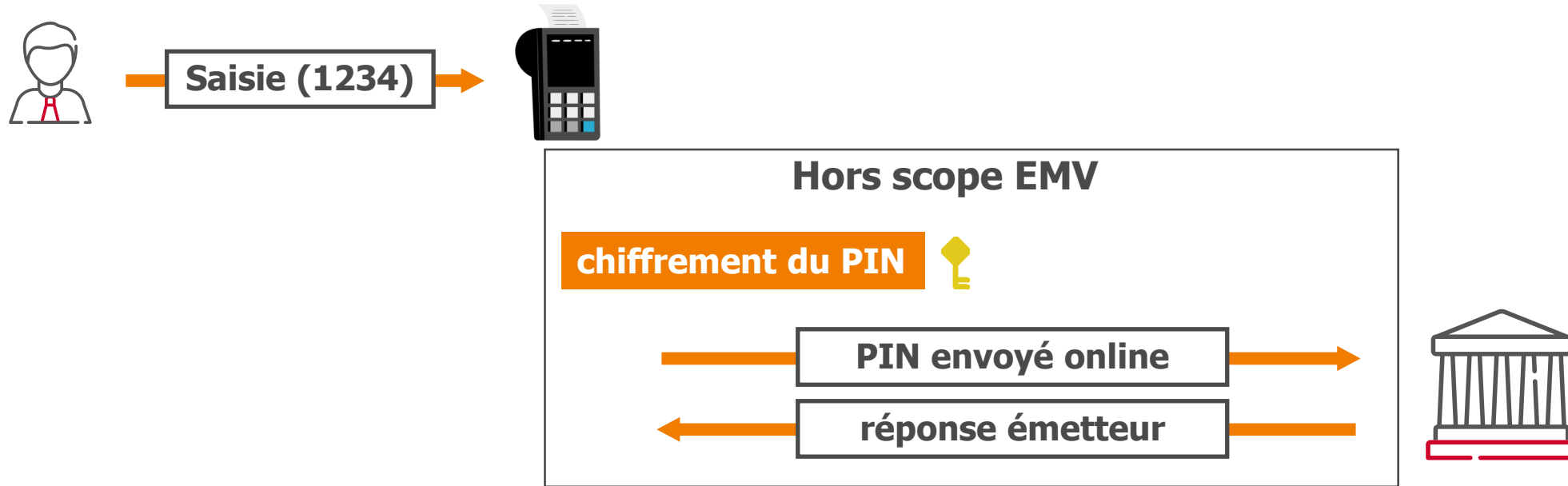
- SW1SW2 = 63CX, avec X=nombre d'essai(s) restant(s)
- SW1SW2 = 6983, le PIN est bloqué (nombre d'essai atteint)

— Vérification OK → Mise à jour du PTC

Vérification du porteur

Contrôle du PIN : PIN online chiffré

— Présentation du PIN chiffré



- **Chiffrement** du PIN par le terminal
- Mise à jour de la **TVR**
- Vérification par l'**émetteur** sur demande d'**autorisation**

Vérification du porteur

Mise à jour de l'octet 3 de la TVR si nécessaire

Octet 1

- B8 : authentification non réalisée
- B7 : authentification statique échouée
- B6 : données absentes
- B5 : présence en liste noire
- B4 : authentification dynamique échouée
- B3 : authentification DDA/AC échouée
- B2 : SDA sélectionné
- B1 : Ruf

Octet 2

- B8 : nos version application différents
- B7 : application périmée
- B6 : application non encore valide
- B5 : service non offert
- B4 : nouvelle carte
- B3 : Ruf
- B2 : Ruf
- B1 : Ruf

Octet 3

- B8 : échec de la Vérification du porteur
- B7 : CVM non reconnue
- B6 : nombre limite d'essais de code atteint
- B5 : pin-pad absent ou hors-service
- B4 : code non saisi
- B3 : contrôle on-line du code
- B2 : Ruf
- B1 : Ruf

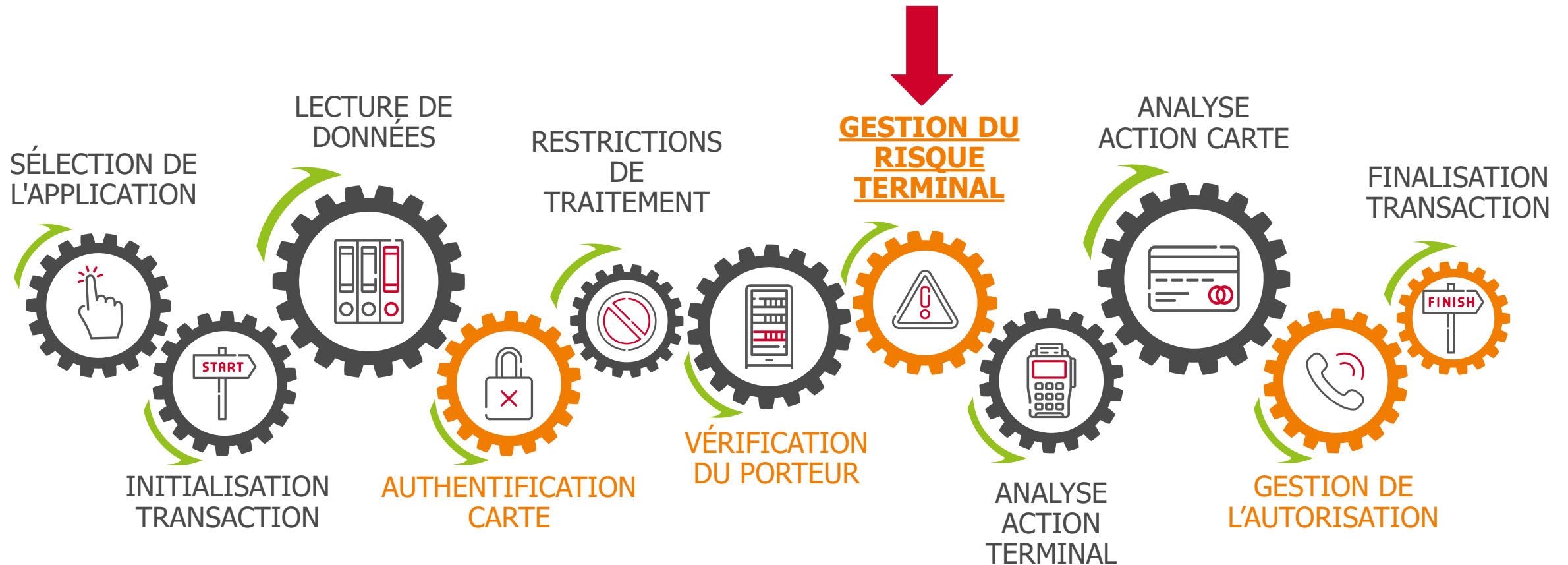
Octet 4

- B8 : cumul porteur dépassé
- B7 : limite inférieure de tr. off-line dépassée
- B6 : limite supérieure de tr. off-line dépassée
- B5 : transaction sélectionnée aléatoirement
- B4 : transaction forcée online par commerçant
- B3 : Ruf
- B2 : Ruf
- B1 : Ruf

Octet 5

- B8 : TDOL par défaut utilisée
- B7 : Authentification émetteur échouée
- B6 : Echec script avant 2ème Generate AC
- B5 : Echec script après 2ème Generate AC
- B4 : Réservé au contactless
- B3 : Réservé au contactless
- B2 : Réservé au contactless
- B1 : Réservé au contactless

Synoptique du déroulement de la transaction



Gestion du risque terminal

Les contrôles

- 3 types de contrôle
 - └ **Cumul porteur** pour contrôle **seuil d'appel** commerçant (floor limit)
 - └ Appel **aléatoire**
 - └ Contrôle de flux (**velocity checking**)
- Dialogue carte-terminal pour lecture des compteurs
- Mise à jour des octets 1, 2 et 4 de la **TVR** si nécessaire

Gestion du risque terminal

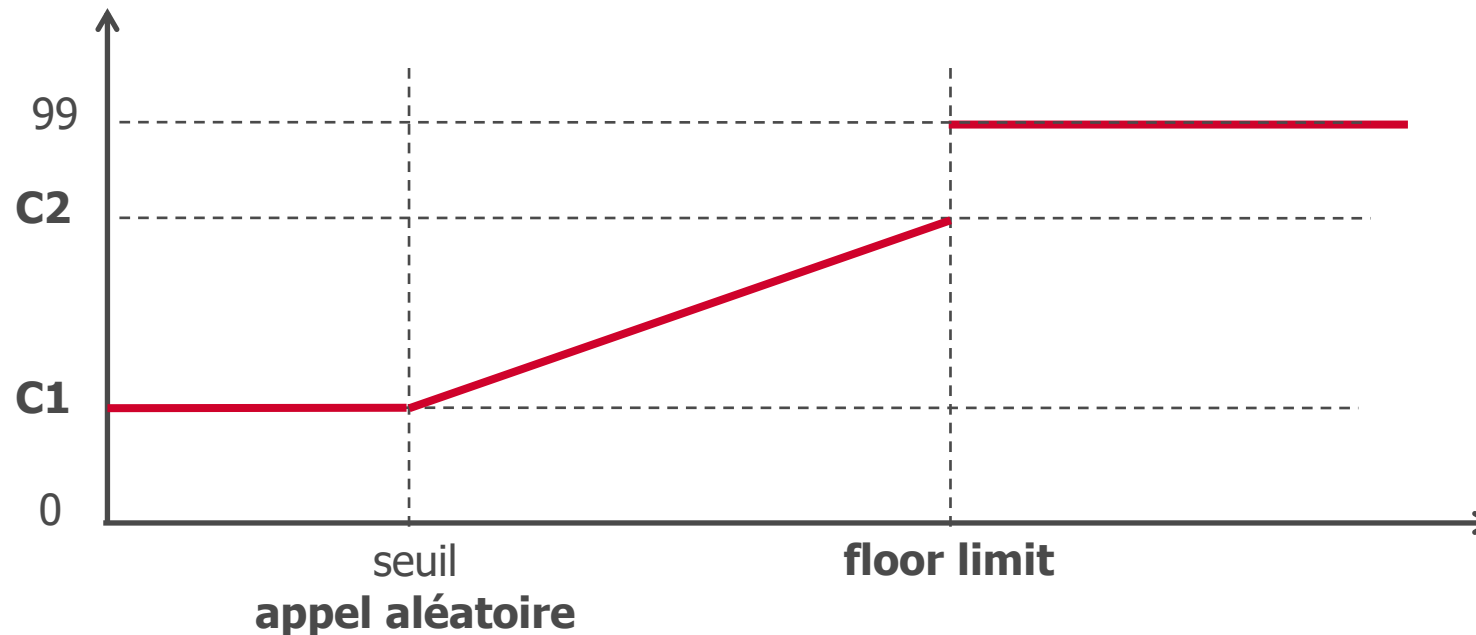
Cumul porteur

- Le terminal dispose d'un **seuil d'appel** « terminal floor limit »
- Le terminal **ne dispose pas** d'un journal des transactions
 - └ Comparaison du montant de la transaction courante avec le seuil d'appel
- Le terminal **dispose** d'un journal des transactions
 - └ Recherche des transactions mémorisées pour le porteur
 - └ **Cumul** montant dernière transaction avec montant transaction courante
 - └ Comparaison du montant calculé avec le seuil d'appel
- **Seuil dépassé → mise à jour TVR (Cumul porteur dépassé)**

Gestion du risque terminal

Appel aléatoire

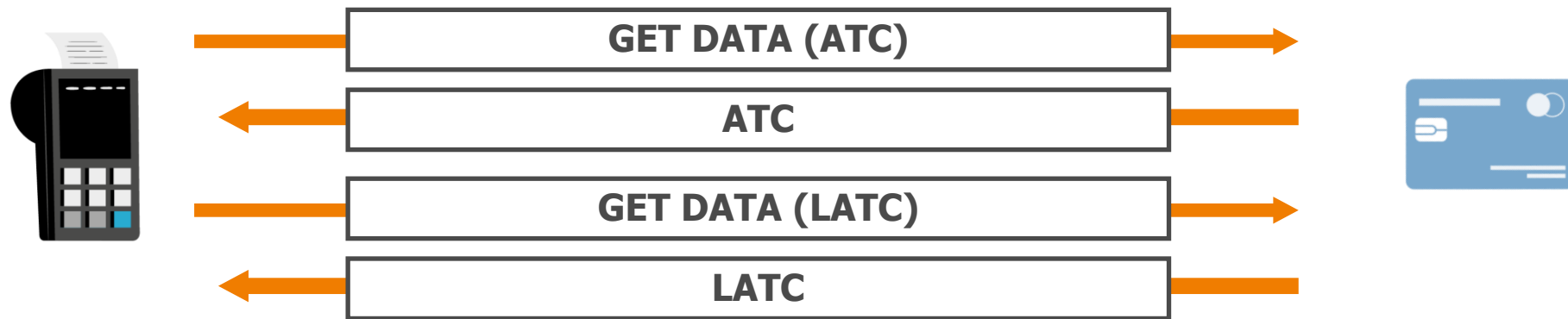
- Le terminal dispose de deux seuils d'appel et de deux coefficients :
 - └ seuil d'appel **floor limit**
 - └ seuil d'**appel aléatoire**
 - └ coefficients ($0 \leq \mathbf{C1} \leq \mathbf{C2} \leq 99$)
- Montant inférieur au floor limit Le terminal génère un nombre aléatoire. Mise à jour TVR éventuellement.



Gestion du risque terminal

Velocity checking

— Lecture des données **ATC** et "**Last OnLine ATC Register**"



— Mise à jour de la **TVR** si

- └ (ATC - Last OnLine ATC) > UCOL* → **Limite supérieure dépassée**
- └ (ATC - Last OnLine ATC) > LCOL* → **Limite inférieure dépassée**
- └ Last OnLine ATC = 0 → **Nouvelle carte**

Gestion du risque terminal

Mise à jour des octets 1, 2 et 4 de la TVR si nécessaire

Octet 1

- B8 : authentification non réalisée
- B7 : authentification statique échouée
- B6 : données absentes
- B5 : présence en liste noire
- B4 : authentification dynamique échouée
- B3 : authentification DDA/AC échouée
- B2 : SDA sélectionné
- B1 : Ruf

Octet 2

- B8 : nos version application différents
- B7 : application périmée
- B6 : application non encore valide
- B5 : service non offert
- B4 : nouvelle carte
- B3 : Ruf
- B2 : Ruf
- B1 : Ruf

Octet 3

- B8 : échec de la Vérification du porteur
- B7 : CVM non reconnue
- B6 : nombre limite d'essais de code atteint
- B5 : pin-pad absent ou hors-service
- B4 : code non saisi
- B3 : contrôle on-line du code
- B2 : Ruf
- B1 : Ruf

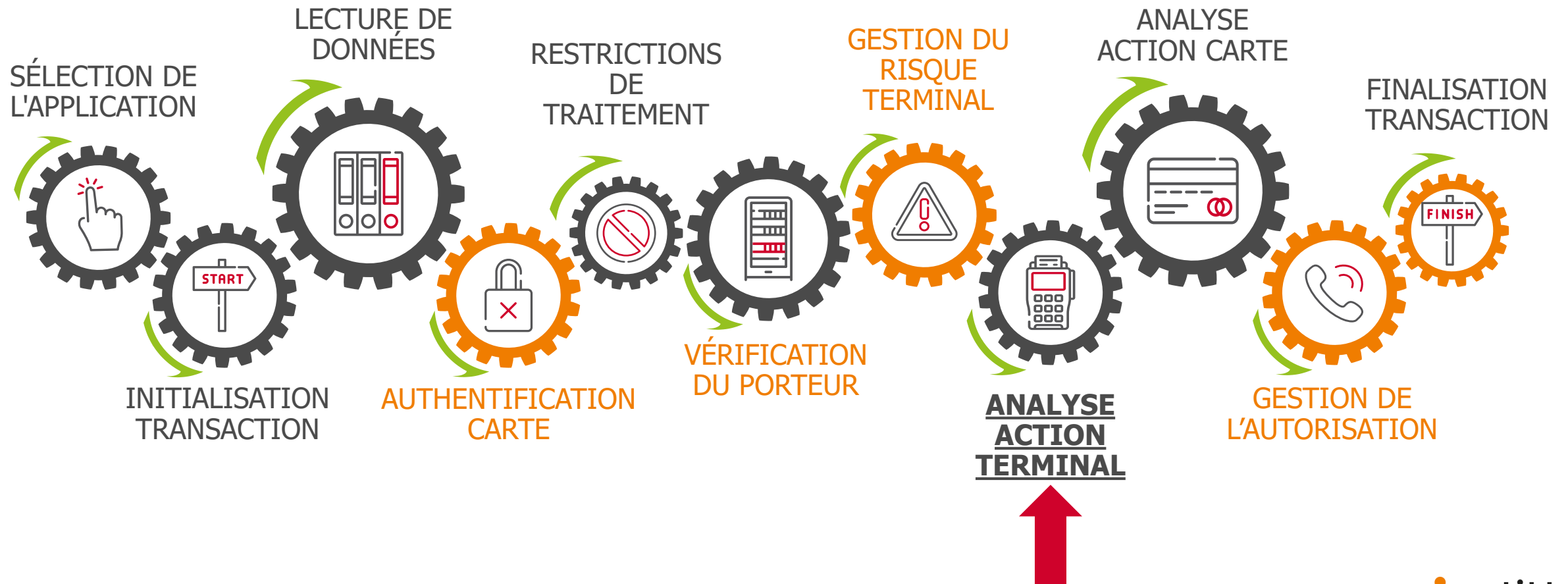
Octet 4

- B8 : cumul porteur dépassé
- B7 : limite inférieure de tr. off-line dépassée
- B6 : limite supérieure de tr. off-line dépassée
- B5 : transaction sélectionnée aléatoirement
- B4 : transaction forcée online par commerçant
- B3 : Ruf
- B2 : Ruf
- B1 : Ruf

Octet 5

- B8 : TDOL par défaut utilisée
- B7 : Authentification émetteur échouée
- B6 : Echec script avant 2ème Generate AC
- B5 : Echec script après 2ème Generate AC
- B4 : Réservé au contactless
- B3 : Réservé au contactless
- B2 : Réservé au contactless
- B1 : Réservé au contactless

Synoptique du déroulement de la transaction



Analyse action terminal

Principe

- Proposer une décision à la carte pour la transaction
 - └ **refus / on-line / acceptation**

- La décision est associée à une demande de **cryptogramme** :
 - └ **refus** : **AAC** (Application Authentication Cryptogram)
 - └ **online** : **ARQC** (Autorisation ReQuest Cryptogram)
 - └ **acceptation** : **TC** (Transaction Certificate)

- Décision collégiale issue
 - └ Du terminal : la **TVR**
 - └ De l'émetteur : le **IAC** de la carte (Issuer Action Code)
 - └ De l'acquéreur : le **TAC** (Terminal Action Code)

Analyse action terminal

Rappel structure TVR / TAC / IAC

Octet 1	B8 : authentification non réalisée
	B7 : authentification statique échouée
	B6 : données absentes
	B5 : présence en liste noire
	B4 : authentification dynamique échouée
	B3 : authentification DDA/AC échouée
	B2 : SDA sélectionné
	B1 : Ruf

Octet 2	B8 : nos version application différents
	B7 : application périmée
	B6 : application non encore valide
	B5 : service non offert
	B4 : nouvelle carte
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

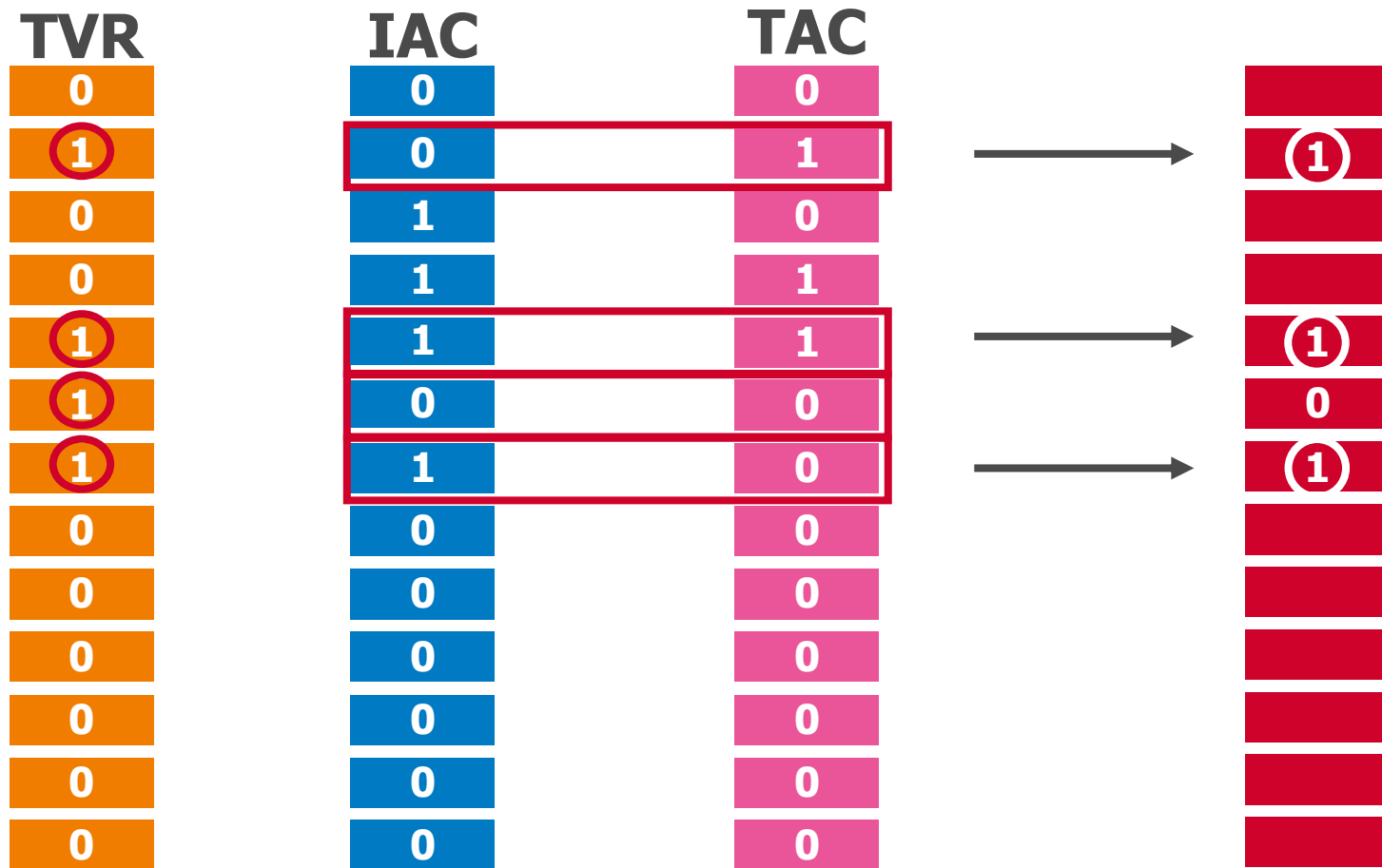
Octet 3	B8 : échec de la Vérification du porteur
	B7 : CVM non reconnue
	B6 : nombre limite d'essais de code atteint
	B5 : pin-pad absent ou hors-service
	B4 : code non saisi
	B3 : contrôle on-line du code
	B2 : Ruf
	B1 : Ruf

Octet 4	B8 : cumul porteur dépassé
	B7 : limite inférieure de tr. off-line dépassée
	B6 : limite supérieure de tr. off-line dépassée
	B5 : transaction sélectionnée aléatoirement
	B4 : transaction forcée online par commerçant
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 5	B8 : TDOL par défaut utilisée
	B7 : Authentification émetteur échouée
	B6 : Echec script avant 2ème Generate AC
	B5 : Echec script après 2ème Generate AC
	B4 : Réserve au contactless
	B3 : Réserve au contactless
	B2 : Réserve au contactless
	B1 : Réserve au contactless

Analyse action terminal

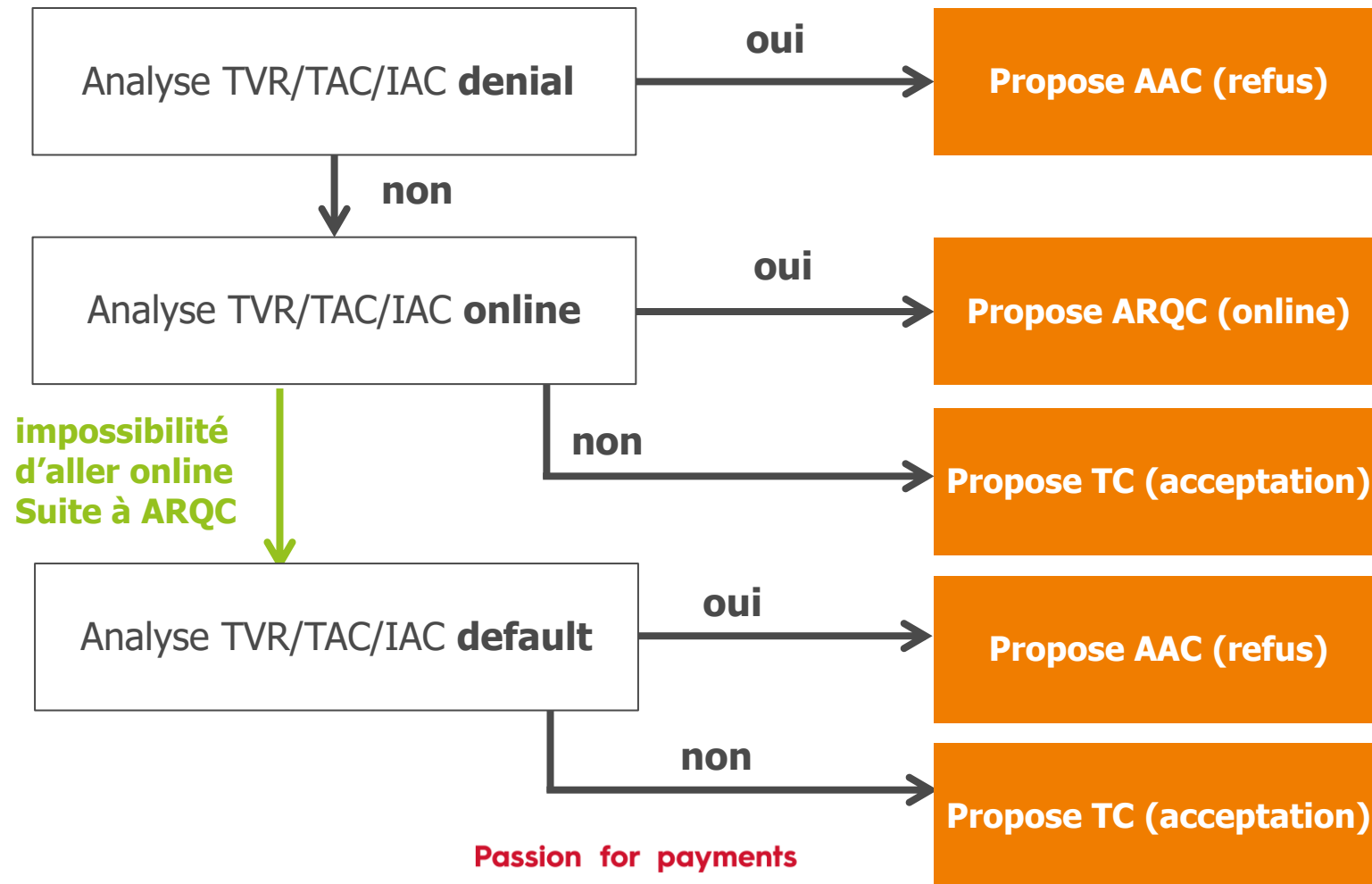
Prise de décision du terminal



Principe d'analyse

Prise de décision du terminal

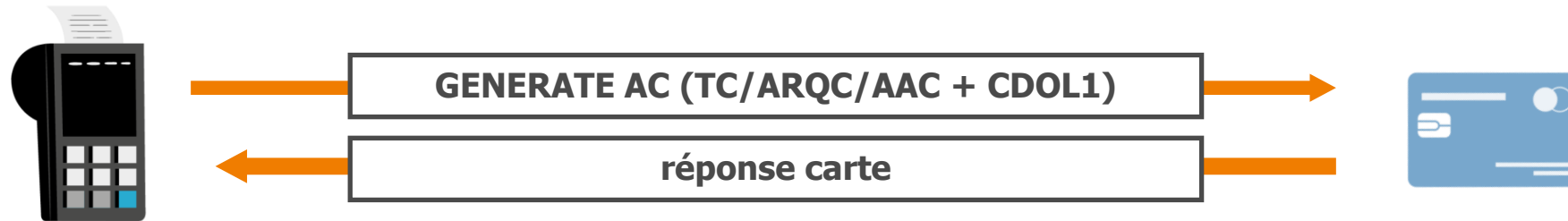
— Analyse des triplets **TVR/TAC/IAC** dans l'ordre suivant:



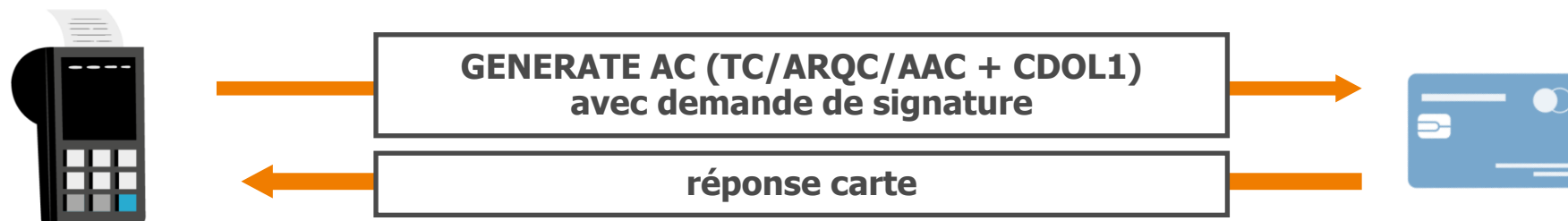
Analyse action terminal

Résultat de l'analyse des triplets (TVR, IAC, TAC)

- Transmission de la décision à la carte : **GENERATE AC**



- Cas d'une **CDA** (Combined Dynamic Data Authentication)



Analyse action terminal

Valeurs par défaut

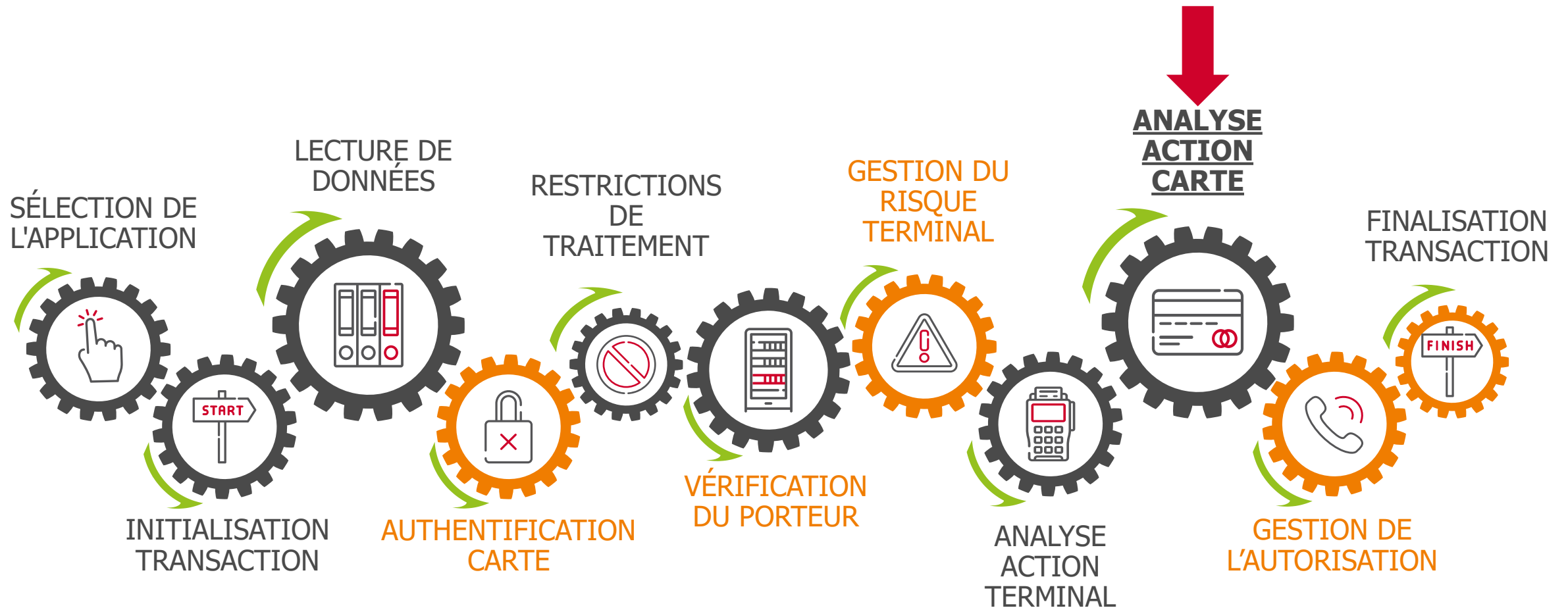
IAC		
refus	on-line	défaut
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1
0	1	1

Oct1 - bit 8
Oct1 - bit 7

Oct1 - bit 4
Oct1 - bit 3

TAC		
refus	on-line	défaut
0	1	1
0	1	1
0	0	0
0	0	0
0	1	1
0	1	1
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0

Synoptique du déroulement de la transaction



Analyse action carte

Principe

- La carte effectue sa propre **gestion du risque** (hors EMV) pour déterminer le type de cryptogramme en réponse

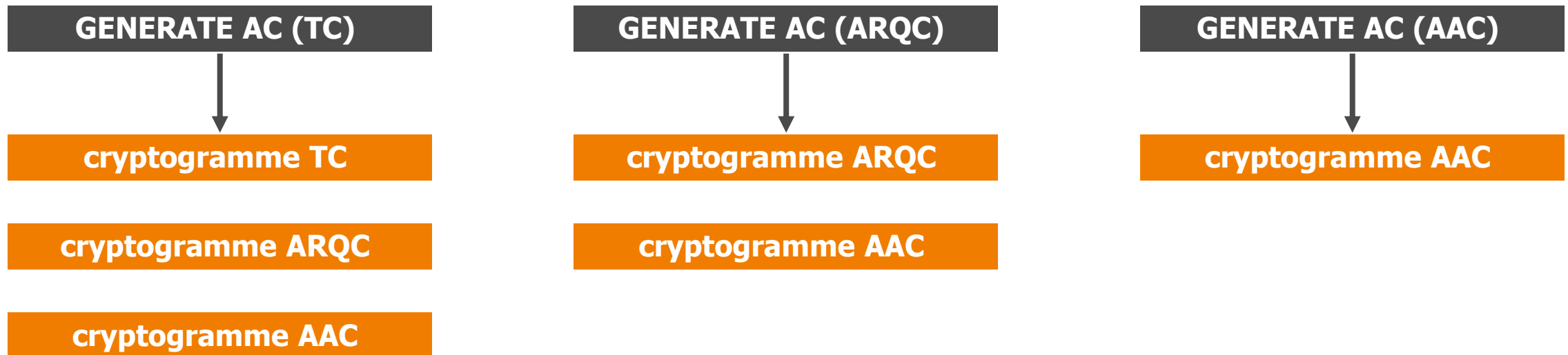
Exemple:

- └ La dernière transaction online n'a pas abouti
 - └ L'authentification émetteur sur la dernière transaction online a échoué
 - └ Le cumul offline vient d'être dépassé
 - └ ...
- La carte calcule un **cryptogramme** (TC/ARQC/AAC)

Analyse action carte

Contrainte sur le type du cryptogramme

- La carte répond obligatoirement par un type de cryptogramme égal ou inférieur à la demande



Analyse action carte

Calcul du cryptogramme

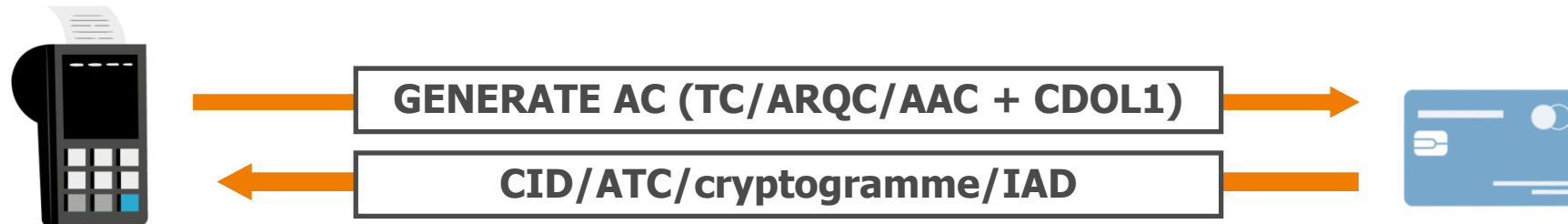
- La carte calcule un cryptogramme avec des données présentes dans la **CDOL1** en clair et/ou dans un TC Hash Value
 - └ Données **Terminal** : code pays du terminal
 - └ Données **Transaction** : montant, devise, TVR, date, type transaction, nombre aléatoire
 - └ Données **Carte** : AIP et ATC
- La carte utilise
 - └ Un algorithme **3DES** ou **AES**
 - └ Une **clé secrète** de calcul de cryptogramme



Analyse action carte

Réponse de la carte

— La carte répond à la demande du terminal



- └ **CID** : type du cryptogramme (1 octet)
- └ **ATC** : compteur de transactions (2 octets)
- └ **cryptogramme** (valeur sur 8 octets)
- └ **IAD** : Issuer Application Data (donnée propriétaire facultative : tag 9F10)

Analyse action carte

Génération du hash du certificat de la transaction

Octet 1	B8 : authentification non réalisée
	B7 : authentification statique échouée
	B6 : données absentes
	B5 : présence en liste noire
	B4 : authentification dynamique échouée
	B3 : authentification DDA/AC échouée
	B2 : SDA sélectionné
	B1 : Ruf

Octet 2	B8 : nos version application différents
	B7 : application périmée
	B6 : application non encore valide
	B5 : service non offert
	B4 : nouvelle carte
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 3	B8 : échec de la Vérification du porteur
	B7 : CVM non reconnue
	B6 : nombre limite d'essais de code atteint
	B5 : pin-pad absent ou hors-service
	B4 : code non saisi
	B3 : contrôle on-line du code
	B2 : Ruf
	B1 : Ruf

Octet 4	B8 : cumul porteur dépassé
	B7 : limite inférieure de tr. off-line dépassée
	B6 : limite supérieure de tr. off-line dépassée
	B5 : transaction sélectionnée aléatoirement
	B4 : transaction forcée online par commerçant
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

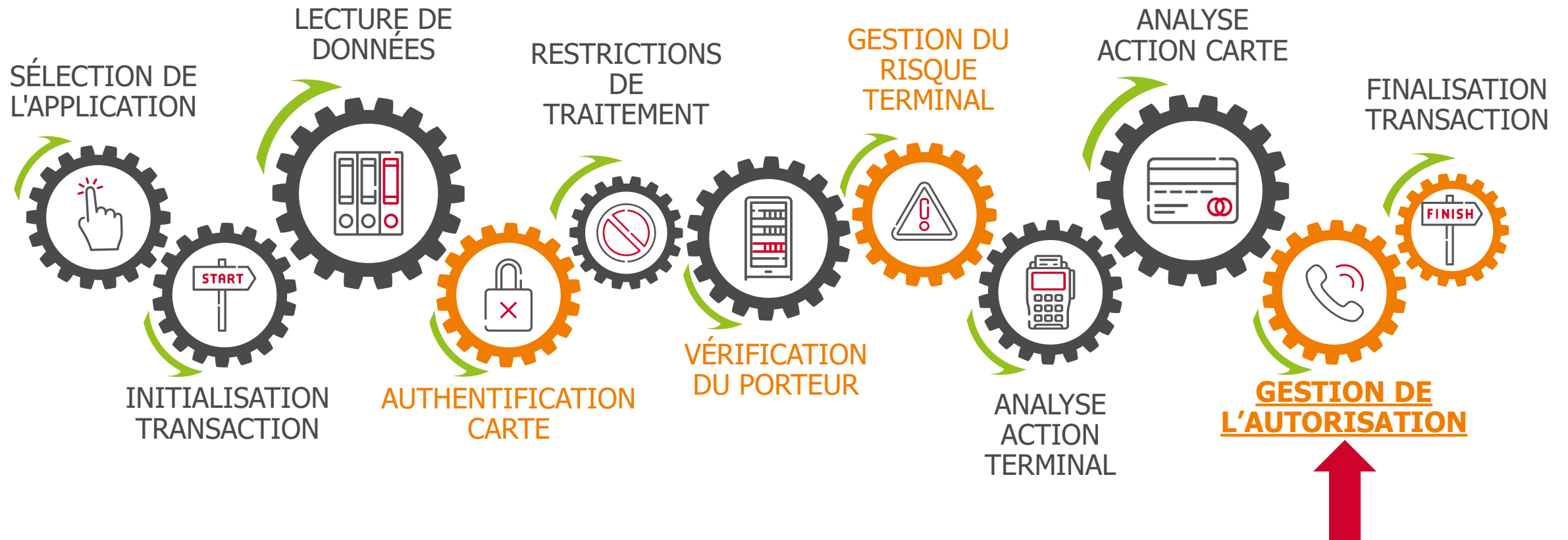
Octet 5	B8 : TDOL par défaut utilisée
	B7 : Authentification émetteur échouée
	B6 : Echec script avant 2ème Generate AC
	B5 : Echec script après 2ème Generate AC
	B4 : Réserve au contactless
	B3 : Réserve au contactless
	B2 : Réserve au contactless
	B1 : Réserve au contactless

Analyse action carte

Prise en compte de la CDA par le terminal

Demande du terminal	Réponse carte	Traitement CDA	Conclusion CDA
GENERATE AC (AAC)	→ AAC	pas de contrôle	→ transaction refusée
GENERATE AC (ARQC)	→ ARQC	contrôle CDA → OK	→ CDA OK
		contrôle CDA → NOK	→ transaction refusée
	→ AAC	pas de contrôle	→ transaction refusée
GENERATE AC (TC)	→ TC	contrôle CDA → OK	→ CDA OK
		contrôle CDA → NOK	→ transaction refusée
	→ ARQC	contrôle CDA → OK	→ CDA OK
		contrôle CDA → NOK	→ transaction refusée
	→ AAC	pas de contrôle	→ transaction refusée

Synoptique du déroulement de la transaction

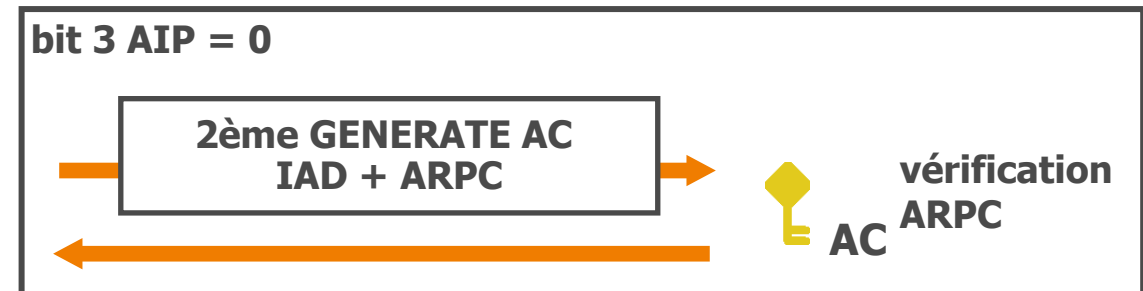
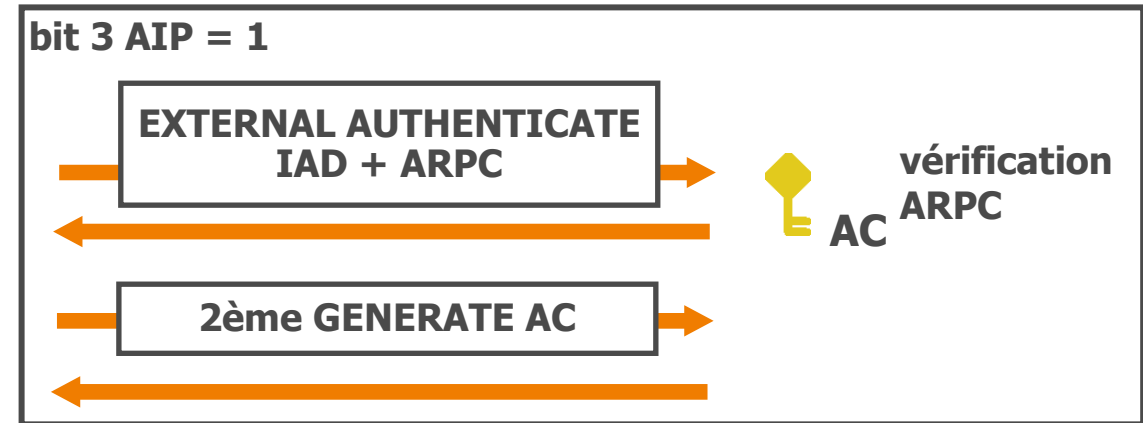
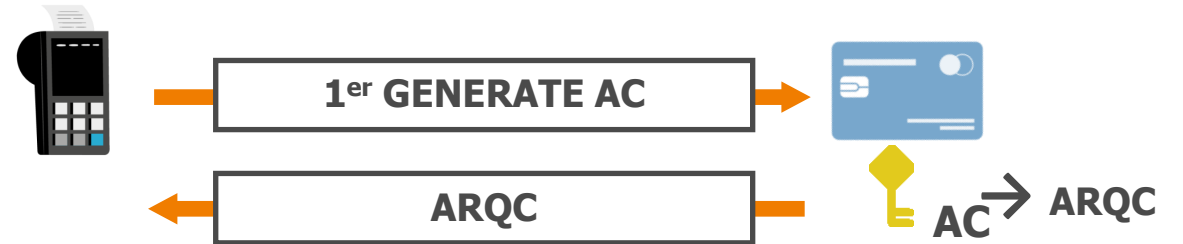
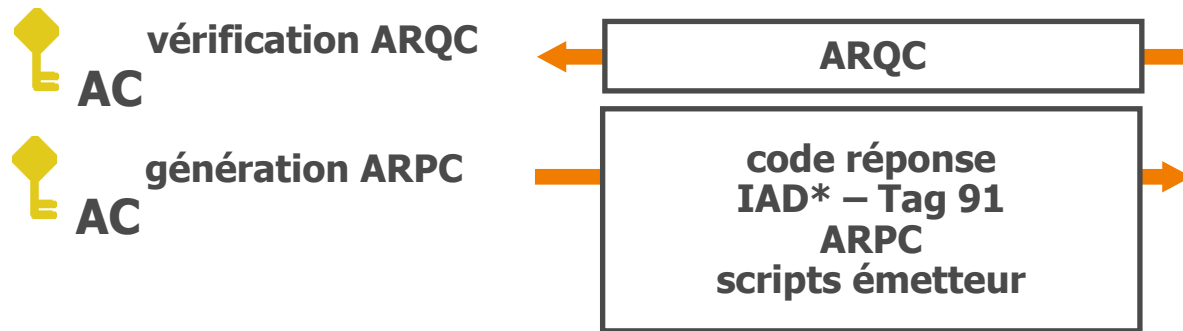


Gestion de l'autorisation

Cinématique



protocole hors spec EMV



*Issuer Authentication Data

Gestion de l'autorisation

Authentification émetteur

— Mise à jour de l'octet 5 de la TVR si nécessaire

Octet 1	B8 : authentification non réalisée
	B7 : authentification statique échouée
	B6 : données absentes
	B5 : présence en liste noire
	B4 : authentification dynamique échouée
	B3 : authentification DDA/AC échouée
	B2 : SDA sélectionné
	B1 : Ruf

Octet 2	B8 : nos version application différents
	B7 : application périmée
	B6 : application non encore valide
	B5 : service non offert
	B4 : nouvelle carte
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 3	B8 : échec de la Vérification du porteur
	B7 : CVM non reconnue
	B6 : nombre limite d'essais de code atteint
	B5 : pin-pad absent ou hors-service
	B4 : code non saisi
	B3 : contrôle on-line du code
	B2 : Ruf
	B1 : Ruf

Octet 4	B8 : cumul porteur dépassé
	B7 : limite inférieure de tr. off-line dépassée
	B6 : limite supérieure de tr. off-line dépassée
	B5 : transaction sélectionnée aléatoirement
	B4 : transaction forcée online par commerçant
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 5	B8 : TDOL par défaut utilisée
	B7 : Authentification émetteur échouée
	B6 : Echec script avant 2ème Generate AC
	B5 : Echec script après 2ème Generate AC
	B4 : Réservé au contactless
	B3 : Réservé au contactless
	B2 : Réservé au contactless
	B1 : Réservé au contactless

Gestion de l'autorisation

Traitement des scripts

- Le terminal n'est qu'un **messenger** : pas d'analyse des commandes
- Les scripts sont transmis à la carte
 - └ Avant le 2^{ème} GENERATE AC (scripts critiques)
 - └ Après le 2^{ème} GENERATE AC (scripts non critiques)
- Secure messaging
 - └ **Authentification** de l'émetteur + **intégrité** du message
 - └ **Confidentialité** (transport du PIN)
 - └ **3DES** ou **AES**

APPLICATION BLOCK
APPLICATION UNBLOCK
CARD BLOCK
PIN CHANGE/UNBLOCK



Gestion de l'autorisation

Scripting

Octet 1	B8 : authentification non réalisée
	B7 : authentification statique échouée
	B6 : données absentes
	B5 : présence en liste noire
	B4 : authentification dynamique échouée
	B3 : authentification DDA/AC échouée
	B2 : SDA sélectionné
	B1 : Ruf

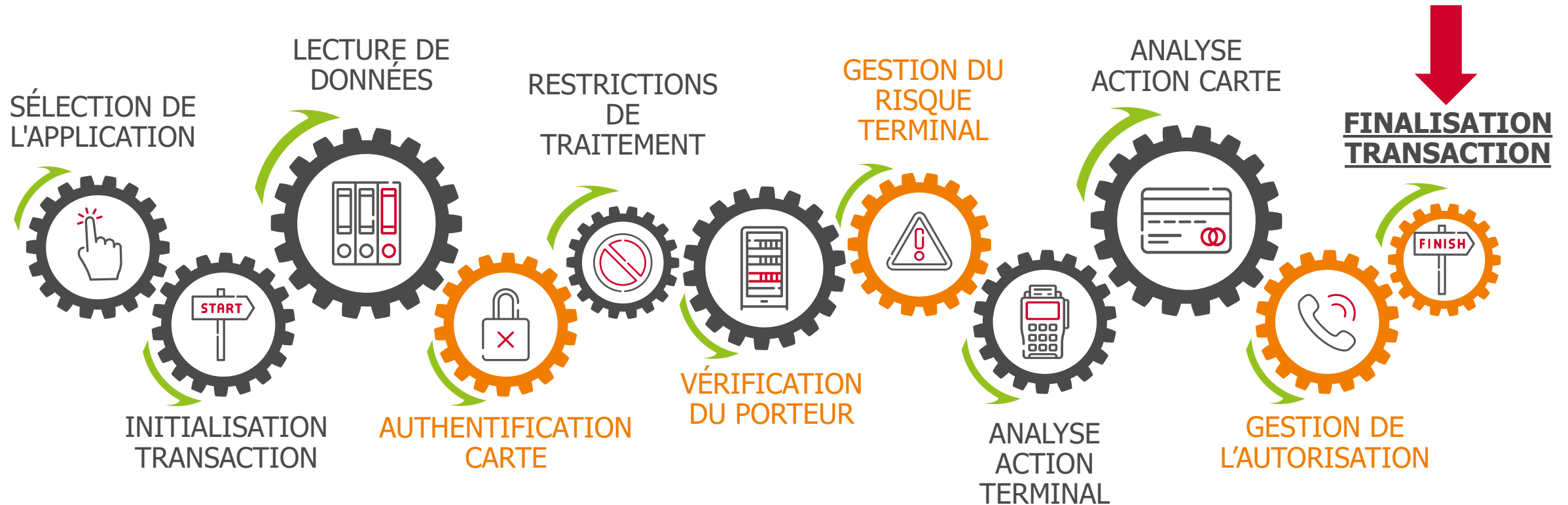
Octet 2	B8 : nos version application différents
	B7 : application périmée
	B6 : application non encore valide
	B5 : service non offert
	B4 : nouvelle carte
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 3	B8 : échec de la Vérification du porteur
	B7 : CVM non reconnue
	B6 : nombre limite d'essais de code atteint
	B5 : pin-pad absent ou hors-service
	B4 : code non saisi
	B3 : contrôle on-line du code
	B2 : Ruf
	B1 : Ruf

Octet 4	B8 : cumul porteur dépassé
	B7 : limite inférieure de tr. off-line dépassée
	B6 : limite supérieure de tr. off-line dépassée
	B5 : transaction sélectionnée aléatoirement
	B4 : transaction forcée online par commerçant
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 5	B8 : TDOL par défaut utilisée
	B7 : Authentification émetteur échouée
	B6 : Echec script avant 2ème Generate AC
	B5 : Echec script après 2ème Generate AC
	B4 : Réserve au contactless
	B3 : Réserve au contactless
	B2 : Réserve au contactless
	B1 : Réserve au contactless

Synoptique du déroulement de la transaction



Finalisation transaction

- La carte a rendu un cryptogramme **TC** hors Combined DDA/AC
 - └ La transaction est acceptée

- La carte a rendu un cryptogramme **TC** avec **Combined DDA/AC**
 - └ La transaction est acceptée si la signature est correcte, sinon la transaction est refusée

- La carte a rendu un cryptogramme **AAC**
 - └ La transaction est refusée

Autres traitements EMV (options)

- **Forçage** de la transaction **on-line** par le commerçant
 - └ Sur une touche du terminal, le bit 4 de l'octet 4 de la TVR est mis à jour

Transaction forcée on-line

- Gestion d'une liste « noire »
 - └ Si la carte est présente, le bit 5 de l'octet 1 de la TVR est mis à jour

Présence en liste noire

- **Forçage** de la transaction par le commerçant
 - └ Sur réponse carte avec cryptogramme AAC, acceptation de la transaction

Autres traitements EMV (options)

Mise à jour des octets 1 et 4 de la TVR si nécessaire

Octet 1	B8 : authentification non réalisée
	B7 : authentification statique échouée
	B6 : données absentes
	B5 : présence en liste noire
	B4 : authentification dynamique échouée
	B3 : authentification DDA/AC échouée
	B2 : SDA sélectionné
	B1 : Ruf

Octet 2	B8 : nos version application différents
	B7 : application périmée
	B6 : application non encore valide
	B5 : service non offert
	B4 : nouvelle carte
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 3	B8 : échec de la Vérification du porteur
	B7 : CVM non reconnue
	B6 : nombre limite d'essais de code atteint
	B5 : pin-pad absent ou hors-service
	B4 : code non saisi
	B3 : contrôle on-line du code
	B2 : Ruf
	B1 : Ruf

Octet 4	B8 : cumul porteur dépassé
	B7 : limite inférieure de tr. off-line dépassée
	B6 : limite supérieure de tr. off-line dépassée
	B5 : transaction sélectionnée aléatoirement
	B4 : transaction forcée online par commerçant
	B3 : Ruf
	B2 : Ruf
	B1 : Ruf

Octet 5	B8 : TDOL par défaut utilisée
	B7 : Authentification émetteur échouée
	B6 : Echec script avant 2ème Generate AC
	B5 : Echec script après 2ème Generate AC
	B4 : Réserve au contactless
	B3 : Réserve au contactless
	B2 : Réserve au contactless
	B1 : Réserve au contactless

Autres traitements EMV (options)

Historisation des transactions

- **Log Entry** : identification du fichier et nombre d'enregistrements
 - └ Le SFI sur 1 octet pour l'identification du fichier contenant les transactions
 - └ Le nombre d'enregistrements sur 1 octet du fichier contenant les transactions
 - └ Donnée rendue sur la commande SELECT (AID) dans le FCI propriétaire, tag'9F4D'

- **Log Data** : la structure d'un enregistrement d'un fichier
 - └ Les tags/longueurs des données enregistrées dans le fichier
 - └ Donnée rendue sur la commande GET DATA (tag'9F4F')

- Les enregistrements sont lus avec la commande READ RECORD

Récapitulatif

