Suivi de la mise en œuvre de la DSP2

Étude empirique menée par 5 TPP

Introduction

A) Contexte

L'entrée en vigueur de la révision de la Directive sur les Services de Paiements (DSP 2) a entraîné une modification profonde des modalités d'échanges de données entre les acteurs de la Place mais également des parcours clients.

En effet, la mise en place d'API pour l'échange de données – sur le périmètre des comptes de paiement - ainsi que la généralisation de l'authentification forte ont nécessité de lourds travaux pour l'ensemble des acteurs, qu'il soit ASPSP ou TPP.

Ces changements n'ont pas été neutres sur l'expérience du client final avec par exemple :

- La généralisation d'utiliser deux moyens d'authentification pour valider certaines opérations définies comme sensibles.
- La mise en place de parcours « *redirect* » obligeant les utilisateurs finaux à être redirigés pour être authentifiés sur le site de l'établissement teneur de comptes.
- Des écarts de fréquence mais également de méthode d'authentification selon le type de comptes concernés.

L'impact sur les différents parcours clients a donc été très fort et avec parfois des effets déplorables sur les nouveaux entrants notamment. En effet, que ce soit sur des parcours d'agrégation de comptes, d'initiation de paiement ou globalement de paiement, l'innovation tient notamment à la fluidité du parcours offert au client final.

Le régulateur a aujourd'hui – en partie - conscience des manques et dangers de l'application de cette Directive, voire les effets contre productifs de son application au regard des ambitions inhérentes à la mise en place de la Directive.

Ainsi une révision de la DSP 2 a été entamée et a notamment commencé par une révision des règles d'authentification forte avec la suppression de la règle des 90 jours. La constitution de groupes de travail afin de suivre, piloter voire amender la DSP 2 a émergé au sein de différents pays, que ce soit au UK avec le groupe Open Banking ou en France avec différents groupes de travail réunissant l'ensemble des parties prenantes.

Aujourd'hui, les travaux réglementaires battent actuellement leur plein pour à la fois revoir en profondeur la DSP 2 mais également étendre ses concepts à l'ensemble de la finance. Il apparaît dans ce contexte de plus en plus nécessaire de piloter et mesurer les effets de la DSP 2 sur les usages clients, et plus globalement en matière d'innovation, de respect des règles de concurrence et de protection des consommateurs.

Fort de ces constats, 5 TPP - Linxo, Lyra Collect, Perspecteev (Bridge), Fintecture et Powens - ont mené à bien une étude approfondie sur les parcours AIS et PIS en s'appuyant sur un cabinet externe afin de garantir la confidentialité des données partagées et échangées.

Cette note détaille les principaux enseignements basés sur l'étude et formule des recommandations concrètes et opérationnelles pour les prochaines évolutions réglementaires attendues.

B) Objectifs de l'étude

Au travers de cette étude, les TPP ont notamment pu :

- Identifier les parcours critiques qu'il convient de « corriger » au plus tôt en validant que le problème est commun à l'ensemble des TPP, en initiant des discussions et/ ou d'alerter les instances de Place le cas échéant.
- Comparer les taux de succès/ échecs entre les différents parcours, notamment intermédiés par des TPP ou EP.
- Identifier des bonnes pratiques qui pourraient être partagées voire remontées au régulateur dans le respect des règles de concurrence.
- Fournir des synthèses claires au régulateur le cas échéant afin d'influer sur les débats en cours, et préparer des éléments tangibles afin d'appuyer les discussions en cours sur la révision de la DSP 2 ou plus généralement en matière d'Open Banking.

Par ailleurs, cette initiative a été menée dans le respect des règles de concurrence les participants ayant veillé à ne pas mettre en place des mesures, remarques ou partage d'informations qui pourraient être considérées comme une entente de Place.

C) Périmètre des données étudiées

Les données étudiées sont relatives à des transactions effectuées dans le cadre de paiements initiés depuis un acteur tiers (PIS) et de parcours relatifs à l'agrégation de comptes (AIS)[1].

[1] Hors Lyra Collect et Fintecture

Partie 1 - Activités d'initiation de paiement (PIS)

1. Périmètre

Les données étudiées s'étendent sur 6 mois, de novembre 2022 à mars 2023. Cette plage de temps nous permet de disposer de suffisamment de données pour mener différentes analyses tout en lissant des effets de saisonnalité qui pourraient impacter les résultats.

Pour étudier les données et normaliser leur traitement, nous nous appuyons sur la nomenclature STET et notamment les messages dits de 1er niveau (*accepted*, *rejected*, *pending, etc.*) et 2nd niveau (NOAS, FRAD, etc.) notamment lors de rejet de l'opération.

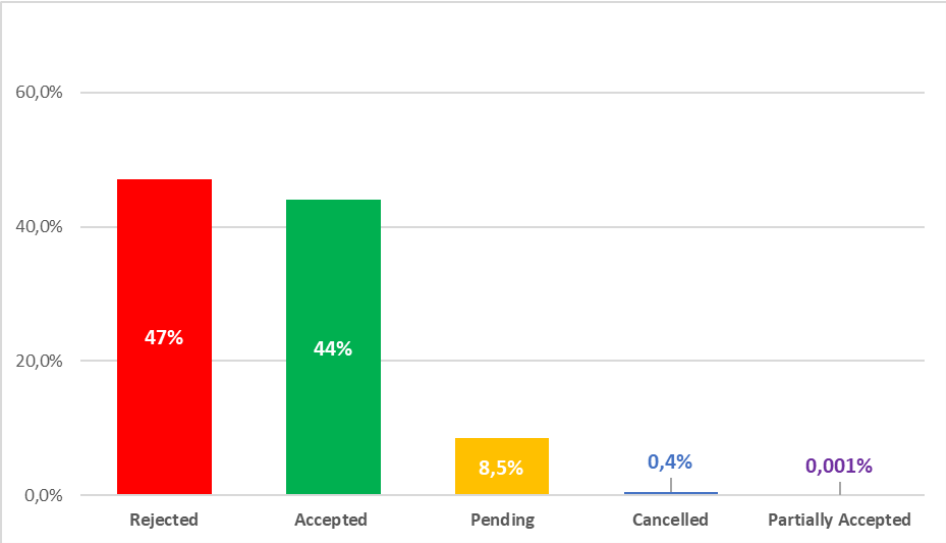
Type	Données
ASPSP	77 dont (19 avec plus de 1 000 requêtes pour les statuts de premier niveau et 16 avec plus de 1 000 requêtes pour les statuts de second niveau)
Dates	Novembre 2022 à mars 2023
Pays	7 (focus sur la France, volume de données suffisant)
Nombre de requêtes	~1 360 000

2. Constats relatifs aux activités d'initiation de paiement

Synthèse des constats	
Constat 1	Un faible taux d'acceptation des transactions via des PISP constaté (44%) ; Des parcours fonctionnels complexes avec des mesures de sécurité mises en place qui jouent sur le niveau d'acceptation global.
Constat 2	Des disparités fortes d'utilisation des statuts de niveau 1 et 2 par les différents ASPSP ; Une mauvaise utilisation des statuts de niveau 1 et 2 qui se traduit par une surutilisation des statuts de premier niveau dit « intermédiaires » et par une surutilisation du statut de second niveau « NOAS ».
Constat 3	Une irrévocabilité des paiements non avérée dans certains cas avec des impacts sur les cas d'usage commerçants.
Constat 4	Des progrès encore possibles dans le partage d'informations pour lutter plus efficacement contre la fraude.
Constat 5	Une faible utilité de la *fallback* au regard des uses cases PIS rendant la dépendance à des API fonctionnelles très élevée.
Constat 6	Des lacunes en matière de suivi des orientations de la DSP 2 notamment sur les communications sur l'utilisation des API (délai de prévenance en lien avec les évolutions, publication d'indicateurs sur les API, disponibilité des API, etc.).

Constat 1 : un faible taux d'acceptation des transactions intermédiées via des PISP ;
Des parcours fonctionnels complexes avec des mesures de sécurité mises en place qui jouent sur le niveau d'acceptation global.

Graphique 1 : ventilation des opérations par statut de niveau 1



L'étude des statuts dit de niveau 1 montre un faible taux de transaction « accepted ».

Sur les 1 360 000 requêtes étudiées, 47% d'entre elles sont rejetées et 44% acceptées. 8,5% de ces demandes restent dans un statut intermédiaire.

- 44% d'entre elles ont le statut final ACSC. Cela signifie que toutes les conditions pour que la transaction soit acceptée ont été respectées.
- A contrario, 47% de ces requêtes n'ont pas rempli toutes les conditions pour que la transaction soit acceptée et par conséquent celle-ci a échoué.
- 8,5% des transactions ont un statut considéré comme intermédiaire.

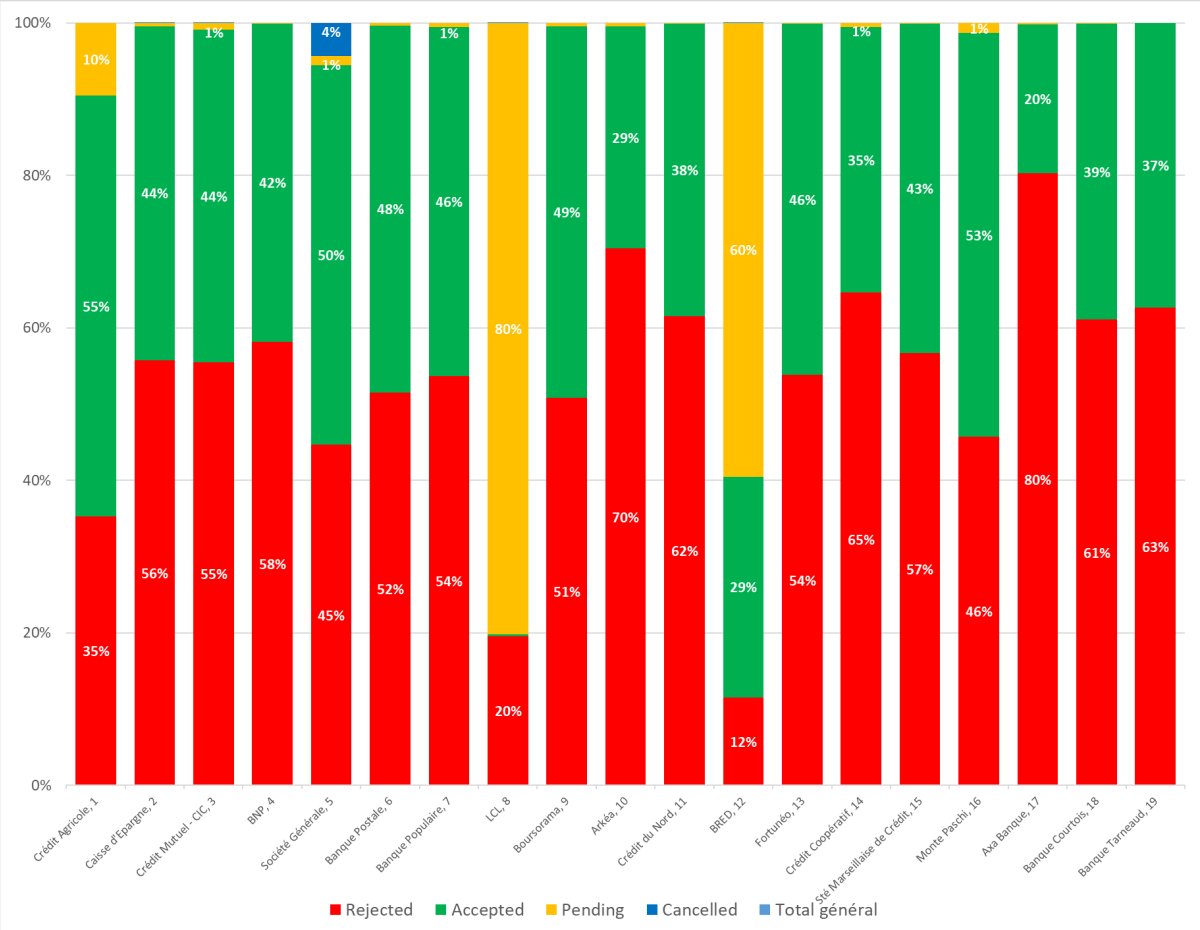
Parmi les transactions rejetées, on note des cas d'usage où des parcours fonctionnels empêchent l'aboutissement de transactions, car jugés trop complexes et ne respectant pas les recommandations EBA par exemple en ne permettant pas l'usage de la biométrie alors qu'elle est disponible lorsque le virement est initié depuis l'application de la banque. Un des ASPSP étudié compte deux mesures de sécurité renforcées dans ses parcours clients, qui incluent la saisie du nom d'utilisateur, du mot de passe, des informations de carte et de SMS. Ces mesures renforcées ont entraîné plusieurs cas d'abandon d'utilisateurs, provoquant ainsi des *timeouts* et le rejet de la transaction.

D'autres cas de figure ont été répertoriés, notamment lors de parcours nécessitant plus de deux signatures pour des opérations en BtoB. Lorsqu'une demande de transaction est réalisée et qu'elle nécessite deux signatures ou plus, le Crédit Mutuel rejette la transaction ou la maintient dans un statut intermédiaire « pending ».

Néanmoins une certaine homogénéité est présente dans les niveaux d'acceptation constatés par les différents TPP.

Constat 2 : de fortes disparités d'utilisation des statuts de niveau 1 et 2 par les différents ASPSP ; Une mauvaise utilisation des statuts de niveau 1 et de niveau 2 qui se traduit par une surutilisation des statuts de premier niveau « intermédiaires » et par une surutilisation du statut de second niveau « NOAS ».

Graphique 2 : ventilation des transactions par statut de niveau 1 par ASPSP, focus sur les 19 plus importants (supérieur à 1 000 requêtes)

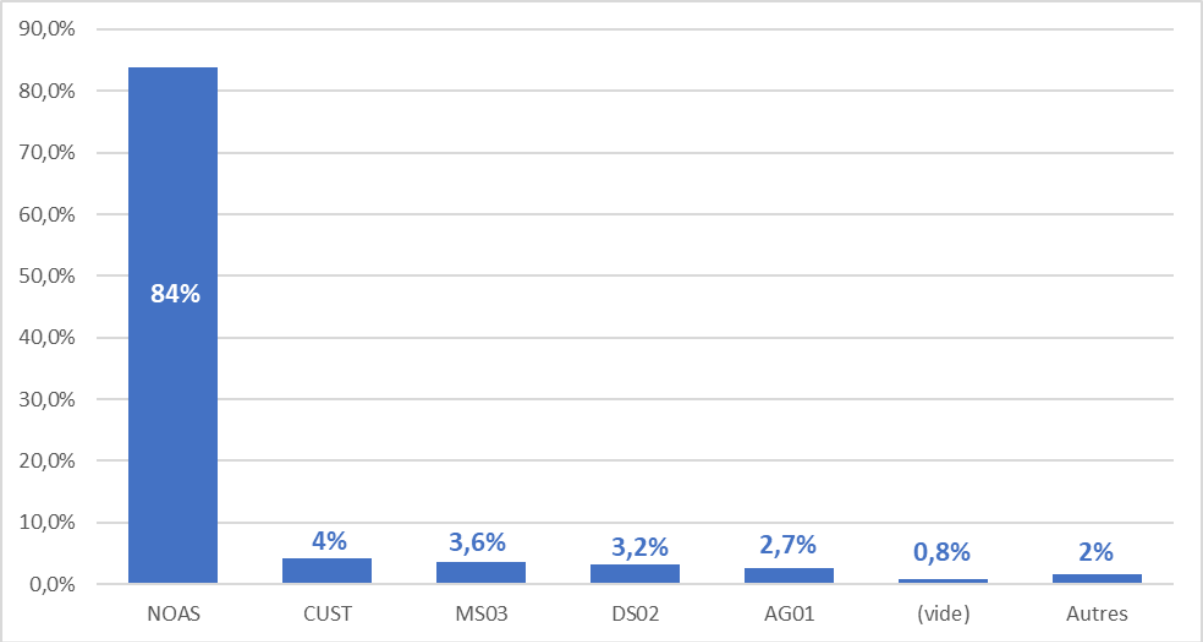


Parmi les différents ASPSP, 4 points notables sont identifiés :

- Seuls 16% des acteurs du panel ont un taux d'acceptation supérieur à 50 % (acteurs 1, 5, et 17).
- Pour au moins 16% des acteurs (acteurs 1, 8 et 12), l'utilisation du statut « pending » pourrait être améliorée au vu des scores trop élevés à priori).
- Ainsi, 74% des acteurs ont un taux de rejet supérieur à 50% dont un acteur à près de 80% de rejet.
- Seulement 1 acteur utilise le statut « *cancelled* » ; ce statut indique qu'une requête a été annulée suite à la demande de l'utilisateur lui-même.

Ces différents éléments interrogent sur l'utilisation par les ASPSP des statuts de niveau 1, plus particulièrement au niveau de l'utilisation importante du statut « pending ». Ceci indique que certains établissements bancaires ne se conforment pas au modèle de fonctionnement des statuts STET, ou bien ne communiquent pas le statut final aux TPP.

Graphique 3 : ventilation des statuts de niveau 2 en cas d'échec de la transaction



Parmi les 47% de statut rejeté, la répartition des statuts de second niveau est très hétérogène avec une surutilisation du statut NOAS.

- Ce statut NOAS (No Answer from Customer) représente près de 84 % de raisons énoncées en cas de rejet. Il détaille les cas où d'après l'ASPSP il n'y a eu ni acceptation ni refus de la part du client final ce qui a entraîné un timeout.
    - Parmi ces différents cas d'usage, certains présentent des parcours jugés complexes qui conduisent à l'abandon du client et, par conséquent, au refus de la transaction.
- Le statut CUST traduit lui un rejet de l'opération par le client final ou en cas de manque de fonds sur le compte du client.
- Le statut DS02 traduit une annulation par un tiers autorisé (à priori différent du client final).
- Le statut MS03 équivaut à une absence de raison par l'ASPSP.
- Moins de 1% des transactions sont rejetées sans motif précis (statut laissé vide).
- L'ensemble des autres statuts représente moins de 2% des transactions (RR01, FRAD, RR04, AC01, FF01, CH03, AC06, RR12, CNOR et AC04).

Graphique 4 : ventilation des statuts de niveaux 2 par ASPSP en cas d'échec de la transaction, focus sur les 16 plus importants (supérieur à 1000 requêtes)

ASPSP	AC01	AC04	AC06	AG01	CH0	CNO	CUST	DS02	FF01	FRAD	MS0	NOAS	RR01	RR04	RR1
Crédit Agricol	-	-	-	16,0%	-	-	4,4%	-	-	-	2,3%	76,7%	-	0,60 %	-
Caisse d'Eparg	0,01%	-	0,03 %	0,01%	-	-	8,7%	-	0,41 %	0,003 %	0,70 %	86,7%	3,5%	0,001 %	-
Crédit Mutuel - CIC	-	-	-	-	-	-	2,4%	1,8%	-	-	0,001 %	95,7%	-	-	-
SG	0,003 %	-	0,003 %	-	-	-	0,19 %	0,22 %	-	0,03 %	0,69 %	98,9%	-	-	-
BNP Paribas	-	-	-	0,001 %	-	-	5,8%	-	-	-	0,06 %	94,2%	-	-	-
La Banque Postale	0,032 %	-	-	2,4%	0,13 %	-	-	1,05 %	-	4,5%	16,8 %	72,7%	-	2,4%	0,03 %
Banque Populai	0,11%	0,002 %	-	0,04%	-	0,02 %	8,0%	-	0,31 %	-	0,69 %	89,0%	1,8%	0,01 %	-
LCL	0,47%	-	-	0,01%	-	-	-	86,0 %	0,02 %	-	13,2 %	0,30%	-	-	-
Bourso rama	-	-	-	-	-	-	0,50 %	3,3%	-	-	0,76 %	95,5%	-	-	-
Arkéa	0,79%	-	-	0,40%	-	-	7,1%	-	-	-	0,20 %	91,5%	-	-	-
Crédit du	-	-	-	-	-	-	7,5%	-	-	-	52,8 %	39,7%	-	-	-
Crédit Coopér atif	-	-	0,03 %	0,09%	-	-	3,1%	-	0,12 %	-	0,06 %	90,9%	5,7%	-	-
Fortun eo	-	-	-	-	-	-	34,34 %	-	-	-	0,21 %	65,5%	-	-	-
Sté Marseil laise	-	-	-	-	-	-	8,3%	-	-	-	52,8 %	38,9%	-	-	-
Monte Paschi	-	-	-	-	-	-	5,8%	2,2%	-	-	-	92,0%	-	-	-
Axa Banque	0,18%	-	-	0,55%	-	-	1,9%	-	-	-	-	97,4%	-	-	-

Parmi les 16 acteurs bancaires présentés ci-dessus :

- 68% ont plus de 75% de statut NOAS,
- À l'inverse, certains ne l'utilisent pas du tout ou très peu (>0,5%).

L'utilisation de ce statut apparaît comme disproportionnée chez certains acteurs, tandis qu'elle est très limitée chez d'autres, ce qui interroge quant à sa bonne utilisation.

D'autre part, l'utilisation du statut NOAS peut être incohérente avec certains parcours fonctionnels. Des cas de figures ont été identifiés avec le Crédit Agricole et La Banque Postale où :

- L’utilisateur valide une transaction, cette validation étant visible par le TPP,
- La transaction est par la suite refusée par le Crédit Agricole et La Banque Postale avec un statut NOAS.

Ce cas d’usage met en évidence une problématique quant à l’utilisation du statut NOAS par certains ASPSP.

On constate également que le statut MS03 est fortement utilisé chez LCL. En réalité, la grande majorité des utilisateurs concernés sont ceux qui n'ont pas activé la double authentification (F2A) du côté de leur banque.

Constat 3 : une irrévocabilité des paiements non avérée dans certains cas avec des impacts sur les cas d'usage commerçants.

Le Crédit Agricole et la Société Générale permettent l'annulation d'un virement initié et réalisé par l'intermédiaire d'un chargé de clientèle mais également directement depuis des interfaces clients et cela sans échange avec la contrepartie commerçant ; ce dernier cas étant davantage problématique.

Les TPP ont ainsi identifié de nombreux cas de tentative de fraude au commerçant avec de multiples annulation immédiatement effectuée après un achat. Un scénario courant, observé par plusieurs TPP, est lorsque le client contacte son chargé de clientèle après avoir effectué un achat chez un fournisseur, lui demandant d'annuler la demande de virement déjà effectuée. Le fournisseur enregistre des pertes de produits non rémunérés. Certains clients ont également la possibilité d'annuler un virement initié à partir de leur compte en ligne.

A titre de comparaison, aucune annulation de ce type n'est possible avec une carte bleue ou avec des virements instantanés.

Il est important de préciser que cette pratique va directement à l'encontre des directives de la DSP 2 et va plus précisément à l'encontre de l'irrévocabilité d'une transaction.

Constat 4 : des lacunes en matière de suivi des orientations de la DSP 2 sur les communications sur l'utilisation des API.

Cette étude a montré que des progrès peuvent encore être réalisés en matière de communication sur les API et notamment sur deux points principaux :

- Dans la communication d'indicateurs de disponibilité des API par les ASPSP (notamment versus les interfaces clients).
- Dans les communications préalables à des changements de l'API (ou de la *fallback*) et pouvant impliquer des interruptions de service coté TPP.

Un cas d'usage est survenu où suite à une MEP de BNPP, aucune transaction n'a pu être effectuée avec ce dernier à travers le TPP Lyra Collect.

Guideline 3: Publication of statistics
3.1 *For the purpose of Article 32(4) of the RTS, the ASPSP should provide its competent authority with a plan for publication of daily statistics on a quarterly basis on the availability and performance of the dedicated interface as set out in Guidelines 2.2 and 2.3, and of each of the interfaces made available to its own PSUs for directly accessing their payment accounts online, together with information on where these statistics will be published and the date of first publication.*
3.2 *The publication referred to in Guideline 3.1 above should enable PISPs, AISPs, CBPIIs and PSUs to compare the availability and performance of the dedicated interface with the availability and performance of each of the interfaces made available by the ASPSP to its PSUs for directly accessing their payment accounts online on a daily basis.*

Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)

Constat 5 : des efforts à faire dans le partage d'informations pour lutter plus efficacement contre la fraude.

Un des enjeux de la DSP 2 est la sécurité des transactions en introduisant des mesures de sécurité renforcées pour réduire les risques de fraude. Les prestataires de services de paiement doivent mettre en place des mécanismes de sécurité supplémentaires lors des transactions en ligne, en s'assurant que l'identité de l'utilisateur est vérifiée de manière fiable et qu'il donne son consentement pour chaque opération.

Plusieurs points de l'étude montrent que des progrès pourraient être fait sur la place en matière de lutte contre la fraude et notamment :

- La faible utilisation du statut « FRAD » pour justifier du refus d'une transaction de la part d'un ASPSP.
- L'absence de certaines informations (non strictement obligatoires) mais indispensables à la lutte contre la fraude comme l'IBAN, le nom du titulaire du compte et le nom de la personne effectuant la demande de transaction (notamment dans le cas où le nom du titulaire du compte est une personne morale)

A titre d'exemple, nous avons constaté qu'un des ASPSP n'envoie pas le nom du titulaire du compte.

Constat 6 : une faible utilité de la *fallback* au regard des uses cases PIS rendant la dépendance à des API fonctionnelles très élevée.

Lors de parcours relatifs à l'agrégation de comptes (AIS), la *fallback* AIS peut être une véritable solution de repli en cas d'indisponibilité de l'API. Inversement, le recours à une *fallback* dans l'exécution d'une requête PIS est presque impossible :

- Les requêtes AIS historiquement réalisées directement depuis les interfaces clients sont maîtrisées par les différents acteurs.
- Les requêtes PIS nécessitant la lecture mais également l'écriture de données rendent difficiles l'appui sur une *fallback*. La dépendance aux API bancaires est donc extrêmement forte dans le cas des requêtes PIS.

Partie 2 - Activités d'agrégation de comptes (AIS)

1. Périmètre

Les informations correspondent aux statistiques AIS fournies par 3 TPP français, principalement durant le premier semestre 2023.

De ces données, nous avons pu réaliser 3 analyses qui se distinguent par leur niveau de granularité :

Niveau 1 : analyse relative à la fiabilité globale des API selon les ASPSP (TPP 1 et 2).

Niveau 2 : analyse relative aux échecs de connexions selon les ASPSP (TPP 1).

Niveau 3 : analyse relative aux parcours de SCA selon les ASPSP (TPP 3).

La liste des ASPSP retenus pour l'étude AIS correspond à celle de l'étude PIS, à l'exception des entités suivantes :

- Monte Paschi, retirée car absente chez les 3 TPP.
- Banque Tarneaud et Banque Courtois, intégrées aux chiffres du Crédit du Nord car non représentatifs unitairement.

Soit un total de 16 ASPSP.

2. Constats relatifs aux activités d'accès aux comptes

Niveau 1 : analyse relative à la fiabilité globale des API selon les ASPSP (TPP1 et 2)

Méthodologie

Les données partagées correspondent aux requêtes d'accès aux comptes auprès des ASPSP réalisées par les TPP 1 et 2. Ces données ont été mensualisées afin d'obtenir des bases comparables entre TPP.

Une requête est équivalente à une connexion entre un TPP et un couple ASPSP-PSU, indépendamment du nombre de comptes de paiement disponibles au sein de l'ASPSP.

Ces requêtes peuvent aussi bien être initiées par le PSU que par le TPP, dans le second cas de figure, le nombre de requêtes est limité à 4 par jour.

Pour analyser les données, nous avons classifié les requêtes en fonction d'un premier échelon de statuts, comme suit :

- **SUCCESS** : correspond aux cas où la requête pour le rafraîchissement des données a été un succès.
- **NOT SUCCESS** : désigne les situations où le rafraîchissement des données a échoué.

Résultats

ASPSP	PART	SUCCESS
SG	8%	97%
Fortuneo	4%	97%
Crédit Mutuel - CIC	10%	97%
Crédit Agricole	18%	96%
Boursorama	10%	96%
Banque Populaire	8%	96%
Caisse d'Epargne	11%	96%
Bred	1%	95%
Crédit Coopératif	0%	95%
LCL	8%	94%
BNP Paribas	3%	92%
Arkéa	1%	90%
Sté Marseillaise de Crédit	0%	89%
Crédit du Nord	1%	89%
La Banque Postale	7%	85%
Axa Banque	0%	76%
TOTAL	**91%**	**95%**

Les établissements sélectionnés représentent 91% de l'ensemble des requêtes issues des échantillons de données fournis par les TPP 1 et 2.

- Le taux de succès est élevé, affichant une moyenne de 95%. Cette uniformité parmi les ASPSP suggère que les API sont généralement fiables.
- Au sein des acteurs représentants les grands volumes (> 5%) nous constatons que :
    - La Banque Postale, avec 7% des volumes, présente le taux de fiabilité le plus bas à 85%, ce qui est inférieur à celui des autres acteurs principaux dont les taux dépassent tous les 94%.
    - LCL, représentant 8% des volumes, a un taux de succès de 94%, proche de la moyenne.
    - SG, également à 8% des volumes, occupe la première place avec un taux de succès de 97%.

Niveau 2 : analyse relative aux échecs de connexions selon les ASPSP (TPP 1)

Méthodologie

Les données partagées correspondent aux requêtes d'accès aux comptes auprès des ASPSP réalisées uniquement par le TPP 1.

Dans le prolongement des analyses de niveau 1, des informations supplémentaires concernant les raisons des échecs de connexions ont été synthétisées et regroupées sous les statuts suivants :

- **FAILED** : signale une connexion qui n'a pas abouti, attribuable à un dysfonctionnement technique du côté de l'ASPSP ou du TPP.
- **SERVICE UNAVAILABLE** : indique une tentative de connexion infructueuse due à l'absence de réponse de l'ASPSP, suggérant un service indisponible au moment de la requête (maintenance par exemple).
- **SCA OR ACTION REQUIRED** : décrit les cas où la récupération de données a échoué en raison d'une SCA non finalisée ou d'une action requise de la part du PSU vis-à-vis de son ASPSP.

Résultats

ASPSP	PART	NOT SUCCESS	Origine du "not success"		
			FAILED	SERVICE UNAVAILABLE	SCA / ACTION REQUIRED
SG	8%	3%	27%	12%	60%
Fortuneo	4%	3%	8%	0%	92%
Crédit Mutuel - CIC	10%	3%	79%	2%	19%
Crédit Agricole	18%	4%	52%	25%	22%
Boursorama	10%	4%	23%	6%	71%
Banque Populaire	8%	4%	70%	3%	27%
Caisse d'Epargne	11%	4%	41%	7%	52%
Bred	1%	5%	20%	58%	22%
Crédit Coopératif	0%	5%	42%	3%	55%
LCL	8%	6%	53%	31%	16%
BNP Paribas	3%	8%	56%	22%	22%
Arkéa	1%	10%	16%	3%	81%
Sté Marseillaise de Crédit	0%	11%	NC	NC	NC
Crédit du Nord	1%	11%	NC	NC	NC
La Banque Postale	7%	15%	52%	16%	32%
Axa Banque	0%	24%	61%	7%	31%
TOTAL	**91%**	**5%**	**47%**	**14%**	**39%**

Les établissements sélectionnés représentent 91% de l'ensemble des requêtes issues de l'échantillon fourni par le TPP 1 ce qui reflète un taux d'échec moyen de 5%.

- Les dysfonctionnements techniques (47%) et les échecs de SCA (39%) sont de manière significative les grandes causes des échecs des connexions. Si les dysfonctionnements techniques représentent un enjeu technique, les SCA échouées peuvent être dues à des parcours de SCA non optimisés pour les PSU de la part de l'ASPSP.
- Les échecs attribuables à une absence de réponse sont en revanche relativement rares, représentant 14% (soit 0,7% du total). Une manière néanmoins de réduire ce chiffre serait de d'améliorer la communication des ASPSP en cas de maintenance de leurs API pour une meilleure anticipation.

Niveau 3 : analyse relative aux parcours de SCA selon les ASPSP (TPP 3)

Méthodologie

Les données partagées correspondent aux demandes de SCA (première demande et renouvellement) de la part des ASPSP à la suite d'une requête d'accès aux comptes réalisée par le TPP 3, initiée par lui-même ou par le PSU.

Une demande de SCA correspond à une authentification forte de la part d'un seul PSU auprès d'un seul ASPSP, indépendamment du nombre de comptes de paiement disponibles au sein de l'ASPSP.

Pour analyser les données, nous avons classifié les demandes de SCA en fonction d'un premier échelon de statuts, comme suit :

- **SUCCESS** : correspond aux cas où la SCA a été réalisée avec succès permettant un rafraîchissement des données.
- **NOT SUCCESS** : correspond aux cas où la SCA n'a pas été réalisée avec succès ne permettant pas un rafraîchissement des données.

Résultats

ASPSP	PART	SCA SUCCESS
Crédit Mutuel - CIC	13%	66%
Boursorama	6%	65%
La Banque Postale	14%	62%
SG	10%	61%
Caisse d'Epargne	10%	59%
Crédit Coopératif	0%	57%
LCL	6%	55%
Crédit Agricole	17%	53%
BNP Paribas	6%	52%
Sté Marseillaise de Crédit	0%	48%
Bred	2%	46%
Banque Populaire	6%	46%
Crédit du Nord	1%	44%
Arkéa	1%	39%
Fortuneo	1%	37%
Axa Banque	0%	32%
TOTAL	**92%**	**58%**

Les établissements listés représentent 92% de l'ensemble des demandes de SCA provenant de l'échantillon fourni par le TPP 2.

- Le taux de succès moyen de la SCA (58%) est faible et semble confirmer le constat de l'analyse de niveau 2 sur les parcours de SCA non optimisés pour les PSU.
- Parmi les taux les plus bas, nous constatons chez Fortuneo que la part très importante d'échecs de connexion due à la SCA (92% cf. Niveau 2) s'explique bien par un taux de réussite de la SCA très faible (37%) et non un effet de nombre. Effectivement, Fortuneo perd 10 places au classement (15e) par rapport aux classements des succès PIS (5e).
- L'ASPSP le plus sollicité, Crédit Agricole (17% de part) présente un taux de réussite de seulement 53%, soit 5 points en dessous de la moyenne constatée (58%). Alors 1er du classement PIS, le Crédit Agricole chute à la 8e place dans ce classement.
- LCL, le plus mal classé du classement PIS (16e) remonte très largement dans ce classement avec une 7e place.

Partie 3 - Recommandations

À la suite des différentes constatations énoncées précédemment, plusieurs recommandations sont formulées. Ces dernières visent à améliorer certains axes de la directive et contribuer plus largement à répondre aux enjeux portés par la DSP 2.

Ainsi, la prise en compte de ces recommandations permettrait de renforcer les apports tangibles de la DSP 2 en matière de protection des consommateurs et d'innovation.

Recommandation 1 : renforcer le suivi des parcours fonctionnels mis en place par les ASPSP afin de détecter toute problématique potentielle et assurer le succès des opérations intermédiées par des TPP.

Au vu des cas d'usage constatés, qui mettent en évidence des parcours fonctionnels perçus comme étant complexes, il est nécessaire de renforcer la surveillance par l'ACPR de ces derniers afin de limiter le nombre de transactions refusées et offrir une meilleure expérience au client final en faisant respecter les recommandations de l'EBA (utilisation de la biométrie par exemple).

Cette surveillance devrait permettre d'identifier des pratiques non conformes à la réglementation et de repérer des comportements déloyaux. Cela devrait permettre par la suite de convertir certaines transactions refusées en transactions validées et améliorer la fluidité des parcours.

Cela permettrait également de limiter, voire empêcher, l'utilisation de statuts intermédiaires comme des statuts finaux. A titre de rappel, la majorité des transactions étudiées ayant le statut "pending" sont des transactions ayant eu lieu il y a plusieurs mois. Or le statut "pending" n'est pas approprié dans ces cas d'usages.

Il est important de noter qu'un lien direct a pu être constaté entre les taux de succès des transactions et des parcours fonctionnels : des parcours fonctionnels ont été modifiés depuis mars 2023 ce qui a entraîné une nette hausse des transactions acceptées.

Il est essentiel de souligner que les parcours fonctionnels qui ne sont pas intermédiés par des TPP sont moins complexes. Ces différences dans les parcours clients constituent des obstacles à l'adoption et à l'utilisation des directives de la DSP2.

Recommandation 2 : renforcer le suivi des opérations intermédiés par des TPP afin de s'assurer de la bonne utilisation des statuts préconisés par STET.

Nous privilégions la mise en place d'un suivi par les Instances de Place visant à s'assurer de l'efficience des API mises en place par les ASPSP ainsi que le respect des normes STET dans les messages d'erreur et d'échanges.

Ceci doit permettre de s'assurer de la mise en place d'un écosystème vertueux traduit par des taux d'acceptation comparables à ceux sans TPP lors du parcours client et garantir une pleine concurrence loyale entre l'ensemble des acteurs de la Place.

Par ailleurs, une surveillance plus fine des statuts de niveau 1 et 2, de leur bonne utilisation par les différents ASPSP devrait permettre de tendre vers des statistiques plus homogènes.

Recommandation 3 : interdiction l'annulation de virement initié avec succès.

Certains établissements bancaires, dont la Société Générale, le Crédit Agricole et BNP Paribas, permettent à leurs clients d'annuler des virements initiés avec succès sur l'interface de l'application mobile.

Ce point va de fait à l'encontre de l'irrévocabilité du paiement et est utilisé par certains pour commettre des opérations frauduleuses.

Par ailleurs, ce type d'annulation n'est pas possible sur d'autres moyens de paiement comme la carte bancaire. Ainsi, si un client souhaite annuler un paiement et obtenir un remboursement, il doit pour cela s'entendre avec le commerçant et ne peut directement annuler un paiement.

Afin de lutter contre ce type de pratique, la généralisation du virement instantané est le moyen le plus efficace de renforcer cette notion d'irrévocabilité et de garantir l'arrivée des fonds sur le compte.

Toutefois et d'ici cette généralisation nous recommandons :

- Une interdiction de cette possibilité d'annuler en autonomie un virement initié et exécuté, notamment lors d'un virement à destination d'un commerçant, et d'autant plus lorsque cela est possible en totale autonomie sur le client
- A défaut d'interdiction, une communication et sensibilisation des ASPSP auprès de leurs clients et/ ou de leur réseau bancaire pour éviter ces pratiques
- Une vigilance du régulateur sur cette pratique favorisant la fraude et contraire à la réglementation.

Recommandation 4 : renforcer l'échange d'informations entre les acteurs de la Place au service d'une lutte contre la fraude plus efficiente.

Au regard de cette analyse, il apparaît que des informations indispensables à la lutte contre la fraude ne sont pas toujours partagées par l'ensemble des ASPSP et devraient être classées comme obligatoire et notamment :

- L'IBAN.
- Le nom du client détenteur du compte *Owner Name* (*Holder*).
- Le nom de la personne effectuant le virement (en particulier dans le cas où le client est une personne morale) (*Sender Name*).
- Une réelle utilisation du statut FRAD en cas de risque de fraude détectée par l'ASPSP lors d'une opération intermédiée par un PISP.

Fournir des informations détaillées sur l'expéditeur et l'IBAN permettrait d'assurer une transparence totale dans les transactions financières et permet aux bénéficiaires de vérifier facilement l'origine des fonds et de suivre les paiements.

Pour donner une perspective comparative, les grands réseaux de cartes sont actuellement beaucoup plus avancés en termes de pilotage et de surveillance. Des sanctions plus exhaustives existent, par exemple pour les demandes de transactions incomplètes, et elles sont appliquées de manière plus cohérente. Un modèle similaire devrait être envisagé pour réglementer les moyens de paiement, afin d'assurer une surveillance efficace et des sanctions appropriées.

Recommandation 5 : mettre en place des messages d'erreurs lors d'authentification en échec sur la *fallback* d'établissements bancaires.

Lorsqu'un user s'authentifie sur le *fallback* d'un établissement bancaire lors d'un parcours AIS ou PIS, et que cette authentification échoue, aucun message d'erreur ne s'affiche.

Mettre en place un message d'erreur permettrait de :

- Informer l'utilisateur sur la raison de l'échec et lui permettre de prendre les mesures appropriées, telles que vérifier ses identifiants.
- Diagnostiquer les problèmes techniques et permettre aux développeurs et aux équipes de support technique de résoudre les problèmes qu'il s'agisse d'une connexion réseau défaillante, d'une erreur de configuration ou d'un dysfonctionnement du système.
- Renforcer la sécurité en signalant les tentatives d'authentification frauduleuse.

Recommandation 6 : améliorer les communications des ASPSP sur les API et leur état de fonctionnement.

A l'instar d'initiatives visibles dans d'autres pays, il conviendrait pour s'assurer du bon respect de la DSP 2 et favoriser l'émergence d'un environnement techniquement pleinement opérationnel que les ASPSP renforcent leur communication et notamment sur les points suivants :

- Disponibilité des API (*healthcheck*), en veillant à :
    - Communiquer en temps réel et de façon publique le statut de fonctionnement des API.
    - Envoyer des alertes lors d'incidents détectés et recommander par exemple d'utiliser la fallback selon les occurrences.

  Ces informations pourraient être mises à disposition très simplement via une URL web. Cela faciliterait la surveillance proactive, le dépannage et la prise de décisions informées pour optimiser l'utilisation de l'API.
- Communication sur les niveaux de disponibilités des API et comparaison avec les niveaux de disponibilité observés sur les autres frontend bancaires *(cf. Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)).*
- Respect du délai légal de 3 mois (article 30 de la DSP2) de notification préalable en cas de modification des API.

Recommandation 7 : harmoniser les pratiques entre les établissements lors des requêtes automatiques initiées par les AISP vers les ASPSP.

Selon les données fournies par les AISP, il existe des divergences dans les méthodes employées par différents acteurs lors des requêtes automatiques vers les ASPSP pour le compte d'un PSU. En effet, certains AISP persistent à demander la SCA après un échec de connexion, diminuant ainsi leur taux de succès comparé à ceux qui, suite à une tentative infructueuse de SCA, ne formulent pas de demande immédiate subséquente. L'adoption d'une stratégie uniforme pourrait standardiser les statistiques, offrant des perspectives précises sur les parcours utilisateurs, y compris les taux de connexions réussies et échouées et ainsi permettre de mieux identifier les principales causes des connexions échouées.

Recommandation 8 : instaurer des messages d'erreur sur l'interface principale des établissements bancaires lors de l'échec de la SCA.

La SCA représente un des principaux irritants au taux de succès des connexions, or, actuellement, lorsqu'un utilisateur ou un TPP agissant pour son compte tente de s'authentifier auprès d'un ASPSP pour une première connexion ou un renouvellement de *token*, l'absence de message d'erreur en cas d'échec d'authentification est notable. Comme mentionné dans la recommandation 5, cette initiative aurait le double avantage d'identifier les pratiques potentiellement déloyales et de constituer une base de connaissances robuste pour affiner les parcours ultérieurement. De plus, cela fournirait des éléments concrets pour prioriser les actions visant à réduire les échecs de la SCA, des initiatives qui figurent notamment dans la proposition de règlement PSR de la Commission européenne (article 44).

Recommandation 9 : optimiser les parcours de SCA.

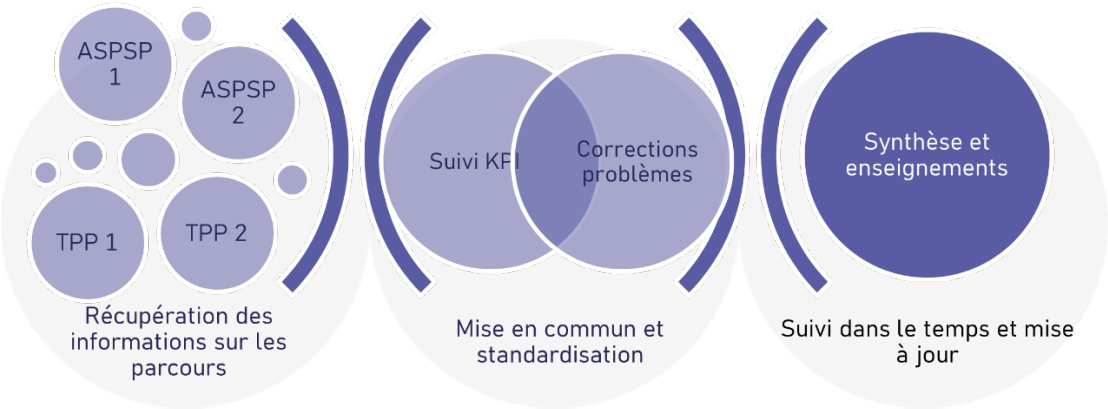
Suite à l'identification des causes principales des échecs de la SCA avec certains ASPSP, il serait judicieux de repenser les parcours afin d'assurer une expérience client améliorée, augmentant ainsi la probabilité de réussite de la SCA. Au-delà de l'élimination des pratiques déloyales (comme les demandes répétitives d'identifiants ou le non-respect de la règle des 180 jours), une expérience client optimisée pourrait se manifester par des parcours plus cohérents et fluides, en particulier lors des redirections entre AISP et ASPSP. De manière générale, un respect des recommandations de l'EBA (exemple avec l'utilisation de la biométrie) semble nécessaire.

Annexes (PIS)

A) Frame

Cette étude a été menée par le cabinet de conseil Frame, de mars 2023 à juin 2023.

Les travaux suivants ont été réalisés :



B) Framework STET PSD2 API

La documentation STET PSD2 API fait référence à la documentation technique fournie par STET (Société d'exploitation de la télétransmission) pour l'API liée à la mise en œuvre de la DSP2 (Directive sur les services de paiements).

L'API STET PSD2 fournit une interface standardisée permettant aux TPP d'accéder aux données et aux fonctionnalités des comptes bancaires des utilisateurs, avec leur consentement.

La documentation STET PSD2 API fournit des informations détaillées sur les endpoints, les paramètres, les formats de données et les flux d'autorisation nécessaires pour utiliser cette API conformément aux spécifications STET PSD2.

Cette documentation fournit notamment deux niveaux de validation des transactions, présentés sous forme de statut, permettant d'identifier l'état d'une transaction en cours ou aboutie.

(i) Statuts de premier niveau

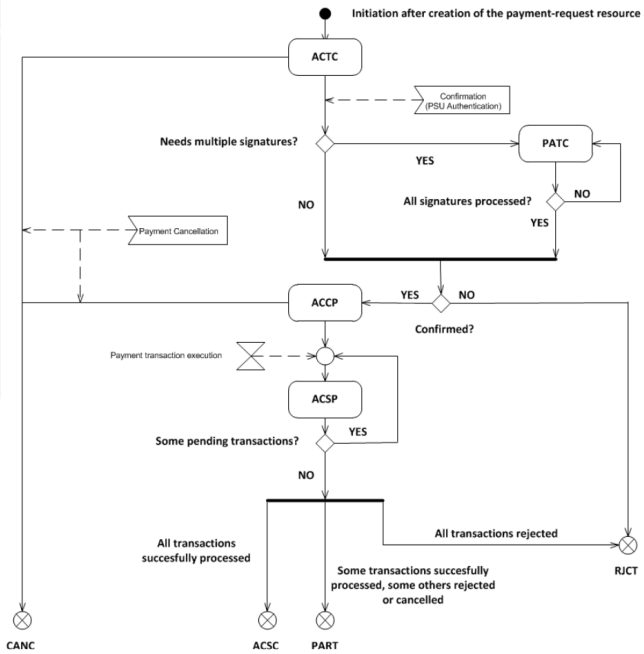
Les 13 statuts de premier niveau sont les suivants :

- ACCO (AcceptedCustomerCOnfirmed): The customer, during his/her authentication, has confirmed the payment request.
- ACCP (AcceptedCustomerProfile): Preceding check of technical validation was successful. Customer profile check was also successful.
- ACSC (AcceptedSettlementCompleted): Settlement on the debtor's account was completed. In the case of SCTInst, this status must not been set by the debtor's Bank before the reception of the positive confirmation.

- ACSP (AcceptedSettlementInProcess): All preceding checks such as technical validation and customer profile were successful. Dynamic risk assessment is now also successful and therefore the Payment Request was accepted for execution.
- ACTC (AcceptedTechnicalValidation): Authentication and syntactical and semantical validation are successful.
- ACWC (AcceptedWithChange): Instruction is accepted but a change will be made, such as date or remittance not sent.
- ACWP (AcceptedWithoutPosting): Payment instruction included in the credit transfer is accepted without being posted to the creditor customer's account.
- CANC (Cancelled): Payment initiation was successfully cancelled after having received a request for cancellation.
- PART (PartiallyAccepted): A number of transactions were accepted, whereas another number of transactions have not yet achieved 'accepted' status.
- PATC (PartiallyAcceptedTechnicalCorrect): Payment initiation needs multiple authentications, where some but not yet all were performed. Syntactical and semantical validations are successful.
- RCVD (Received): Payment initiation was received by the receiving agent.
- PDNG (Pending): Payment request or individual transaction included in the Payment Request is pending. Further checks and status update will be performed.
- RJCT (Rejected): Payment request was rejected.

Dans le cadre de cette étude, ces statuts ont été regroupés en 5 catégories : « accepted » (ACSC), « *partially accepted* » (PART), « *pending* » (ACCO, ACCP, ACSP, ACTC, ACWC, RCVD, PDNG), « *cancelled* » (CANC) et « *rejected* » (RJCT).

Parmi ces 5 statuts, 4 sont considérés comme des statuts « finaux », comme illustré ci-dessous :



Les statuts « *pending* » sont considérés comme des statuts intermédiaires.

(ii) Statuts de second niveau

Les statuts de deuxième niveau permettent de classifier les statuts rejetés (RJCT) de premier niveau en 21 catégories :

- AC01 (IncorectAccountNumber): the account number is either invalid or does not exist.
- AC04 (ClosedAccountNumber): the account is closed and cannot be used.
- AC06 (BlockedAccount): the account is blocked and cannot be used.
- AG01 (TransactionForbidden): Transaction forbidden on this type of account.
- AG03 (TransactionNotSupported): Transaction type not supported/authorized on this account.
- AM18 (InvalidNumberOfTransactions): the number of transactions exceeds the ASPSP acceptance limit.
- CH03 (RequestedExecutionDateOrRequestedCollectionDateTooFarInFuture): The requested execution date is too far in the future.
- CH04 (RequestedExecutionDateOrRequestedCollectionDateTooFarInPast): Value in Requested Execution Date or Requested Collection Date is too far in the past.
- CNOR (CreditorBankIsNotRegistered): Creditor bank is not registered under this BIC in the CSM.
- CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity.
- DS02 (OrderCancelled): An authorized user has cancelled the order.
- DUPL (DuplicatePayment): Payment is a duplicate of another payment. Can only be set by a PISP for a payment request cancellation.
- FF01 (InvalidFileFormat): The reject is due to the original Payment Request which is invalid (syntax, structure or values).
- FRAD (FraudulentOriginated): the Payment Request is considered as fraudulent.
- MS03 (NotSpecifiedReasonAgentGenerated): No reason specified by the ASPSP.
- NOAS (NoAnswerFromCustomer): The PSU has neither accepted nor rejected the Payment Request and a time-out has occurred.
- RR01 (MissingDebtorAccountOrIdentification): The Debtor account and/or Identification are missing or inconsistent.
- RR03 (MissingCreditorNameOrAddress): Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing.
- RR04 (RegulatoryReason): Reject from regulatory reason.
- RR12 (InvalidPartyID): Invalid or missing identification required within a particular country or payment type.
- TECH (TechnicalProblem): Technical problems resulting in an erroneous transaction. Can only be set by a PISP for a payment request cancellation.

Ces différentes catégories permettent d'informer le TPP de la raison du refus de la transaction.

C) Count API

Les données ont été comptabilisée de la manière suivante :

- 1 call API, aussi appelé « *count* », équivaut à une requête.

Ainsi, si lors d'une transaction plusieurs call API ont été effectué, plusieurs requêtes seront comptabilisées.