Résilience des paiements par carte

Comprendre les différents modes de secours et préparer la continuité des paiements en magasin

À RETENIR | Une panne de connexion ou d'autorisation ne signifie pas toujours l'arrêt de tous les paiements. Selon les équipements et leur paramétrage, certains paiements peuvent être acceptés en mode secours. Attention : un paiement enregistré ou accepté en mode secours n'est pas nécessairement garanti.

1. Pourquoi parle-t-on de résilience ?

La résilience est la capacité d'une solution de paiement à continuer de réaliser tout ou partie des paiements pendant un incident technique, puis à reprendre son fonctionnement nominal. Une panne peut toucher la liaison du magasin, le serveur d'acceptation, un intermédiaire bancaire ou le système d'autorisation de la banque émettrice.

Les travaux de FrenchSys visent à harmoniser les mécanismes de secours, sans supprimer les contrôles de risque. La présente note se concentre sur les paiements de proximité (contact et sans contact) en magasin.

2. Trois mécanismes de secours à distinguer

Mécanisme	Principe	Intérêt / vigilance
1. Transaction EMV « renforcée »	Traitement local de transactions EMV autorisées par les règles carte/terminal, sans solliciter l'autorisation en ligne.	Uniquement pour les solutions réparties (les solutions autonomes pouvant déjà faire des transactions EMV offline) ; toutes les transactions ne sont pas éligibles.
2. Forçage commerçant étendu	Possibilité supplémentaire d'accepter certaines transactions qui nécessiteraient normalement une autorisation, dans les cas d'incident et limites prévus.	Le forçage peut entraîner des impayés ; il n'est ni général ni libre de toute condition.
3. Demande d'autorisation différée (DAD) en mode résilience	Enregistrement local d'une transaction éligible pendant l'incident, puis transmission ultérieure de la demande d'autorisation après rétablissement.	Peut étendre le champ des paiements maintenus, notamment en sans contact. Une demande ultérieure peut être refusée.

3. Exemple en magasin : une liaison est interrompue

Lors d'une forte affluence, la connexion devient indisponible. Si un mode de secours compatible a été installé, autorisé et configuré, il peut s'activer automatiquement ou être déclenché de manière sécurisée. Le magasin poursuit uniquement les transactions éligibles, dans les plafonds prévus. Au retour du réseau, la solution revient en fonctionnement nominal et transmet les opérations enregistrées selon le mécanisme utilisé.

Point d'attention – DAD (en mode résilience) : le bien ou le service a été remis avant la réponse de la banque. Un refus de paiement ultérieur de la part de l'émetteur reste possible.

4. Quels moyens de paiement sont concernés ?

Les travaux présentés en juin 2026 portent sur les transactions de paiement de proximité par carte en contact et en sans contact. Le mode EMV « renforcé » concerne spécifiquement les solutions monétiques réparties car il leur permet de réaliser des transactions EMV sans connexion au serveur d'acceptation (élément d'architecture logicielle n'existant pas en monétique autonome) ; la DAD vise les solutions réparties et les terminaux autonomes.

Les cartes à autorisation systématique (CAS), les titres-restaurant dématérialisés (TRD), les téléphones et objets connectés font partie des extensions possibles étudiées pour la DAD. Leur acceptation en mode secours ne doit pas être supposée acquise : elle dépendra des règles et implémentations effectivement disponibles.

Dans le périmètre fonctionnel présenté, les crédits/remboursements, annulations, préautorisations, retraits, SoftPOS et automates sont exclus. Des études spécifiques sont prévues pour certains automates, notamment les distributeurs de carburant.

5. Qui décide de l'activation et des limites ?

- Dans son paramétrage, l'Acquéreur indique les modes autorisés, par marque de paiement. Les préférences du commerçant ne neutralisent pas les règles des réseaux bancaires.
- Le commerçant et son prestataire/mainteneur définissent le mode préféré du commerçant et sa modalité d'activation (automatique ou manuelle).
- Lors d'une transaction en mode résilience, le terminal ou la solution applique les paramètres prévus par l'Acquéreur et par la marque du paiement pour le mode de résilience activé : montant maximal spécifique, seuil d'appel, nombre d'opérations par carte et par jour.
- Les règles des réseaux de paiement et les accords avec l'Acquéreur conditionnent l'éligibilité et la répartition du risque financier.

6. Comment préparer ses magasins ?

- Recenser les solutions de caisse, terminaux autonomes et serveurs d'acceptation ; faire confirmer les fonctions effectivement disponibles.
- Valider avec l'Acquéreur le cadre contractuel, les conditions d'activation et les limites de paiements.
- Organiser un test avec le mainteneur : bascule, stockage sécurisé, reprise des échanges et rapprochement des transactions.
- Formaliser une consigne simple pour les équipes : quand activer le secours, quels paiements privilégier et qui contacter.
- Contrôler après incident les transactions enregistrées et leur traitement financier ; identifier les éventuels refus.
- Vérifier l'alimentation électrique et les équipements critiques : un mode secours n'assure pas la continuité si les équipements indispensables sont hors service.

7. Que faire pendant un incident ?

En pratique, les conseils sont les suivants : vérifier le passage en mode secours, privilégier si possible la carte physique insérée avec code PIN, respecter les montants autorisés et proposer une autre carte éligible en cas d'échec. Ces consignes doivent être adaptées à l'équipement du magasin.

8. Où en sont les travaux ?

En septembre 2025, les commerçants ont demandé une meilleure maîtrise de leur exposition au risque, une communication plus rapide lors des incidents et des solutions adaptées aux automates. En juin 2026, FrenchSys a publié le Bulletin 4 « Résilience » standardisant les mécanismes de résilience vus plus haut, ainsi qu'un calendrier prévisionnel de versions et d'évolutions protocolaires.

Ces présentations constituent un état des travaux à date ; elles ne permettent pas, à elles seules, de confirmer la disponibilité générale des fonctionnalités dans les points de vente en octobre 2026.

Les 4 questions à poser à votre prestataire de paiement

1. Quels modes de secours sont aujourd'hui opérationnels sur mes équipements et pour quelles marques ?
2. Qui peut déclencher ou arrêter le mode secours et comment mes équipes le vérifient-elles ?
3. Quels types de paiement, montants et moyens de paiement sont éligibles pendant une panne ?
4. Comment sont suivies les opérations enregistrées et qui supporte le risque en cas d'impayé ?

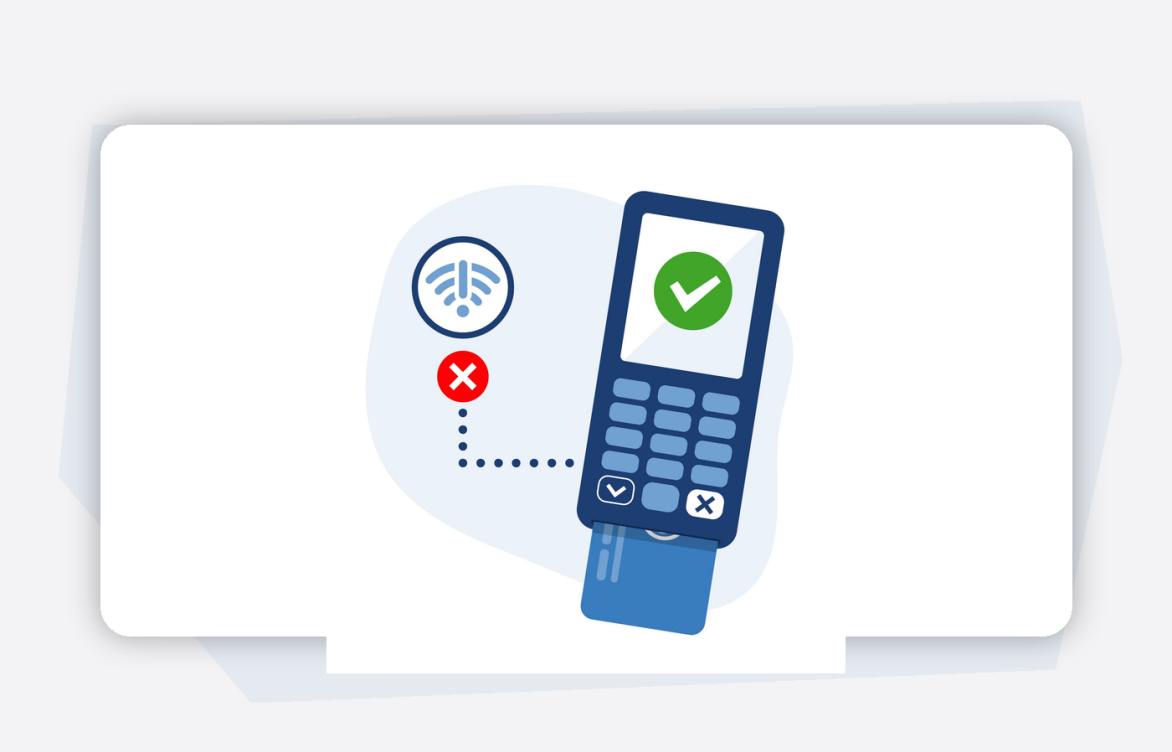
Schémas explicatifs

Les schémas ci-dessous illustrent de manière simplifiée les trois principaux cas de fonctionnement évoqués dans la note. Ils ont une vocation pédagogique et ne remplacent pas les paramétrages, règles d'éligibilité et dispositions contractuelles applicables.

1. Fonctionnement nominal : la transaction suit le circuit habituel jusqu'à l'obtention d'une réponse en temps réel.



2. Incident avec mode secours local : certaines transactions peuvent être traitées localement si le dispositif de secours est disponible et autorisé.



3. Demande d'autorisation différée (DAD) : la transaction est enregistrée pendant l'incident puis transmise après rétablissement de la connexion.

