American Express SafeKey®
Foire aux questions

SECTION 1 : FAQ GÉNÉRALE

Q1.1 QU'EST-CE QUE LE SERVICE AMERICAN EXPRESS SAFEKEY®?

Le service American Express SafeKey est une solution de sécurité qui tire parti de normes industrielles mondiales pour détecter et réduire la fraude en ligne en ajoutant un niveau supplémentaire de sécurité lorsque les titulaires de Cartes magasinent en ligne ou à l'aide de leurs appareils mobiles. Le service SafeKey 2.0 est basé sur le protocole EMV[MD] 3-D Secure.

Les données du titulaire fournies pendant l'achat, dont le nom, l'adresse électronique, le numéro de téléphone et l'adresse d'expédition, peuvent aider à identifier avec plus d'exactitude les opérations légitimes ainsi que celles qui sont frauduleuses.

En exploitant les méthodes d'authentification basée sur le risque utilisées par l'émetteur, SafeKey peut assurer une expérience plus simple et plus harmonieuse. De plus, les titulaires peuvent profiter de SafeKey lorsqu'ils utilisent leurs appareils préférés pour effectuer leurs achats, y compris les achats intégrés à partir d'appareils intelligents.

Q1.2 QUELS SONT LES PRINCIPAUX AVANTAGES DE SAFEKEY?

SafeKey peut contribuer à réduire les opérations de commerce électronique frauduleuses. Il aide à protéger les titulaires contre l'utilisation non autorisée de leur Carte, permet à l'émetteur de participer au processus d'authentification et donne au marchand la possibilité de transférer la responsabilité en cas de fraude (pour plus de détails, voir la section Transfert de la responsabilité en matière de fraude (TRF)).

Q1.3 COMMENT FONCTIONNE SAFEKEY?

Le service SafeKey contribue à réduire la fraude en ligne en demandant à l'émetteur de confirmer l'identité du titulaire de la Carte avant que l'opération de ce dernier soit autorisée.

1. Le processus d'authentification est lancé lorsque le titulaire effectue un achat en ligne auprès d'un marchand.
2. Le marchand présente une transaction SafeKey au serveur répertoire d'American Express par l'intermédiaire de son fournisseur de serveurs 3DS (module d'extension de marchand ou MPI).
3. Le serveur répertoire transfère la demande au serveur de commande d'accès pertinent de l'émetteur.
4. Le serveur de commande d'accès utilise ensuite des techniques perfectionnées de modélisation du risque pour confirmer l'identité du titulaire de la Carte.
5. Dans certains cas, le titulaire peut être invité à renvoyer un mot de passe à usage unique au serveur de commande d'accès.

Q1.4 OÙ LE SERVICE SAFEKEY EST-IL OFFERT?

SafeKey est proposé dans n'importe quel marché où des banques administratrices et des émetteurs décident de mettre en œuvre ce service. Un marchand ne peut utiliser le service SafeKey que si sa banque administratrice possède la certification nécessaire.

Q1.5 EN QUOI CONSISTE LA NORME 3-D SECURE (3DS) 2.0 ET POURQUOI L'INDUSTRIE A-T-ELLE BESOIN D'UNE NOUVELLE VERSION DE CETTE NORME?

La version initiale de SafeKey, basée sur le protocole 3DS 1.0.2, était conçue pour prendre en charge l'authentification des titulaires de Cartes qui effectuaient des opérations de commerce électronique au moyen d'un navigateur installé sur un ordinateur personnel. L'organisme technique mondial EMVCo, dont American Express fait partie, a élargi la portée de ses activités afin d'amener le secteur des paiements à développer davantage sa spécification 3DS 2.0 ainsi que son programme connexe d'essais et d'approbations.

La spécification 3DS 2.0 prend en charge les paiements à distance effectués à l'extérieur d'un navigateur, notamment ceux faits à partir d'applications, d'appareils mobiles et de portefeuilles numériques. De plus, l'approche visait à fournir de nouvelles capacités en matière de technologie, de sécurité, de performance, d'expérience utilisateur et de souplesse afin d'assurer la pérennité de la spécification.

Q1.6 COMMENT LE SERVICE SAFEKEY REFLÈTE-T-IL L'ÉVOLUTION DES SPÉCIFICATIONS EMV 3DS (P. EX., ENTRE LA VERSION 2.1.0 ET LA VERSION 2.2.0)?

Les caractéristiques et la fonctionnalité de SafeKey 2.0 sont mises à jour pour tenir compte de chacune des nouvelles versions des spécifications EMV 3DS. Pour tirer parti de toutes les caractéristiques de la plus récente version, les participants au service SafeKey doivent obtenir une nouvelle certification.

Q1.7 QUELLES SONT LES CARACTÉRISTIQUES DE LA SPÉCIFICATION 3DS 2.0?

La spécification EMV 3DS 2.0 vise à répondre à l'évolution des besoins de l'environnement de paiement à distance, notamment au moyen des caractéristiques ci-dessous.

- Prise en charge et intégration directe des achats effectués à partir d'un navigateur ou à l'aide d'une fonction d'achat intégré (application)
- Meilleure évaluation des risques par l'émetteur grâce aux données enrichies
- Prise en charge de diverses méthodes d'authentification, y compris codes d'accès à usage unique, données biométriques et authentification hors bande
- Prise en charge des transactions basées sur des jetons pour une sécurité accrue et pour tenir compte du recours grandissant aux jetons dans l'industrie
- Possibilité d'authentification des opérations autres que paiements, par exemple, lors de l'ajout d'une Carte à un portefeuille numérique
- Possibilité pour les marchands d'établir l'authentification (p. ex., pour la facturation récurrente, les commandes postales et les commandes par téléphone)

- Amélioration de l'expérience utilisateur pour les titulaires de Cartes et du traitement à la caisse
- Soutien supplémentaire pour PSD2

Remarque : Voir l'annexe pour une comparaison détaillée des caractéristiques de chaque version de SafeKey

Q1.8 OÙ PUIS-JE TROUVER LES SPÉCIFICATIONS DE SAFEKEY 2.0?

Les spécifications SafeKey 2.0 ainsi que le guide de mise en œuvre de ce service se trouvent aux adresses ci-dessous.

- Émetteurs et banques administratrices : https://network.americanexpress.com/globalnetwork/sign-in/
- Fournisseurs de serveurs de commande d'accès et de serveurs 3DS (MPI) : https://network.americanexpress.com/globalnetwork/amex-enabled/
- Marchands : http://www.americanexpress.com/merchantspecs
- Spécifications de base d'EMV : www.emvco.com

Q1.9 QUEL EST L'ENGAGEMENT D'AMERICAN EXPRESS RELATIVEMENT À SAFEKEY 1.0?

American Express surveille l'utilisation de SafeKey 1.0 au sein de l'industrie et continuera de prendre en charge ce service au fil de la croissance de l'adoption de SafeKey 2.0. American Express annoncera à quel moment le service SafeKey 1.0 sera complètement remplacé par la version 2.0 en prévoyant un délai approprié.

Q1.10 LES SERVICES SAFEKEY 1.0 ET SAFEKEY 2.0 PEUVENT-ILS COHABITER?

Oui. Les versions 1.0 et 2.0 du service SafeKey sont autonomes et peuvent donc cohabiter. Le service SafeKey 2.0 devrait remplacer progressivement la version 1.0. Pendant cette période de transition, il est recommandé aux marchands de recourir aux services de fournisseurs de serveurs 3DS (MPI) qui prennent en charge les deux produits. Lorsqu'un marchand demande l'authentification d'une opération, il incombe au fournisseur du serveur 3DS (MPI) d'utiliser la version appropriée du service SafeKey.

Q1.11 COMMENT LE SERVEUR 3DS (MPI) SAIT-IL QUELLE VERSION DE SAFEKEY IL DOIT UTILISER?

Le service SafeKey gère des registres de gammes de Cartes (NIB) pris en charge par SafeKey 2.0 auxquels chaque serveur 3DS (MPI) peut accéder. Lorsqu'un marchand demande l'authentification du titulaire de la Carte, le serveur 3DS (MPI) vérifie si la Carte en question peut être gérée par SafeKey 2.0. Si c'est le cas, le service SafeKey 2.0 devrait être utilisé. Dans le cas contraire, il faut utiliser la version 1.0.

Q1.12 EST-IL POSSIBLE DE METTRE EN ŒUVRE LE SERVICE SAFEKEY 2.0 SANS SAFEKEY 1.0?

Oui. Au fil du temps, il s'agira de l'approche privilégiée pour les nouveaux utilisateurs. Les participants doivent savoir qu'il y aura une période de transition avant que le service SafeKey 2.0 soit pleinement établi.

Q1.13 LES TITULAIRES DE CARTES DÉJÀ INSCRITS AU SERVICE SAFEKEY 1.0 DOIVENT-ILS S'INSCRIRE AU SERVICE SAFEKEY 2.0?

Les titulaires de Cartes n'ont pas à s'inscrire au service SafeKey 2.0 puisque tous les titulaires admissibles seront déjà inscrits par les émetteurs, comme l'exige la spécification d'EMVCo.

Q1.14 PEUT-ON UTILISER LE SERVICE SAFEKEY POUR LES OPÉRATIONS EN LIGNE EFFECTUÉES AVEC N'IMPORTE QUELLE CARTE?

SafeKey permet de confirmer que la personne qui effectue l'opération est bel et bien le titulaire de la Carte. Par conséquent, ce service ne peut pas être utilisé pour des produits anonymes comme les cartes prépayées, car l'identité de l'utilisateur de tels produits n'est pas enregistrée.

SECTION 2 : TRANSFERT DE LA RESPONSABILITÉ EN MATIÈRE DE FRAUDE (TRF) – FOIRE AUX QUESTIONS

Q2.1 EN QUOI CONSISTE L'OPTION DE TRANSFERT DE LA RESPONSABILITÉ EN MATIÈRE DE FRAUDE (TRF) DU SERVICE SAFEKEY?

Si une opération admissible donne lieu à une fraude, l'option TRF de SafeKey transfère la responsabilité correspondante du marchand à l'émetteur.

Q2.2 COMMENT UN MARCHAND PEUT-IL SE PRÉVALOIR DU TRF?

Un marchand bénéficie de l'option TRF pour les opérations authentifiées par le service SafeKey, à condition que les critères énoncés dans les lignes directrices TRF soient respectés. Les marchands devraient veiller à ce que les taux de fraude demeurent bas et devraient également satisfaire aux exigences des spécifications du service SafeKey, dont la communication de données exactes dans les messages SafeKey. Pour en savoir plus au sujet des lignes directrices TRF, les marchands sont invités à communiquer avec leur banque administratrice.

Q2.3 EN QUOI CONSISTE UNE OPÉRATION AUTHENTIFIÉE PAR SAFEKEY?

On dit qu'une opération est authentifiée lorsque l'émetteur a confirmé l'identité du titulaire de la Carte au moyen d'une valeur d'authentification dans le message de réponse. Pour plus de détails, veuillez consulter les spécifications du service SafeKey.

Q2.4 EN QUOI CONSISTE UNE TENTATIVE D'AUTHENTIFICATION D'OPÉRATION PAR SAFEKEY?

Une tentative d'opération se produit lorsqu'un marchand tente de faire authentifier la transaction au moyen de SafeKey, mais que l'émetteur ne prend pas en charge ce service ou que le serveur de commande d'accès de l'émetteur n'est pas disponible. Il est possible que le service SafeKey accorde une tentative d'authentification, signalée par une valeur d'authentification dans le message de réponse; pour de plus amples renseignements, consultez les spécifications du service SafeKey.

SECTION 3 : QUESTIONS FRÉQUENTES DES MARCHANDS

Q3.1 COMMENT PUIS-JE DÉTERMINER CE QUE JE DOIS FAIRE POUR ADOPTER LE SERVICE SAFEKEY?

Les marchands qui désirent adopter le service SafeKey doivent en parler à leur fournisseur potentiel de serveurs 3DS (MPI) ou à leur banque administratrice.

Q3.2 QUE DOIT FAIRE UN MARCHAND POUR S'INSCRIRE AU SERVICE SAFEKEY?

Pour s'inscrire au service SafeKey, les marchands doivent communiquer avec leur fournisseur de serveurs 3DS (MPI) ou avec leur banque administratrice. Il existe également un portail d'inscription en ligne pour certaines banques administratrices au www.amexsafekey.com.

Q3.3 COMMENT UN MARCHAND PEUT-IL SAVOIR QUELLE VERSION DE SAFEKEY IL DOIT UTILISER?

Il est recommandé de recourir à un fournisseur de serveurs 3DS (MPI) qui prend en charge toutes les versions de SafeKey, et qui sera en mesure de choisir celle qui convient puisqu'il saura quelles versions l'émetteur prend en charge et quelles caractéristiques améliorées pourront être utilisées.

Q3.4 COMMENT UN MARCHAND PEUT-IL SAVOIR SI SON FOURNISSEUR DE SERVEURS 3DS (MPI) PREND EN CHARGE SAFEKEY 2.0?

Les fournisseurs de serveurs 3DS (MPI) collaborent avec EMVCo et American Express pour obtenir la certification SafeKey 2.0. Les marchands devraient discuter de leurs plans avec leur fournisseur. Vous trouverez une liste de fournisseurs de serveurs 3DS (MPI) accrédités auprès d'American Express et inscrits au programme AMEX Enabled au www.amexenabled.com.

Q3.5 LES MARCHANDS DÉJÀ INSCRITS AU SERVICE SAFEKEY 1.0 DOIVENT-ILS S'INSCRIRE AU SERVICE SAFEKEY 2.0?

Les marchands doivent consulter leur fournisseur de serveurs 3DS (MPI) afin de comprendre la marche à suivre pour tirer parti du service SafeKey 2.0.

Q3.6 JE SUIS UN MARCHAND QUI N'UTILISE PAS ENCORE LE SERVICE SAFEKEY. COMMENT PUIS-JE M'INSCRIRE AU SERVICE SAFEKEY 2.0?

Les marchands qui désirent s'inscrire au service SafeKey devraient tout d'abord en parler à leur fournisseur de serveurs 3DS (MPI). Vous trouverez une liste de fournisseurs de serveurs 3DS (MPI) certifiés inscrits auprès d'American Express sur le site Web du programme AMEX Enabled (www.amexenabled.com).

Q3.7 COMMENT LE SERVEUR DU MARCHAND OU LE SERVEUR 3DS (MPI) RECONNAÎT-IL LA VERSION DE SAFEKEY PRISE EN CHARGE PAR L'ÉMETTEUR?

Le serveur 3DS (MPI) reçoit des données qui lui indiquent quels émetteurs prennent en charge le service SafeKey 2.0 et quelles versions de ce service ils peuvent utiliser. Le serveur 3DS (MPI) utilise ces données pour déterminer le type d'authentification à effectuer.

Q3.8 QUE DOIT FAIRE UN MARCHAND POUR ACTIVER SON APPLICATION POUR SAFEKEY?

Les marchands doivent intégrer une trousse de développement logiciel (ou trousse SDK) 3DS à leur application de marchand pour que celle-ci puisse utiliser le service SafeKey 2.0. Les marchands devraient prendre les mesures à cette fin en collaboration avec leur fournisseur de serveurs 3DS (MPI) ou avec un fournisseur de trousses SDK 3DS. Les trousses SDK 3DS doivent être testées et approuvées par l'entremise d'EMVCo. Pour obtenir la liste des fournisseurs de trousses SDK approuvés, visitez www.emvco.com.

Q3.9 QU'EST-CE QU'UNE TROUSSE DE DÉVELOPPEMENT LOGICIEL (OU TROUSSE SDK) 3DS?

La trousse SDK 3DS est intégrée à l'application de marchand. Cette trousse gère le traitement effectué par SafeKey pour l'application et établit le lien avec le serveur 3DS.

Q3.10 AMERICAN EXPRESS APPLIQUE-T-ELLE DES FRAIS DE TRANSACTION POUR L'UTILISATION DU SERVICE SAFEKEY?

Non. Veuillez vous adresser à votre fournisseur de serveurs 3DS (MPI) pour bien comprendre le coût de ses services.

Q3.11 QUE SE PASSE-T-IL SI L'ÉMETTEUR NE PREND PAS EN CHARGE LE SERVICE SAFEKEY?

Bien que le service SafeKey soit actuellement facultatif pour les émetteurs, ceux d'entre eux qui n'y sont pas inscrits pourraient être tenus responsables en cas de fraude s'il y a eu tentative d'authentification de l'opération par le marchand. Pour en savoir plus au sujet des lignes directrices TRF du service SafeKey, les marchands sont invités à communiquer avec leur banque administratrice.

Q3.12 QUE SE PASSE-T-IL SI LA BANQUE ADMINISTRATRICE DU MARCHAND NE PREND PAS EN CHARGE LE SERVICE SAFEKEY?

La banque administratrice du marchand doit posséder la certification SafeKey. Cette exigence vise à assurer le traitement des messages d'autorisation et de présentation requis ainsi que le transfert approprié de la responsabilité en matière de fraude. Remarque : le processeur du marchand doit également être capable de prendre en charge SafeKey et de transmettre les données nécessaires à la banque administratrice.

Q3.13 LE SERVICE SAFEKEY PRÉSENTE-T-IL DES CARACTÉRISTIQUES QUI AIDENT LES MARCHANDS À PRENDRE EN CHARGE UNE AUTHENTIFICATION RENFORCÉE DES CLIENTS?

Oui, toutes les versions de SafeKey prennent en charge les protocoles d'authentification renforcés, comme les exigences de PSD2.

Q3.14 OÙ LES MARCHANDS PEUVENT-ILS OBTENIR LES SPÉCIFICATIONS RELATIVES À L'AUTORISATION ET À LA PRÉSENTATION POUR LE SERVICE SAFEKEY?

Pour connaître les plus récentes spécifications techniques, communiquez avec votre banque administratrice. Les marchands recrutés directement par American Express peuvent visiter le www.americanexpress.com/merchantspecs.

SECTION 4 : QUESTIONS FRÉQUENTES DES FOURNISSEURS DE SERVEURS DE COMMANDE D'ACCÈS ET DE SERVEURS 3DS (MPI)

Q4.1 QUE DOIVENT FAIRE LES FOURNISSEURS DE SERVEURS DE COMMANDE D'ACCÈS ET DE SERVEURS 3DS (MPI) POUR OBTENIR LA CERTIFICATION SAFEKEY?

La première étape du processus de certification SafeKey consiste à s'inscrire au programme AMEX Enabled. Pour accéder à la documentation SafeKey, les fournisseurs doivent remplir le formulaire d'inscription au www.amexenabled.com.

Q4.2 OÙ PEUT-ON TROUVER UNE LISTE DE FOURNISSEURS DE SERVEURS DE COMMANDE D'ACCÈS ET DE SERVEURS 3DS (MPI) CERTIFIÉS?

Vous trouverez une liste de fournisseurs de serveurs de commande d'accès et de serveurs 3DS (MPI) certifiés inscrits auprès d'American Express sur le site Web du programme AMEX Enabled (www.amexenabled.com).

Q4.3 LA CERTIFICATION SAFEKEY 2.0 EST-ELLE NÉCESSAIRE SI L'ON A DÉJÀ LA CERTIFICATION SAFEKEY 1.0?

Oui. Les fournisseurs de serveurs de commande d'accès et de serveurs 3DS (MPI) doivent obtenir des certifications distinctes pour les différentes versions du service SafeKey. Pour en savoir plus, visitez le www.amexsafekey.com. EMVCo fournit un service d'approbation obligatoire pour les fournisseurs de serveurs de commande d'accès et de serveurs 3DS (MPI), dont les exigences doivent être satisfaites pour pouvoir obtenir la certification American Express SafeKey 2.0.

Q4.4 COMMENT PUIS-JE M'INSCRIRE POUR OBTENIR LA CERTIFICATION ET PARTICIPER AUX ESSAIS?

Pour amorcer le processus de certification SafeKey, veuillez vous inscrire au www.amexenabled.com. Un analyste de certification American Express vous expliquera comment accéder au laboratoire SafeKey.

SECTION 5 : QUESTIONS FRÉQUENTES DES ÉMETTEURS ET DES BANQUES ADMINISTRATRICES

Q5.1 QUE DOIVENT FAIRE LES ÉMETTEURS ET LES BANQUES ADMINISTRATRICES POUR OBTENIR LA CERTIFICATION SAFEKEY?

Pour en savoir plus à ce sujet, les émetteurs et les banques administratrices devraient s'adresser à leur représentant American Express ou visiter le www.amexsafekey.com.

Q5.2 LES ÉMETTEURS ET LES BANQUES ADMINISTRATRICES QUI POSSÈDENT LA CERTIFICATION SAFEKEY 1.0 DOIVENT-ILS OBTENIR LA CERTIFICATION SAFEKEY 2.0?

Les messages réseau des versions 1.0 et 2.0 de SafeKey concordent et aucune recertification n'est nécessaire à ce niveau. Toutefois, le processus d'authentification pour les serveurs de commande d'accès doit être certifié.

ANNEXE : TABLEAU COMPARATIF DES CARACTÉRISTIQUES

American Express SafeKey® – Comparaison

Caractéristique	SafeKey 1.0	SafeKey 2.0	
		SafeKey 2.1 (EMV 2.1.0)	SafeKey 2.2 (EMV 2.2.0)
Service basé sur la norme industrielle 3-D Secure	●	●	●
Niveau additionnel de sécurité à la caisse	●	●	●
Authentification du paiement	●	●	●
Authentification selon le navigateur	●	●	●
Flexibilité pour les émetteurs, qui peuvent utiliser une variété de méthodes d'authentification (codes d'accès à usage unique, décisions basées sur le risque, etc.)	●	●	●
Prise en charge de la conformité à PSD2	●	●	●
Prise en charge d'un plus grand nombre d'éléments de donnée pour favoriser une authentification sans heurt	Offerte aux États-Unis et dans les territoires américains	●	●
Prise en charge des achats intégrés (à partir d'une application)	—	●	●
Authentification des opérations autres que paiements	—	●	●
Transactions basées sur des jetons	—	●	●
Authentification hors bande	—	●	●
Authentification établie par le marchand	—	—	●
Authentification découplée	—	—	●
Indicateurs supplémentaires pour PSD2	—	—	●

Remarque : Certaines de ces caractéristiques pourraient exiger d'autres certifications.

AMERICAN EXPRESS SafeKey®