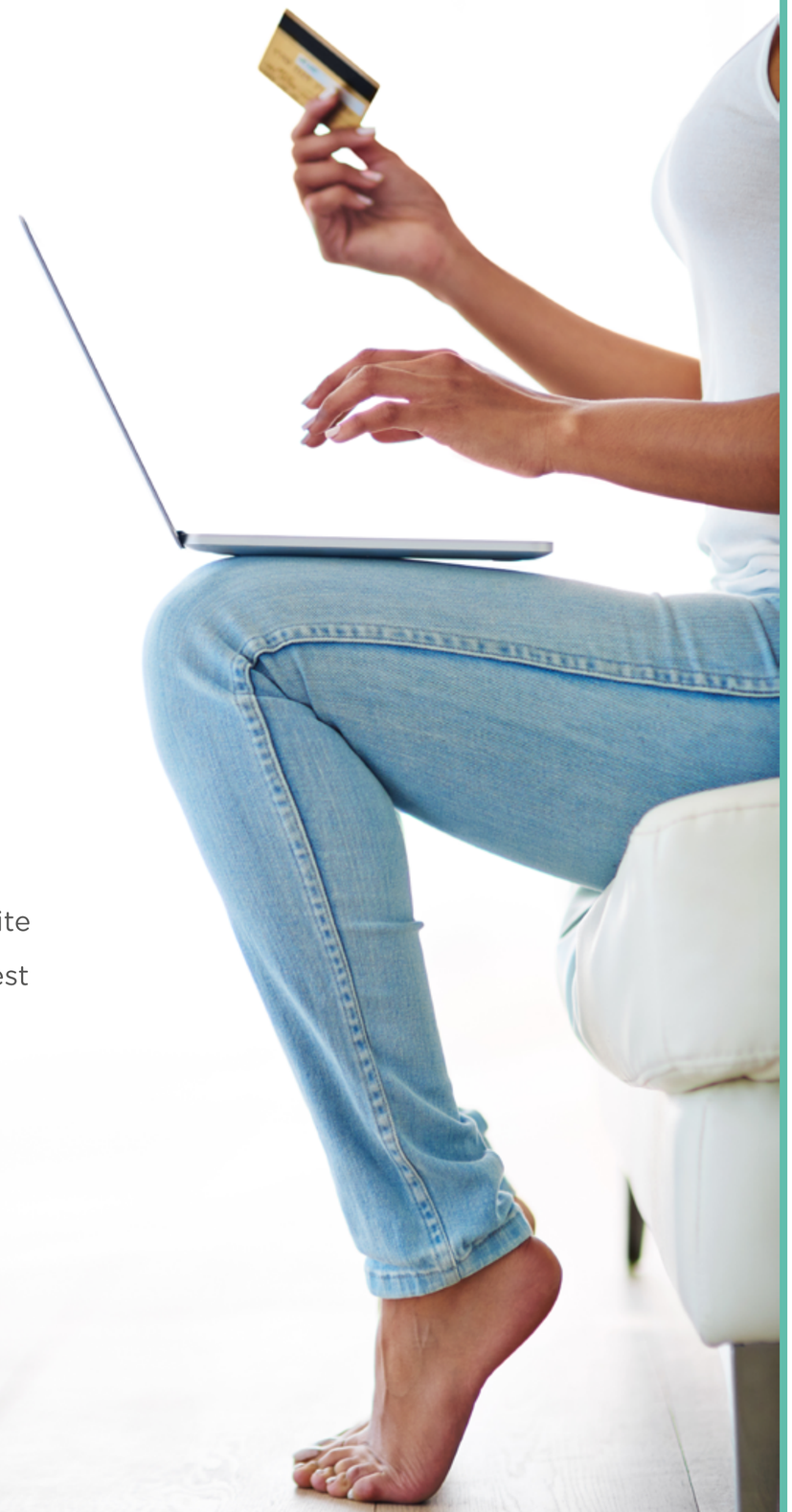
COMMENT SE PRÉPARER À LA DSP2 AVEC FAST'R BY CB

VOLET AUTHENTIFICATION FORTE

à destination des commerçants
et des prestataires d'acceptation
technique

www. cartes-bancaires.com - Septembre 2019

PAIEMENT SÉCURISÉ



AVERTISSEMENT

SOMMAIRE

PRÉAMBULE

OBJECTIF DU DOCUMENT

La Directive européenne sur les Services de Paiement (DSP2), en vigueur depuis janvier 2018, instaure de nouvelles règles entrant en application depuis le 14 septembre 2019.

Parmi ces nouvelles règles : les normes techniques réglementaires relatives à l'authentification forte du client, dites aussi RTS SCA (Regulatory Technical Standards on Strong Customer Authentification) qui consistent à vérifier via différentes méthodes que le client est bien détenteur de la carte de paiement présentée dans l'objectif de lutter contre la fraude en ligne.

Dans ce contexte, CB a développé un nouveau service pour mieux sécuriser les paiements en ligne : FAST'R by CB.

Ce guide a ainsi vocation à accompagner les e-commerçants et les Prestataires d'Acceptation Technique (PAT) dans la compréhension de cette réglementation ainsi que la mise en œuvre opérationnelle de la solution FAST'R by CB.

Toutes les terminologies propres au sujet sont décrites dans le glossaire en pages 37 à 39.

CARTES BANCAIRES CB EN BREF

CB est un Groupement d'Intérêt Économique qui définit les modalités de fonctionnement du schéma de paiement par carte CB (physique ou dématérialisée).

Créé en 1984, CB n'a pas cessé de développer le paiement par carte en y intégrant les dernières évolutions technologiques et sécuritaires pour le rendre toujours plus ergonomique, performant et sécurisé.

COMMUNIQUÉ DE PRESSE

Le 11 septembre 2019, l'Observatoire des moyens de paiement (OSMP) a publié un communiqué de presse pour annoncer le calendrier de migration de la Place française sur le volet DSP2/RTS SCA.

Deux calendriers sont à distinguer dans ce communiqué :

- Le calendrier de migration des méthodes d'authentification forte des clients. Il s'agit de remplacer progressivement le code SMS à usage unique par des solutions plus avancées. Ce calendrier prévoit qu'une très grande majorité des clients sera équipée d'ici juin 2022.
- Le calendrier de migration des infrastructures techniques au standard 3-D Secure EMVCo v2. Il s'étend sur une période de 18 mois de septembre 2019 à mars 2021. Il prévoit que d'ici à mars 2021, l'ensemble des acteurs se connectera à cette nouvelle infrastructure et appliquera les règles de fonctionnement définies par la DSP2/RTS SCA.

Retrouvez ces informations sur les liens suivants :

>>https://www.banque-france.fr/sites/default/files/medias/documents/2019-09-11_osmp_-_cp_migration_dsp2.pdf

>> https://www.banque-france.fr/sites/default/files/medias/documents/2019-09-11_osmp_-_plan_de_migration_dsp2.pdf

NOS ATOUTS

Le GIE CB a développé de nombreux services à valeur ajoutée qui font aujourd'hui de CB, le schéma de paiement par carte et par mobile le plus utilisé en France. Le schéma CB, c'est la garantie de plusieurs avantages compétitifs :

LA SÉCURITÉ DU SYSTÈME CB

Hautement sécurisé, le système CB dispose d'un taux de fraude faible.

LA PERFORMANCE

Une connaissance étendue du marché qui permet un taux d'acceptation très élevé.

LA PROTECTION DES DONNÉES

Le GIE CB garantit le traitement et le stockage des données en Europe et tout particulièrement en France, et cela, en complète conformité avec la réglementation sur la protection des données personnelles.

LA ROBUSTESSE DE NOS INFRASTRUCTURES

Le système CB utilise des infrastructures techniques avec un niveau élevé de disponibilité (à plus de 99%, 7 jours sur 7, 24 heures sur 24).

L'INNOVATION AU COEUR DE NOTRE ADN

Le système CB innove en permanence que ce soit pour le renforcement de la sécurité ou la mise à disposition de nouveaux services à valeur ajoutée.

UN RÉSEAU OPTIMAL

Le réseau CB est économique grâce à une optimisation et une mutualisation permanente des coûts.

(*) Chiffres CB 2018

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.

Des ateliers de travail sur l'implémentation de la DSP2 ont été menés depuis fin 2017 et dans lesquels différentes familles du e-commerce ont participé ainsi que les établissements bancaires membres du GIE CB.

LES FÉDÉRATIONS PRÉSENTES

AFTE – Association Française des Trésoriers d'Entreprise

FCA – Fédération du Commerce Coopératif et Associé

fcd

fevad – www.fevad.com

Mercatel – Pour le Commerce et la Distribution

U2P – union des entreprises de proximité

(*) Chiffres CB 2018

RAPPEL DU CONTEXTE RÈGLEMENTAIRE DE FAST'R BY CB

LES OBJECTIFS DE LA DSP2 : RENFORCER L'INNOVATION ET PROTÉGER LE CONSOMMATEUR

La DSP2 est entrée en vigueur en janvier 2018. Cette deuxième directive vise à :

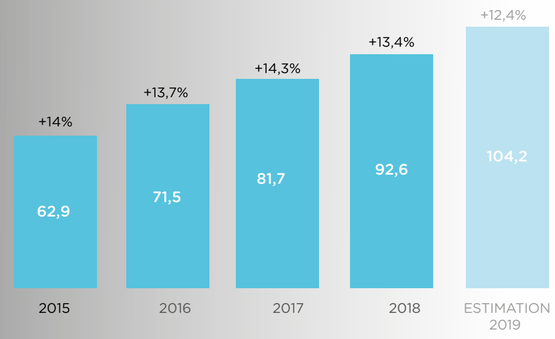
1. Favoriser l'innovation
2. Renforcer la sécurité des paiements

Dans le cadre de la DSP2, les normes techniques de règlementation (dites aussi RTS – Regulatory Technical Standards) de la DSP2 ont été rédigées par l'Autorité Bancaire Européenne (ABE) puis votées par le parlement européen le 13 mars 2018, pour une entrée en vigueur au 14 septembre 2019. Ces RTS viennent compléter la DSP2, lui donnant un cadre technique de mise en œuvre sur deux points :

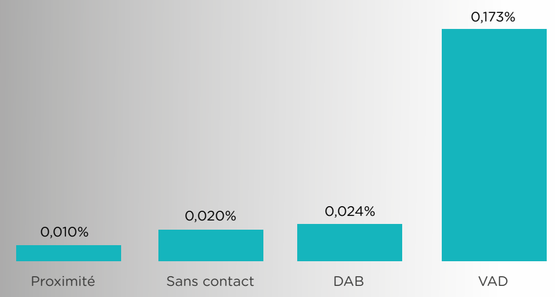
- L'authentification forte pour les paiements électroniques (SCA – Strong Customer Authentication),
- Les normes ouvertes communes sécurisées de communication (CSC).

Ce présent document se focalise sur les RTS SCA pour les paiements à distance..

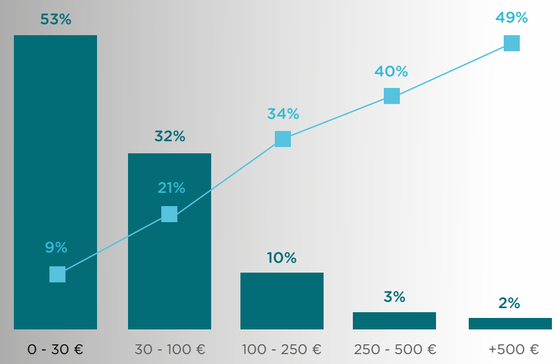
CHIFFRES CLÉS DE LA VENTE À DISTANCE (VAD) EN FRANCE



CHIFFRE D'AFFAIRES E-COMMERCE (MD €)
SOURCE FEVAD



TAUX DE FRAUDE EN 2018
SOURCE RAPPORT OSMP



EN 2018

RÉPARTITION DES OPÉRATIONS DE PAIEMENT CB

OPÉRATIONS DE PAIEMENT CB AUTHENTIFIÉES

SOURCE CB

UNE AUTHENTIFICATION FORTE SYSTÉMATIQUE

Les RTS SCA imposent l'authentification forte du porteur de la carte lorsque celui-ci initie une opération de paiement à distance.

Cette authentification, dite aussi authentification à deux facteurs, implique la vérification de deux éléments indépendants parmi 3 catégories :

UN ÉLÉMENT D'INHÉRENCE

ce que l'utilisateur « est »
(empreinte digitale, reconnaissance faciale, etc).

UN ÉLÉMENT DE CONNAISSANCE

ce que l'utilisateur « sait »
(mot de passe, PIN, etc.)

UN ÉLÉMENT DE POSSESSION

ce que l'utilisateur « possède »
(token, mobile, carte, etc.)

En France, les transactions cartes réalisées en proximité avec saisie d'un code confidentiel sont déjà aujourd'hui conformes aux RTS SCA.

Les transactions sans contact sans authentification font l'objet d'une dérogation prévue par le règlement.

Ce guide d'utilisation se focalise sur les transactions à distance. Celles-ci peuvent faire l'objet d'une authentification non systématique aujourd'hui, le plus souvent via 3-D Secure v1.

Quel avenir pour le code SMS à usage unique ?

La méthode d'authentification forte la plus utilisée à ce jour est l'OTP, one-time-password (86% des authentification fortes en 2017).

Cette solution repose sur la réception par le porteur de la carte d'un code à usage unique par message. Or, l'ABE a indiqué en 2018 que l'OTP SMS n'était pas une méthode d'authentification forte conforme aux RTS SCA.

La deuxième méthode d'authentification forte la plus utilisée en France est l'authentification sur application mobile. Elle nécessite que le porteur possède un smartphone. Elle n'a pas encore été adoptée par toutes les banques, et représente uniquement 12% des authentifications fortes, bien qu'elle soit en constante progression.

Dans ce cadre, la Banque de France a initié des travaux en concertation avec les banques, les commerçants et CB afin que l'usage de nouvelles méthodes d'authentification forte se développe rapidement et couvre l'ensemble de la population.

Le rapport de l'OSMP publié en juillet 2019 confirme l'acceptation du SMS jusqu'en juin 2022.

LES OPÉRATIONS DE PAIEMENT HORS CHAMP D'APPLICATION DES RTS SCA

Pour entrer dans le périmètres 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).

L'ABE a désigné expressément trois types de paiements VAD qui sont hors du champ d'application des RTS SCA :

LES PAIEMENTS INITIÉS PAR LE COMMERÇANT

L'authentification forte est complexe car l'opération de paiement n'est pas initiée par le porteur

LES PAIEMENTS DITS MO/TO
(MAIL ORDER, TELEPHONE ORDER)

Ceux-ci ne sont pas perçus comme des paiements électroniques

LES PAIEMENTS ONE-LEG

Les paiements dont l'acquéreur ou l'émetteur se trouve hors de l'Union Européenne

Pour ces 3 cas...

Le commerçant n'est pas tenu d'initier un processus d'authentification.

L'opération de paiement peut faire l'objet d'une demande d'autorisation sans être précédée d'une demande d'authentification.

LES DÉROGATIONS À L'AUTHENTIFICATION FORTE

La DSP2 impose une authentification forte du porteur systématique pour les opérations de paiement (cf. page 10).

Cependant, cinq cas de dérogations sont activables sur les paiements e-commerce par carte.

Le Régulateur estime que le risque de fraude de ces opérations de paiement est suffisamment bas pour ne pas solliciter le porteur. Être éligible à un seul cas de dérogation est suffisant pour bénéficier de l'authentification passive, dite aussi frictionless.

L'application de la dérogation est à la main du PSP émetteur de la carte.

Parce que la fluidité des parcours clients est également importante...

Ces cinq cas de dérogations permettent de bénéficier d'une authentification passive, c'est-à-dire que l'opération de paiement sera bien authentifiée, mais le porteur de la carte ne sera pas sollicité.

Un cryptogramme d'authentification est généré par l'émetteur, adressé au commerçant, et repris dans la demande d'autorisation.

	Petits montants	Transactions Risk Analysis	Paiement récurrent	Bénéficiaires de confiance	Carte non-nominative
0 - 30€	Sauf toutes les 6 opérations de paiement ou montant cumulé > 100€	Si le taux de fraudedu PSP émetteur OU acquéreur est < 0,13%	Si l'opération de paiement est effectuée dans le cadre d'un paiement récurrent à montant et bénéficiaire constants (hors première opération de paiement)	Si le bénéficiaire est inscrit par le payeur sur la liste des bénéficiaires de confiance Le whitelisting ne sera disponible qu'à partir de fin 2020.	Cette dérogation vise les paiements initiés par des payeurs « personnes morales » (cf article 17 des RTS SCA)
30 - 100€		Si le taux de fraude du PSP émetteur OU acquéreur est < 0,06%			
100 - 250€		Si le taux de fraude du PSP émetteur OU acquéreur est < 0,01%			
250 - 500€		Le taux de fraude est calculé par établissement bancaire, par moyen de paiement. Le PSP émetteur ou acquéreur doivent réaliser une analyse de risque.			
+ de 500€					

LA GESTION DES DÉROGATIONS

Pour les opérations CB, le commerçant exprime un souhait sur le type d'authentification à mettre en œuvre (authentification forte ou frictionless).

C'est toujours l'émetteur qui décide de mettre en œuvre ou non une dérogation, ainsi que sa nature (sa base légale vis-à-vis du Règlement).

LE DISPOSITIF PROPOSÉ POUR UN PAIEMENT CB AVEC 3-D SECURE

RAPPEL DES FLUX DE PAIEMENT

Les opérations de paiement génèrent quatre types de flux différents :

1. Le flux d'authentification permet à l'émetteur d'authentifier l'utilisateur de la carte aux fins de s'assurer qu'il en est bien le titulaire.
2. Le flux d'autorisation permet à l'émetteur de réaliser différents contrôles de gestion du risque liés au fonctionnement de la carte, notamment les contrôles relatifs aux plafonds de paiement, aux fins d'accepter ou de refuser le paiement.
3. Le flux de remise permet de remonter toutes les transactions traitées par le commerçant à son acquéreur aux fins de créditer son compte.
4. Le flux de compensation organise l'échange financier entre l'acquéreur et l'émetteur aux fins de débiter les comptes de paiement des porteurs.

Actuellement, le commerçant a le choix d'effectuer ou non une demande d'authentification. A cet effet, il utilise le plus souvent le protocole d'authentification 3DS V1.

Dans le cadre des RTS SCA, toute opération de paiement qui est dans le champ d'application doit être authentifiée (de façon forte ou passive).

Les dérogations peuvent permettre au porteur d'être authentifié de manière passive, dite aussi frictionless. Un cryptogramme est généré par l'émetteur à l'issue de l'opération attestant de l'authentification du porteur.

Il est important de noter que les paiements soumis à exemption présentent également un cryptogramme d'authentification assurant qu'une analyse de risque a bien été réalisée.

La gestion de ces exemptions nécessite d'utiliser le protocole EMVCo 3DS v2 pour bénéficier de l'authentification passive et d'utiliser pour les opérations CB, le service FAST'R by CB.

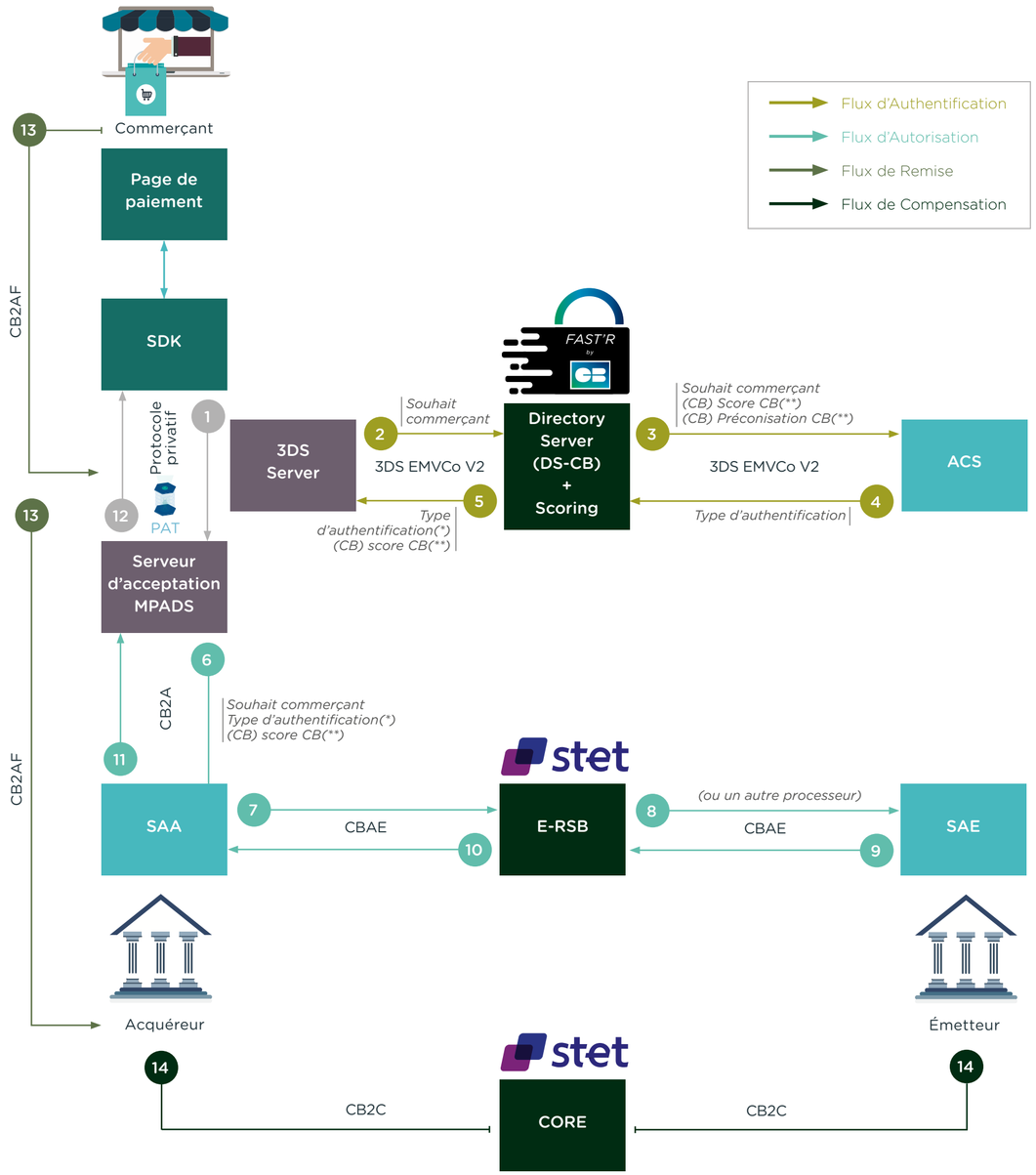
Si une opération de paiement entrant dans le champ des RTS SCA fait l'objet d'une demande d'autorisation sans avoir fait l'objet d'une authentification forte ou passive au préalable, les émetteurs peuvent refuser l'autorisation et demander au commerçant de réaliser une demande d'authentification forte ou passive.

L'utilisation du protocole d'authentification 3DS v1 reste possible pour les opérations CB jusqu'à fin 2020.

Ce protocole ne permet pas la gestion des exemptions prévues par les RTS ni la mise en œuvre de l'authentification passive.

Schéma type d'une opération de paiement CB en 3DS EMVCo v2

La solution FAST'R s'intègre dans les flux existants.



(*) *Authentification forte ou authentification passive*

(**) *Champs liés au scoring FAST'R by CB*

1 Les données de l'opération de paiement devant être transmises avec le protocole d'authentification 3D Secure EMVCo sont envoyées du serveur du commerçant (SDK) au Prestataire d'Acceptation Technique (PAT).

Le flux d'Authentification

2 Le message de demande d'authentification contenant les données et le souhait du commerçant est envoyé au Directory Server CB (DS-CB) de la solution FAST'R by CB par le PAT.

3 FAST'R by CB analyse le risque de l'opération de paiement, et émet une recommandation qu'il transfère à l'ACS de l'émetteur de la carte.

4 L'ACS authentifie fortement ou passivement le porteur. Le type d'authentification mis en œuvre ainsi que le cryptogramme d'authentification sont indiqués dans le flux de réponse.

5 FAST'R by CB transfère ces informations ainsi que son propre score de l'opération de paiement au 3DS Server du PAT.

Le flux d'Autorisation

6 7 Le PAT envoie à l'acquéreur l'opération de paiement dans la demande d'autorisation, qui la transfère à l'émetteur. Le flux d'autorisation permet d'identifier le cas d'usage, le fait que l'opération soit dans le champ d'application du RTS, l'éligibilité à une exemption et. les résultats de la demande d'authentification forte.

8 9 L'émetteur reçoit une demande d'autorisation et effectue plusieurs vérifications : identification du cas d'usage, règles d'authentification forte applicable, gestion du risque, vérification que la transaction a fait ou non l'objet d'une demande d'authentification. Il transfère sa réponse à l'acquéreur.

10 11 La banque acquéreur reçoit la réponse et partage l'information avec le PAT du commerçant.

12 Le PAT informe le commerçant de l'acceptation ou du refus de l'opération de paiement.

Le flux de Remise

13 Le commerçant envoie la remise à son acquéreur.

Le flux de Compensation

14 Le mouvement de compensation est envoyé par l'acquéreur à l'émetteur, à travers le système interbancaire de compensation.

LA SOLUTION FAST'R BY CB

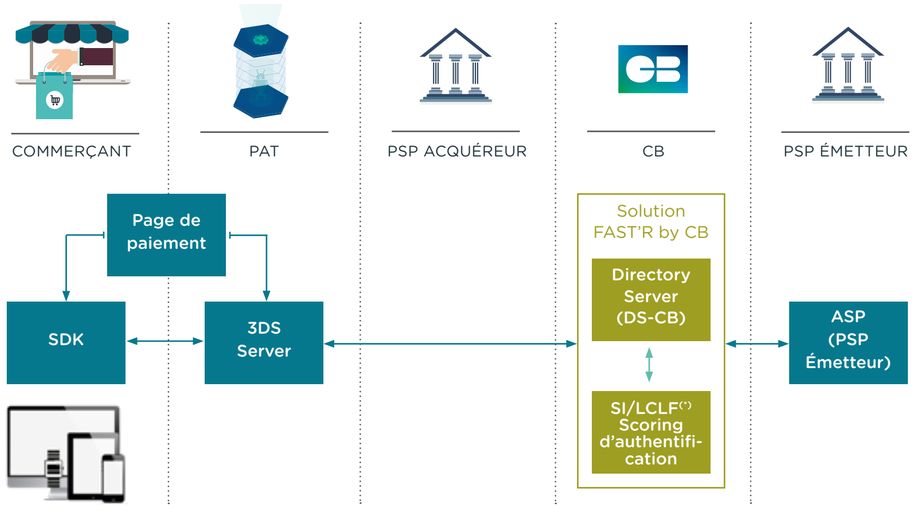
L'architecture de la solution FAST'R by CB

La solution FAST'R by CB répond à un besoin de lutte contre la fraude e-commerce et de fluidification des parcours client dans le cadre des nouveaux RTS SCA.

C'est une solution créée en concertation avec les commerçants et les banques, afin de s'adapter aux différents cas d'usage remontés dans le cadre du CCC.

L'ensemble des acteurs (PAT, acquéreur, émetteur) doit être raccordé pour que les opérations de paiement CB soient authentifiées et bénéficient des services CB.

Illustration de l'architecture de FAST'R by CB



(*) Système d'Information de lutte contre la fraude

Page de paiement

La page de paiement est hébergée par le PAT ou le commerçant. Si la marque CB est choisie, alors l'opération de paiement doit donner lieu à une demande d'authentification transmise à la solution FAST'R by CB avec le protocole 3DS EMVCo.

SDK

Le SDK est un élément logiciel permettant au commerçant de véhiculer des données à son PAT au cours d'un processus d'achat.

3DS SERVER

Le 3DS Server permet la transmission des données du SDK commerçant à la solution FAST'R by CB pour la mise en œuvre d'une authentification 3-D Secure.

PAIEMENT SÉCURISÉ

DIRECTORY SERVER (DS-CB)

Le Directory Server (DS-CB) est l'annuaire des cartes de paiement CB qui route vers la demande d'authentification vers l'émetteur. FAST'R by CB assure 99,995% de disponibilité de service.

SI/LCLF

CB possède un système d'information dédié à la lutte contre la fraude. Il s'appuie sur les données contenues dans les flux d'authentification, d'autorisation, et de compensation. Depuis sa mise en place en 2014, l'outil de scoring a permis une baisse du taux de fraude de 20%.

SCORING D'AUTHEN-TIFICATION

Le scoring d'authentification intègre le scoring CB de lutte contre la fraude ainsi qu'un scoring à part nouvellement développé par CB, basé sur la gestion du risque du commerçant.

ACS (PSP EMETTEUR)

L'ACS est le serveur d'authentification de la banque émetteur. L'ACS évalue le risque de l'opération de paiement, basé sur sa connaissance du client, la recommandation CB ainsi que les données contenues dans le protocole EMVCo. Il prend la décision d'authentifier fortement ou non l'opération de paiement. En cas de panne, CB peut se substituer à l'ACS, permettant l'aboutissement de l'opération de paiement.

Chacun des acteurs de la chaîne a accès à des informations spécifiques.

Le commerçant a notamment accès à des données sur le client, le dispositif utilisé et l'opération de paiement.

CB a accès à l'historique de la carte et la banque émetteur connait les habitudes du porteur.

Ensemble, ces informations permettent d'évaluer le risque conformément aux RTS SCA et de manière optimale (cf. page 34).

LA SOLUTION
FAST'R BY CB

Souhait commerçant et transfert de responsabilité interbancaire

Le commerçant ne dispose pas de la décision finale d'authentifier fortement ou passivement l'opération de paiement. Ce choix appartient à l'émetteur. Le commerçant peut en revanche faire connaître sa préférence : trois choix sont disponibles, applicables pour chaque opération de paiement :

- Souhait d'une authentification passive,
- Souhait d'une authentification forte,
- Pas de préférence.

L'expression de ce souhait entre en compte dans le scoring CB et il est communiqué à l'émetteur.

De plus, ce souhait a un impact sur le transfert de responsabilité interbancaire CB (voir schéma ci-dessous).

La charge de la fraude est toujours supportée par l'émetteur, sauf dans le cas où le commerçant demande de l'authentification passive (frictionless) et l'émetteur applique ce choix.

Le commerçant transmet son souhait dans un champ prévu à cet effet dans l'extension CB du protocole 3DS EMVCo V2.

Un commerçant qui souhaite de l'authentification forte peut se voir attribuer du frictionless, dans le cas où l'émetteur juge la transaction suffisamment peu risquée pour solliciter le porteur.

Le type d'exemption appliquée par l'ACS (Ex : TRA Acquéreur, Petits montants, TRA Emetteur,...) n'a aucun impact sur le transfert de responsabilité.

L'application de la garantie de paiement sera précisée dans le contrat d'acceptation entre l'acquéreur et le commerçant.

Matrice interbancaire du transfert de responsabilité

	Si l'émetteur applique de l'authentification passive	Si l'émetteur applique de l'authentification forte
Avec souhait commerçant « authentification passive » Champ 3DS Requestor Challenge Indicator = « 02 »	Coût de la fraude supporté par l'acquéreur	Coût de la fraude supporté par l'émetteur
Avec souhait commerçant « authentification forte » Champ 3DS Requestor Challenge Indicator = « 03» (Challenge Requested : 3DS Requestor Preference) ou « 04 » (Challenge Requested : Mandate)	Coût de la fraude supporté par l'émetteur	Coût de la fraude supporté par l'émetteur
Avec « pas de souhait » Champ 3DS Requestor Challenge Indicator = « 01 »	Coût de la fraude supporté par l'émetteur	Coût de la fraude supporté par l'émetteur

NOTE

La matrice ci-dessus s'applique uniquement pour la 1ere opération (excepté pour le cas du paiement à l'expédition : dans la limite de 30 jours après la demande d'authentification).

LA SOLUTION
FAST'R BY CB

Partage de données

La solution FAST'R by CB utilise le protocole d'échange 3DS V2 EMVCo. Ce protocole est un langage dédié au flux d'authentification, permettant le transfert d'informations entre le PAT du commerçant et la banque émettrice.

Deux types de données circulent dans le protocole :

1. Les données obligatoires,
2. Les données optionnelles.

Les données obligatoires sont nécessaires à l'envoi de l'opération de paiement dans le flux d'authentification.

Les données optionnelles entrent aussi en compte dans le scoring CB. Ces données sont indiquées en REC – recommandée pour obtenir du frictionless – dans le guide d'intégration pour les 3DS Server. Elles concernent :

- Les données du commerçant,
- Les données de l'opération de paiement,
- Les données de la carte et de son porteur,
- Les données de l'appareil utilisé pour cet achat.

Parmi ces données optionnelles, un certain nombre sont jugées particulièrement pertinentes par CB dans le cadre du calcul d'un taux de risque de fraude, afin de pouvoir bénéficier d'une authentification passive. Les données jugées prépondérantes sont :

- Le scoring commerçant. Chaque commerçant possède un scoring avec son format propre. La solution FAST'R by CB pourra l'exploiter (avec un temps d'apprentissage),
- Le nombre d'articles dans la commande,
- Le nom du client,
- L'adresse de livraison ou adresse de facturation,
- L'adresse e-mail ou numéro de téléphone,
- Le shipping indicator (mode de livraison : point relais, domicile, magasin, etc.).

Ces données sont traitées en conformité avec le RGPD et le PCI DSS (norme de sécurité de l'industrie des cartes de paiement).

Ces données sont exploitées uniquement dans le cadre de la prévention et de la lutte contre la fraude.

Au regard du RGPD, CB considère qu'il est **responsable de traitement** pour les données qui lui sont transférées, et ce dans une finalité de prévention et de lutte contre la fraude.

CB recommande aux commerçants de définir leur statut avec leur PAT. En tout état de cause, CB ne considère ni le PAT ni le commerçant comme ses sous-traitants (cf. page 34).

LA SOLUTION
FAST'R BY CB

Low Risk Merchant Program

Les commerçants présentant un faible taux de fraude peuvent bénéficier du Low Risk Merchant Program pour les montants allant de 0 à 100€.

BESOIN

Lorsqu'un commerçant demande à l'émetteur de ne pas authentifier fortement le payeur, il n'a aucune garantie que l'émetteur accepte et procède à une authentification passive.

SOLUTION CB

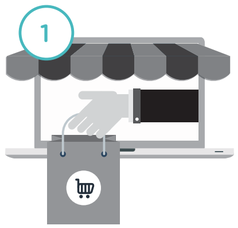
Les émet-teurs s'engagent à respecter le souhait du commerçant adhérant au programme lorsqu'il exprime le souhait de ne pas authentifier le payeur sur la tranche 0-100€ (pas de transfert de responsabilité).

Ce programme permet de valoriser les investissements du commerçant dans les outils de gestion et d'analyse du risque.

Le commerçant est invité à se rapprocher de son acquéreur principal pour connaître son éligibilité au programme.

En cas de réponse positive, l'acquéreur fera la demande auprès de CB.

Illustration de la cinématique de paiement pour un commerçant adhérent au programme



Dans le protocole 3DS v2, via son souhait, le commerçant demande à l'émetteur de ne pas authentifier fortement le porteur suite à son analyse de risque.

Cela est possible grâce au flag « frictionless obligatoire ».

L'émetteur reconnait que le commerçant est adhérant du programme et que l'opération de paiement entre dans le cadre d'une exemption.

L'émetteur respecte la demande du commerçant et applique la dérogation.

ÉVOLUTION DES
RÈGLES CB

A l'occasion de la mise en œuvre des RTS SCA, CB fait évoluer ses règles sur les opérations de paiement VAD, afin de mieux répondre à l'évolution des pratiques des commerçants.

4 évolutions principales des règles CB

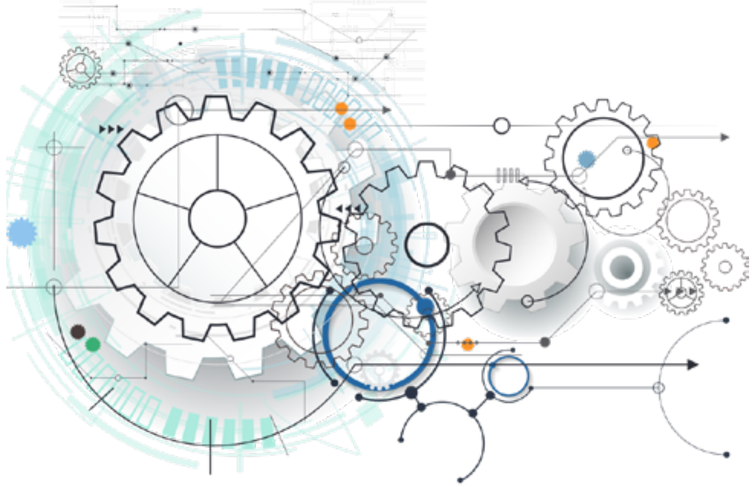
1. Les règles CB permettent l'identification des cas de paiement pour l'application des cas de dérogation à l'obligation d'authentification forte (pour les opérations dans le scope des RTS SCA).

2. Pour le cas d'usage de paiement à l'expédition, les opérations pourront bénéficier du transfert de responsabilité dans la limite de 30 jours suivants la commande.

3. Il devient possible d'utiliser une même authentification pour plusieurs demandes d'autorisation liées à une même commande (cette utilisation est limitée à une durée de 180 jours pour le cas de paiement à l'expédition). Les opérations doivent être liées entre elles par une référence de chaînage.

4. Le cryptogramme visuel (CVx2) devient optionnel pour les opérations de paiement avec authentification, cela correspond notamment aux cas du One Clic et de l'utilisation d'un wallet.

Ces règles sont applicables à partir du 1er octobre 2019.



LE CHAINAGE DES OPÉRATIONS DE PAIEMENT

CB a développé une fonctionnalité de chaînage des opérations de paiement.

Le chaînage des opérations dans les flux d'autorisation permet aux émetteurs d'identifier une série d'opérations de paiement liées entre elles et de garantir qu'une authentification a été mise en œuvre pour une série d'opérations. Cette référence s'applique pour toutes les opérations de paiement à distance quelle que soit la solution d'authentification utilisée (3DS EMVCo V2, 3DS V1, Paylib).

La référence unique de transaction est renseignée par l'émetteur dans la réponse à la demande d'autorisation (ou de renseignement) d'une opération de type paiement unique, ou d'une première opération de paiements multiples.

Le périmètre concerné par le chaînage englobe tout paiement à distance (e-commerce, MO/TO) unique ou pouvant faire l'objet d'une récurrence. La référence unique de transaction renseignée en réponse d'autorisation (ou de renseignement) est aussi reprise en compensation.

Afin de mettre en place ce chaînage, le protocole d'autorisation CB2A a évolué : le champ 47 type 95 devient la donnée « Référence unique de transaction ». Afin de rendre cette donnée utilisable par tous les réseaux, un identifiant de nomenclature est ajouté en premier caractère de cette donnée.

Comment est valorisée la référence de chaînage dans la réponse à la demande d'autorisation ?

Pour toutes les transactions de vente à distance, l'émetteur doit générer sa propre référence de transaction et la transmettre dans le champ 47 type 95 des messages réponse avec en première position la valeur « 1 » qui définit une nomenclature CB.

Cette référence de transaction est une valeur alphanumérique sur 15 caractères.

Cette référence sera conservée par les e-commerçants ou leur PAT. Elle est reprise dans les demandes d'autorisations subséquentes sous l'appellation « identifiant de regroupement ».

Les cas de paiements récurrents

Pour les paiements récurrents dont la réponse à la demande d'autorisation (ou de renseignement) initiale ne contient pas une « Référence unique de transaction », qu'ils soient initiés avant ou après le 14 septembre 2019 :

- Le commerçant peut envoyer ses demandes d'autorisation subséquentes sans identifiant de regroupement jusqu'à l'échéance où il reçoit une « Référence unique de transaction » dans le champ 47 type 95 de la réponse à la demande d'autorisation.
- Toutes les demandes d'autorisation subséquentes suivantes doivent contenir la valeur de cette « Référence unique de transaction » dans le champ « Identifiant de Regroupement » 47 type 99.
- Les SAE doivent envoyer une « Référence unique de transaction » pour toutes les opérations de paiement e-commerce au plus tard en T4 2019.
- CB recommande aux SAE de refuser les demandes d'autorisation subséquentes – sans identifiant de regroupement – à partir du 1er janvier 2022.

Pour les paiements récurrents initiés après le 14 septembre 2019 dont la réponse à la demande d'autorisation (ou de renseignement) initiale contient une « Référence unique de transaction » :

- Dans toutes les demandes d'autorisation subséquentes, le commerçant doit valoriser le champ 47 type 99 « Identifiant de Regroupement » en utilisant la « Référence unique de transaction » reçue dans le champ 47 type 95 de la réponse à la demande d'autorisation (ou de renseignement) initiale.

La **demande de renseignement** rassure le commerçant sur la validité de la carte.

Dans la majorité des cas, la demande d'autorisation s'effectue lorsque la commande est validée.

Mais, dans certains achats (précommande, réservation anticipée, etc.), **la demande d'autorisation peut intervenir plusieurs jours après la commande**.

Quelles sont les autres données à valoriser pour le chaînage des opérations de paiement ?

Pour le chainage, plusieurs données ont été ajoutées aux messages d'autorisation comme les données e-commerce de la première transaction, le numéro et le nombre total des échéances, la date de fin d'échéance et la somme des montants déjà autorisés.

Note : Pour la première demande d'autorisation (ou de renseignement) :

- le N° échéance est égal à 1 pour une demande d'autorisation et à 0 pour une demande de renseignement,
- la somme des montants déjà autorisés est valorisée à 0,
- le nombre total d'échéances n'est pas à valoriser pour le cas d'usage « Autre abonnement ».

Schéma simplifié de la mise en place du chaînage pour une opération de paiement de rang 1

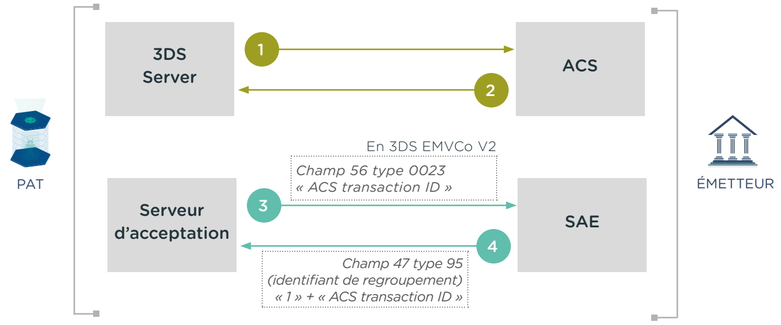
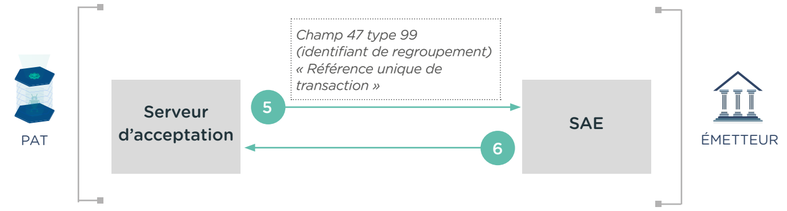


Schéma simplifié de la mise en place du chaînage pour une opération de paiement de rang > 1



Le flux d'Authentification

1 2 Pour le chainage, plusieurs données ont été ajoutées aux messages d'autorisation comme les données e-commerce Lors d'une opération de paiement de rang 1, le PAT demande l'authentification de l'opération de paiement sur le montant total de l'achat. L'émetteur réalise une authentification forte ou passive

Le flux d'Autorisation

3 Le PAT remonte à l'émetteur toutes les données de l'authentification, notamment le champ 56 type 0023 de la demande d'autorisation « l'ACS transaction ID ». Cela n'est disponible qu'en 3DS EMVCo V2.

4 L'émetteur génère l'identifiant unique de transaction, précédé de la valeur « 1 », dans la réponse à la demande d'autorisation (champ 47 type 95).

5 Le commerçant reprend cette valeur dans « l'identifiant de regroupement », champ 47 type 99.

6 Le SAE répond à la demande d'autorisation.

LES AVANTAGES DU DISPOSITIF CB

Jusqu'à 85% d'authentification passive en cible

Grâce aux analyses de fraudes CB Scoring, CB est en mesure de déceler les opérations de paiement à risque et recommande une authentification forte si nécessaire.

Taux d'autorisation parmi les plus élevés en Europe

Fondé sur l'analyse de milliards de paiements CB, le score CB optimise les taux de transformation du e-commerce.

99,99% de disponibilité de service

Une disponibilité maximale garantissant la transformation des achats, avec la possibilité de se substituer aux ACS quand nécessaire.

Adapté à tous les parcours client

Service disponible sur tous les dispositifs en mode « browser » et « in-app ».

Un programme récompensant les commerçants peu fraudés

Ce programme permet aux commerçants peu fraudés d'influer sur la décision de l'émetteur de procéder à une authentification forte ou non.

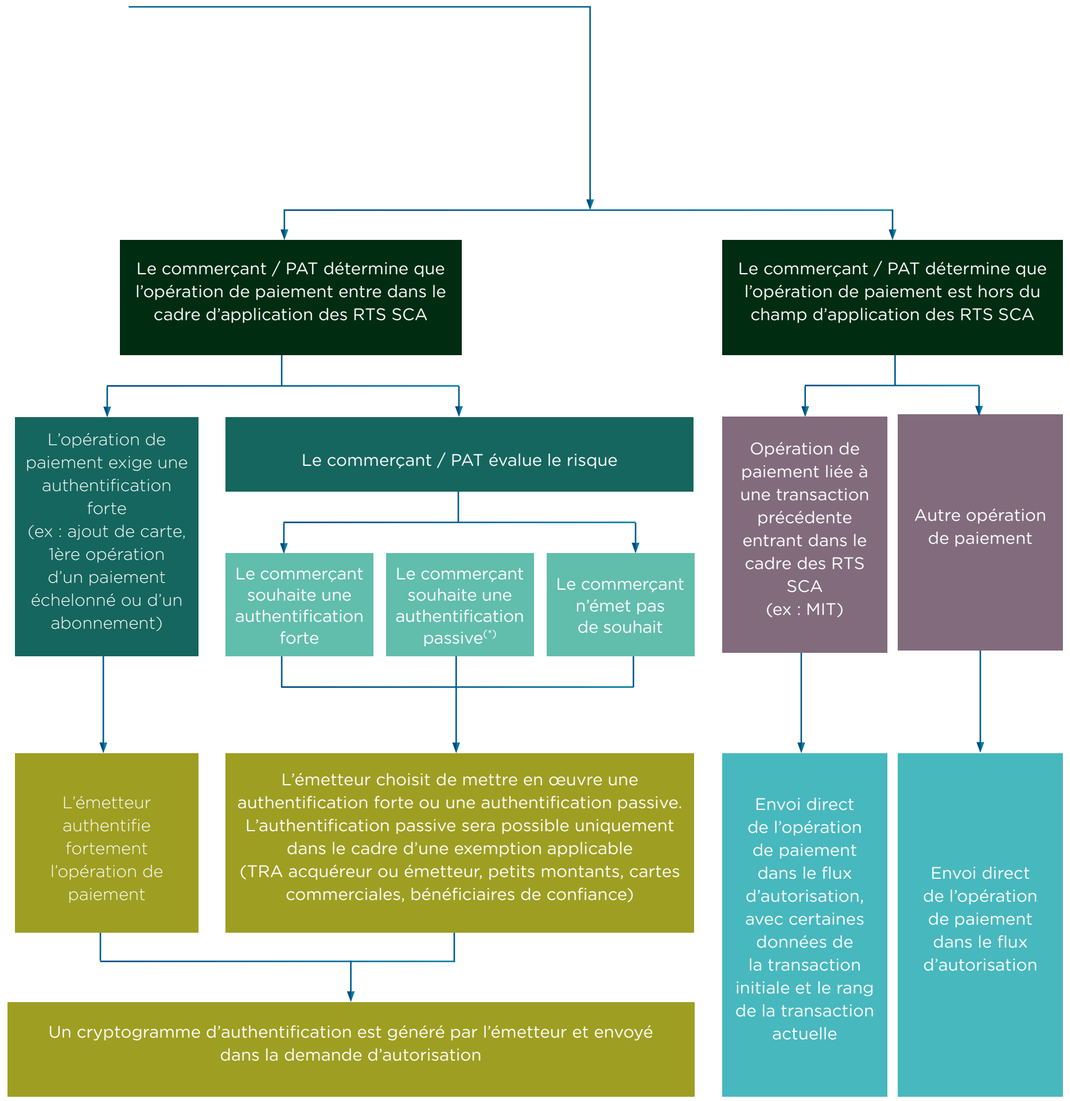
Facilité d'utilisation

bénéficier de la solution FAST'R by CB dès lors qu'il possède un SIRET valide.

OPÉRATION DE PAIEMENT AVEC FAST'R BY CB ET CARTOGRAPHIE DES CAS D'USAGE À DISTANCE

VISION GÉNÉRALE DES ÉTAPES D'UNE OPÉRATION DE PAIEMENT AVEC FAST'R BY CB :

UNE OPÉRATION DE PAIEMENT EST INITIÉE



(*) Le commerçant peut indiquer s'il est éligible à la TRA acquéreur

CARTOGRAPHIE
DES CAS D'USAGE À DISTANCE
Les opérations simples

1 — Paiement unique (à la Commande)

Authentification forte ou passive + Demande d'autorisation / remise — CIT

2 — Paiement unique (à l'expédition / livraison / délivrance du service)

Ex : paiement d'un produit dont le règlement intervient au moment de son expédition.

Authentification forte ou passive + Demande de renseignement — CIT

\+

A l'envoi du produit
Autorisation / remise sur le montant total

NOTE

Dans certaines situations le montant total dépasse le montant initialement prévu (ex : VTC), le commerçant génère une nouvelle transaction (MIT) sans lien avec la première

3 — Ajout / Modification de données carte en dehors d'un parcours de paiement

Ex : enregistrement de données carte dans le compte d'un client.

Authentification forte + Demande de renseignement — CIT

4 — Paiement agrégé d'achats multiples

Ex : règlement en une fois de plusieurs achats de petit montant sur une durée limitée.

Authentification forte ou passive sur le montant maximum + Demande d'autorisation / remise sur le montant maximum — CIT

5 — Paiement pour la Locaion de Biens et Services (PLBS)

Ex : location d'une voiture.

Authentification forte ou passive sur le montant estimé + Demande d'autorisation sur montant estimé / clôture et remise sur le montant réel (dans les 30 jours) — CIT

6 — Paiement complémentaire / No-show

Ex : facturation d'une réservation de chambre d'hôtel non honorée, ou paiement de la facture de mini-bar établie après le départ du client.

Demande d'autorisation / remise sur le montant de la facture — MIT

CIT MIT

CARTOGRAPHIE
DES CAS D'USAGE À DISTANCE
Les opérations multiples

7 — Paiement multiple à l'expédition

Ex : paiement d'une commande livrée en plusieurs fois.

Authentification forte ou passive sur le montant total + Demande de renseignement — CIT

\+

A chaque expédition
Demande d'autorisation / remise sur le montant du produit expédié.

8 — Paiement échelonné

Ex : paiement en 3-4 fois.

Authentification forte sur le montant total + Demande d'autorisation / remise sur le montant du premier paiement — CIT

\+

Pour les paiements suivants
Demande d'autorisation / remise sur chaque montant de paiement.

9 — Abonnement à montant total connu

Ex : abonnement d'une année dont le montant total est connu à la commande.

Authentification forte sur le montant total + Demande d'autorisation / remise sur le montant du premier paiement — CIT

\+

Pour les paiements suivants
Demande d'autorisation / remise sur chaque montant de l'échéance.

10 — Abonnement de montant variable ou date de fin inconnue

Ex : abonnement opérateur téléphonique avec facture sur consommation.

Authentification forte sur le montant de la première échéance + Demande d'autorisation / remise sur le montant du premier paiement — CIT

Pour les paiements suivants
Demande d'autorisation / remise sur chaque montant de l'échéance — MIT

CIT MIT

ANNEXES

LOGOS CB

CB a développé un nouveau logo

Le logo Paiement Sécurisé est à implémenter sur les pages de paiement.

Il est l'élément de référence d'une opération de paiement traitée par CB. Il a pour but de rassurer le client sur la sécurité du processus de paiement.

Validé par les internautes lors d'une étude réalisée fin 2017, le logotype Paiement Sécurisé conjugue un cadenas fermé et une expression française pour conforter le client d'un traitement sécurisé effectué en France.

PAIEMENT SÉCURISÉ

Pour télécharger le logo CB Paiement Sécurisé :

www. cartes-bancaires.com/a-propos/chartes-graphiques-et-telechargements-logos

TEMPLATE DE PAIEMENT RECOMMANDÉ PAR CB

Votre panier

Article 1	xx,xx €
Article 2	xx,xx €
Total	**xx,xx €**

Votre adresse de livraison

Choix du moyen de paiement

Carte — Choisir

Wallet — Pay — Choisir

Autres — Choisir

La sélection d'un bouton unique pour le paiement par carte.

Votre paiement est sécurisé par le système 3D Secure
Votre banque va vérifier votre identité afin de vous prémunir de toute utilisation frauduleuse de votre carte bancaire.

Numéro de la commande: COFWGG8RX0TTJ6 MARCHAND A

Payer avec

Titulaire de la carte* Prénom Nom

Numéro de la carte* 4974 4521

Date d'expiration (MM/AAA)* 09 2019

Code de vérification de la carte* 123 Qu'est ce que c'est ?

Un * indique les champs obligatoires

Confirmer le paiement

Si vous voulez choisir une autre marque de paiement, cliquer ici

PAIEMENT SÉCURISÉ — Verified by VISA — MasterCard SecureCode

A propos de Ogone | Protection des données
Sécurité | Informations légales

Norton SECURED

Annulation

Affichage dynamique de la marque préférée du commerçant et possibilité pour le client de changer.

PROTECTION DES DONNÉES PERSONNELLES

Le service FAST'R by CB est développé par CB pour répondre aux objectifs suivants :

- Prévenir et lutter contre la fraude à la carte de paiement dans le système CB,
- Permettre à ses membres, et en particulier aux émetteurs, de se conformer aux nouvelles dispositions légales qui leur sont applicables,
- Permettre aux commerçants de préserver la fluidité de leur parcours client dans le respect du cadre légal applicable.

Ces objectifs s'inscrivent pleinement dans le contexte de l'entrée en vigueur des RTS SCA le 14 septembre 2019 qui prévoient notamment :

Un principe d'authentification forte systématique du porteur de la carte lors de chaque opération de paiement ;

Des dérogations à ce principe et notamment quand une analyse des risques permet de considérer le niveau de risque de fraude lié à l'opération comme faible (article 18).

Pour atteindre ces objectifs, les différents intervenants au service FAST'R by CB (commerçants, PATs, CB et émetteurs) traitent et se transmettent des données prévues par le protocole d'échange 3DS EMVCo V2 EMVCo.

Certaines de ces données, qui concernent le porteur de la carte de paiement, sont protégées par la règlementation applicable en matière de protection des données à caractère personnel et notamment le Règlement (UE) 2016/679 (RGPD).

Sous réserve du respect des dispositions du RGPD, le traitement de ces données par les différents intervenants au service FAST'R by CB est légitime car elles sont nécessaires à la réalisation de l'analyse des risques de fraude.

En effet, l'article L521-6 du Code monétaire et financier dispose que les systèmes de paiement et les prestataires de services de paiement (PSP) sont légitimes à mettre en œuvre des traitements de données à caractère personnel lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements.

La DSP2 (considérant 95) et les RTS SCA (considérant 1er) prévoient clairement que l'authentification sûre du porteur a notamment pour objectif la prévention de la fraude.

L'article 18 des RTS SCA dispose qu'un PSP peut ne pas authentifier fortement le payeur lorsque, suite à une analyse des risques, il considère le risque de fraude comme étant faible et que cette analyse des risques est notamment (il existe d'autres conditions et notamment le respect des seuils de taux de fraude) réalisée dans les conditions évoquées ci-dessous :

L'analyse des risques doit permettre de déceler l'inexistence des éléments suivants :

- des dépenses anormales ou un type de comportement anormal du payeur ;
- des informations inhabituelles concernant l'utilisation du dispositif ou logiciel du payeur à des fins d'accès ;
- des signes d'infection par un logiciel malveillant lors d'une session de la procédure d'authentification ;
- un scénario connu de fraude dans le cadre de la prestation de services de paiement ;
- une localisation anormale du payeur ;
- une localisation du bénéficiaire présentant des risques élevés.

Dans son rapport annuel 2017, l'Observatoire de la sécurité des moyens de paiement (OSMP) indique qu'en raison de l'évolution majeure opérée par la DSP2 dans le processus de décision en matière d'authentification désormais « à la main de l'Emetteur », des échanges d'information entre le Commerçant et l'Emetteur peuvent avoir lieu pour « alimenter le dispositif d'évaluation des risques » de l'Emetteur et faciliter l'éventuelle application de la dérogation prévue à l'article 18 des RTS SCA,. comme cela est techniquement prévu dans les spécifications du protocole 3D-Secure 2.0.

Par ailleurs, les différents intervenants de la solution FAST'R by CB sont tenus de se conformer à l'ensemble des dispositions prévues par la législation applicable en matière de protection des données à caractère personnel et en particulier au RGPD. Chaque intervenant devra notamment :

- Déterminer avec les autres intervenants le statut au titre duquel il traite les données à caractère personnel. En tout état de cause, CB traite, en tant que responsable du traitement, les données à caractère personnel qui lui sont transmises par le PAT pour la finalité qui lui est propre, c'est-à-dire la lutte contre la fraude à la carte de paiement dans le système CB. CB ne considère, ni les commerçants, ni les PATs comme étant ses sous-traitants.
- S'assurer, lorsqu'il est responsable du traitement, que les données à caractère personnel qu'il traite le sont pour des finalités déterminées, explicites et légitimes.
- Se conformer autres dispositions de la règlementation qui lui serait applicable en matière de protection des données à caractère personnel : registre, analyse d'impact, transparence et droits des personnes concernées, sécurité et confidentialité des données...

L'analyse des risques doit tenir compte, « au moins », des facteurs suivants :

- les habitudes de dépenses antérieures de l'utilisateur individuel de services de paiement;
- l'historique des opérations de paiement de chacun des utilisateurs de services de paiement du prestataire de services de paiement ;
- 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 PSP ;
- l'identification de comportements de paiement anormaux de l'utilisateur de services de paiement par rapport à l'historique de ses opérations de paiement.

GLOSSAIRE

ABE (Autorité Bancaire Européenne)

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.

ACS (Access Control Server)

Serveur d'authentification de la banque du payeur.

Authentification forte

Procédure d'identification du payeur avec sollicitation du payeur basée sur 2 éléments ou plus parmi les catégories suivantes : connaissance (ce que l'utilisateur sait), possession (ce que l'utilisateur possède) et inhérence (ce que l'utilisateur est). Les éléments doivent être indépendants.

Authentification passive

Procédure d'identification du payeur ne nécessitant pas d'action du client.

En anglais : frictionless authentication

Autorisation

Flux d'information entre les PSP acquéreur et émetteur afin de s'assurer que le compte émetteur est en position d'accepter le débit.

CB2A

Protocole d'échange CB entre Accepteur et Acquéreur qui se décline pour les autorisations et la télécollecte.

CBAE

Protocole d'échange CB entre l'Acquéreur et l'Emetteur.

CB2AF

Protocole d'échange CB Accepteur et Acquéreur utile pour la transmission de fichiers à destination des grands remettants.

CB2C

Format CB de Compensation Carte entre banque acquéreur et émetteur.

Cryptogramme Visuel

Le cryptogramme visuel désigne une suite de 3 chiffres présents au dos de la carte permettant une protection additionnelle contre la fraude par carte.

Directory Server (DS)

Plateforme de sécurisation des paiements à distance qui permet de faire le lien entre le commerçant et la banque de l'émetteur, pour la mise en œuvre de l'authentification du titulaire de la carte.

DSP2 (Directive Européenne sur les services de Paiement 2ème version)

Cette directive européenne (2015/2366/UE) est entrée en vigueur le 13 Janvier 2018 et remplace la DSP1 (2007/64/CE).

EMVCo

Organisme qui défini les standards internationaux de sécurité des paiements par carte bancaire.

MO/TO (mail order/telephone order).

Paiement non-électronique, par courrier ou téléphone.

MPADS (Manuel de Paiement à Distance Sécurisé)

Manuel définissant le cadre des opérations de paiement CB à distance. Ce manuel peut être mis à disposition des commerçants par leur PAT.

Opération initiée par le commerçant

Opération initiée par le commerçant en l'absence du porteur. Elle doit obligatoirement être précédée par une opération initiée par le porteur à laquelle elle fait référence.

En anglais : Merchant Initiated Transaction (MIT)

Opération initiée par le porteur

Opération initiée par le porteur, soit par entrée de coordonnées, soit par déclenchement d'une opération card on file.

En anglais : Customer Initiated Transaction (CIT)

Opération One Leg

Opération pour laquelle un des PSP (acquéreur ou émetteur) se trouve hors de l'UE.

OSMP (Observatoire de la Sécurité des Moyens de Paiement)

L'OSMP est une instance de la Banque de France destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées (consommateurs, commerçants et entreprises, autorités publiques et administrations, banques et gestionnaires de moyens de paiement) par le bon fonctionnement des moyens de paiement et la lutte contre la fraude (Source : Banque de France).

Paiement à l'expédition

Opération pour laquelle l''ordre de paiement est initié par le porteur lors de l'achat du bien/service, et la remise en compensation réalisée au moment de l'expédition par le commerçant.

Paiement échelonné

Opération pour laquelle un ordre de paiement est initié par le porteur lors de l'achat d'un bien/service et qui fait l'objet de plusieurs opérations de remises en compensation de même montant en suivant un échéancier accepté par le porteur.

PLBS

(Paiement pour la location de biens et services) est une solution d'acceptation de cartes bancaires destinée aux acteurs de l'hôtellerie et de la location.

Prestataire d'Acceptation Technique (PAT)

Le PAT opère techniquement le système d'acceptation du commerçant. Il organise les échanges entre le commerçant et les parties prenantes du paiement (DS des réseaux, SAA du PSP acquéreur, ...).

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.

RTS (Regulatory Technical Standards)

Normes techniques réglementaires publiées par l'Autorité Bancaire Européenne afin de spécifier les exigences techniques pour la mise en place de la DSP2.

SAE

Serveur d'autorisation émetteur.

SDK (Software Development Kit)

Elément logiciel permettant au commerçant de véhiculer des données à son prestataire de paiement au cours d'un processus d'achat.

Transaction Risk Analysis (TRA)

Les analyses de risque sur l'opération de paiement, prévues par les RTS SCA, constituent un motif qui peut conduire à une dérogation pour les opérations de paiement identifiées comme à faible risque.

Transfert de responsabilité

Transfert de la charge financière des opérations de paiement frauduleuses.

En anglais : liability shift

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.

151bis, rue Saint Honoré
75001 Paris
www.cartes-bancaires.com