GT MIGRATION

16 avril 2021

Conditions de mise en œuvre de l'authentification forte du porteur pour les transactions par carte du commerce en ligne

Le recours à l'authentification forte du payeur pour l'initiation d'un paiement électronique est une disposition clé en matière de sécurité des paiements introduite par la deuxième directive européenne sur les services de paiement (DSP2). Les conditions de mise en œuvre de cette disposition ont été précisées par les normes techniques de réglementation relatives à l'authentification forte du client édictées par l'Autorité bancaire européenne (RTS SCA/CSC), ainsi que par les différentes réponses apportées aux questions complémentaires adressées par les acteurs de marché.

Le présent document vise (i) à rappeler les règles de qualifications des transactions établies par la règlementation et les obligations qui en découlent en matière d'authentification, et (ii) à expliquer comment ces règles s'appliquent dans certains cas d'usage particuliers.

RAPPEL DES RÈGLES DE QUALIFICATION DES TRANSACTIONS

En ce qui concerne les paiements par carte à distance, la réglementation prévoit **différentes qualifications** qui déterminent l'obligation d'application ou non de l'authentification forte :

- Les **transactions initiées électroniquement par le client** (*Customer Initiated Transaction* – **CIT**) correspondent aux paiements effectués par le porteur de la carte sur internet, que ce soit au travers d'un navigateur ou d'une application. Ces transactions sont visées par l'obligation d'authentification forte du porteur, mais peuvent toutefois faire l'objet d'une exemption prévue par les RTS dès lors que les conditions d'application de celle-ci sont réunies (voir ci-après).

- Les **transactions initiées électroniquement par le commerçant** (*Merchant Initiated Transaction* – **MIT**) correspondent aux opérations initiées par le commerça nt sans présence active du porteur de la carte, dans des situations où l'émission du paiement est dissociée de l'engagement à payer, par exemple : dans le cas d'un abonnement, d'un paiement en plusieurs fois, d'un service payé en fonction de la consommation (abonnement modulable, réservation d'un moyen de transport…), de paiements exécutés en plusieurs fois au moment de la livraison des différents éléments d'un panier d'achat, ou encore de frais de garantie de réservation payables en cas de non présentation du client. Ces transactions, généralement émises en-dehors de la présence active du client sur le site du commerçant, ne sont pas soumises à l'obligation d'authentification forte du porteur, mais doivent comporter la trace d'une authentification forte réalisée au moment de l'engagement à payer du client (selon un processus dit de « chainage » des transactions). Cet engagement, correspondant à un « mandat MIT », doit préciser les conditions de règlement auquel s'engage le client (montant, nombre d'opérations, périodicité, durée de validité).

31, RUE CROIX-DES-PETITS-CHAMPS – 75049 PARIS CEDEX 01
CODE COURRIER : 11-2324 – TÉL : 01 42 92 96 13 – TÉLÉCOPIE : 01 42 92 31 74

- Les **transactions à distance émises par un canal non électronique** (*Mail order/telephone order* – **MOTO**), qui correspondent aux transactions pour lesquelles les données de carte ont été transmises par le porteur via un canal ne permettant pas leur traitement automatique (par exemple par courrier, fax, courriel, appel téléphonique ou serveur vocal), et dont la saisie à des fins de paiement est assurée par le commerçant. Ces transactions sont exclues du périmètre de la DSP2 et ne sont pas soumises à l'exigence d'authentification forte du porteur.

- Les **transactions effectuées avec des instruments de paiement anonymes**, notamment des cartes prépayées anonymes, ne sont pas soumises à l'obligation d'authentification forte du porteur.

- Les **transactions dites « *one-leg* » pour lesquelles l'émetteur de la carte ou l'acquéreur de la transaction n'est pas localisé dans l'Espace Économique Européen,** qui ne peuvent pas toujours être authentifiées et pour lesquelles l'authentification forte est seulement requise sur une base du meilleur effort (« *best effort* »).

Dans le cas des transactions de type CIT initiées par carte sur internet, **cinq motifs d'exemption à l'authentification** forte sont prévus par les RTS :

- **Les paiements de faible valeur** (article 16) : cette exemption porte sur les paiements d'un montant unitaire d'au plus 30 euros, et est applicable dès lors que le montant cumulé des dernières opérations consécutives exemptées à ce titre au moyen d'une carte donnée ne dépasse pas 100 euros ou que leur nombre n'excède pas cinq opérations. Le fonctionnement de cette exemption est similaire avec celui du sans contact pour les paiements au point de vente (prévu à l'article 11, avec des plafonds plus élevés).

- **Les paiements présentant un faible niveau de risque** (article 18) : cette exemption porte sur les opérations reconnues par le commerçant et/ou par la banque du porteur et/ou par la banque du commerçant comme présentant un niveau de risque réduit, au motif que les paramètres de la transaction correspondent aux habitudes de paiement du porteur (achat depuis son terminal habituel, adresse de livraison connue, nature de l'achat, montant…).

- **Les paiements récurrents** (article 14) : cette exemption porte sur les paiements d'un montant et d'une périodicité fixes, à compter de la 2ème transaction. Cette exemption présente toutefois un intérêt limité pour les paiements par carte, dont les opérations au-delà de la souscription sont initiées par le commerçant (de type MIT).

- **Les paiements vers un bénéficiaire de confiance** (article 13) : cette exemption porte sur les paiements à destination d'un bénéficiaire qui aurait été désigné comme de confiance par le porteur de la carte. Dans ce cas, l'opération d'enregistrement du bénéficiaire de confiance doit elle-même faire l'objet d'une authentification forte du porteur de la carte.

  Les paiements initiés électroniquement via des processus ou protocoles de paiement sécurisés réservés à un usage entre professionnels (article 17) : le recours à cette exemption nécessite une évaluation préalable des processus et des protocoles par l'autorité nationale compétente (en France, par la Banque de France) visant à assurer que le niveau de sécurité offert est au moins équivalent à celui d'une authentification forte.

La DSP2 prévoit qu'il appartient à l'établissement teneur de compte du porteur de protéger ce dernier contre la fraude. Cette disposition implique que l'application d'une exemption ne peut être tenue pour acquise de façon certaine : même si une transaction répond aux critères d'éligibilité du point de vue du bénéficiaire, la banque du porteur peut rejeter son application dès lors qu'elle identifie un risque aggravé pour son client, et alors demander une authentification forte pour sécuriser l'opération.

L'Observatoire invite les commerçants et leurs prestataires d'acceptation et d'acquisition à veiller à la bonne qualité des qualifications des transactions qu'ils émettent, lesquelles conditionnent les règles d'authentification applicables.

Par ailleurs, l'Observatoire invite tout commerçant qui souhaite recourir aux exemptions à l'authentification forte prévues par la DSP2 à recourir à un protocole d'échange répondant au standard EMV 3D-Secure (dit « 3D-Secure v2 »), nécessaire pour assurer de façon intégrée l'échange entre les parties prenantes à la transaction, à la fois dans la transmission des demandes d'exemption et dans l'activation d'une authentification forte à l'initiative de l'émetteur. À défaut d'initier un processus d'authentification, le commerçant s'expose à devoir traiter les messages de refus (ou *soft decline*) qui seraient adressés par les banques émettrices.

APPLICATION DES RÈGLES DE QUALIFICATION ET DES EXIGENCES ASSOCIÉES À CERTAINS CAS D'USAGE

Cas d'usage		Description	Qualification et exigences associées
	**Paiement « *one-click* »**	Paiement initié en ligne par le porteur, à l'achat d'un service ou d'un bien physique ou numérique, à l'aide d'une carte enregistrée dans l'espace client (« *card on file* »)	Transaction initiée par le client (CIT) qui nécessite une authentification forte sauf en cas d'applicabilité d'une des 5 exemptions prévues par les RTS. L'enregistrement de la carte dans l'espace client doit faire l'objet d'une authentification forte systématique au titre des actions susceptibles de comporter un risque de fraude.
	**Paiement(s) à l'expédition ou différé(s)**	Paiement(s) lié(s) à une commande en ligne et faisant l'objet d'un différé(précommande, paiement à l'expédition …)	Au moment de l'achat, obligation d'authentification forte (CIT) sauf en cas d'applicabilité d'une des 5 exemptions prévues par les RTS. L'authentification au moment de l'achat doit correspondre à la totalité du panier. Au moment de l'expédition, une autorisation est demandée, sans authentification car la transaction s'effectue en dehors de la présence du client, accompagnée de la preuve d'authentification initiale (MIT avec chainage).

Cas d'usage		Description	Qualification et exigences associées
	**Transactions récurrentes ou échelonnées**	Série de paiements liée à un abonnement souscrit en ligne ou d'un paiement en plusieurs fois (facilité de paiement accordée au client…)	Au moment de l'achat ou de la souscription de l'abonnement, obligation d'authentification forte (CIT) : - sur un montant correspondant à la totalité du panier s'il est connu à l'avance. - sur un montant à 0 euro (ou « demande d'information ») si le montant total n'est pas connu ou estimable Pour les échéances ultérieures, une autorisation est demandée, sans authentification car la transaction s'effectue en dehors de la présence du client, accompagnée de la preuve d'authentification initiale (MIT avec chainage).
	**Paiement associé à une réservation**	Paiement d'un bien ou d'un service dont le déclenchement et le montant sont conditionnés par la consommation effective. Ce cas d'usage couvre également la non-consommation, lorsque le porteur ne se présente pas pour consommer le service réservé (« *no show* »)	Au moment de la réservation, obligation d'authentification forte (CIT) : - sur la valeur maximale si elle est connue ; - sur un montant à 0 euro (ou « demande d'information ») si le montant n'est pas connu. Quand le montant définitif est connu, une autorisation est demandée, sans authentification car la transaction s'effectue en dehors de la présence du client, accompagnée de la preuve d'authentification initiale (MIT avec chainage).

PROTOCOLES TECHNIQUES REQUIS POUR LE SUPPORT DES EXEMPTIONS

Réseaux de carte	CB	Mastercard	Visa	American Express
Support de l'authentification forte	3D-Secure (toutes versions)	Identity Check (toutes versions)	Visa Secure (toutes versions)	Safekey (toutes versions)
Support des exemptions dans 3D-Secure				
- Faible montant	CB2A v1.5	3DSv2.1+ et supporté en autorisation	*Supporté en autorisation (hors 3D-Secure)*	Safekey toutes versions – règle émetteur
- Niveau de risque	CB2A v1.5	3DSv2.1+ et supporté en autorisation	3DS v2.1 / CB2A v1.6	Safekey toutes versions – règle émetteur
- Bénéficiaire de confiance	3DS v2.2 / CB2A v1.5	3DSv2.1+ et 3DSv2.2	3DS v2.2 / CB2A v1.6	Safekey toutes versions – règle émetteur
- Paiement récurrent	CB2A v1.5	3DSv2.1	*Pas de support spécifique – assimilé à un MIT*	Safekey v2.1 / GCAG Oct 2020 (DF113)
- Protocoles sécurisés inter-entreprises	3DS v2.1 / CB2A v1.5	3DSv2.1+	3DS v2.1 / CB2A v1.6	
Support du chainage des transactions MIT	CB2A v1.6		CB2A v1.6	GCAG Oct 2020 (DF113 & DF60)
Support de l'authentification en achat sur mobile in-App	CB2A v1.5 + SDK 3DS v2.1 à intégrer à l'App		CB2A v1.5	Safekey v2.1 (SDK associé)
Support du fallback en autorisation (indicateur d'indisponibilité de l'infra 3D-Secure)	CB2A v1.6	CB2A v1.6	CB2A v1.6	

Lien vers les références documentaires :

- **CB :** https://www.cartes-bancaires.com/produits-services-2/les-solutions-cb/fastr_by_cb/
- **Mastercard :** Mastercard Identity Check | Secure ID Check Standards - Sur MC Connect : accéder à "Mastercard Authentication Guide for Europe" et " Mastercard Identity Check Program Guide"
- **Visa :** https://fr.review.visa.com/devenir-partenaire/technologie-de-paiements/strong-customer-authentication/resources.html

  American Express : https://www.americanexpress.com/fr/merchant/safekey.html
  https://merchantharbor.americanexpress.com/merchantlogin
- **Worldline Sips :** https://documentation.sips.worldline.com/fr/WLSIPS.344-UG-3-D-Secure.html
- **Fédération du e-commerce et de la vente à distance (FEVAD) :**
  https://www.fevad.com/regul/paiements/ ; contact : Bertrand Pineau (bpineau@fevad.com)
- **Mercatel** : www.mercatel.info ; contact : Jean-Michel Chanavas (jmchanavas@mercatel.info)