

Acceptation EMV en France

PARTIE 4 ACCEPTATION EMV EN FRANCE

JUIN 2021

Passion for payments



DISCOVER

JCB



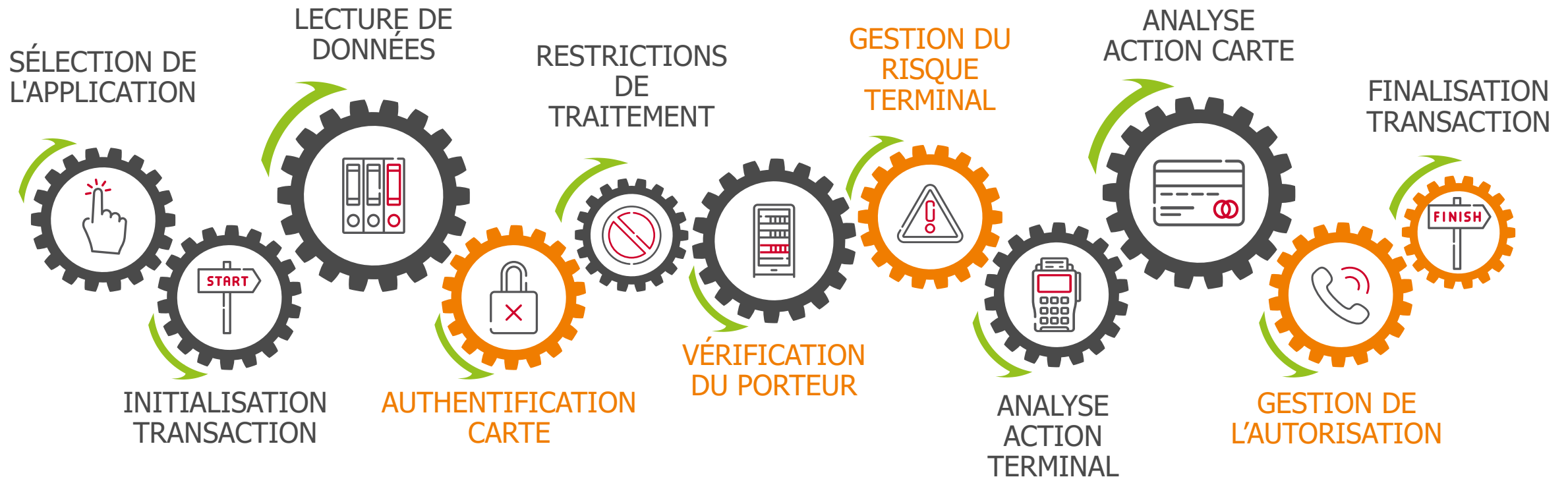
UnionPay

中国银联
China UnionPay

VISA



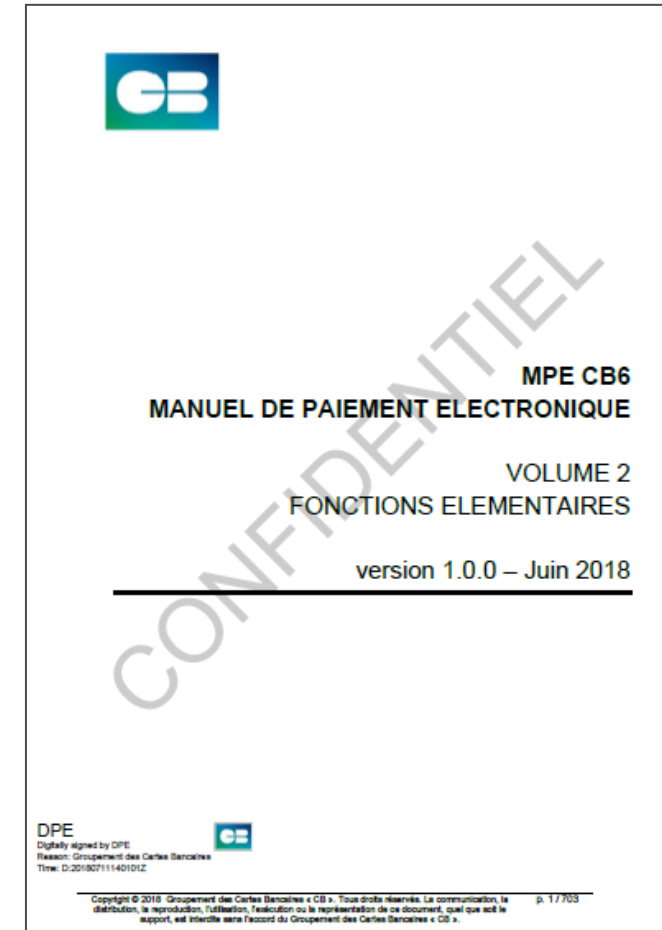
Synoptique du déroulement de la transaction



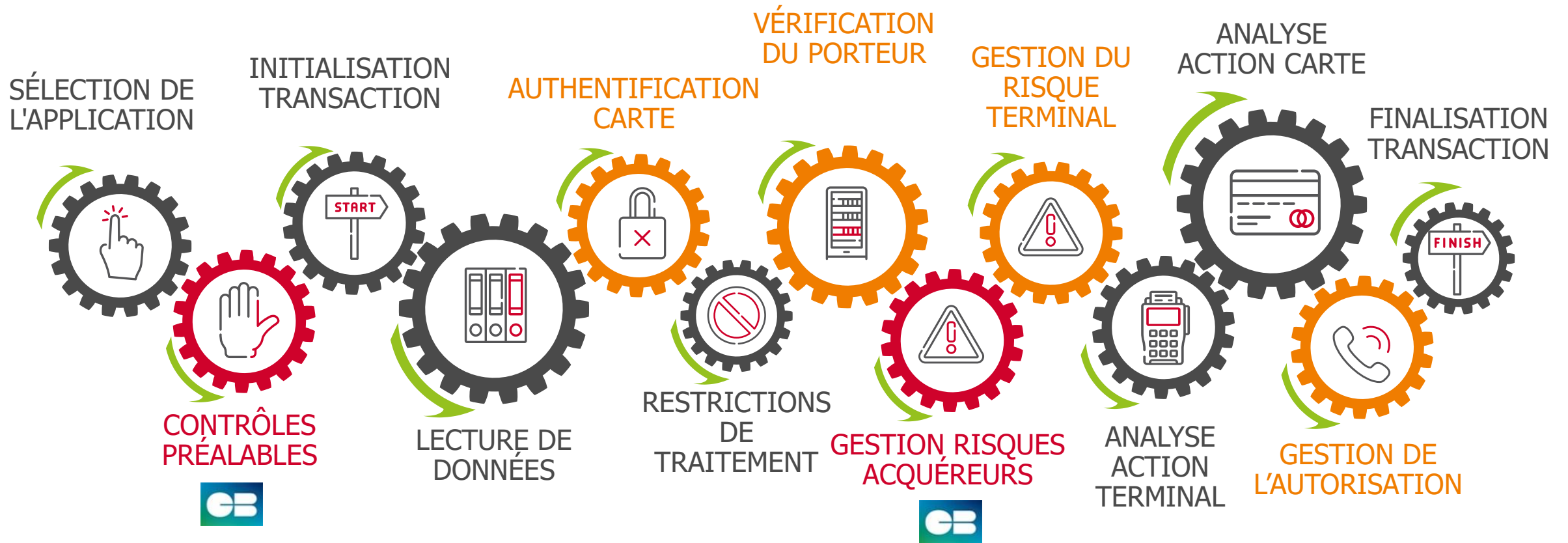
Spécificités d'une transaction CB

Les spécifications

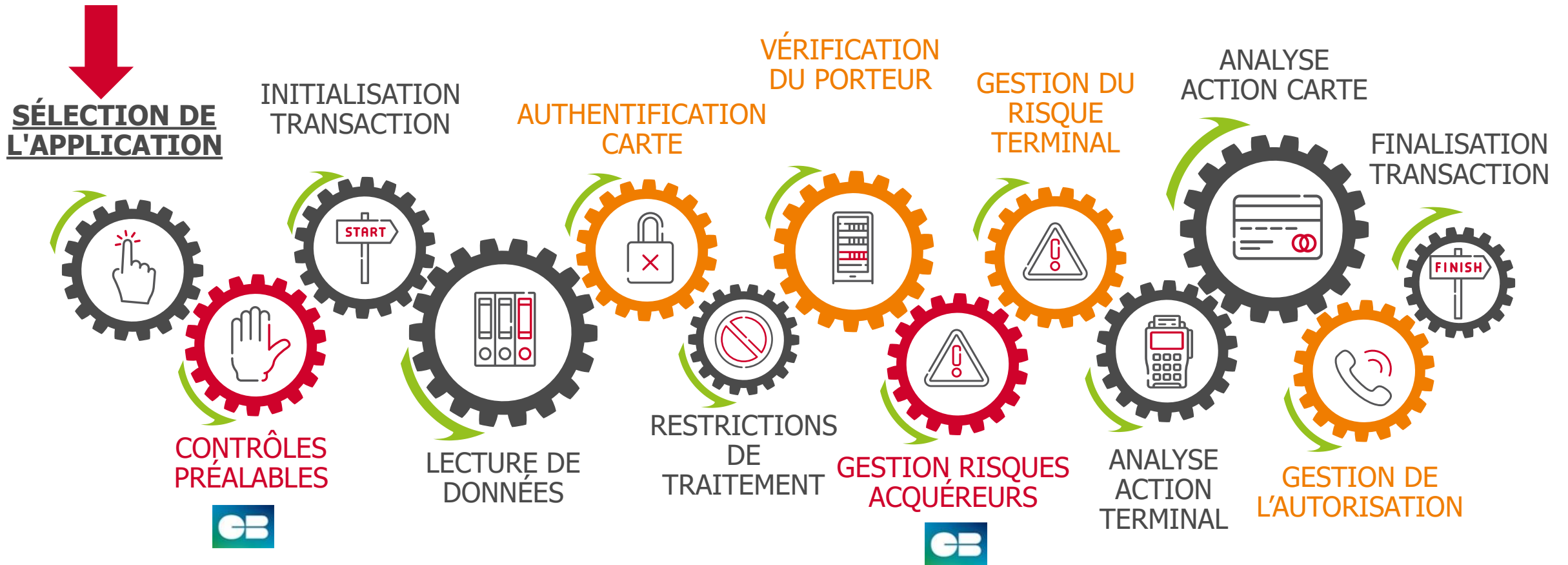
- Manuel de paiement électronique **MPE CB6**
- Intégration du sans contact
- Evolution majeure : **PIN Online**
 - Pour les débits effectués avec une carte EMV contact, un dispositif sans contact, ou une carte à piste magnétique iso2.



Spécificités d'une transaction CB : synoptique



Spécificités d'une transaction CB : synoptique



Sélection de l'application

Choix de la technologie piste ou puce

- **Le traitement puce et prioritaire**
- **Le traitement piste sera accepte dans les conditions suivantes:**
 - └ La table des BIN impose le traitement piste pour le porteur
 - └ Le repli piste n'est plus supporté suite à un incident puce
- **Échec de la connexion puce :**
 - └ Le terminal positionne un incident puce

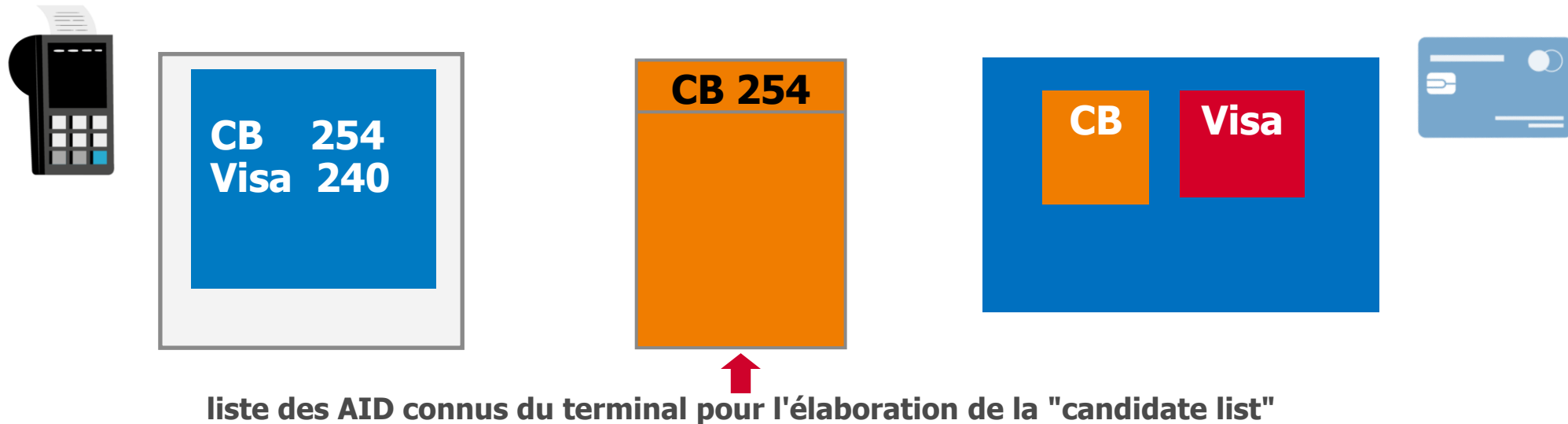
Sélection de l'application

Choix de l'application carte : l'historique

— Principes EMV avec spécificité suivante pour l'élaboration de la "candidate list"

- Priorité des AID CB : si le logiciel CB EMV reconnaît dans la carte un AID avec une priorité terminal égale à 254 ou 255, seul cet AID sera proposé pour être dans la liste des AID connus du terminal
→ N'est plus obligatoire depuis fin 2007

— Tous les AID de la "candidate list" sont proposés au porteur



Sélection de l'application

Choix de l'application carte : choix du porteur

- **Spécification CB6**

- **En début de transaction :**

- └ Option 1

- Tous les AID de la "candidate list" sont proposés au porteur

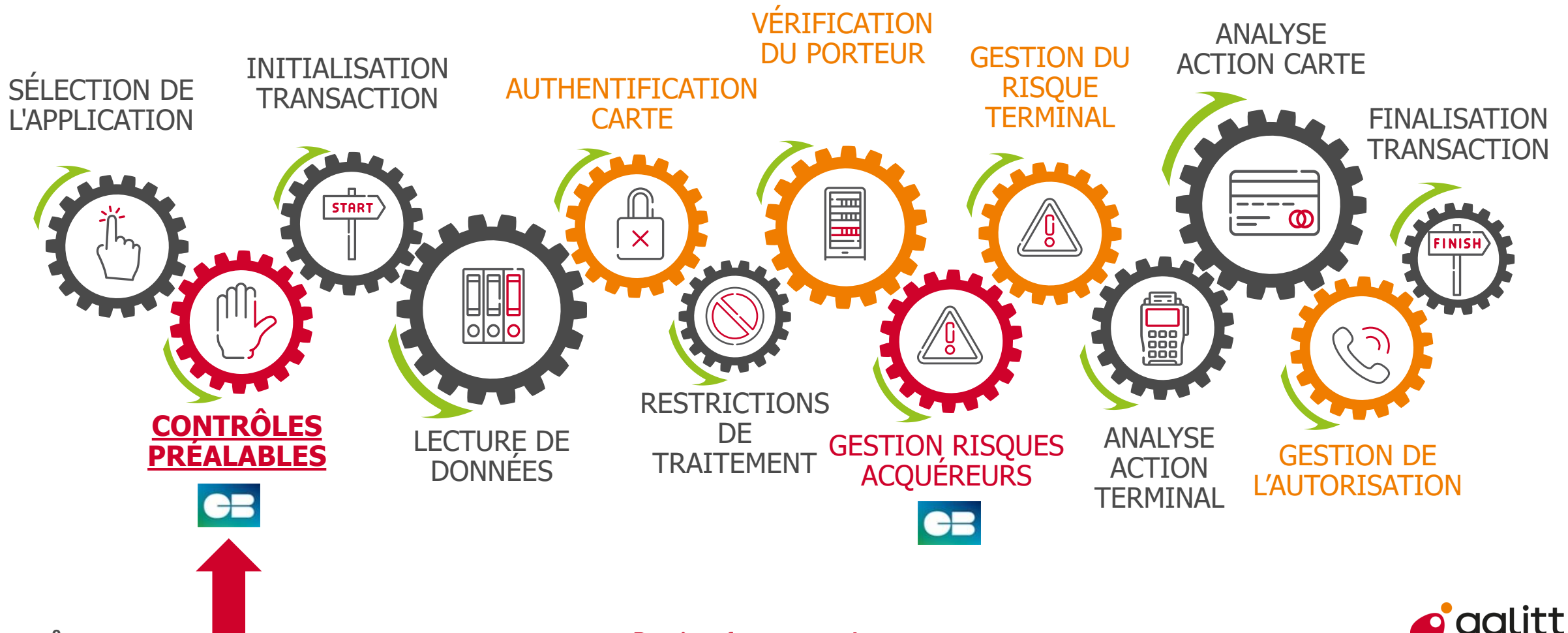
- Affichage de l'**Application Preferred Name** (sinon **Application Label**) selon l'ordre de priorité carte (**API**)

- └ Option 2

- Possibilité pour le commerçant de rendre un **schéma de paiement prioritaire** (article 8 "Cobadging et sélection d'application" de la réglementation européenne).

- Ce **choix du commerçant peut être invalidé par le porteur** qui peut à partir de l'écran de validation du code confidentiel demander par touche de fonction à choisir une nouvelle application carte (**touche correction** "jaune").

Spécificités d'une transaction CB : synoptique



Contrôles préalables

— Contrôles au contexte de la transaction : les contrôles négatifs conduisent à l'abandon de la transaction

- └ Type de transaction
- └ Devise de la transaction : bit 4 octet 4 TVR
- └ Montant compris entre un minimum et un maximum
- └ Montant de double authentification

Transaction forcée online

Signature du porteur requise

— Sélections supplémentaires

- └ Code langue par le porteur si plusieurs codes langues gérés par le terminal
- └ Différé de recouvrement par le commerçant si service ouvert

→ **Données spécifiques acquéreur pour l'application**

Contrôles préalables

Mise à jour de l'octet 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 : Échec script avant 2ème Generate AC
B5 : Échec script après 2ème Generate AC
B4 : Réserve au contactless
B3 : Réserve au contactless
B2 : Réserve au contactless
B1 : Réserve au contactless

Spécificités d'une transaction CB : synoptique



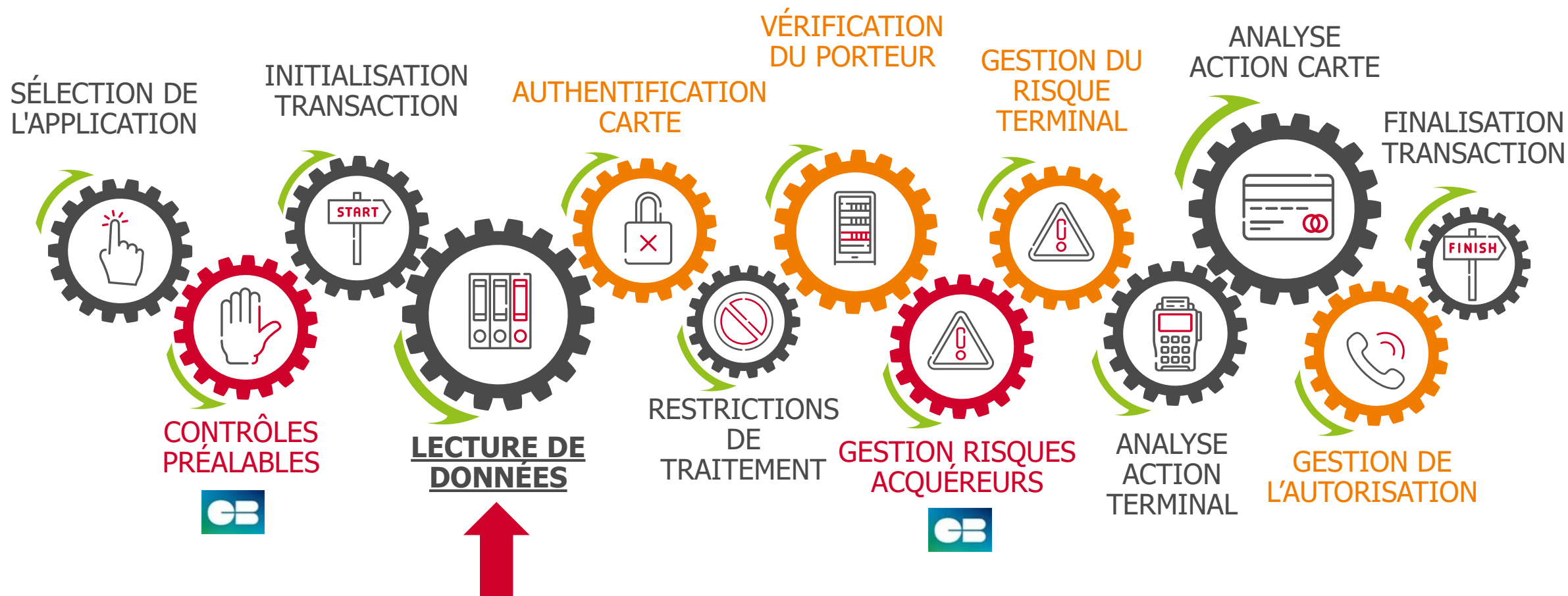
Initialisation transaction

— Initialisation transaction avec l'application carte sélectionnée



└─ Aucune spécificité CB

Spécificités d'une transaction CB : synoptique

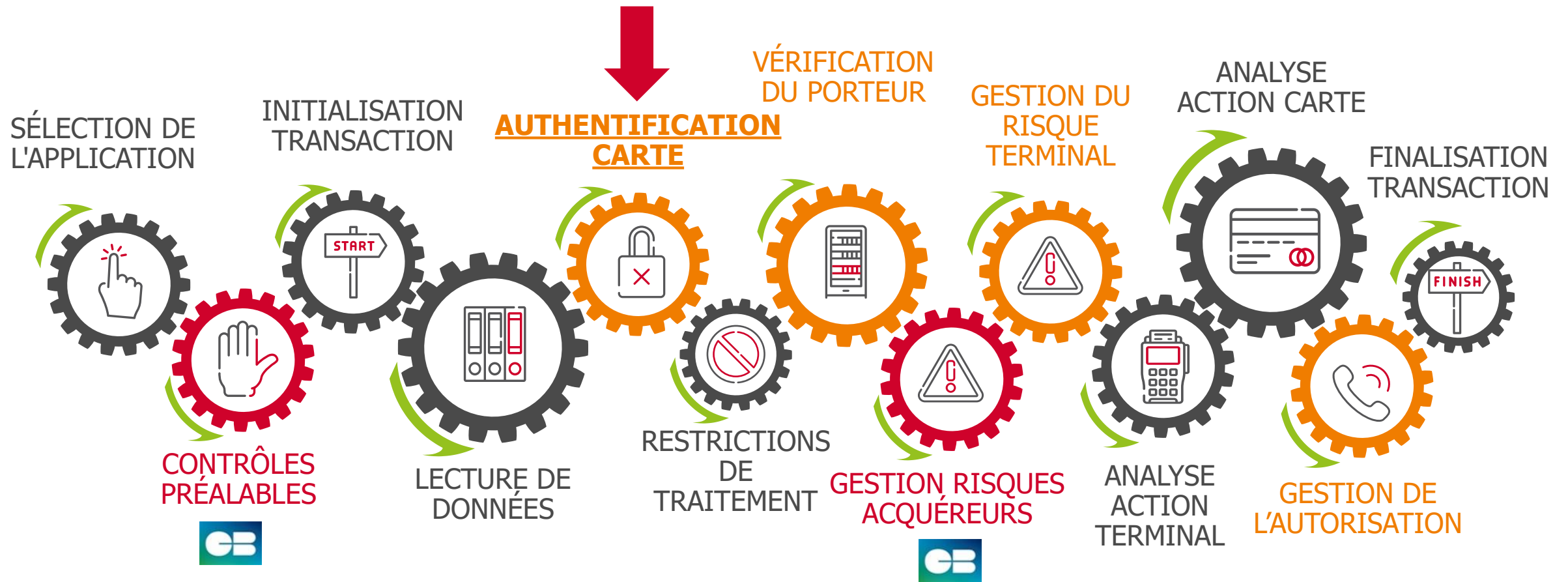


Lecture des données

— Lecture des données de l'application carte

- └ Aucune spécificité CB

Spécificités d'une transaction CB : synoptique

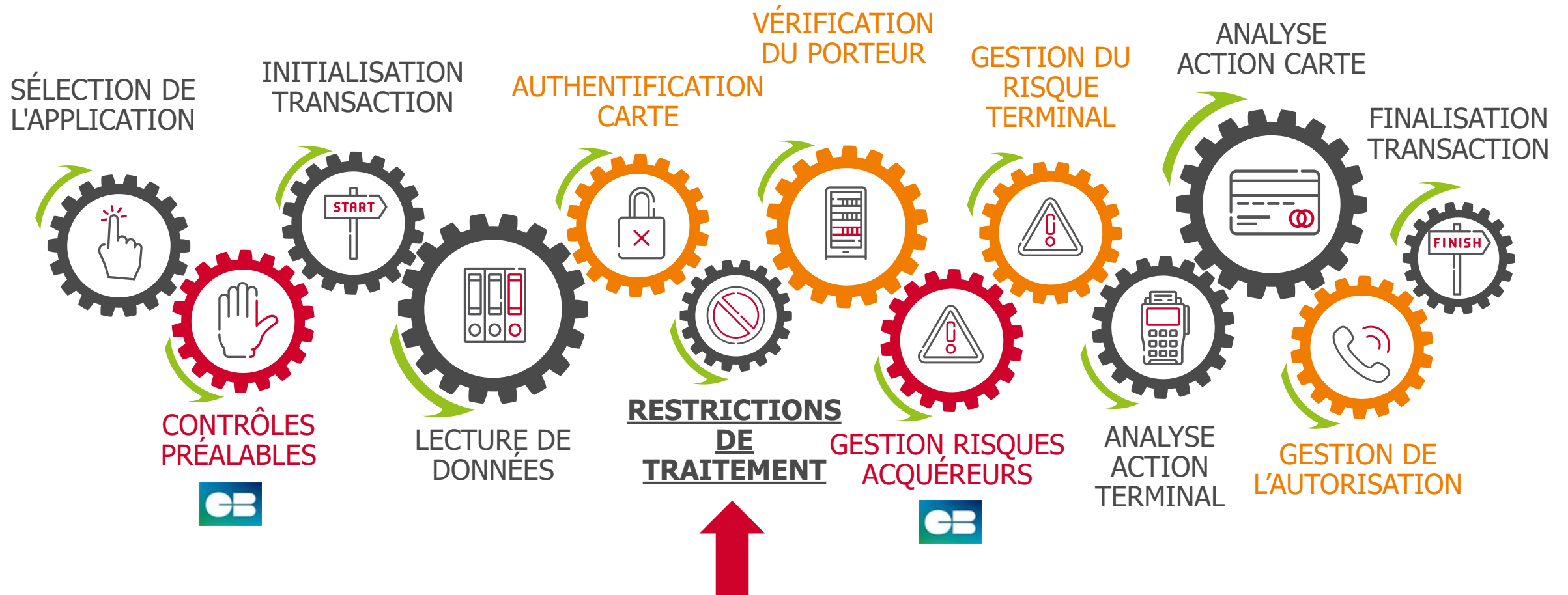


Authentification carte

Authentification carte

- **Obligation** pour le terminal de supporter les méthodes d'authentification **statique et dynamique**
- Réalisée en fonction de l'AIP de la carte
- Aucune autre spécificité CB

Spécificités d'une transaction CB : synoptique



Restrictions de traitement

- **Cashback** autorisé (montant max 60€)
- AUC non pris en compte

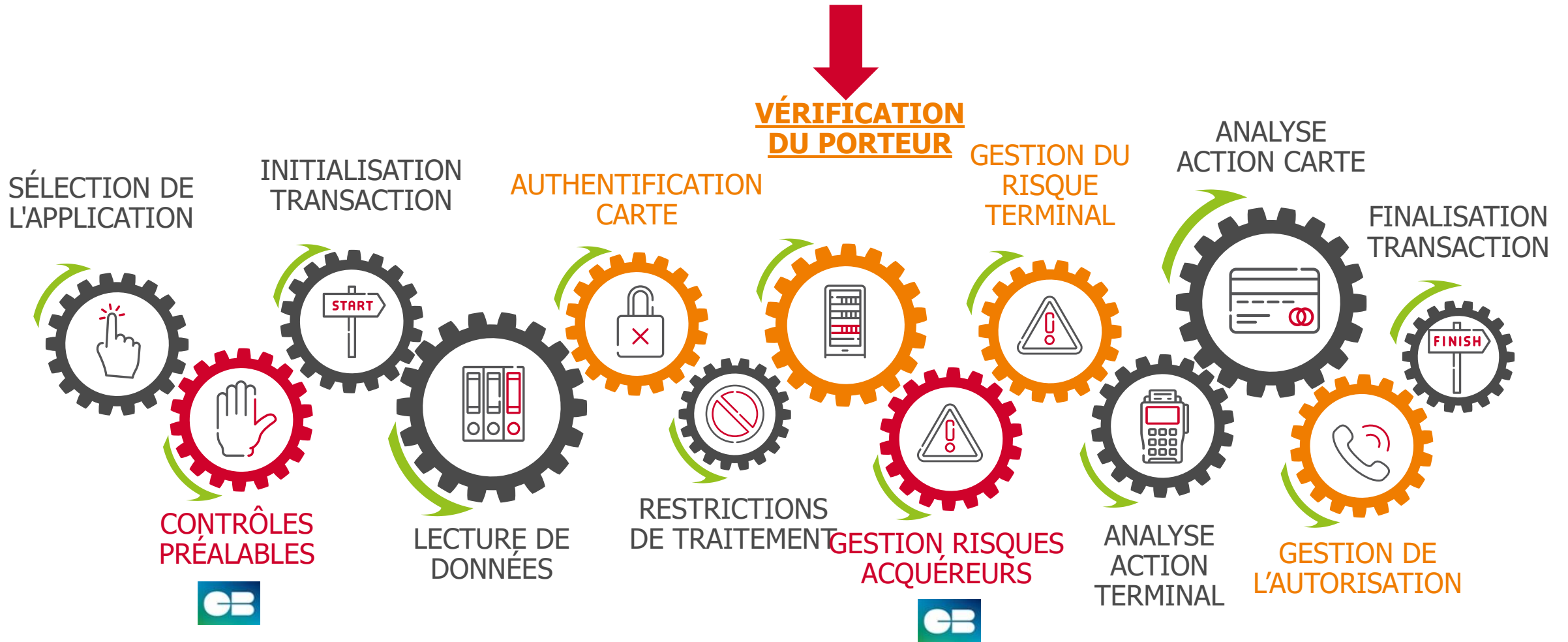
Application Usage Control Byte 1 (Leftmost)

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

Spécificités d'une transaction CB : synoptique



Vérification du porteur

Généralités

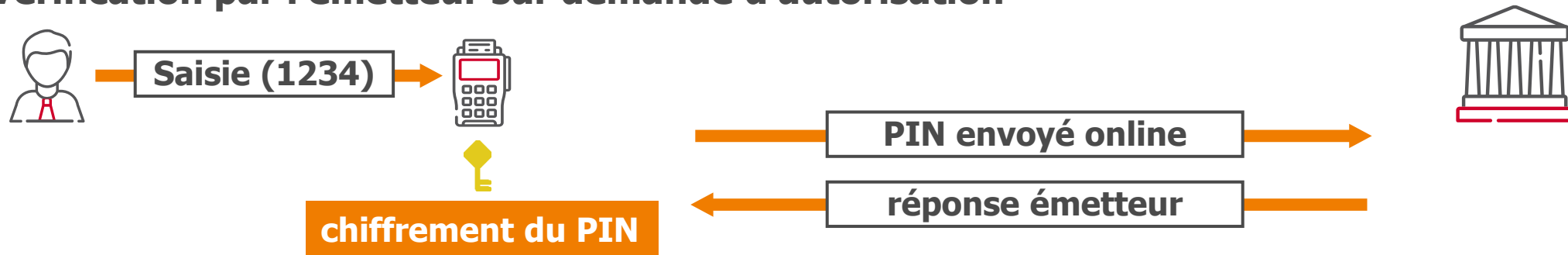
- **Abandon de la transaction si annulation porteur pendant la saisie du code**
- **Méthode de vérification du porteur par défaut**
 - └ Carte agréée CB : aucune méthode réalisée
 - Demande de signature du porteur
 - └ Carte CB : conforme à EMV
- **Support de la méthode "code chiffré on-line" (nouveau CB6)**



Vérification du porteur

PIN online (CB6) : généralités

- Chiffrement du PIN par le terminal
- Vérification par l'émetteur sur demande d'autorisation



— Les enjeux

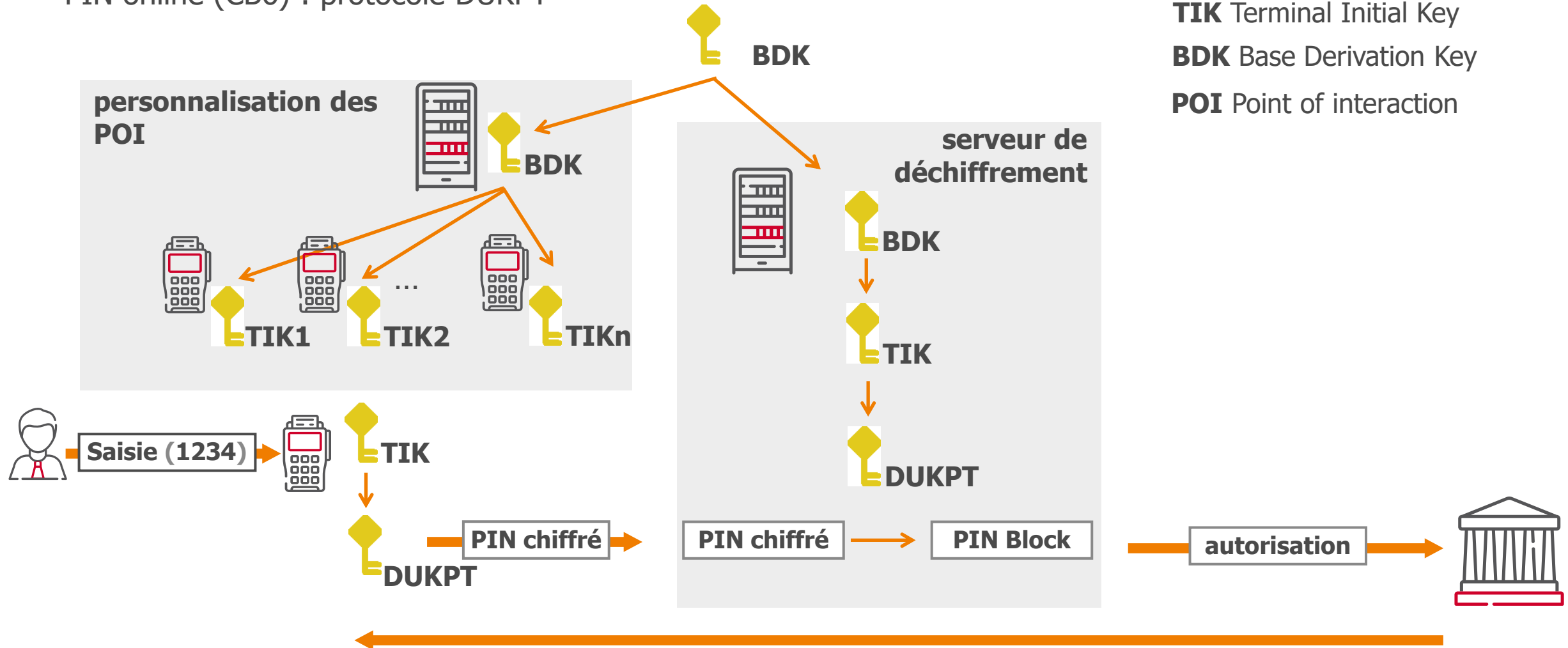
- Le chiffrement du PIN par le terminal
- L'injection de la clé de chiffrement dans le terminal

→ Protocole **DUKPT***
Serveur de **déchiffrement**

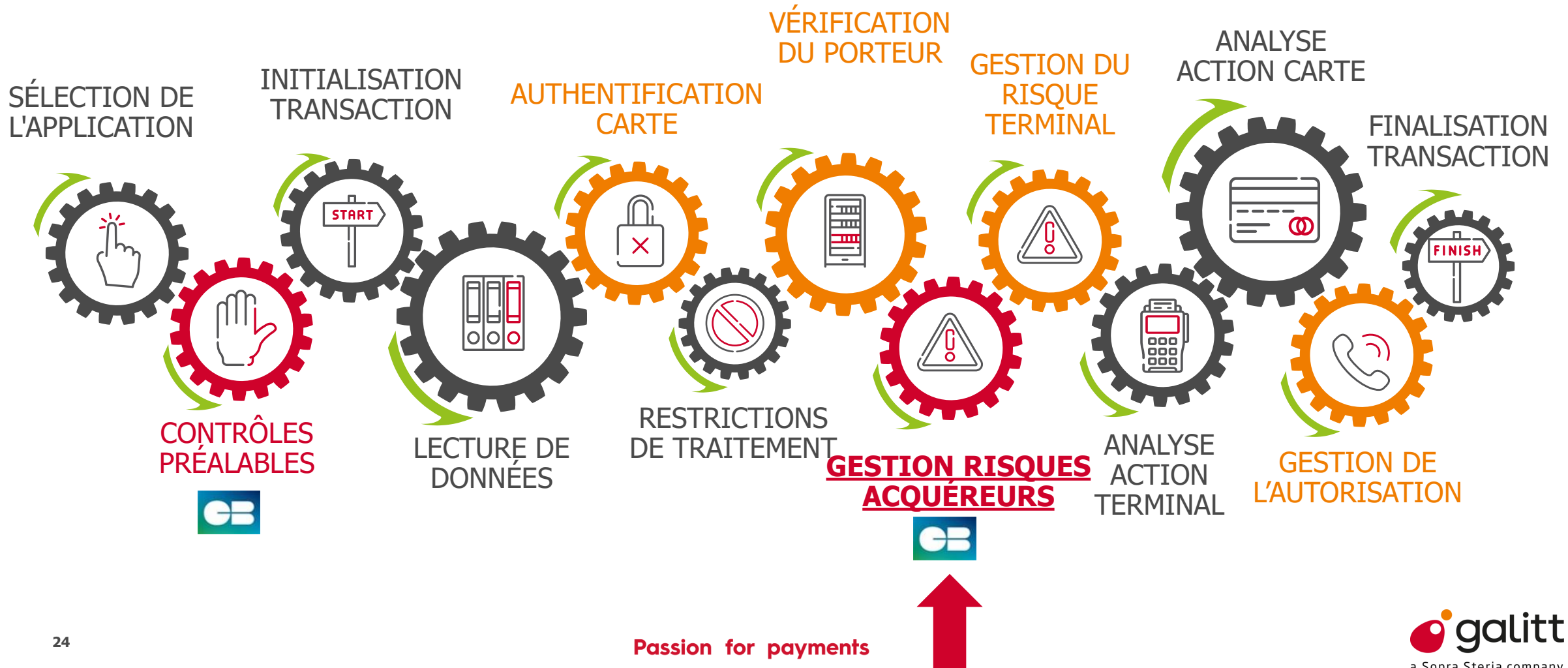
*Derived Unique Key Per Transaction

Vérification du porteur

PIN online (CB6) : protocole DUKPT



Spécificités d'une transaction CB : synoptique



Gestion du risque acquéreur

— Contrôle de la présence de la carte dans une liste de bins

- └ Absence : bit 4 octet 4 TVR
- └ Présence : contrôle du niveau d'acceptation
 - Surveillé : bit 4 octet 4 TVR
 - Refusé ou interdit : bit 5 octet 1 TVR

Transaction forcée on-line

Transaction forcée on-line

Présence en liste noire

— Contrôle de la présence de la carte dans une liste de contrôle

- └ Surveillé : bit 4 octet 4 TVR
- └ Refusé ou interdit : bit 5 octet 1 TVR

Transaction forcée on-line

Présence en liste noire

Gestion du risque acquéreur

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

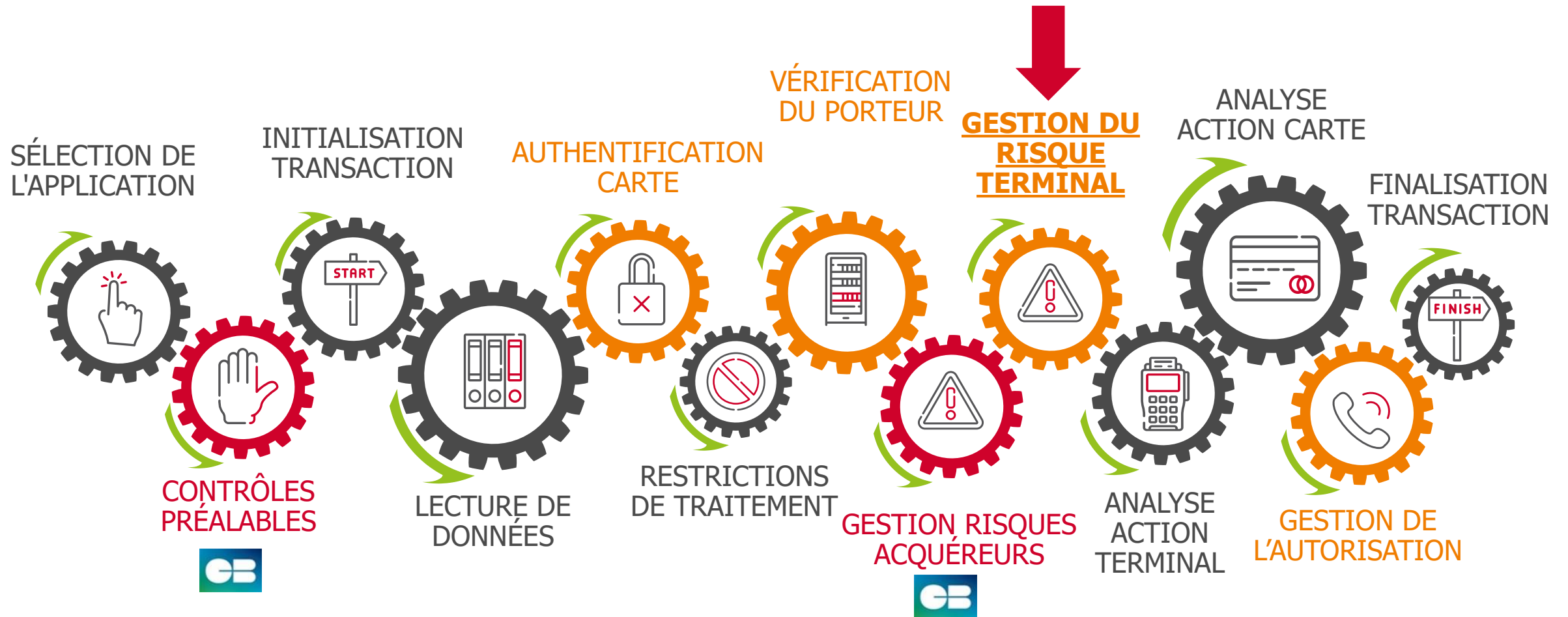
Octet 4

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 : Échec script avant 2ème Generate AC
B5 : Échec script après 2ème Generate AC
B4 : Réservé au contactless
B3 : Réservé au contactless
B2 : Réservé au contactless
B1 : Réservé au contactless

Spécificités d'une transaction CB : synoptique



Gestion du risque terminal

- **Cumul porteur (« floor limit ») réalisé sans condition de valeur AIP sur toutes les transactions financières du fichier**
- **Appel aléatoire réalisé sans condition de valeur AIP**
- **Ajout du traitement « suspicion commerçant » : en option**
 - Mise à jour bit 4 octet 4 TVR

transaction forcée on-line

Gestion du risque terminal

Mise à jour de l'octet 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

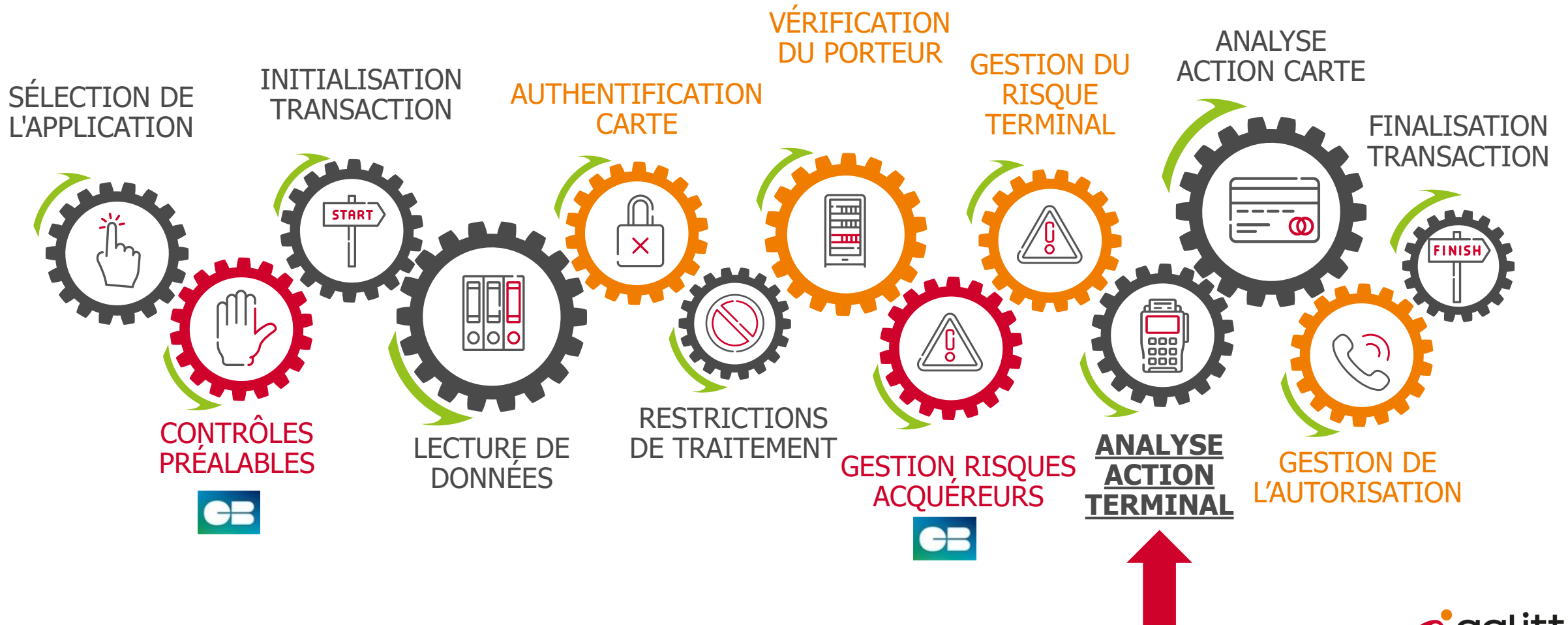
Octet 4

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 : Échec script avant 2ème Generate AC
B5 : Échec script après 2ème Generate AC
B4 : Réservé au contactless
B3 : Réservé au contactless
B2 : Réservé au contactless
B1 : Réservé au contactless

Spécificités d'une transaction CB : synoptique



Analyse action terminal

Spécificité CB : analyse action terminal ARQC

- **Chaque application terminal dispose d'un déclenchement automatique ou manuel et d'une possibilité de forçage**
- **Chaque AID dispose d'une autorisation ou interdiction de forçage**
- **Si l'appel n'est pas validé et autorisation de forçage, la transaction est forcée**
 - └ Sur double validation du commerçant (clé ou carte commerçant)
 - └ Avec demande de cryptogramme AAC et non ARQC
 - └ La transaction est enregistrée en tant que aboutie, le ticket de paiement édité

→ **Forçage non autorisé pour les « réponses positives obligatoires » (RPO)**

Exemple de RPO

*BIN inconnu
CDA/DDA échouée*

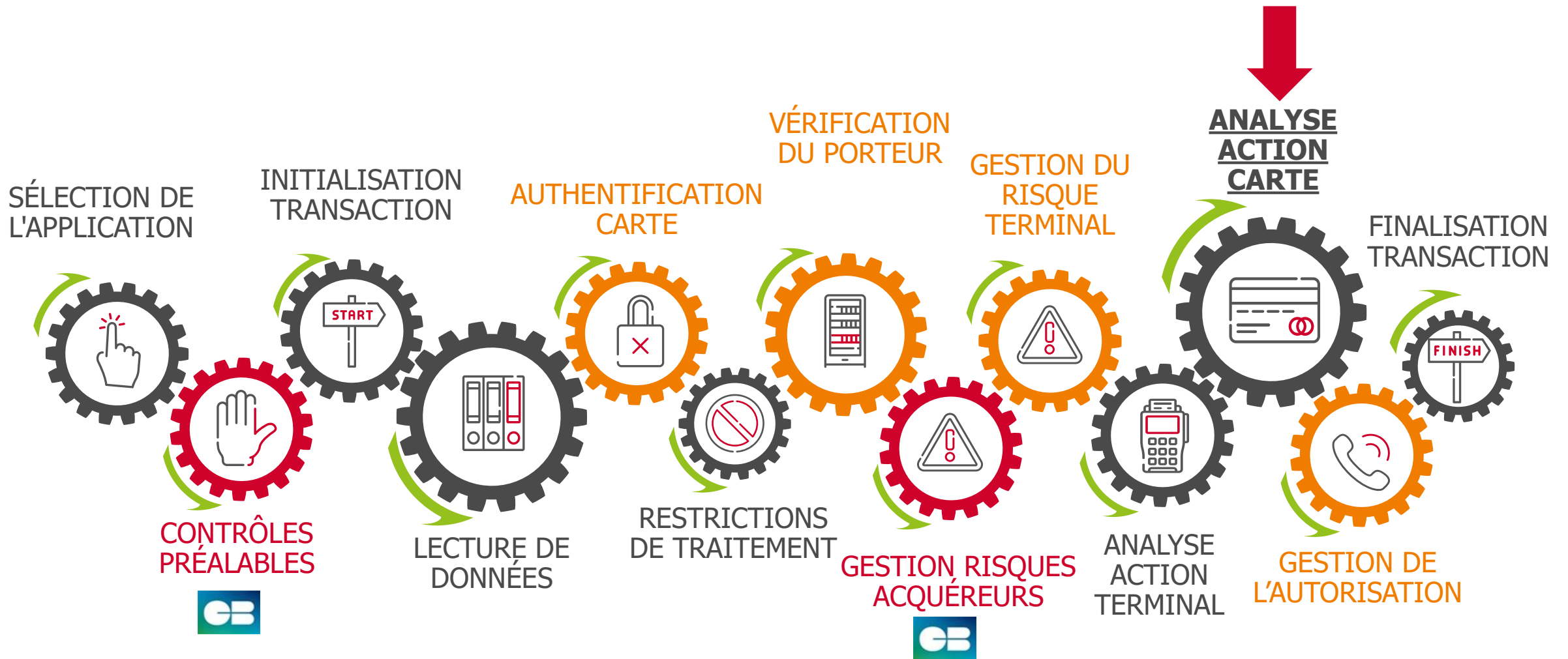
...

Pas de RPO pour

*Cumul porteur dépassé
Appel aléatoire*

...

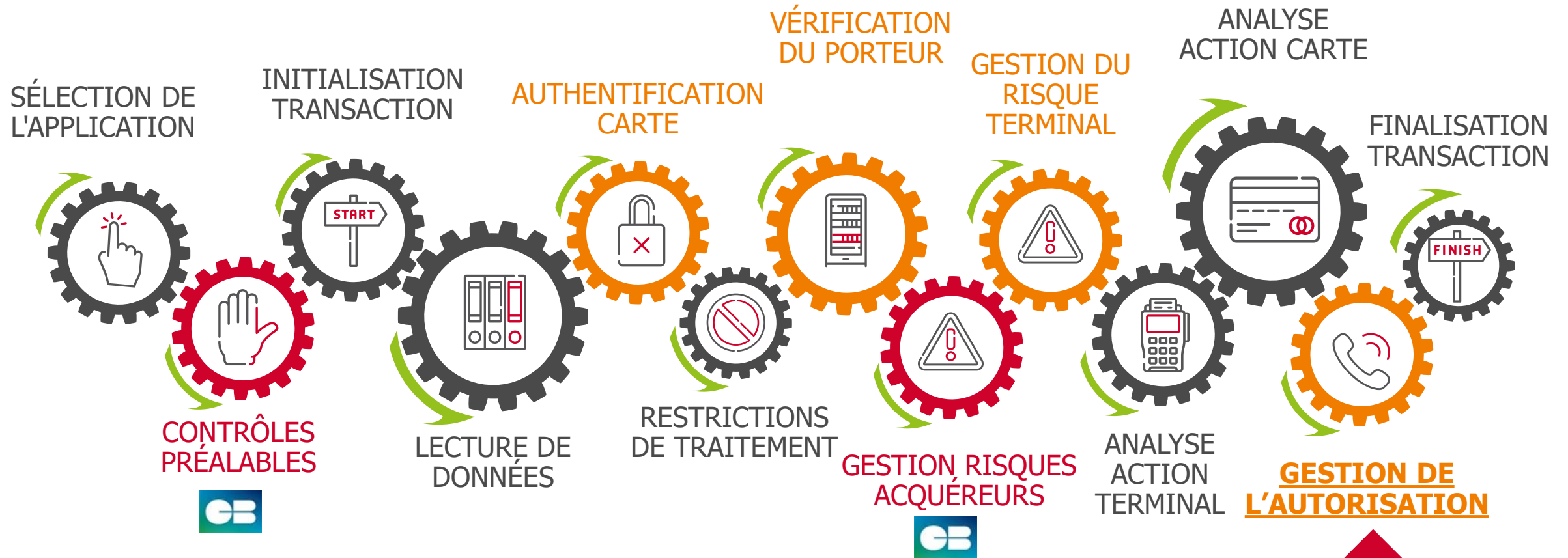
Spécificités d'une transaction CB : synoptique



Analyse action carte

— Aucune spécificité CB

Spécificités d'une transaction CB : synoptique



Gestion de l'autorisation

- **Le terminal envoie un message pour l'émetteur selon le protocole CB2A**
 - └ Raison d'appel avec ou sans « réponse positive obligatoire »
 - └ Information émetteur



Gestion de l'autorisation

Structure du message 0100 : demande d'autorisation

2 : n° porteur	3 : code traitement	4 : montant	11 : no transaction	12 : heure	13 : date	18 : MCC
22 : mode lecture	23 : pan seq. nb	25 : conditions	32 : code, bin banque	41 : env. 41	42 : env. 42	
47 08 : type site	96 : SIRET	97 : IDPA	A0 : IDSA	49 : code monnaie	53: informations sécurité	
55 57 : track2	82 : AIP	95 : TVR	9C : type tr.	5F24 : date fin	9F06: AID	9F10 : IAD
	9F26 : crypto.					
55 9F27 : CID	9F33 : terminal cap.	9F36 : ATC	9F37 : aléa	DF80 : résultats puce	DF81 : type puce	
59 0101 : code raison	0102: année	0200 : ERT	0201 : ITP	0202: n° contrat	0203 : NLSA	0204 : NLPA

59 0205 : code pays	0207 : montant cumulé	020B : TASA
------------------------	-----------------------	-------------

Légende couleurs :

Carte

Système Acceptation

Transaction

Commerçant

Gestion de l'autorisation

Structure du message 0110 : réponse à la demande d'autorisation

2 : n°porteur	3 : code traitement	4 : montant	11 : no transaction	12 : heure	13 : date	18 : MCC
22: mode lecture	23: pan seq. nb	25: conditions	32 : code, bin banque	38: n° auto.	39 : code rép.	
41: env. 41	42: env. 42	47 08: type site	96: SIRET	97 : IDPA	A0 : IDSA	44 AF: Service
BB: num tél.						
44 BC : msg	49 : code monnaie	53: infos sécurité	55 71 : script	72 : script	91 : IAD (ARPC)	5F24 : date fin
55 DF80 : résultats puce	DF81 : type puce	59 0101 : code raison	0102 : année	0200 : ERT	0201 : ITP	
59 0202 : n°contrat	0203: NLSA	0204 : NLPA	0205 : code pays	0207 : montant cumulé	020B : TASA	

Légende couleurs :

Carte

Système Acceptation

Transaction

Commerçant

Gestion de l'autorisation

— Le terminal ne reçoit pas de réponse de l'émetteur

- └ Possibilité de forçage de la transaction si l'analyse des « TAC/IAC défaut » conduit à la demande d'un cryptogramme AAC

Paramétrage de l'application et AID permettent le forçage

Pas de raison d'appel "réponse positive obligatoire"

— Le terminal reçoit une réponse de l'émetteur

- └ Acceptation

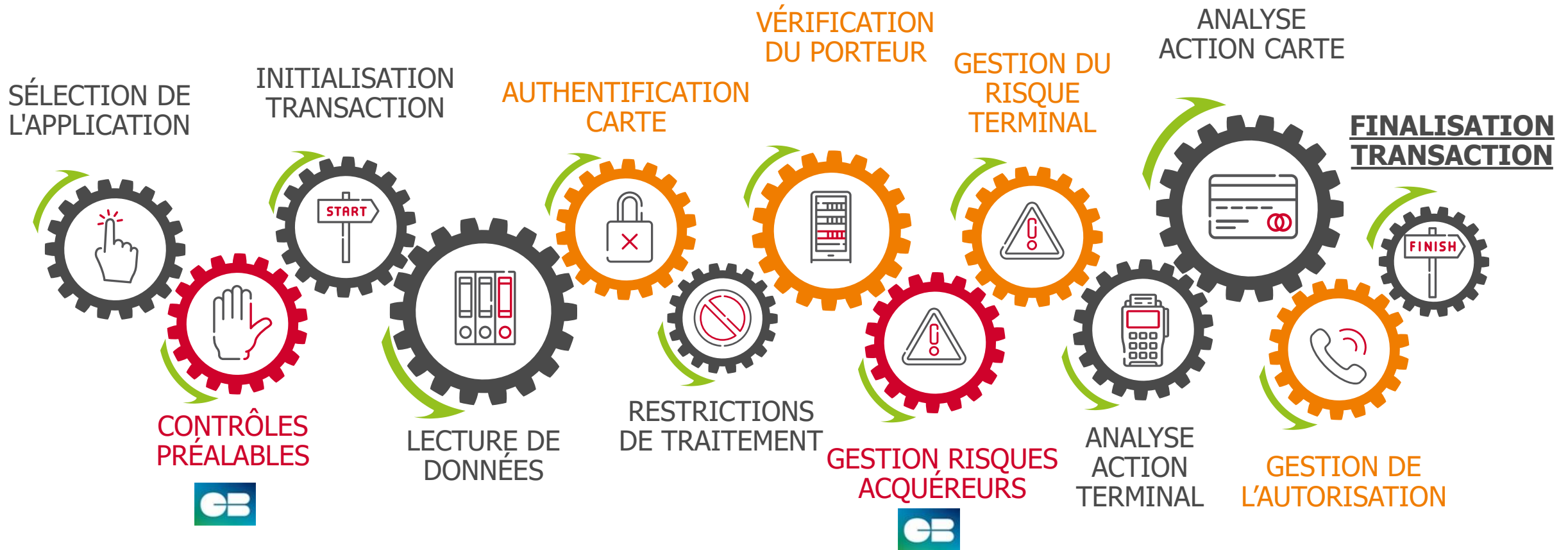
Seul code possible pour accepter la transaction pour les demandes avec "réponse positive obligatoire"

- └ Refus avec forçage possible

Si l'AID et le paramétrage de l'application le permettent (demande de cryptogramme AAC avec enregistrement de la transaction)

- └ Refus sans forçage possible

Spécificités d'une transaction CB : synoptique



Finalisation transaction

— La carte a rendu un cryptogramme TC ou AAC "forcée"

- └ La transaction est acceptée et enregistrée dans le fichier transaction
- └ Les tickets porteur et commerçant sont édités
 - Édition de l'AID et du label
 - Mesures sécuritaires sur le ticket porteur :
 - Numéro porteur tronqué
 - Date de fin de validité absente

— La carte a rendu un cryptogramme AAC (pas de forçage)

- └ La transaction est refusée
- └ Une TNA est enregistrée.
- └ Édition des tickets TNA en fonction du paramétrage manuel du commerçant

Fonctions d'environnement

Téléparamétrage avec protocole CB2A

- **Messages porteur et commerçant**
- **Entête, pied de ticket porteur et compte-rendu fonction commerçant**
- **Identification de l'application (enseigne, numéro commerçant ...)**

- **Appel serveur (téléparamétrage, télécollecte, autorisation, téléchargement)**
- **Seuils commerçant (floor limit et appel aléatoire)**
- **Risque acquéreur (liste de bins, liste de contrôle)**
- **Devises autorisées, montant minimum, maximum, double authentification**
- **Horodatage local**

- **AIDs avec priorité et autorisation de forçage**
- **Clés publiques de l'autorité de certification**
- **TAC rejet, on-line et défaut**
- **DOL par défaut (DDOL et TDOL)**
- **Liste des données complémentaires en télécollecte**
- **Liste des données spécifiques EMV (TCC Europay)**

Fonctions d'environnement

Télécollecte avec protocole CB2A

- **Numéro porteur**
- **Code traitement (identifie le différé de recouvrement)**
- **Montant, date, numéro de la transaction**
- **Raisons d'appel, no d'autorisation, code réponse émetteur, code forçage**
- **Données puce EMV**

Cryptogramme	Résultat des scripts
Dates début*/fin de validité	AUC*
AID	CVM list*
AIP	CVM results*
ATC	TAC*(rejet, on-line, défaut)
TVR	IAC* (rejet, on-line, défaut)
Nombre aléatoire	Capacités du terminal*