

**Groupe de travail « Interface DSP2 d'accès aux comptes de paiement »**

**Relevé des principales décisions**

***2019-2020***

<b>API et solution de secours</b>	
Les TPP doivent utiliser en priorité les API. En cas de dysfonctionnement, ils doivent le signaler à l'ACPR, suivant une procédure et avec un formulaire fournis par l'ACPR, et utiliser la solution de secours	31/07/2019 30/09/2019 (procédure)
Si les API ne fonctionnent pas au 14/09/2019, les ASPSP doivent documenter les fonctions manquantes pour que les TPP puissent utiliser l'accès direct	31/07/2019
La solution de secours ne doit pas pallier les manques de l'API. L'ASPSP ne peut pas se contenter d'une API incomplète ou inefficace	18/05/2020
Accord donné à l'utilisation du parallel run (connexion via l'API et l'accès direct en parallèle) tant que cette méthode permet d'accélérer la migration vers les API et qu'elle ne devient pas une solution de long-terme	05/03/2020
Les obligations en matière d'information préalable liées aux évolutions d'interface d'accès aux comptes s'appliquent aux ASPSP qui ont décidé de mettre à disposition une interface de banque en ligne adaptée.	18/05/2020
Les autorités rappellent que le recours à la fallback doit être transparent pour l'utilisateur, et notamment ne pas induire de réauthentification systématique de l'utilisateur (notamment si son jeton d'authentification est toujours dans sa période de validité de 90 jours)	29/09/2020

<b>Comptes accessibles</b>	
Les comptes de personnes protégées (enfants mineurs, personnes sous tutelle ou curatelle de l'utilisateur) doivent être intégrés dans l'API dès lors qu'ils sont disponibles au travers des interfaces de banque en ligne	05/03/2020
Les ASPSP ne peuvent pas intégrer un bouton de révocation des droits d'un TPP dans le tableau récapitulatif des consentements	15/06/2020
L'ACPR juge que les ASPSP n'ont pas à contrôler que les TPP n'accèdent que 4 fois par jour au compte d'un client. Les TPP étant des entités agréées, ils sont tenus de respecter les exigences réglementaires fixées par la DSP2, et c'est aux autorités compétentes de s'en assurer	02/04/2020
Les TPP doivent pouvoir en parallèle obtenir plusieurs jetons d'accès pour un même utilisateur de manière à leur permettre l'accès à des services différents à un même PSU (par exemple, en cas d'utilisation de services proposés par différents agents d'un même TPP)	20/01/2020

<b>Authentification forte</b>	
Seul un accord contractuel entre un TPP et un ASPSP peut conduire à une délégation de SCA	03/07/2019
Les ASPSP doivent communiquer la documentation de la SCA pour les solutions en accès direct ou de secours ; ainsi que surtout changement significatif de l'API sans délai	03/07/2019
Les ASPSP doivent commencer à déployer la SCA sur l'interface utilisateur et l'interface de secours à partir du 4 <sup>ème</sup> mois après la communication active de la documentation correspondante aux TPP	29/08/2019
Le déploiement de la SCA sur l'interface utilisateur devra couvrir une nette majorité des clients en janvier 2020 et être complètement achevé en mars 2020	29/08/2019
Le token d'authentification doit être accordé par l'ASPSP au TPP dès l'authentification du client réussie, indépendamment de la reconnexion de ce dernier à son service d'agrégation ou d'initiation	03/12/2019
Lors d'une SCA en redirection, la ressaisie d'une information constitue de facto un obstacle dans l'API dès lors que cette ressaisie n'est pas nécessaire dans l'accès via l'interface directe du l'ASPSP.	18/05/2020

Une redirection fluide (pas d'obstacles supplémentaires par rapport à ce que le client rencontre dans son espace de banque en ligne) est nécessaire pour être en conformité avec les RTS. Les ASPSP doivent donc tout mettre en œuvre pour que la redirection soit fluide, y compris en assurant le fonctionnement du app to app, le cas échéant, en proposant à court terme un autre mode d'authentification conforme à la réglementation et pour lequel la fluidité de parcours peut être assurée.	03/12/2019
L'exemption de solution de secours sur les API ne pourra être accordée aux établissements qui n'assurent pas une redirection fluide.	03/12/2019
La définition d'un parcours de redirection fluide proposée par le GT Afepame est validée : <ul style="list-style-type: none"> <li>- L'intégration de redirections automatiques entre TPP et ASPSP ou ASPSP et TPP.</li> <li>- Le principe de non-discrimination entre le parcours app-to-app et les parcours en accès direct (type banque en ligne).</li> <li>- L'absence de vérification de consentement ou d'étape le sous-entendant (case à cocher, mot « consentement », etc.).</li> </ul>	24/04/2020
Le parcours de redirection doit être familier pour l'utilisateur, c'est-à-dire ne pas générer des doutes quant à l'authenticité de la page de redirection (absence de logo, adresse URL suspecte...)	18/05/2020
L'exemption d'application de l'authentification forte du client pour l'accès aux informations sur les comptes de paiement est généralement utilisée pour la clientèle des particuliers. Concernant la clientèle des professionnels et des entreprises, la non- application de l'exemption de 90 jours devra être justifiée par l'ASPSP notamment en matière de confidentialité et de niveau de sécurité exigés. Pour cette clientèle, la règle des 4 accès par jour pour les TPP milite toutefois pour un token ayant une validité d'au moins 24h.	15/06/2020

### **Initiation de paiement**

Les bénéficiaires (dans les espaces de banque en ligne) et les bénéficiaires de confiance (DSP2) renvoient à des notions distinctes	05/06/2019
L'API doit proposer la même offre d'émission de virement que l'espace de banque en ligne. Si l'enregistrement préalable d'un bénéficiaire est nécessaire à l'émission d'un virement sur la banque en ligne, alors cette fonctionnalité doit être proposée aux PISP via l'API. Si cela est impossible, le virement à la volée doit être rendu possible	03/12/2019
La temporisation des nouveaux bénéficiaires enregistrés peut constituer une entrave à la fourniture des services d'initiation de paiement ; cette pratique devrait donc être évitée pour les opérations émises via l'API, étant entendu qu'elle pourrait être conservée à discrétion de l'ASPSP pour les opérations traitées via l'espace de banque en ligne	03/12/2019
Il serait préférable, dans l'intérêt des ASPSP et pour des raisons de sécurité, que les virements d'un compte de paiement vers un compte interne se fassent via les API	03/12/2019
L'étape de consultation du solde n'est pas nécessaire pour transmettre un ordre de paiement. Il n'est donc pas justifié d'imposer une deuxième SCA. Celle-ci constitue en effet un obstacle à l'exercice du service d'initiation de paiement	20/01/2020
La transmission d'informations clients des TPP (tels que l'adresse IP, les données de localisation, le terminal ou le navigateur utilisé...) vers les ASPSP ne doit pas être rendue obligatoire par ces derniers ; elle est toutefois possible sous réserve de respect des obligations en matière de protection de données individuelles et susceptible de renforcer les moyens de lutte contre la fraude de l'ASPSP au bénéfice de l'utilisateur.	05/03/2020 29/09/2020
Si la possibilité d'initier un virement sans IBAN est donnée au PISP, l'ASPSP doit tout de même fournir l'IBAN du payeur au moment de la confirmation quand la même information est montrée au client lorsqu'il fait un virement directement depuis sa banque en ligne.	24/04/2020

<b>Reporting</b>	
Demande d'envoi de remises mensuelles des ASPSP et des TPP sur l'avancement de la migration vers les API	05/11/2019
Demande aux ASPSP de répondre au questionnaire ACPR sur les obstacles à la migration vers les API sur la base de l'Opinion de l'ABE du 4 juin 2020	21/07/2020
Demande d'un calendrier de remédiation des points bloquants aux ASPSP et d'un calendrier de migration aux TPP pour la rentrée 2020	21/07/2020