fime

L'authentification forte (SCA) : pourquoi, quand, comment ?

Livre blanc

Mars 2022

Sommaire

interactive

Introduction

Les paiements électroniques sont devenus omniprésents dans nos parcours d'achat, que ce soit :

- Avec la carte bancaire, le mobile et les objets connectés.
- En point de vente, par internet.
- Ou encore via les virements et les prélèvements de compte à compte.

A cela s'ajoutent toutes les innovations proposées par les fintechs et différents wallets de paiement.

Aujourd'hui, toutes les transactions que nous faisons et la manière dont nous gérons nos finances s'effectuent dans un monde de plus en plus numérique.

Ces évolutions rapides des usages nous exposent néanmoins à de nouveaux risques de fraude et de tentatives d'usurpation d'identité. Ceci est d'autant plus vrai qu'une part importante de la fraude s'est organisée et professionnalisée sous forme de réseaux mafieux.

Pour mieux comprendre comment tous les acteurs de l'écosystème du paiement luttent contre ce nouveau type de fraude, ce document retrace les grandes étapes récentes de la sécurisation des paiements et présente les directives actuelles et leurs mises en application.

> "Avec la multiplicité des canaux, des moyens de paiement et la possibilité de nouveaux parcours d'achat, la sécurisation des transactions est devenue un enjeu crucial pour la protection des clients. Les nouvelles règles veillent à ce que l'expérience utilisateur ne soit pas sacrifiée.
>
> Arnaud Crouzet, VP Consulting Fime

1. Principales étapes de la sécurisation des paiements.

1.1. La DSP1 : première directive sur les services de paiement.

L'Europe a adopté dès 2007 une première Directive sur les Services de Paiement (DSP1[1]) dont l'un des objectifs était de créer un espace unique de paiement dans l'Espace Economique Européen[2], permettant notamment de garantir un accès équitable et ouvert aux marchés des paiements ainsi que de renforcer la protection des consommateurs.

Elle préconisait l'usage de la carte à puce pour les paiements de proximité et l'usage du protocole 3-D Secure (mis en place par les schémas de paiement comme Visa avec « Verified By Visa » ou Mastercard avec « Mastercard SecureCode ») pour sécuriser les transactions en ligne.

> La DSP1 concrétise la création d'un espace unique de paiement dans l'Espace Economique Européen.

1.1.1. La généralisation du protocole de paiement 3-D Secure.

Le protocole 3-D Secure (ou « Three Domain Secure ») est un protocole de messagerie standard utilisé pour identifier les parties prenantes d'une transaction dite « à distance » (Card Not Present – CNP), et en particulier pour authentifier le payeur de manière efficace.

Ce processus inclut trois types d'acteurs (d'où le nom) :

- Les domaines acquéreurs (banques et marchands notamment).
- Les domaines émetteurs (banques et porteurs principalement).
- Des acteurs interbancaires (les réseaux de paiement aussi appelés systèmes de paiement ou schémas de paiement).

Il laisse à chacun la responsabilité du choix de la solution d'authentification dans son domaine de responsabilité : l'émetteur authentifie le porteur, l'acquéreur authentifie le commerçant, le réseau authentifie les banques émettrices et acquéreures.

En bref, il vise à offrir une solution de sécurisation des paiements en ligne amenant un niveau de confiance équivalent au paiement de proximité, tout en cherchant à réduire les frictions induites par les authentifications nécessaires.

1 Directive 2007/64/CE 2007-11-13

2 Espace Economique Européen (EEE) : zone composée des 28 États membres de l'Union européenne (UE) et de trois pays de l'Association européenne de libre-échange (AELE) (tous, à l'exception de la Suisse, notamment: Islande, Liechtenstein et Norvège).

1.1.2. Première version 3DS : 3-D Secure V1.

La plupart des mises en œuvre de cette première version 3DS v1 consistaient à entrer, en plus des données de la carte, un code spécifique qui pouvait être reçu par SMS, ou un mot de passe préalablement renseigné par le client auprès de sa banque émettrice.

En 2019, cette technologie était utilisée en France pour 43% des paiements en ligne[3] (en légère décroissance par rapport à l'année précédente du fait de l'utilisation progressive du scoring permettant de connaître le profil des transactions et le risque inhérent).

Sa mise en place avait permis de réduire fortement les fraudes mais il était reproché des difficultés dans l'implémentation et surtout une baisse significative du taux de transformation lié à :

- Un parcours client trop compliqué (bascule d'une page à une autre pour la saisie des codes).
- Une bascule complexe voire impossible entre les applications du mobile pour passer de l'acte de vente à l'authentification et revenir à la vente.
- Une non réception des SMS en zone blanche.
- Des infrastructures techniques parfois déficientes.

Certains marchands optaient alors parfois pour la désactivation du 3DS et prenaient ainsi le risque de supporter une partie de la fraude.

Initialement imposé pour toutes les transactions, il a rapidement été autorisé de ne l'appliquer qu'au cas par cas, dans une version appelée « 3-D Secure débrayable ». Cela permettait aux commerçants de sécuriser leurs transactions selon leurs propres besoins, et ainsi de déléguer aux banques émettrices la gestion du risque de fraude uniquement lorsqu'ils le jugeaient nécessaire (principe du « liability shift »).

3 Source Statista – Part des paiements sécurisés 3DS

1.2. La DSP2 : seconde directive sur les services de paiement.

Ces dernières années, de nouveaux facteurs de risques sont apparus en lien avec :

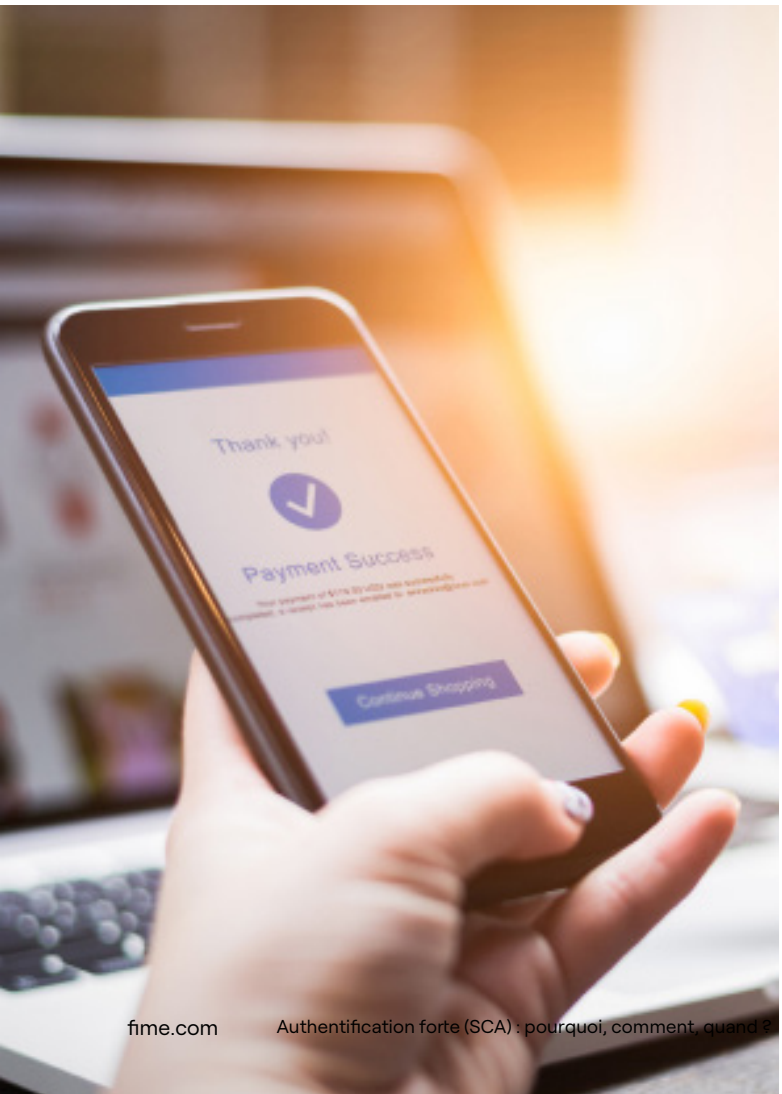
- L'émergence de nouveaux acteurs dans la chaîne des paiements.
- L'hébergement externe de données.
- La désintermédiation par des tiers telle que l'agrégation de comptes et l'initiation de paiement.
- La professionnalisation de la fraude et la sophistication croissante des attaques.

Alors que les fraudes sur les opérations de cartes en point de vente et de retrait restent maitrisées (ex : 0,009% au premier semestre 2021[4] en France), elles restent plus importantes pour les paiements en ligne (elles atteignent 0,149%[5] en France à la même période), et les difficultés d'application de 3DS V1 n'ont pas permis de réduire fortement ces chiffres.

Dans ce contexte, l'Europe a publié le 25 Novembre 2015 une seconde Directive[6] – DSP2. Elle a introduit le renforcement de l'authentification forte (Strong Customer Authentication – SCA) des clients pour tous les moyens de paiement (cartes et non-cartes), et a précisé leurs applications dans les RTS[7] (Regulatory Technical Standards) adoptés le 27 Novembre 2017.

Ainsi, la DSP2 a rendu la SCA obligatoire, alors qu'au préalable elle était surtout « recommandée ».

Bien que répondant à son premier objectif, la version 1 de 3DS a marqué ses limites et n'est dorénavant plus autorisée. Selon une migration progressive, depuis 2021 toutes les authentifications 3DS doivent maintenant utiliser la nouvelle version 3DS v2 reprise sous l'égide d'EMVCo (et nommée EMV 3-D Secure).



> Avec la DSP2, l'authentification forte est devenue la règle par défaut pour toutes les transactions de paiement.

4 OMSP, Note fraude 1er trimestre 2021

5 Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2020 | Banque de France (banque-france.fr)

6 Directive sur les services de paiement 2 (UE) 2015/2366 adoptée le 25 novembre 2015

7 Regulatory Technical Standards règlement délégué (UE) 2018/389 – 2017-11-27

1.2.1. Seconde version de 3-D Secure : EMV® 3-D Secure.

L'ancien protocole a démontré que s'appuyer uniquement sur la réception d'un simple code SMS sur mobile n'est plus suffisamment sécurisé, et que des usurpations sont possibles et de plus en plus observées (SIM Swapping, Attaques SS7, Social Engineering…).

Le nouveau protocole permet de résoudre plusieurs problèmes techniques de l'ancienne version :

- Une optimisation des parcours acheteurs, rendant ainsi le processus de paiement plus aisé pour les achats sur navigateur et in-app.
- L'introduction d'un flux d'authentification sans friction.
- Une sécurité renforcée.

Il permet de répondre aux exigences techniques de la DSP2 en véhiculant, en complément de l'authentification des acteurs, les éléments de preuve de ces authentifications, ainsi que les éléments permettant d'évaluer le risque lié à la transaction en cours et potentiellement appliquer une dérogation à la SCA.

Les dernières versions EMV 3-D Secure améliorent la communication «en arrière-plan» entre la banque émettrice, l'acquéreur et le commerçant.

Ainsi, plutôt que de demander des informations à l'utilisateur, les informations de base sur le titulaire du compte et les conditions de la transaction sont désormais automatiquement récupérées et vérifiées.

Des algorithmes plus intelligents sont en place pour s'assurer que les demandes d'authentification supplémentaires ne sont faites que lorsque cela est vraiment nécessaire, ce qui améliore la sécurité des paiements tout en fluidifiant le parcours client par rapport à la précédente version.

Pour comprendre l'écart entre les deux versions, il faut constater que le flux de données est passé de 15 champs en v1 à plus de 150 champs en v2, avec de nouvelles fonctionnalités telles que :

- Plus d'options d'authentification (mot de passe dynamique, biométrie…).
- Une meilleure gestion des multiples canaux numériques (in-app, navigateur mobile, wallets).
- Des demandes d'identification et de vérification uniquement, en plus des demandes de transactions de paiement.
- La possibilité de limiter les demandes d'authentification telles que l'ajout des commerçants en « liste blanche » (commerçant déclaré de confiance par le client), ou encore les demandes de « non-challenge » lorsque le commerçant est prêt à prendre lui-même le risque (pas de « liability shift » dans ce cas).

Sur ce dernier point, la mise en place du **« soft decline »** (rejet par l'émetteur de la carte d'une transaction non conforme DSP2 avec la possibilité pour le e-commerçant de soumettre une nouvelle fois la transaction via 3-D Secure), et **des listes blanches** permettent d'éviter les dégradations des taux de conversion comme c'était souvent le cas avec la version 1 de 3-D Secure.

> "
>
> Fime a publié un guide détaillé précisant les caractéristiques du protocole EMV 3-D Secure V2.

2. Les principes de l'authentification forte (SCA).

L'authentification forte contribue à sécuriser les connexions et les transactions grâce à une authentification mettant en œuvre au moins deux facteurs parmi les trois suivants :

- **La connaissance**
  Quelque chose que seul l'utilisateur connaît : mot de passe, code pin…
- **La possession**
  Quelque chose que seul l'utilisateur possède : mobile, carte, token…
- **L'inhérence ou caractéristique biométrique**
  Quelque chose que l'utilisateur est : empreinte digitale, reconnaissance faciale ou vocale…

Ces éléments doivent être indépendants les uns des autres et la violation de l'un ne doit pas compromettre la fiabilité des autres.

Ces règles nécessitent de repenser les critères d'authentification. Ainsi, les mots de passe simples par SMS ne sont plus suffisants et doivent être remplacés par des authentifications plus complexes incluant par exemple des mots de passe dynamiques à usage unique et de la biométrie, telle que la reconnaissance faciale et les empreintes digitales, lorsqu'elles sont disponibles et que le processus de reconnaissance est certifié fiable[8].

À noter que les données inscrites sur une carte de paiement (PAN, date de validité et CVV) ne peuvent pas constituer l'un des facteurs d'authentification même si le porteur pourrait être le seul à le connaître ou à le posséder.

Au moins deux facteurs sont nécessaires parmi les trois suivants :

- La connaissance
- La possession
- L'inhérence

Connaissance

Quelque chose que seul le client connaît.

Possession

Quelque chose que seul l'utilisateur possède.

Inhérence

Quelque chose que l'utilisateur est.

8 PSD2 Q&A Strong customer authentication and common and secure communication

2.1. Champs d'application de l'authentification forte.

2.1.1. Concernant les paiements.

Cette authentification s'applique à tous les paiements initiés en Europe (Zone EEE). Elle concerne donc tous les paiements par carte bancaire et les virements bancaires dans cette zone.

Elle ne concerne pas les paiements dont l'un des deux acteurs, le titulaire de la carte bancaire ou le marchand, est en dehors cette zone, ni les paiements qui sont initiés en l'absence du client comme les prélèvements par abonnements[9].

L'initialisation de l'abonnement reste quant à elle soumise à l'authentification forte du client.

.2.1.2. Concernant les consultations et les initiations de paiement (via PISP[10] et AISP[11])

La Directive des Paiement a introduit de nouveaux acteurs :

- Les initiateurs de paiement ou PISP.
- Les agrégateurs de comptes ou AISP.

Ils sont directement concernés par le renforcement de l'authentification forte et soumis à sa mise en œuvre, ce qui peut complexifier leur service.

Leur différenciateur est souvent de proposer des nouveaux cas d'usages et services, ou une meilleure expérience client sur les cas d'usages existants.

Tout en renforçant la protection du client, l'authentification forte vient donc contraindre la mise en place de leur service souvent basé sur la fluidité du parcours client.

Alors que l'adoption par le client était parfois difficile à obtenir (transmission de code client et mot de passe sur des sites internet autres que ceux de la banque), ils doivent ajouter une nouvelle zone de friction à l'expérience utilisateur.

En outre, les particuliers devront renouveler l'authentification forte au minimum tous les 90 jours pour accéder aux services bancaires à distance.

9 RTS Article 14

10 Payment Initiation Service Provider

11 Account Information Service Provider

2.2. Principe de l'authentification déléguée.

L'émetteur peut déléguer l'authentification à un marchand ou un wallet (Token Requestor) sans que cela ne soit considéré comme une exemption : la SCA a bien eu lieu.

Le commerçant ou le wallet doivent au préalable avoir fait la preuve que l'authentification qu'ils ont réalisée, a bien la force d'une SCA.

2.3. Domaines de responsabilité et exemptions.

L'authentification forte est obligatoire mais pour rendre le parcours client fluide, des procédures de dérogation (exemptions) sont prévues.

Ainsi, la banque émettrice décide d'authentifier ou non le porteur, en fonction de sa propre analyse des risques.

Pour ce faire, elle dispose de plus de données (incluses dans le message des demandes d'exemption) et notamment des indications d'évaluations du risque réalisées par les autres acteurs impliqués dans la chaine des paiements : commerçant, prestataire technique, banque d'acquisition, réseau de carte, wallet...

Le marchand est en capacité de faire une demande d'exemption, auprès de la banque émettrice, sur une transaction (dans certaines conditions). Si l'exemption est acceptée, il est alors responsable de la transaction en cas de fraude éventuelle.

L'acquéreur peut également le demander pour le compte du marchand. Une seule catégorie d'exemption peut être appliquée sur une transaction (un choix doit être fait si plusieurs sont possibles, par exemple une transaction de montant faible ou une transaction récurrente).

Toutes les demandes d'exemption doivent être évaluées par l'émetteur selon certains critères (RTS Art 18.2) et facteurs de risque (RTS Art 18.3).

L'émetteur peut lui aussi appliquer une exemption même si le marchand et l'acquéreur ne l'ont pas demandée.

> "Pour rendre le parcours client fluide, des procédures de dérogation (exemptions) sont prévues.

2.3.1. Mesures à l'initiative de l'acquéreur (à la demande du marchand).

Cas des Recurring transactions (art.14 RTS)

Il s'agit des transactions faites en l'absence du porteur de la carte telles que les prélèvements mensuels suite à un abonnement.

La souscription initiale de l'abonnement donnant lieu à ces prélèvements est soumise à SCA même si aucun flux financier n'est échangé à cette occasion.

Le premier paiement doit intervenir dans les 90 jours pour que l'authentification forte faite lors de la souscription soit encore valable. Les paiements suivants ne sont pas soumis à SCA tant qu'ils restent au plus égaux au paiement initial.

Cas des Low-value transactions (art.16 RTS)

Cette exemption peut être appliquée si 1) le montant de la transaction est inférieur à 30€ et que 2) :

- Le montant cumulé des transactions faites depuis la dernière SCA ne dépasse pas 100€.

ou

- Le nombre de transactions faites depuis la dernière SCA ne dépasse pas 5 transactions.

Le marchand et l'acquéreur ne peuvent considérer que le premier critère pour émettre une telle demande d'exemption du fait qu'ils n'ont pas connaissance des éléments pour le critère du montant cumulé ou du nombre de transactions.

L'émetteur fera son analyse et soumettra ou pas le porteur à la SCA.

Cas du Transaction Risk Analysis (Art.18 RTS)

Cette exemption peut être utilisée par l'acquéreur (à la demande du marchand) en fonction du risque de fraude auquel il est exposé. Plus ce niveau est faible plus le marchand et l'acquéreur peuvent utiliser cette possibilité d'exemption pour des montants de transaction élevés. A chaque niveau de fraude correspond une valeur seuil d'exemption (ETV[12]) :

- Entre 6 et 13 points de base : exemption possible des transactions jusqu'à 100€.
- Entre 1 et 6 points de base : exemption possible des transactions jusqu'à 250€.
- Inférieure à 1 point de base (<0,01%), exemption possible des transactions jusqu'à 500€.

Si l'acquéreur est en dessous de ces seuils, il peut faire une analyse de risque (TRA[13]) en s'appuyant sur les conditions des articles 18.2 et 18.3, et évaluer s'il peut demander une exemption.

L'émetteur conduit ensuite la même analyse avec ses propres seuils et indicateurs de risques.

A noter que ces taux sont perçus par beaucoup comme très restrictifs. A titre de comparaison, la moyenne française est sensiblement supérieure avec 15 points de base. L'Observatoire note un repli significatif passant de 0,174% en 2020 à 0,149% au premier semestre 2021, ceci étant majoritairement dû à la mise en conformité avec les prérequis d'authentification forte énoncés dans la DSP2.

12 Exemption Threshold Value

13 Transaction Risk Analysis

2.3.2. Mesures à l'initiative de l'émetteur.

Cas des Trusted beneficiaries (art.13 RTS)

Cette exemption peut être sollicitée par le marchand / acquéreur mais appliquée par l'émetteur.

L'émetteur peut proposer à ses porteurs de gérer une liste de Trusted Beneficiaries (marchands de confiance) pour lesquels il ne demandera pas systématiquement une SCA au porteur. L'inscription du marchand dans cette « liste blanche » doit se faire avec une SCA initiale du porteur.

Si le marchand a reçu une confirmation d'inscription en liste Trusted Beneficiaries, il peut demander une exemption de ce type.

L'émetteur peut également appliquer cette exemption même si elle n'est pas demandée par le marchand / acquéreur.

Cas des Low-value transactions (art.16 RTS)

Cette exemption peut être appliquée si le montant de la transaction est inférieur à 30€ et que :

- Le montant cumulé des transactions faites depuis la dernière SCA ne dépasse pas 100€.

ou

- Le nombre de transactions faites depuis la dernière SCA est inférieur ou égal à 5.

L'émetteur doit évaluer si cette exemption est applicable ou non en tenant compte de sa propre évaluation de risque selon l'un des deux critères définis (montant cumulé ou nombre de transactions depuis la dernière SCA). L'émetteur soumettra ou non le porteur à la SCA selon le résultat de son analyse.

Cas du Secure corporate payment processes and protocols (art.17 RTS)

Cette exemption correspond principalement à deux cas :

- L'utilisation d'un numéro de carte virtuelle unique généré par le porteur, à condition qu'une authentification forte réussie ait été faite durant le process de génération.
- Les transactions B2B avec des cartes logées (comme les dépenses de frais de voyage passées sur le compte de l'entreprise).

Cas du Transaction Risk Analysis (Art.18 RTS)

Une valeur seuil (ETV), pour pouvoir appliquer l'exemption, est définie en fonction du niveau de fraude auquel l'émetteur est exposé. Plus sa lutte contre la fraude brute est performante, plus l'émetteur peut utiliser cette possibilité d'exemption pour des montants de transaction élevés.

La règle de calcul de l'ETV est la même que pour les acquéreurs (100€ entre 6 et 13 points de base de fraude brute, 250€ entre 1 et 6 points de base, 500€ en dessous de 1 point de base) mais elle s'applique à la fraude subie par l'émetteur.

L'émetteur peut décider d'appliquer une exemption si le montant de la transaction est en dessous du seuil. Il doit pour cela faire une analyse de risque (TRA) en s'appuyant sur les conditions des articles 18.2 et 18.3 pour évaluer si l'exemption peut être appliquée.

L'émetteur peut appliquer une exemption TRA même si l'acquéreur ne l'a pas demandée.

2.4. Focus sur la biométrie.

Les technologies biométriques ont considérablement évolué ces dernières années et pourraient devenir un élément de plus en plus utilisé pour l'authentification forte.

Selon le cas d'usage, plusieurs types de biométries sont possibles, notamment :

- La biométrie physiologique, liée aux caractéristiques de la personne telles que l'empreinte digitale, la paume de la main, le visage, l'iris et la voix.
- La biométrie comportementale, liée à des caractéristiques comportementales dynamiques, telles que la façon dont une personne se déplace, les gestes et les frappes au clavier.

Les progrès actuels permettent de coupler la biométrie avec l'intelligence artificielle pour assurer la sécurité tout en gardant une expérience de paiement simple, intuitive et transparente.

> Les différentes méthodes de biométrie sont autant de possibilités d'accompagner l'authentification forte du client.
>
> Dans ses articles de blog, Fime détaille quelques-unes des possibilités d'utilisation de la biométrie.

3. Plan de migration.

3.1. Plan de migration de l'OMSP.

Le plan de migration tel qu'il a été validé par l'Observatoire de la sécurité des moyens de paiement (OSMP[14]) comprend deux volets : le premier à l'attention des consommateurs et le deuxième à l'attention des acteurs du paiement.

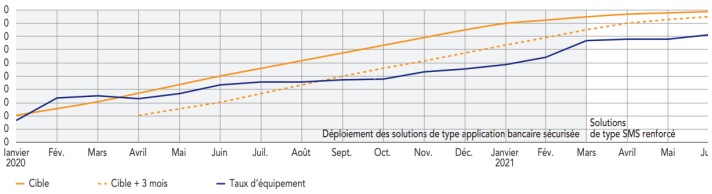
3.1.1. Volet pour les consommateurs.

Ce volet est de la responsabilité des banques émettrices. Il consiste à enrôler progressivement les porteurs de carte dans le nouveau dispositif d'authentification (exemple : l'enrôlement sur mobile en remplacement du code envoyé par SMS).

Cet enrôlement a été temporisé pendant la crise sanitaire par les banques qui craignaient, si elles poursuivaient la migration, d'affecter la capacité des consommateurs à recourir au e-commerce dans une période où ce dernier était davantage sollicité sur certains produits.

Cependant, fin juin 2021, l'Observatoire estimait que plus de 80% des porteurs de carte actifs sur internet (ayant réalisé au moins un paiement en ligne au cours des trois derniers mois) étaient équipés d'un nouveau dispositif d'authentification forte (ex : application bancaire).

L'enrôlement des porteurs non éligibles à des solutions mobiles (porteurs n'ayant pas de smartphones, ne voulant pas utiliser d'application, etc.) a été réalisé plutôt à partir du second trimestre 2021, avec des solutions plus « universelles » (ex : SMS renforcé).



Suivi de l'équipement des porteurs.

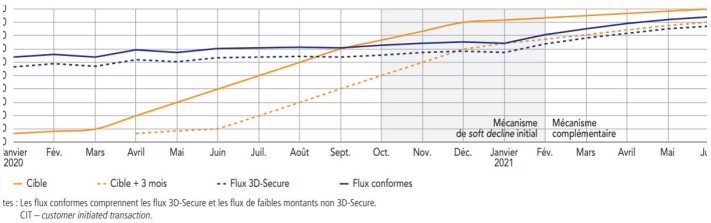
3.1.2. Volet pour les acteurs professionnels de la chaîne des paiements.

Ce volet concerne tous les acteurs qui doivent s'adapter à l'évolution de l'infrastructure d'authentification, notamment au protocole technique 3-D Secure en version 2 (EMV 3-D Secure), afin d'assurer la gestion des règles de responsabilité et des cas d'exemption prévus par la nouvelle directive.

La majorité des petits commerçants délègue la gestion de la page de paiement à un prestataire, ce qui facilite la migration.

Les grands commerçants qui gèrent eux-même leurs pages de paiement font face à une migration plus complexe.

L'Observatoire note qu'à fin juin 2021, 87 % des flux de paiement éligibles à la DSP2 utilisaient le protocole 3-D Secure, et étaient donc conformes. Sur les 13% restants, plus de 7% bénéficiaient de l'exemption sur les faibles montants. Ainsi, le taux de conformité atteignait environ 95%.



Suivi de l'équipement des commerçants.

14 Plan de migration DSP2

3.2. Mise en œuvre de la migration.

Pour assurer le respect du calendrier de migration établi en 2019 (et reporté à plusieurs reprises, notamment pour limiter la gêne client occasionnée et prendre en compte la crise sanitaire), la Banque de France a mené une stratégie basée sur les 3 volets suivants et décrits ci-après :

1. Clarification des critères d'exemption des transactions.
2. Utilisation du **soft decline**.
3. Renforcement de la continuité des infrastructures d'authentification.

3.2.1. Clarification des critères d'exemption des transactions.

La DSP2 prévoit différentes qualifications pour les paiements effectués par carte et à distance. L'obligation d'authentification forte ou non de la transaction dépend de sa qualification.

Ces qualifications, évoquées au chapitre 2.1. (Champs d'application de l'authentification forte) sont les suivantes :

Transactions sujettes à l'authentification forte du porteur (sauf exemption).

- Transaction initiée par le client (« Customer Initiated Transaction », CIT).

Transactions sujettes à l'authentification forte du porteur uniquement lors du premier paiement (sauf exemption).

- Transaction initiée par le marchand (« Merchant Initiated Transaction », MIT).

Transactions non sujette à l'authentification forte du porteur.

- Transaction non émise par un canal électronique (« Mail Order / Telephone Order », MOTO).
- Transaction effectuée avec un instrument de paiement anonyme.
- Transaction pour laquelle l'émetteur de la carte ou l'acquéreur de la transaction n'est pas localisé dans l'Espace économique européen.

Les différentes exemptions applicables sont mentionnées au paragraphe 2.3 (Domaines de responsabilité et exemptions).

> "La migration à l'authentification forte doit prendre en compte à la fois l'enrôlement du consommateur (partie émetteur), et les mises à jour côté commerçant (partie acceptation et acquisition).

3.2.2. Utilisation du soft decline.

Le **soft decline** permet de soumettre une transaction non conforme à la DSP2 à une authentification forte via 3-D Secure (V1 ou V2), et ce sans la rejeter. Ainsi, le porteur n'a pas à tenter d'effectuer son paiement à plusieurs reprises en cas de non-conformité.

Ce mécanisme standardisé fut l'un des piliers de la migration vers des paiements plus sécurisés. Introduit en avril 2020, il a permis aux e-commerçants de capter des transactions qui, auparavant, étaient refusées d'emblée.

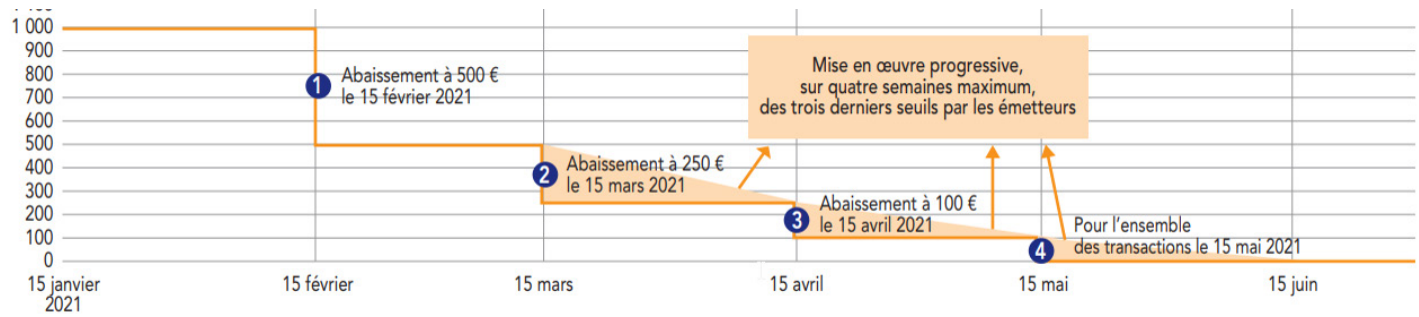
Le soft decline a servi de levier de mise en conformité progressive, en utilisant une approche par seuils décroissants. Ainsi, au 1er octobre 2020, toute transaction de plus de 2000€ non conforme passait en soft decline. Au 15 janvier 2021, ce furent les transactions de plus de 1000€, pour finalement passer toutes les transactions non conformes en soft decline au 15 mai 2021 (voir le détail des paliers dans le graphique ci-dessous).

3.2.3. Renforcement de la continuité des infrastructures d'authentification.

Parce que la migration vers un haut niveau d'authentification forte passe par un usage plus généralisé du protocole 3D-Secure, toutes les infrastructures qui permettent son bon fonctionnement deviennent systémiques pour le e-commerce.

Ainsi, les ACS (Access control server, ou serveur d'authentification) des banques, par lesquels transitent les demandes d'authentification, ainsi que leurs directory servers (serveurs de routage, qui routent ces demandes d'un acteur à un autre) prennent une importance cruciale, et doivent rester opérationnels en permanence pour permettre une continuité de service en tout temps.

Mise en place du soft decline au 1er semestre 2021 :



4. Conclusion.

Le déploiement de EMV 3-D Secure, notamment sous sa version 2, continue de se poursuivre en France et sur l'ensemble de l'Europe.

Après une première phase de migration « simple », c'est-à-dire de porter les mécanismes de la v1 à la v2, les différents acteurs, notamment les commerçants, ont compris l'intérêt d'enrichir les données de la transaction pour permettre d'alimenter le RBA des émetteurs, ainsi que d'être en mesure de gérer les possibilités d'exemption.

L'enjeu est d'améliorer le taux de transformation dans les parcours clients, tout en conservant un haut niveau de sécurité.

Les modèles 3 coins semblent tirer pleinement partie des possibilités d'analyse de risque avec la connaissance directe à la fois du client et du commerçant. Les retours confirment une amélioration des parcours d'achat sans friction, c'est-à-dire en évitant de déclencher systématiquement de nouvelles authentifications fortes auprès de l'utilisateur.

De manière générale, l'amélioration de l'analyse de risque, ainsi que le recours aux exemptions pour les transactions de faibles montants permettent d'éviter d'impacter les taux de conversion.

Bien que la mise en place puisse être relativement complexe selon les acteurs et les environnements techniques, les retours sont positifs. Ainsi, la Banque de France annonçait la réussite de la migration, avec un haut niveau de conformité à la fois sur les volets consommateurs et commerçants. On observe notamment une amélioration globale de l'expérience client par rapport à la version précédente, et la sécurisation des paiements en ligne a été renforcée.

Elle annonçait donc avec la publication du dernier Observatoire de la sécurité des moyens de paiement la fin du plan de migration collective débuté en 2019. Elle assurera la mise en conformité résiduelle avec l'Autorité de contrôle prudentiel et de résolution (ACPR).

Fort heureusement, l'authentification forte n'est plus vécue uniquement comme une contrainte, mais également et surtout comme une opportunité de combattre la fraude et de revoir les performances des partenaires de paiement (PSP) sur leur gestion et leur niveau de fraude.

> La mise en place de l'authentification forte, couplée aux différentes exemptions autorisées, permet de réduire les risques de fraude tout en réduisant l'impact sur le parcours client.

back to contents

Auteurs

Edouard BAROIN
Directeur Fime Consulting

Arnaud CROUZET
VP Fime Consulting

Alexis DEFFON
Consultant Paiement Fime Consulting

fime

Fime – Immeuble Antony – Parc 1
2-4-6, place du Général de Gaulle
92160 Antony – France