CONSEIL CONSULTATIF DU COMMERCE CB

Position sur l'évolution de l'authentification forte des transactions cartes e/m commerce

dans le cadre de la Directive révisée sur les Services de Paiement

Conseil Consultatif du Commerce

AFTE Association Française des Trésoriers d'Entreprise

FCA FÉDÉRATION DU COMMERCE COOPÉRATIF ET ASSOCIÉ

fcd

fevad

Mercatel Pour le Commerce et la Distribution

U2P union des entreprises de proximité

CB

Octobre 2018

SOMMAIRE

PREAMBULE

A L'OBJECTIF DE CETTE CONTRIBUTION DU CONSEIL CONSULTATIF DU COMMERCE

La version finale des RTS SCA* publiée le 13 mars 2018 est le fruit de nombreux échanges entre plus de 200 parties prenantes des paiements en Europe. Des incertitudes subsistent à la lecture des textes et des interprétations divergentes émergent au sein de la Place européenne.

Cette contribution propose une interprétation fidèle à l'esprit des textes, cohérente avec des parcours clients démontrés et appréciés à la fois par les banques, les commerçants et les consommateurs. Il se fait l'écho de la volonté partagée par l'ensemble des acteurs de la nécessité de ne pas mettre en difficulté l'activité existante et future des commerçants, tant en proximité qu'en e-commerce.

La mise en œuvre de ces normes doit contribuer à l'objectif de baisse de la fraude en e/m commerce de manière générale. Il faut d'ailleurs souligner que cette fraude a connu en France une baisse significative pour la 6ème année consécutive comme le rappelle le rapport de l'Observatoire sur la sécurité des Moyens de Paiement publié le 10 juillet dernier.

Elle est destinée tant aux régulateurs qu'aux différentes parties prenantes du monde des paiements (émetteurs, acquéreurs, commerçants, prestataires d'acceptation technique …), et a pour objectif de permettre une mise en œuvre pragmatique des RTS SCA sur le terrain pour les paiements par carte.

- Trois sujets traités -

LE PERIMETRE DES RTS SCA

LES DEROGATIONS A L'AUTHENTIFICATION FORTE

L'ÉVOLUTION DES MÉTHODES D'AUTHENTIFICATION FORTE

** Règlement délégué (UE) 2018/389 de la commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client.*

B LE CONTEXTE REGLEMENTAIRE

La seconde version de la Directive européenne sur les Services de Paiement (DSP2) **s'applique depuis le 13 janvier 2018**. Cette nouvelle directive vise à :

1. Favoriser l'innovation sur le marché européen des services de paiement
2. Renforcer la sécurité des paiements et la protection des clients

Le considérant 95 de la DSP2 dispose que « *La sécurité des paiements électroniques est fondamentale pour garantir la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique. Tous les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude* »

Les normes techniques de règlementation (RTS – Regulatory Technical Standards) de la DSP2 ont été publiées par l'Autorité Bancaire Européenne (ABE) le 13 mars 2018 et entreront en vigueur le 14 septembre 2019. Ces RTS viennent compléter la DSP2 en lui donnant un cadre technique de mise en œuvre sur deux points :

- L'authentification forte pour les paiements électroniques (SCA – Strong Customer Authentication) ;
- Les normes ouvertes communes sécurisées de communication.

Les règles sur l'authentification forte des paiements électroniques vont générer des changements majeurs chez les parties prenantes du paiement électronique (commerçants, PSP émetteurs, PSP acquéreurs, PATs, …). Ce document présente notre interprétation partagée des normes techniques de réglementation sur l'authentification forte et vise à l'amélioration de la compréhension des textes par les acteurs du e/m commerce.

C LES TRAVAUX MENES DANS LE CADRE DU CONSEIL CONSULTATIF DU COMMERCE

1 Le Conseil Consultatif du Commerce (CCC)

Dans un contexte de transformation numérique et du déploiement de nouveaux parcours d'achats, le Conseil Consultatif du Commerce (CCC) au sein du Groupement des Cartes Bancaires CB associe ce dernier et 6 fédérations de commerçants. Le CCC répond au besoin de renforcer la coopération des acteurs du paiement, anticiper et co-construire des solutions et des services adaptés aux nouveaux environnements.

Il traite les thèmes suivants :

- La transformation des usages, des parcours d'achats et de paiement ;
- L'évolution des produits et des services de paiement CB ;
- L'innovation dans l'écosystème de paiement;
- La lutte contre la fraude et la sécurisation des données de paiement ;
- Les conséquences de l'entrée en vigueur de nouvelles régulations applicables au paiement (DSP2, RTS, RGPD…).

Le Conseil Consultatif du Commerce est notamment composé de 6 organisations professionnelles représentatives de toutes les formes de commerce* :

- Association Française des Trésoriers d'Entreprise (AFTE)
- Fédération du Commerce Coopératif et Associé (FCA)
- Fédération du Commerce et de la Distribution (FCD)
- Fédération du e-commerce et de la vente à distance (FEVAD)
- Mercatel
- Union des Entreprises de Proximité (U2P)

Les représentants du commerce

Cette initiative s'inscrit dans la continuité de la Stratégie Nationale des Moyens de Paiement qui vise à *« favoriser le développement des paiements par carte et des paiements sans contact en France et à étudier le potentiel ainsi que les impacts éventuels des nouvelles technologies de paiement qui viendraient à apparaître, notamment dans le domaine des portefeuilles électroniques, paiements mobiles, paiements instantanés, etc. ».*

2 Le groupe de travail sur l'authentification forte

Dans le cadre de ce CCC, un groupe de travail dédié au sujet de l'authentification forte pour les achats à distance réalisés avec une carte bancaire CB a été mis en place en novembre 2017*.

Ce groupe d'experts a élaboré ce document qui ne constitue pas une position juridique.

Huit ateliers de travail en présence des commerçants, des organisations professionnelles, des Banques et CB ont été consacrés à :

- Les conséquences opérationnelles des RTS SCA (périmètre, dérogations, …)
- Les cinématiques de paiement par carte impactées par l'application des RTS SCA
- La conception de solutions pour obtenir des parcours sécurisés et fluides
- L'évolution des méthodes d'authentification forte

** L'Union des Métiers et des Industries de l'Hôtellerie (UMIH) n'est pas membre du CCC mais a participé aux travaux.*

1 LE PERIMETRE D'APPLICATION DE L'AUTHENTIFICATION FORTE

A INTERPRÉTATION DES TEXTES

Pour entrer dans le périmètre des RTS SCA, une opération de paiement doit remplir 2 critères :

1. Être un paiement électronique
2. Être initiée par le payeur (personne physique ou morale)

1 Les paiements électroniques

Les RTS SCA s'appliquent uniquement aux paiements électroniques comme indiqué dans le considérant (1) des RTS SCA. Ils englobent notamment :

- Les paiement électroniques par cartes bancaires.
- Les virements électroniques.

Les prélèvements (à l'exception des mandats de prélèvement SEPA électroniques) et les paiements non électroniques par carte (ex : MO/TO) paraissent exclus du champ d'application des RTS.

Cette contribution se focalise uniquement sur le cas des paiements électroniques à distance par carte

Dans le cas particulier où le client utilise une solution de paiement embarquée dans un mobile (un wallet) pour payer en magasin, le paiement peut se dérouler :

- Soit sans passage en caisse, avec une interaction à distance entre le wallet et le système d'information du commerçant :
  - ➔ ***ces transactions sont considérées comme à distance et donc incluses dans le périmètre de ce document.***
- Soit avec un passage en caisse et une interaction entre le wallet et un système d'encaissement : il s'agit alors d'un paiement sans contact de proximité quelle que soit la technologie d'interaction (NFC, QR code, etc.) :
  - ➔ ***ces transactions sont considérées comme sans contact de proximité et donc non couvertes dans le périmètre de ce document.***

Les paiements par courrier et téléphone ne sont pas des paiements électroniques

Nous comprenons que les paiements initiés par courrier ou par téléphone (MO/TO) sortent du cadre d'application des RTS SCA. Ils doivent néanmoins continuer à bénéficier des dispositifs de lutte contre la fraude mis en place par les différents acteurs.

Considérant 95 de la DSP2 : « *Tous les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude. Il ne semble pas nécessaire de garantir le même niveau de protection aux opérations de paiement initiées et exécutées par des moyens autres que l'utilisation de plates-formes ou de dispositifs électroniques, telles que les opérations de paiement sur support papier, les ordres de paiement passés par courrier ou par téléphone.* »

2 Les paiements par carte initiés par le payeur vs déclenchés par le commerçant

Seules les opérations initiées par le payeur entrent dans le champ d'application du RTS SCA. Selon notre compréhension du texte il s'agit de :

« Toute opération de paiement ou toute série d'opérations de paiement par carte ayant fait l'objet d'un consentement ad hoc du client pour un montant global maximum déterminé »

A contrario, toute opération de paiement pour laquelle lors de l'achat du bien ou du service :

- Le montant ne peut être ni déterminé, ni estimé par le commerçant,

et

- Le consentement du payeur sur ce montant déterminé ne peut pas être recueilli.

devrait être considérée comme une opération déclenchée par le commerçant et être hors du champ d'application des RTS SCA ou bénéficiant d'une exemption.

Cette position s'appuie sur deux éléments :

- L'article 5 des RTS SCA dispose que l'authentification du porteur est *« spécifique au montant de l'opération ».* Cela implique que le commerçant puisse définir le montant global du paiement ou de la série de paiements.
- Le considérant (5) précise *que « pour les situations dans lesquelles le montant final n'est pas connu au moment où le payeur initie une opération de paiement électronique à distance »* l'authentification forte du client « soit spécifique au montant maximal auquel le payeur a donné son consentement ».

Les opérations de paiement hors champ des RTS SCA ou bénéficiant de dérogations doivent faire l'objet de mesures de lutte contre la fraude, de la même manière que les opérations concernées par les RTS SCA.

Les paiements « One Leg » ?

Les paiements « one leg » font référence aux opérations de paiement pour lesquelles un des prestataires de services de paiement participant à l'opération de paiement est basé hors de l'Union Européenne.

Dans la DSP2, l'article 2 qui présente le champ d'application de la nouvelle directive limite le périmètre *« aux opérations de paiement dans la devise d'un État membre lorsque le prestataire de services de paiement du payeur et celui du bénéficiaire sont tous deux situés dans l'Union ou lorsque l'unique prestataire de services de paiement intervenant dans l'opération de paiement est situé dans l'Union ».*

Une opération de paiement entre dans le champ d'application de la DSP2 et donc de l'authentification forte uniquement si le PSP émetteur ET le PSP acquéreur sont dans l'Union Européenne.

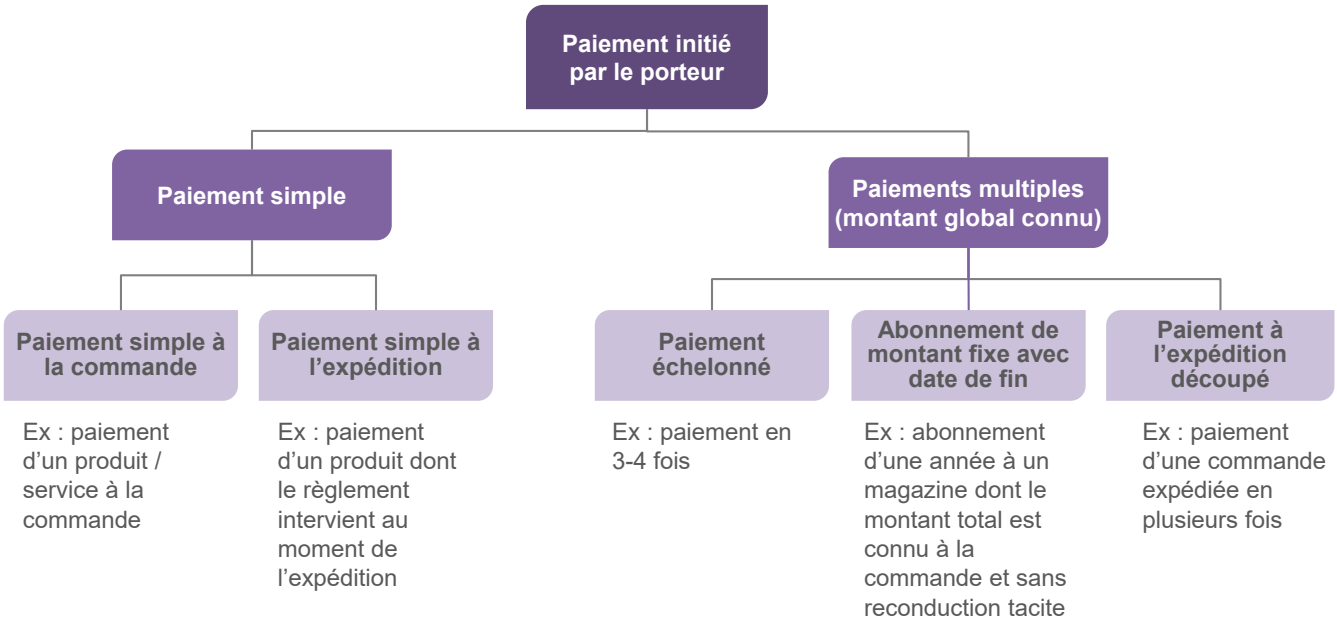
Dans ce contexte, **nous prenons acte que les opérations de paiement « one leg » n'entrent pas dans le périmètre d'application des RTS SCA.**

Cette interprétation est confirmée par l' « Opinion Paper » de l'EBA publié le 13 juin 2018 qui dispose que les PSP émetteurs sont tenus de fournir les « meilleurs efforts » pour respecter les RTS SCA dans les paiements one leg. La notion de « meilleurs efforts » devra être explicitée par le Régulateur.

B ETUDE DES CAS DE PAIEMENT

1 Les cas d'usages de paiement initiés par les porteurs

Le graphique ci-dessous présente les cinématiques de paiement initiées par le porteur (voir glossaire),



Le paiement peut être initié par le porteur :

- Par saisie de ses informations carte
- Par l'utilisation d'une solution de wallet fournie par son PSP
- Par l'utilisation d'une application proposée par le commerçant (Card on file/wallet tiers commerçant) dans laquelle le porteur a préalablement enregistré ses informations cartes.

Ces trois cas de figure entrent dans le champ d'application des RTS SCA.

Note : les paiements « One Click » à partir d'une application commerçant sont souvent exempts d'une authentification forte par l'émetteur car le commerçant considère que sa connaissance du client et ses outils de gestion du risque sont suffisants. Dès septembre 2019 ces paiements « One Click » pourront donner lieu à une authentification forte par l'émetteur si aucune dérogation prévue par les RTS ne s'applique.

2 cas particuliers

Enregistrement / renouvellement

Le cas d'enregistrement ou de renouvellement d'une carte dans un wallet tiers **fait également partie des cas entrant dans le cadre d'application des RTS SCA** et nécessite une authentification forte,

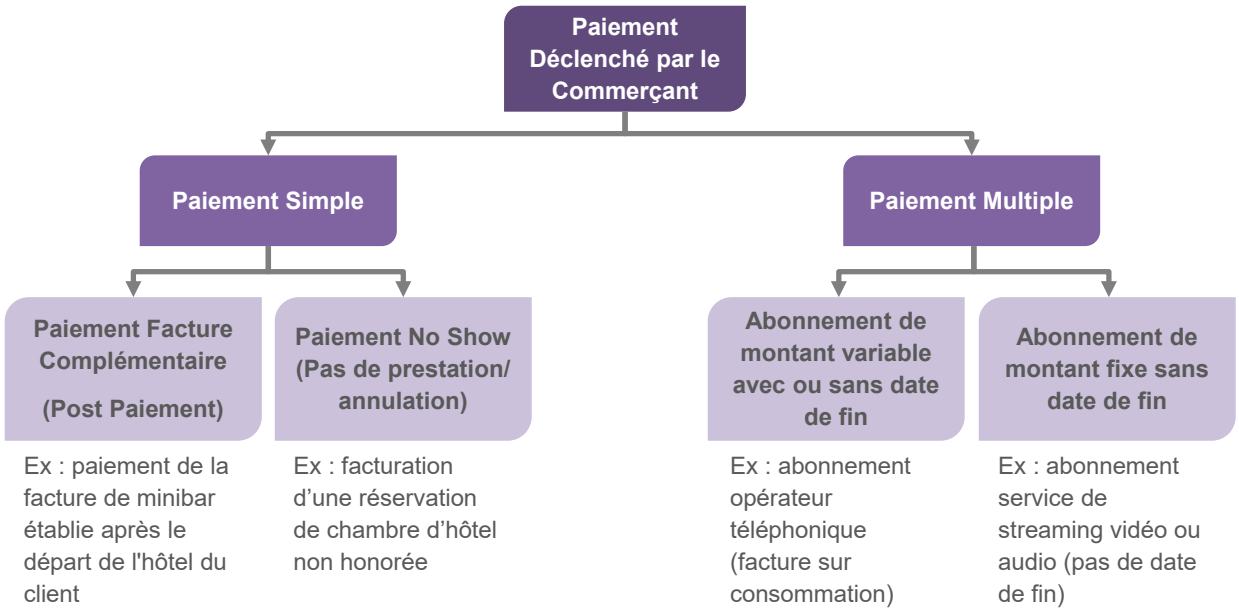
Paiements échelonnés avec remboursement partiel

Cette situation implique une **réévaluation à la baisse** du montant des paiements restants.

Cela n'a **pas d'impact sur l'exemption d'authentification forte** du porteur sur les paiements de rang supérieur à 1 car le porteur avait donné son accord sur un montant maximal (**cf. considérant 5**).

2 Les cas d'usages de paiement déclenchés par les commerçants

Le graphique ci-dessous présente les cas de paiement déclenchés par les commerçants en l'absence du porteur pour lesquels l'authentification forte ne peut pas être opérationnellement mis en œuvre. Pour éviter la remise en cause de ces usages il conviendrait de les placer hors du champ d'application des RTS SCA ou bien de les faire bénéficier d'une exemption à l'instar de celle prévue par l'article 14.



Ces cas de paiement ne peuvent faire l'objet d'une authentification du porteur pour les raisons suivantes :

- **Paiement de facture complémentaire** : Le commerçant déclenche le paiement par carte postérieurement à la fourniture/consommation de la prestation complémentaire, en dehors de la présence du porteur et sans interaction préalable avec ce dernier pour recueillir son consentement. L'authentification forte ne peut opérationnellement pas être mise en œuvre dans ce cas d'usage.
- **Paiement No Show :** Le commerçant déclenche le paiement par carte en dehors de la présence du porteur et sans interaction préalable avec ce dernier. Une authentification porteur a pu être réalisée au moment de la réservation, sur un montant éventuellement plus important.
- **Paiement d'abonnements de montant variable ou de montant fixe** et de durée indéterminée (en dehors de la première transaction) : le commerçant déclenche le paiement à chaque échéance de l'abonnement pour le montant de la prestation consommée pendant l'échéance. Celle-ci ne peut être ni connue, ni estimée au moment de la conclusion du contrat. Le client ne peut pas s'authentifier sur un montant global défini au moment de la conclusion du contrat. Le commerçant déclenche le paiement en dehors de la présence du porteur et sans interaction préalable avec ce dernier. Conditionner le paiement à l'authentification forte du porteur dans ce cas d'usage complexifierait le parcours client et pourrait entrainer la suspension de la prestation.

Note : Le fait que les paiements soient réalisés à des fréquences irrégulières n'est pas un motif de sortie du périmètre des RTS SCA, si le montant global est connu au moment de la conclusion du contrat entre le commerçant et le porteur.

Cas des paiements dont le montant est défini postérieurement à la prestation

Les paiement dont le montant est défini postérieurement à la prestation ne sont pas traités dans le cadre de ce document. Notamment rencontrés dans le cadre de prestations de mobilité urbaine / VTC), ils feront l'objet de travaux complémentaires avec des professionnels du secteur et une concertation au niveau européen.

2 LES DEROGATIONS A L'AUTHENTIFICATION FORTE

A PRESENTATION GENERALE DES DEROGATIONS

La mise en œuvre des dérogations sur l'authentification forte doit doit s'inscrire dans l'objectif général de réduction de la fraude des RTS. Elle nécessite de maintenir et de renforcer l'ensemble des dispositifs de lutte contre la fraude sur l'ensemble de la chaine : commerçants, PSP et schéma carte. Le Régulateur a fixé 5 dérogations optionnelles à l'obligation d'authentification forte du payeur concernent les paiements par carte à distance.

1. Bénéficiaire de confiance *(Art 13)*

La liste des bénéficiaires de confiance est déclarée par le porteur auprès de son PSP émetteur, en réalisant une authentification forte. C'est donc uniquement ce dernier qui peut appliquer la dérogation.

2. Opérations de faible valeur *(Art 16)*

Cette dérogation est valable pour toutes les opérations de paiement d'un montant inférieur ou égal à 30€ dans la limite, au choix de l'émetteur, soit d'un montant cumulé de 100€, soit de 5 transactions consécutives. Le PSP émetteur est donc le seul à pouvoir appliquer la dérogation.

3. Procédures et protocoles de paiement sécurisés par les entreprises *(Art 17)*

Nous considérons que cette dérogation vise les paiements initiées par des payeurs « personnes morales » et requiert des processus spécifiques de sécurisation dont le niveau de sécurité satisfait les autorités compétentes. S'inscrivent dans ce cadre :

- Les factures crédit par carte/ transferts de fonds déclenchés par les commerçants ;
- Les cartes entreprises de types achats ou logés.

4. Analyse des risques liée à l'opération *(Art 18)*

Cette dérogation peut être appliquée par le PSP émetteur suite à une analyse de risque de la transaction sous condition qu'à la fois le PSP acquéreur et le PSP émetteur aient un taux de fraude sous les seuils définis dans les RTS SCA. L'acquéreur ou l'accepteur peuvent demander à bénéficier de cette dérogation.

5. Opérations récurrentes *(Art 14)*

Cette dérogation peut être appliquée pour les opérations suivant la première opération initiée par le porteur. Le commerçant doit informer les PSP acquéreur et émetteur que l'opération de paiement entre dans cette dérogation en l'informant qu'il s'agit d'un paiement récurrent consécutif à un premier paiement ayant fait l'objet d'une authentification forte.

Le commerçant / acquéreur peut demander au PSP émetteur de bénéficier d'une dérogation. A cette fin, il est fortement recommandé que le commerçant ou son PAT fournisse au PSP émetteur les éléments de gestion du risque dont :

- L'enrichissement des données du contexte de l'opération à l'authentification et à l'autorisation.
- L'appréciation par le commerçant de son niveau de risque (en s'appuyant sur les outils dont il dispose).

L'émetteur décide en dernier ressort d'appliquer ou non la dérogation en s'appuyant sur les éléments fournis par les commerçants, les informations de gestion de risque fournies par le schéma carte et sa propre gestion du risque. Le CCC considère qu'il faut favoriser la mise en œuvre des dérogations dès que cela est possible afin de préserver la fluidité des parcours clients sur internet.

Une seule dérogation est suffisante

Répondre aux critères d'un seul cas de dérogation est suffisant pour en bénéficier. Par exemple, une transaction qui entre dans le cadre de la dérogation petits montants sera bien exemptable d'authentification forte même si elle ne satisfait pas aux exigences de la dérogation « Analyse des risques ».

B ZOOM SUR LA DÉROGATION : ANALYSE DES RISQUES LIÉS À L'OPÉRATION

L'article 18 des RTS dispose : « Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client lorsque le payeur initie une opération de paiement électronique à distance que le prestataire de services de paiement considère comme présentant un faible niveau de risque conformément aux mécanismes de contrôle des opérations visés à l'article 2 et au paragraphe 2, point c), du présent article ».

CB, ses membres et les e-commerçants CB mettent en œuvre les actions nécessaires pour poursuivre la réduction de la fraude sur Internet observée depuis 4 ans sur les transactions CB.

Ces actions doivent notamment permettre de maintenir un taux de fraude pour les paiements électroniques à distance inférieurs à 100€ en dessous du seuil de référence de 0,13% fixé par les RTS SCA.

Le respect de cet objectif permettra de préserver la fluidité des parcours clients des porteurs CB sur internet pour près de 85% des transactions en limitant le recours à l'authentification forte aux seules transactions à risque (authentification passive/ frictionless dans les autres cas).

Objectif 0,13%

L'atteinte de ce cet objectif par tous les PSP nécessite la mise en œuvre de plusieurs actions, notamment :

- Une identification de la « friendly fraud » et son exclusion du calcul des taux de fraude utilisés dans le cadre de la dérogation TRA (article 18).
- L'amélioration continue des outils de lutte contre la fraude de l'ensemble des acteurs (e-commerçants, PSP, schéma carte).

1 Le déclenchement de la dérogation sur l'analyse des risques (TRA) est sous la responsabilité des PSP émetteurs et acquéreurs

« Les prestataires de services de paiement qui entendent exempter des opérations de paiement électronique à distance de l'authentification forte du client au motif qu'elles présentent un risque faible tiennent au moins compte des facteurs suivants liés aux risques :

a) Les habitudes de dépenses antérieures de l'utilisateur individuel de services de paiement ;

b) L'historique des opérations de paiement de chacun des utilisateurs de services de paiement du prestataire de services de paiement ;

c) La localisation du payeur et du bénéficiaire au moment de l'opération de paiement dans les cas où le dispositif d'accès ou le logiciel est fourni par le prestataire de services de paiement ;

d) L'identification de comportements de paiement anormaux de l'utilisateur de services de paiement par rapport à l'historique de ses opérations de paiement » (art 18 3 b) des RTS SCA ».

L'Opinion Paper de l'ABE considère que l'application de la dérogation nécessite que **les deux PSP participant à l'opération de paiement par carte soient éligibles à la dérogation** en respectant les seuils de fraude définis.

Cependant, nous considérons que seul le taux de fraude du PSP émetteur est déterminant dans l'application des dérogations de l'article 18 :

- **En s'appuyant sur les informations communiquées en amont (notamment par le commerçant et son PSP), seul le PSP émetteur, avec sa connaissance de ses porteurs et de leurs habitudes, est à même de finaliser l'analyse complète du risque en respectant les différents facteurs mis en avant dans le texte.**
- **La prise en compte du taux de fraude du PSP acquéreur n'est pas pertinente et risque de complexifier et de réduire la possibilité d'activation effective de la dérogation TRA.**

2 Définition de la fraude

L'article 96(6) de la DSP2 dispose que les PSP doivent fournir à l'EBA les données de fraude sur les différents moyens de paiement.

Pour permettre une application uniforme à travers les différentes juridictions, l'EBA a publié en août 2017 un draft de support de déclaration trimestrielle et annuelle. Une version stabilisée a été publiée le 18 juillet 2018.

La notion de fraude variant dans les différents pays de la zone UE, l'EBA a fourni les catégories de fraude dans son draft du formulaire de report de fraude partagé en août 2017 (cf. encadré ci-contre).

La deuxième catégorie définie ci-contre correspond à de la **«first party fraud / friendly fraud ».**

Les catégories de fraude carte

1. Un paiement non-autorisé résultant d'une perte, d'un vol ou d'un détournement des données sensibles de paiement ou d'un moyen de paiement qu'il soit détectable ou non par le payeur avant le paiement qu'il soit causé par une négligence du payeur ou exécuté en l'absence du consentement du payeur.
2. Un paiement fait et réalisé par le payeur mais qui fait l'objet d'une contestation de sa part (malhonnête ou non), avec ou sans intention de réaliser un gain pour lui ou autrui.
3. Les opérations de paiement étant réalisées à la suite d'une manipulation du payeur.

La «first party fraud/ friendly fraud » peut être :

- involontaire : le payeur conteste une opération de paiement qu'il a réellement initiée dans les faits, mais dont il ne se souvient plus ou bien dont il n'a pas connaissance. Ex: achat effectué par un membre de son entourage à son insu,
- volontaire : le porteur conteste sciemment une opération de paiement qu'il a réellement initiée afin d'en tirer un bénéfice financier.

Nous considérons que la « first party fraud» ne doit pas entrer dans le calcul des taux de fraude pour la dérogation d'analyse de risque. Selon la clarification apportée par l'ABE, le 18 juillet 2018 dans ses « Guidelines on fraud reporting under PSD2 », la «first party fraud» ne doit pas être reportée.

CB et ses membres travaillent à l'identification de cette fraude.

Une baisse attendue de la fraude

Le renforcement des outils de lutte contre la fraude qui accompagneront la mise en œuvre du RTS contribueront à réduire l'ensemble des types de fraude.

Il permettra également de réduire la «friendly fraud / first party fraud» particulièrement élevée chez certains commerçants du fait du faible taux d'authentification forte mis en œuvre.

C ZOOM SUR LA DÉROGATION : BÉNÉFICIAIRES DE CONFIANCE

L'article 13 des RTS SCA, dédié à la dérogation « bénéficiaires de confiance », dispose :

1. *Les prestataires de services de paiement appliquent l'authentification forte du client lorsqu'un payeur crée ou modifie une liste de bénéficiaires de confiance par l'intermédiaire du prestataire de services de paiement gestionnaire de son compte.*
2. *Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences générales en matière d'authentification, lorsque le payeur initie une opération de paiement et que le bénéficiaire figure dans une liste de bénéficiaires de confiance préalablement créée par le payeur.*

Pour les commerçants, la mise en place de cette dérogation est primordiale car elle s'applique aux les opérations de paiement de montant supérieur à 100€, qui représentent 15% des opérations de paiement CB et plus de 30% des montants.

Sa mise en place permettra donc de maintenir des conditions de fluidité indispensable pour les paiements de type One Click largement plébiscités par les clients et synonymes de gain de temps et de facilité d'usage.

La mise en place de cette dérogation nécessite des travaux complexes dont certains ont cependant été identifiés dans le cadre du groupe du travail :

- La construction du dispositif global de mise en place de cette dérogation devra surmonter plusieurs difficultés :
  - La nécessité d'engager des développements du système informatique côté PSP émetteur pour rapprocher les systèmes d'information carte et ceux de la banque en ligne ;
  - La nécessité de gérer les multiples identifiants d'un même commerçant / de reconnaître l'ensemble des commerçants français et internationaux ;
  - La nécessité de mettre en place un parcours fluide de déclaration d'un bénéficiaire et de validation du bénéficiaire par le porteur sur l'espace sécurisé de son PSP.
- Si ils souhaitent la mettre en œuvre dans des conditions optimales, les PSP émetteurs vont devoir travailler avec tous les acteurs à la construction d'un dispositif dont la charge leur incombe en grande partie.

De manière générale, le fait de réunir toutes les conditions pour parvenir à appliquer ces dérogations à l'authentification forte est un enjeu important pour favoriser la fluidité des parcours clients et, en particulier, pour les commerçants au panier moyen élevé.

Le groupe de travail va poursuivre les travaux pour lever les freins et favoriser la mise en place de cette dérogation tout en maitrisant le risque de fraude.

D ZOOM SUR LA DÉROGATION : OPERATIONS RECURRENTES

L'article 14 des RTS SCA, dédié à la dérogation pour les « opérations récurrentes », dispose :

1. *Les prestataires de services de paiement appliquent l'authentification forte du client lorsqu'un payeur crée, modifie ou initie pour la première fois une série d'opérations récurrentes ayant le même montant et le même bénéficiaire.*
2. *Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client, sous réserve du respect des exigences générales en matière d'authentification, pour l'initiation de l'ensemble des opérations de paiement ultérieures comprises dans la série d'opérations de paiement visées au paragraphe 1.*

Rappelons que les paiements qui entrent dans cette dérogation sont uniquement les opérations récurrentes de même bénéficiaire, de même montant, et dont le montant global maximum est déterminable. Nous comprenons que pour ces cas**, le PSP émetteur doit réaliser une authentification forte lors de la création, la modification ou pour la première opération d'une série de paiements.** Ensuite, l'opération bénéficie de la dérogation pour les paiements de rang suivant.

Le groupe de travail s'interroge sur la nécessité de procéder à une authentification forte systématique sur le premier paiement.

Il est demandé dans quelle mesure, pourrait relever de la décision du PSP émetteur, la décision d'appliquer ou non une authentification forte pour la première opération d'une série d'opérations récurrentes sous réserve :

- **de l'analyse de risque du PSP émetteur,**
- **et du fait que cette première opération puisse entrer dans le cadre d'une autre dérogation prévue par le RTS.**

Dans le cadre d'un abonnement de même montant avec reconduction tacite comme un abonnement de type « musique en ligne», « vidéo à la demande », « dating », seul le premier paiement entre dans le périmètre des RTS. Ensuite, les échéances sont en dehors du périmètre d'application des RTS et ne nécessitent pas d'authentification forte du client.

Opérations récurrentes initiées avant le 14 septembre 2019

Le RTS SCA entrent en vigueur le 14 septembre 2019, toutes les opérations initiées préalablement n'entrent pas dans son champ d'application.

3 L'ÉVOLUTION DES MÉTHODES D'AUTHENTIFICATION FORTE

A L'AUTHENTIFICATION FORTE EN FRANCE

Définition de l'authentification forte dans les RTS SCA

Selon la DSP2, une authentification forte du client implique la vérification d'au moins deux catégories différentes parmi les 3 catégories suivantes :

- Un élément de connaissance : ce que l'utilisateur sait (mot de passe, PIN, …)
- Un élément de possession : ce que l'utilisateur possède (token, mobile, carte, …)
- Un élément d'inhérence : ce que l'utilisateur est (empreinte digitale, reconnaissance faciale, …)

Avec la révision de la Directive européenne sur les Services de Paiement, l'authentification forte du payeur devient obligatoire, sauf dérogation sous la responsabilité des PSP émetteurs. De ce fait, les commerçants perdent dans la majorité des cinématiques de paiement la maîtrise finale de la demande d'authentification qui relève désormais de la responsabilité des PSP émetteurs.

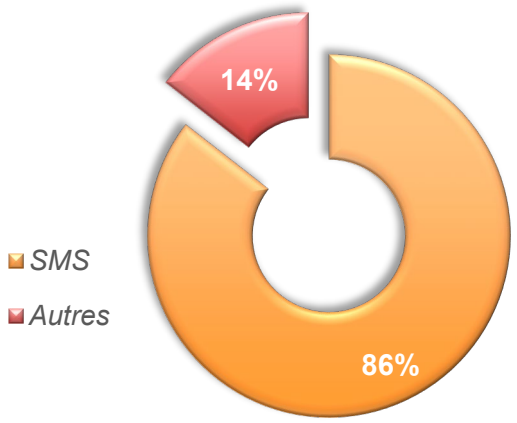
Dans ce cadre, il est important pour les commerçants de s'assurer que les méthodes d'authentification forte appliquées par les PSP émetteurs seront efficaces et fluides, afin de ne pas altérer la qualité des parcours client, notamment au sein des applications mobiles.

Nous avons lancé auprès de 7 grands PSP émetteurs français **une étude sur les méthodes d'authentification** utilisées actuellement, ainsi que sur les évolutions à venir.

Cette étude révèle que l'OTP SMS (One Time Password) est de loin la méthode d'authentification la plus utilisée par les PSP émetteurs (86%) suivi de l'authentification via l'application banque mobile (12%).

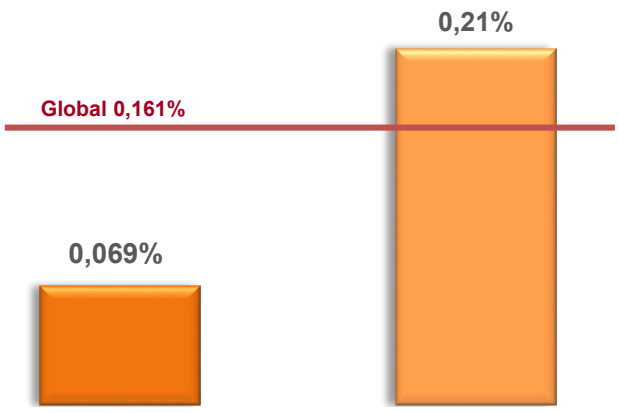
On observe un taux global de fraude sur les opérations de paiement à distance avec une authentification 0,06% vs. 0,21% en cas d'absence d'authentification. Cette étude illustre l'efficacité du l'OTP SMS dans la réduction de la fraude sur les opérations de paiement à distance.

Répartition des méthodes d'authentification utilisées



Source :
Echantillon de 7 établissements CB sur 2017-2018

Taux de fraude 3DS vs hors 3DS sur les transactions VAD



Sources OSMP 2017

B LA NECESSITE DE TRAVAILLER À DES METHODES ALTERNATIVES AU ONE TIME PASSWORD (OTP) SMS

L'OTP SMS est la méthode d'authentification la plus répandue chez les PSP émetteurs en France (86%).

Cette méthode a l'avantage de ne pas nécessiter que le porteur possède un smartphone ou installe l'application mobile de sa banque.

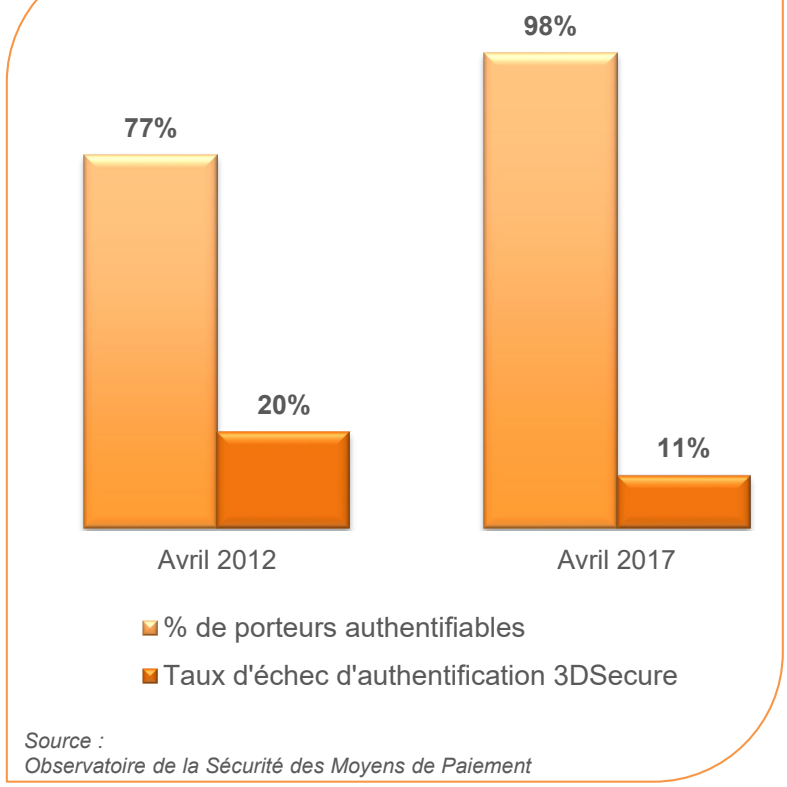
Elle est en outre relativement simple à utiliser pour le porteur et déjà adoptée par la grande majorité des acheteurs en ligne.

On observe qu'en 2017, 98% de porteurs peuvent être authentifiés, en majeure partie via l'OTP SMS.

C'est l'aboutissement de plusieurs années de travail par les PSP émetteurs.

En parallèle, le taux d'échec d'authentification forte a été fortement réduit et est passé de 20% à 11% entre 2012 et 2017.

Evolution du % de porteurs authentifiables et du taux d'échec d'authentification 3DS



Source :
Observatoire de la Sécurité des Moyens de Paiement

Plusieurs questions se posent sur l'utilisation de l'OTP SMS :

1. La méthode est potentiellement vulnérable à certains types d'attaques ;
2. Les serveurs SMS des opérateurs rencontrent des problèmes de fiabilité, souvent pendant les pics de consommation ;
3. **La conformité de cette méthode vis-à-vis des RTS SCA est remise en cause par l'ABE**. En effet, l'OTP SMS permet de valider la **possession** du téléphone via l'envoi d'un code unique. Ainsi, cette méthode valide un seul facteur (la possession) et devrait être associée à un second élément de connaissance ou inhérent à l'utilisateur pour être conforme,

Dans ce cadre, une stratégie de **migration progressive** vers de nouvelles méthodes d'authentification forte doit être mise en place, en concertation avec l'ensemble des acteurs.

En attendant le déploiement de méthodes d'authentification alternatives, les acteurs du groupe de travail souhaitent poursuivre **l'utilisation de l'OTP SMS dans le cadre des RTS SCA. Cette méthode a contribué à faire baisser significativement les taux de fraude pour les paiements carte e/m commerce, a été adoptée massivement par les clients et possède l'avantage de ne pas nécessiter un smartphone avec une connexion internet,**

Le développement de nouvelles méthodes d'authentification forte plus fiables, plus fluides, et adaptées à tous les parcours client digitaux doit être encouragé.

Authentification banque mobile

L'authentification par application banque en ligne mobile via code confidentiel est fonctionnelle ou en développement par les PSP émetteurs. Elle propose un parcours client plus fluide mais nécessite un smartphone et une connexion au réseau de données.

Authentification biométrique

Les PSP émetteurs réfléchissent à la biométrie comme une alternative au code confidentiel pour sécuriser les paiements en ligne : empreinte digitale, faciale, réseaux veineux, vocale, … L'horizon de déploiement dépendra de l'évolution de la maturité des différentes technologies.

C LA DÉLÉGATION D'AUTHENTIFICATION FORTE À UN WALLET TIERS

Deux constats peuvent être faits sur les wallets tiers :

1. Les méthodes d'authentification forte actuelles (notamment l'OTP SMS) sont peu adaptées aux parcours de paiement sur wallet mobile en proximité ou online, en raison des nombreuses manipulations qu'elles requièrent.
2. Pour garantir des parcours d'achat fluides, les fournisseurs de wallets tiers privilégient des méthodes d'authentification propres afin d'éviter l'authentification forte par le PSP émetteur. Cette évolution est une réponse aux nouveaux usages qui se développent (wallet, paiement via assistants vocaux, ...).

Dans le cadre des RTS SCA, les fournisseurs de wallet tiers ne peuvent pas décider seuls de ne pas recourir à une authentification forte du porteur. Ceci pourrait menacer la fluidité de leurs parcours clients. En effet le risque est d'aboutir à une double authentification du client, par le wallet puis par le PSP Emetteur. Face à cette situation, des solutions sont en cours de d'étude parmi lesquelles la délégation d'authentification de l'émetteur vers un wallet tiers. L'Opinion Paper de l'ABE du 13 juin 2018 a confirmé cette dernière possibilité tout en rappelant que l'émetteur restait alors responsable du respect des obligations des RTS.

2 types d'opérations de paiement via wallet

A distance

Les transactions initiées sans passage en caisse, avec une interaction à distance entre le wallet et le système d'information du commerçant.

Ex : achat sur internet, achat en magasin sans passage en caisse

Ces transactions sont considérées comme à distance et donc incluses dans le périmètre de ce document.

En proximité

Les transactions initiées lors d'un passage en caisse avec interaction entre le wallet et le système d'encaissement.

Ex: NFC, QR code…

***Pour ces transactions, les préconisation proposées dans ce document restent valables**, sauf les montants de l'exemption petits montants (cf p 9) qui augmentent à 50€ et 150€ en cumulé.*

GLOSSAIRE

Authentification forte

S'entend d'une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories " connaissance " (quelque chose que seul l'utilisateur connaît), " possession " (quelque chose que seul l'utilisateur possède) et " inhérence " (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification (article L133-4 du Code monétaire et financier).

Autorité Bancaire Européenne (ABE)

Créée en 2010, l'Autorité a pour mission de contribuer à la stabilité et à l'efficacité à court, moyen et long terme du système financier européen.

Card on File

Service d'enregistrement des données carte des payeurs - mis en place côté commerçant ou tout tiers habilité - permettant au porteur de ne pas avoir à saisir ses données cartes à chaque achat. Ce service a pour finalité de proposer un parcours fluide pour les porteurs et d'augmenter le taux de conversion des commerçants.

Carte Commerciale

Instrument de paiement utilisé uniquement pour les frais professionnels facturés directement sur le compte de l'entreprise, de l'organisme public ou de la personne physique exerçant une activité indépendante (Source : Règlement MIF).

DSP2

La Directive européenne (2015/2366/UE) sur les Services de Paiement 2ème version dont la transposition en droit français est entrée en vigueur le 13 Janvier 2018 et remplace la DSP1 (2007/64/CE).

One Click

Simplification du parcours d'achat paiement à partir des données qui ont été enregistrées préalablement par le tiers (cf Card On File).

OTP SMS « One Time Password SMS »

Méthode d'authentification des utilisateurs caractérisée par l'envoi d'un SMS avec un code à usage unique sur le numéro de téléphone portable de l'utilisateur.

Paiement à l'expédition

L'ordre de paiement est initié par le porteur lors de l'achat du bien/service, mais la remise à l'encaissement par le commerçant à son PSP est réalisée à l'expédition.

Paiement découpé

L'ordre de paiement est initié par le porteur lors de l'achat d'un ensemble de biens/services avec une authentification sur le montant total. Le paiement fait l'objet de plusieurs opérations remises à l'encaissement par le commerçant vers son PSP acquéreur en fonction des livraisons successives des biens achetés selon un échéancier.

Paiement échelonné

L'ordre de paiement est initié par le porteur lors de l'achat du bien/service, avec une authentification sur le montant total. Le paiement fait l'objet de plusieurs transactions remises à l'encaissement, par le commerçant à son PSP acquéreur, en fonction des échéances convenues avec le porteur.

Paiement No Show

Correspond à la situation où un client ayant réservé une chambre ne se présente finalement pas sans pour autant avoir annulé sa réservation. Un montant forfaitaire est débité sur la carte du porteur dans les conditions convenues lors de la réservation,

GLOSSAIRE

Prestataire d'Acceptation Technique (PAT)

Opère techniquement le système d'acceptation du e-commerçant / la page de paiement et le dispositif de déclenchement 3D Secure. Il organise les échanges de transactions avec les acquéreurs des e-commerçants

Prestataire de Services de Paiement (PSP)

Une entreprise agréée pour offrir des services de paiement. Il peut s'agir soit d'un établissement de crédit soit d'un établissement de paiement / de monnaie électronique.

PSP Acquéreur

Etablissement de crédit ou de paiement, qui acquiert, traite et introduit dans un système d'échanges les données relatives aux opérations de paiement effectuées par les cartes chez des commerçants avec lesquels il est lié par un contrat d'acceptation.

PSP Emetteur

Etablissement de crédit ou de paiement, qui a émis une carte au profit du titulaire de la carte. L'émission de la carte n'est possible que lorsqu'un contrat lie l'émetteur et le titulaire de la carte.

Regulatory Technical Standards (RTS)

Règlement relatif aux « normes techniques de règlementation » (RTS) de la DSP2, publiées par l'Autorité Bancaire Européenne afin de spécifier les exigences techniques pour la mise en place de la DSP2 (Règlement délégué (UE) 2018/389 de la commission du 27 novembre 2017).

Schéma carte / card scheme

Ensemble unique de règles, de pratiques, de normes et/ou de lignes directrices de mise en œuvre régissant l'exécution d'opérations de paiement liées à une carte (cf règlement européen sur les commissions d'interchanges carte 2015/751).

Strong Customer Authentification (SCA)

Cf. « Authentification forte ».

Transaction Risk Analysis (TRA)

Les analyses de risque sur la transaction, prévues par les RTS SCA (article 18), constituent une dérogation pour les transactions identifiées comme « à faible risque ».

Wallet tiers

Fourni par un autre acteur que le PSP émetteur de la carte, un wallet tiers permet l'enregistrement des cartes de n'importe quel émetteur selon un processus propre à la solution et une authentification forte de l'utilisateur. Le wallet tiers permet de réaliser des paiements chez un commerçant en mettant en œuvre sa propre méthode d'authentification.

LA PLATEFORME DE SECURISATION « FAST'R BY CB » POUR 3D SECURE V2 EMV CO

UNE NOUVELLE OFFRE CB ELABORÉE EN CONCERTATION AVEC LE COMMERCE

Une nouvelle offre de services CB adaptés à la mise en conformité DSP2

Afin de répondre aux attentes des e-commerçants CB exprimées dans le cadre du Conseil Consultatif CB,

- **CB met en place en 2018 une plate-forme de sécurisation des paiements CB** sur internet s'appuyant sur le standard 3DS v2 EMVCO et bénéficiant des outils de lutte contre la fraude éprouvés du schéma CB. Cette plate-forme sera utilisée par les e-commerçants CB lorsque la marque CB sera choisie, et permettra la mise en œuvre de la DSP2 et des RTS SCA dans le schéma CB en préservant la fluidité des parcours clients et en renforçant la sécurité des transactions.

- **CB adapte ses règles pour certains cas d'usage en e-commerce**, notamment pour les paiements échelonnés et les paiements décalés par rapport à la commande (ex. paiement à l'expédition).

- **CB crée un logo de confiance** pour son offre de sécurisation des transactions à distance :

ONT CONTRIBUÉ À CE DOCUMENT

Conseil Consultatif du Commerce

AFTE Association Française des Trésoriers d'Entreprise

FCA FÉDÉRATION DU COMMERCE COOPÉRATIF ET ASSOCIÉ

fcd

fevad

Mercatel Pour le Commerce et la Distribution

U2P union des entreprises de proximité

CB

Commerçants

ACCOR

Auchan RETAIL

Carrefour

Cdiscount N'ÉCONOMISEZ PAS VOTRE PLAISIR.

meetic

orange

SNCF

Système U

vente-privee

VESTIAIRE COLLECTIVE

151bis rue Saint Honoré
75001 Paris

www.cartes-bancaires.com

02 octobre 2018 – RCS PARIS C 331 302 794 – APE 6619B