

Payments Processing Fallback Example of France

18th June 2026 – London

AGENDA

Payment systems processing resilience & fallback

How resilient the French payment system would be in the event of a major crisis and no service provision ?

1. Critical failure/weakness points of the French domestic payment systems
2. Review of schemes networks, processors/suppliers, issuers/acquirers
3. Actions should be taken if the US turned off the V/MC service

Payment systems resilience & fallback

The French ecosystem – Context

- Payment ecosystem, where **62% of payments are card payments** (and 68% of those payments are contactless)
- **Leading market stakeholders** : Cartes bancaires (card scheme), Stet (card network and ACH), 6 major banking groups, Thalès, Idemia, Worldline, Monext,..
- 100 M of debit and credit cards in total : “CB” cards and **more than 20 M of Visa or Mastercard (only branded) cards**



Cartes bancaires “CB” in a nutshell – Activity in 2025

78 Million active “CB” co-badged cards (V/MC brand)

14,5 billion “CB” transactions in total (payments, withdrawals)

8 billion contactless transactions

2,1 billion remote transactions (e-commerce)



For Cartes bancaires scheme, resilience means :

the ability to ensure, through a set of preventive or corrective measures, the continuity of card payments in the event of a major incident affecting one or more links in the chain between the merchant’s payment terminal, the acquirer, and the card issuer

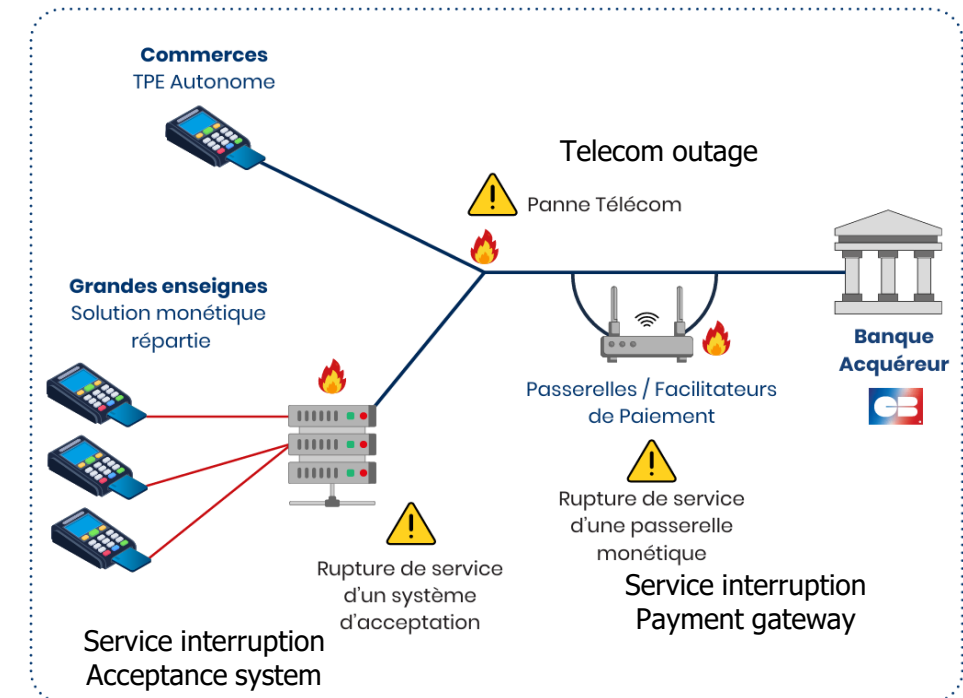
Payment processing fallback

Critical failure/weakness points of the French domestic payment systems

- A concentrated market : dominated by a few legacy banks and PSP (card issuing and acquiring activities)
- Mainly dependent on the CB credit/debit payment system: more than $\frac{3}{4}$ of all card payment transactions
- One unique ACH infrastructure for all payments processed: Stet
- Co-badging of 100% of "CB" cards with one ICS brand: either Visa or Mastercard brand
- Apple Pay: the leading payment wallet by far

In case of major breakdown in "CB" payment scheme:

- No capacity to process most of contactless payments (see next slide: "CB" resilience program)
- No soft POS, tablet or mobile payments
- Technical dependency:
 - On POS terminal application layer (EMV Kernel) with Visa and Mastercard technologies (for contactless interface) - CB' answer with involvement in CPACE initiative and deployment of CPACE products
 - On tokenization (Visa TSP and Token Management Service)



Review of schemes, schemes network and PSP - Cartes Bancaires “CB”

CB has developed its own resilience program

“Ensuring the continuity of payments in stores in case of a technical failure”

How does it work ?

In the event of a failure (technical glitch, power outage, server failure, cyberattack,..), most CB terminals can automatically **switch to offline mode** and continue to process payments.

- ✓ The POS terminal has two operating modes: Online (internet/4G) and Offline
- ✓ **Offline “CB” mode:** the POS terminal operates even in the event of a network outage or internet disconnection

In case of major “payment crisis”, in order to ensure business continuity, merchants are invited to:

- **Prioritize physical credit cards** and avoid mobile payments, cards requiring real-time authorization, and meal voucher cards, that rely on online systems
- **Encourage to pay by inserting the card into the terminal** and limit contactless payments
- **Prioritize payments under €100;** this reduces authorization requests to the issuer
- **Clearly inform customers:** display of guidelines at the register; reassure customers by letting them know that card payments are accepted
- If necessary, accept and offer **alternative payment methods**



Review of schemes, schemes network and PSP - Cartes Bancaires “CB”

Most POS terminals offline capable



A POS terminal can operate in offline mode, and a distributed terminal has a **backup mode for processing transactions offline, which is automatically activated in the event of an incident.**

Generally, a payment terminal can store about 250 to 300 transactions, which allows it to handle a certain volume of activity before the outage is resolved.

Soft POS systems, tablets, and smartphones that support contactless payment apps require an online connection and cannot accept payments in the event of a failure (such as a telecom or internet outage).

LES DIFFÉRENTS CAS A CONSIDÉRER SELON L'EQUIPEMENT SUR LE POINT DE VENTE ET LE MOYEN DE PAIEMENT DU CLIENT

1 – Le niveau de résilience d'un système d'acceptation dépend de sa capacité à réaliser des transactions offline

En France, un terminal de paiement est paramétré pour traiter des transactions « **online** » ou « **offline** » :

- **online** : le terminal de paiement interroge la banque Emettrice⁽⁴⁾ de la carte pour autoriser et valider le paiement. Les transactions sont traitées par un échange de données entre le TPE et la banque, par le biais d'une connexion télécom (internet ou autre ...).
- **offline** : le terminal de paiement traite la transaction de paiement sans interroger la banque Emettrice de la carte. La connexion télécom (internet ou autre...) n'est pas requise au moment de l'opération.

Aussi, lors d'une défaillance, le terminal ne peut traiter que les transactions de paiement en mode offline. Favoriser ce mode d'utilisation permet d'améliorer la résilience du paiement par carte bancaire CB.

Les transactions réalisées offline seront télécollectées une fois l'incident résolu dès que le terminal sera en capacité de se connecter à la Banque Acquéreur.

- ✓ **Un TPE autonome peut fonctionner en mode offline et un terminal réparti dispose d'un mode secours** (permettant de traiter des transactions offline) dont le déclenchement est automatique lors d'un incident.

En moyenne, **un terminal de paiement peut stocker environ 250 à 500 transactions**, ce qui permet de supporter un volume d'activité d'environ 48h selon le cas.

- ✗ **Les SoftPOS, tablettes ou smartphones** supportant une application de paiement sans-contact, imposent un fonctionnement systématique en mode online et **ne permettent donc pas d'accepter des paiements en cas de défaillance** de type panne télécom/internet.

Review of schemes, schemes network and PSP

Stet : the leading card authorization switching network & ACH for all payment instruments in France + Belgium

CORE (Stet ACH system) classified by the Eurosystem as a **Systemically Important Payment System (SIPS)**

CORE clearing instances by Stet: **3 IT platforms in operation**

- ❑ **CORE.FR**: all French payment operations (including SDD)
 - ❑ **CORE.BE** (since 2012): all Belgium payment operations (domestic and SEPA)
 - ❑ **SEPA.EU**: white-label outsourcing platform for CSM clients
 - ❑ **IP CSM (SWIP (Single Window for Instant Payments))**: processing of SCT-Inst operations
- + interoperability with/connection to TIPS and RT1 from EBA Clearing

Key Figures 2025

17.5
billion



Cleared payment processed in
CORE

14.8
billion



Authorized transactions

1.5
billion



Tokenized payments

1.1
billion



Instant payments

16.1
billion



Transactions scored

358
million



VoP operated

Review of schemes, schemes network and PSP

Stet – Classified as SIPS by the Eurosystem

A set of resilience mechanisms as required by the Eurosystem

Resilience mechanism	Description	Further information
Full redundancy of critical components	Systematic redundancy for critical HW and SW components. Each component has a backup capable of taking over operations in the event of a failure	Process recovery through alternate systems
For Stet ACH: 2 data centers synchronised in real time	The CORE system is based on two datacenters with real-time data replication. If one site becomes unavailable, a switchover to the second site can be carried out quickly with minimal loss of synchronisation	Between 2 datacenters, short synchronization window and rapid switchover in the event of a failure at one site
For Stet card authorization network	3 active-active service center in France A back-up Network Monitoring and Management Centre	2 IP-VN access networks provided by two separate operators Switching service instances distributed across three sites and accessible to all clients
Business Continuity Plan (BCP)	A business continuity plan covering critical services: the CORE interbank clearing system and the card authorisation network	
Network access resilience	Participants (banks, payment service providers, infrastructure providers) have access via several channels: ▪ the encrypted Stet private network ▪ the SWIFTNet network ▪ a secure Stet extranet	Stet network itself relies on several telecoms operators to avoid dependence on a single provider
Crisis management and cyber resilience	Stet's security policy based on ISO 27001 and ISO 27002 standards	1/Network segmentation 2/Data encryption 3/Continuous monitoring 4/Vulnerability management 5/Improvement of security

Banque de France & Comité national des moyens de paiement (CNMP)

“Groupe de Place Robustesse” (GPR) & Stratégie nationale des moyens de paiement

Objective

At national level, same objective of Banque de France & National Committee on Payment Methods

- Resilience of the payment sector is a top-priority objective of CNMP: in Stratégie nationale des moyens de paiements 2025-2030 document
- Crisis unit to ensure that payments, financial markets, cash dispensers and essential banking services continue to function even in exceptional circumstances

Action plan

- Operational crisis management : coordination of all stakeholders of the payments market in the event of a major incident
- Preparation of Business continuity plans
- Regular stress tests conducted by Banque de France, covering the cash management sector and, more broadly, all means of payment
- Communication unit to prepare and address relevant messages to banks, merchants and to the public

Examples of activities (GPR Groupe)

- ✓ Simulations of cyberattacks and natural disasters, such as a major flood of the River Seine (Headquarters of Banque de France and other banks..)
- ✓ Preparations relating to the risk of national power cuts
- ✓ COVID-19 pandemic, to ensure the continuity of the financial system and access to cash

GPR Group of Banque de France

Organisation and structure

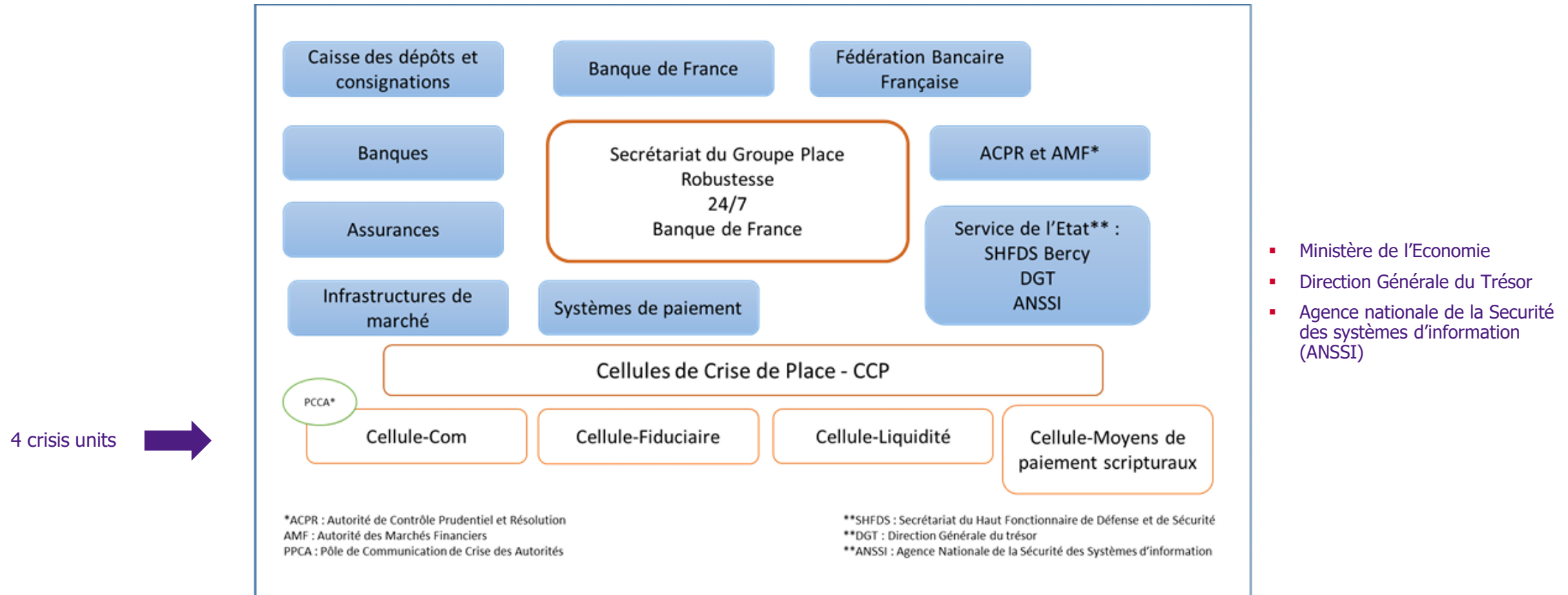


Figure 1 structure du GPR

Payment processing fallback

Actions should be taken in the event of major incidents // if the US turned off the Visa/Mastercard service

	Actions/initiatives	Who's in charge?	Impact	Remarks
Power cut Telecom outage	Fallback on CB card and offline CB mode	Merchants + Acquirers (banks), technical service providers and vendors	Cardholder: requires a "CB" Contact transaction only Information and communication	Loading capacity of the terminal (hundreds of transactions)
Service suspension for +20M of V/MCW only card	Fallback on CB card and offline CB mode	Merchants + Acquirers (banks), technical service providers and vendors	Cardholder: requires a "CB" + Contact transaction only Merchant adaptation Issuing of ++ "CB" cards	Ambition for 2030: 100M "CB" co-badged card Instant issuing program?
EU interoperability: no more cross-border card transactions (no ICS networks)	Rely SEPA rails : SCT, SDD Instant Payment with Wero	Banks and PSP	Significant impact on cross- border zones, touristic areas, e- commerce and sector (luxury)	Need urgent action plan to deploy "SEPA solutions"
No Apple Pay available (wallet)	Switch to others wallet solutions (Wero Pay, other XPay, other wallets..)	Banks, PSP and Wero consortium	Very significant impact on payment journeys (transport,..)	Would need very fast response Value proposition equivalent to Apple Pay, etc.?
Ban by Visa or Mastercard (technological dependence)	Fallback to contact transactions with CB cards	Merchants + Acquirers (banks)	Contactless capability of some POS terminals off	Need to accelerate the deployment of CPACE
Tokenisation (V/MC TSP) and Mobile payment application set- up	Need to rely on CB/Stet tokenization service	CB/Stet + issuers	Need new enrollment and registration process	Long process to convert and enroll new users

Payments Processing Fallback - France

Q&A

Emmanuel CARON

+ 33 (0) 623 295 756

