American Express SafeKey®

FOIRE AUX QUESTIONS

1. Questions générales

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

American Express SafeKey est une solution de sécurité qui tire parti de normes industrielles mondiales pour détecter et réduire les fraudes en ligne, ajoutant une couche supplémentaire de sécurité lorsque les titulaires de Carte magasinent en ligne et sur leurs appareils mobiles. SafeKey est basé sur le protocole EMV®* 3-D Secure (3DS).

Les données des titulaires qui sont fournies dans le cadre de l'expérience d'achat, comme leur nom, adresse de courriel, numéro de téléphone et adresse de livraison, peuvent aider à reconnaître plus exactement les transactions légitimes et les transactions frauduleuses.

Par l'utilisation de méthodes d'authentification basées sur les risques d'un émetteur, SafeKey aide à réduire la friction et à offrir une expérience plus fluide de passage à la caisse. Les titulaires de Carte peuvent utiliser SafeKey et magasiner sur les appareils qu'ils préfèrent, y compris les appareils intelligents, pour effectuer des achats dans les applications.

Q1.2 QUELS SONT LES PRINCIPAUX AVANTAGES DE SAFEKEY?

SafeKey peut aider à réduire la fraude pour les transactions sans présentation de Carte. Il aide à protéger les titulaires contre l'utilisation non autorisée de leur Carte, permet à l'émetteur de participer à l'authentification, et peut fournir aux marchands le transfert de la responsabilité pour les fraudes (voir la section sur le transfert de responsabilité pour les fraudes pour plus de détails).

Q1.3 COMMENT FONCTIONNE SAFEKEY?

SafeKey aide à réduire les fraudes en ligne en demandant à l'émetteur de confirmer l'identité des titulaires de Carte avant qu'une transaction soit autorisée.

1. Le processus d'authentification commence lorsqu'un titulaire effectue un achat en ligne auprès d'un marchand.
2. Le marchand soumet une transaction SafeKey au serveur répertoire d'American Express par l'entremise de son fournisseur de serveurs 3DS.
3. Le serveur répertoire transfère la demande au serveur de contrôle d'accès approprié de l'émetteur.
4. Le serveur de contrôle d'accès utilise des techniques raffinées de modélisation des risques afin de confirmer l'identité des titulaires de Carte.
5. Dans certaines situations, il est possible qu'on demande aux titulaires de confirmer leur identité en interagissant avec leur émetteur.

* EMV® est une marque de commerce déposée aux États-Unis et dans d'autres pays, et une marque de commerce non déposée ailleurs. La marque de commerce « EMV » appartient à EMVCo.

1. Questions générales

Q1.4 OÙ SAFEKEY EST-IL OFFERT?

SafeKey est offert aux émetteurs et banques administratrices dans toutes les régions desservies par Amex. Pour qu'un marchand puisse bénéficier du transfert de la responsabilité pour les fraudes, son émetteur doit avoir la certification pour SafeKey.

Q1.5 COMMENT SAFEKEY TIENT-IL COMPTE DES SPÉCIFICATIONS CHANGEANTES D'EMV 3DS (comme 2.2.0 et 2.3.1)?

Les caractéristiques et fonctionnalités de SafeKey sont mises à jour pour tenir compte de chaque nouvelle version d'EMV 3DS. Les fournisseurs de serveurs de contrôle d'accès et de serveurs 3DS pour SafeKey doivent obtenir la certification pour la plus récente version afin de profiter de toutes les caractéristiques.

Q1.6 QUELLES SONT LES CARACTÉRISTIQUES D'EMV 3DS?

EMV 3DS cherche à répondre aux exigences changeantes de l'environnement de paiements à distance, y compris ce qui suit :

- La prise en charge et l'intégration directe pour les besoins de magasinage sur navigateur et dans les applications.
- Une évaluation améliorée des risques pour les émetteurs à l'aide de données rehaussées.
- La prise en charge d'une variété de méthodes d'authentification, y compris des codes d'accès à usage unique, l'authentification biométrique et l'authentification hors bande.
- La prise en charge de transactions basées sur des jetons pour une sécurité rehaussée et pour tenir compte de l'augmentation de l'utilisation de jetons dans l'ensemble de l'industrie.
- Fournir une authentification pour d'autres activités, comme l'ajout d'une Carte à un portefeuille numérique.
- Permettre aux marchands d'effectuer des authentifications (exemples : factures récurrentes, commandes postales, commandes téléphoniques).
- Des améliorations de l'expérience d'utilisation et des processus de passage à la caisse des titulaires de Carte.
- Plus de soutien pour DSP2.

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

1. Questions générales

Q1.7 OÙ PUIS-JE TROUVER LES SPÉCIFICATIONS DE SAFEKEY?

Les spécifications et les guides de mise en œuvre de SafeKey se trouvent aux adresses suivantes :

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

Q1.8 COMMENT UN SERVEUR 3DS SAIT-IL QUELLE VERSION DE SAFEKEY DOIT ÊTRE UTILISÉE?

Le service de SafeKey conserve des registres des plages de Cartes (NIB) prises en charge par SafeKey, ainsi que des caractéristiques facultatives que les émetteurs et leur fournisseur de serveurs de contrôle d'accès prennent en charge. Tous les serveurs 3DS ont accès à ces registres. Lorsqu'un marchand demande une authentification de titulaire de Carte, le serveur 3DS vérifie si la Carte en particulier prend en charge SafeKey, puis envoie un message de la version appropriée.

Q1.9 LES TITULAIRES DE CARTE DOIVENT-ILS S'INSCRIRE À SAFEKEY?

Les titulaires de Carte n'ont pas besoin de s'inscrire à SafeKey parce que tous les titulaires admissibles* sont préinscrits** par les émetteurs; c'est une exigence de la spécification d'EMVCo.

Q1.10 PEUT-ON UTILISER SAFEKEY POUR LES TRANSACTIONS EN LIGNE AVEC TOUTES LES CARTES?

SafeKey offre l'avantage d'authentifier la personne qui effectue la transaction comme titulaire de Carte. En conséquence, SafeKey peut seulement être utilisé pour les transactions sans présentation de Carte à l'aide de Cartes pour lesquelles l'émetteur peut communiquer directement avec les titulaires (par courriel, message texte, notification poussée, etc.), lorsque les titulaires de Carte peuvent recevoir des demandes de réponse de la part de l'émetteur et y répondre.

* S'applique aux Cartes pour lesquelles l'émetteur peut identifier un seul titulaire de Carte et authentifier la personne utilisant la Carte. Voir la question 1.10.

** Sous réserve de la réglementation applicable aux différents marchés.

2. Questions sur le transfert de responsabilité pour les fraudes

Q2.1 QU'EST-CE QUE LE TRANSFERT DE RESPONSABILITÉ POUR LES FRAUDES DE SAFEKEY?

Si une transaction admissible est frauduleuse, SafeKey transfère la responsabilité pour la fraude du marchand à l'émetteur.

Q2.2 COMMENT UN MARCHAND PEUT-IL OBTENIR LE TRANSFERT DE LA RESPONSABILITÉ POUR LES FRAUDES?

Les marchands obtiennent le transfert de la responsabilité pour les fraudes pour les transactions authentifiées par SafeKey s'ils ont respecté les critères de la politique de transfert de responsabilité pour les fraudes. Les marchands doivent maintenir un faible taux de fraudes et respecter les exigences des spécifications de SafeKey, par exemple en fournissant des données exactes dans les messages de SafeKey. Les marchands doivent consulter leur banque administratrice pour obtenir les détails de la politique de transfert de la responsabilité pour les fraudes.

Q2.3 QU'EST-CE QU'UNE TRANSACTION SAFEKEY AUTHENTIFIÉE?

Une transaction authentifiée est une transaction pour laquelle l'émetteur a confirmé l'identité du titulaire de Carte, ce qui est indiqué par une valeur d'authentification dans le message fourni au marchand. Veuillez consulter les spécifications de SafeKey pour plus de détails.

Q2.4 QU'EST-CE QU'UNE TRANSACTION SAFEKEY TENTÉE?

Une transaction tentée est une transaction où le marchand a essayé d'effectuer une authentification par SafeKey, mais l'émetteur ne prend pas en charge la version de SafeKey requise par la politique, ou le serveur de contrôle d'accès de l'émetteur n'est pas disponible. SafeKey peut accorder une authentification tentée indiquée par une valeur d'authentification dans le message transmis au marchand. Veuillez consulter les spécifications de SafeKey pour plus de détails.

3. Questions des marchands

Q3.1 JE SUIS UN MARCHAND QUI N'UTILISE PAS SAFEKEY. COMMENT PUIS-JE COMMENCER À L'UTILISER?

Les marchands doivent d'abord s'adresser à leur fournisseur de serveurs 3DS pour faire activer SafeKey. Pour obtenir une liste de fournisseurs de serveurs 3DS détenant une certification auprès d'American Express, veuillez visiter le site Web AMEX Enabled. Les marchands doivent aussi discuter avec leur banque administratrice ou fournisseur de services de paiement pour vérifier si les données de SafeKey peuvent être transmises dans les messages d'autorisation et de soumission.

Q3.2 DOIS-JE INTERAGIR DIRECTEMENT AVEC AMERICAN EXPRESS POUR UTILISER SAFEKEY?

Les marchands n'ont pas besoin de s'inscrire directement auprès d'American Express pour utiliser SafeKey. Votre fournisseur de serveurs 3DS veillera à ce que vous soyez prêt pour les messages d'authentification de SafeKey. Les marchands doivent aussi discuter avec leur banque administratrice ou fournisseur de services de paiement pour vérifier si les données de SafeKey peuvent être transmises dans les messages d'autorisation et de soumission.

Q3.3 EN TANT QUE MARCHAND, COMMENT PUIS-JE SAVOIR QUELLE VERSION DE SAFEKEY JE DOIS DEMANDER À MON FOURNISSEUR DE SERVEURS 3DS D'UTILISER?

On recommande aux marchands de demander à leur fournisseur de serveurs 3DS d'utiliser la plus récente version de SafeKey.

Q3.4 COMMENT PUIS-JE SAVOIR QUELLES VERSIONS DE SAFEKEY SONT PRISES EN CHARGE PAR UN FOURNISSEUR DE SERVEURS 3DS?

Les marchands doivent discuter avec leur fournisseur de serveurs 3DS pour savoir quelles versions il prend en charge. Une liste de fournisseurs de serveurs 3DS qui ont la certification requise pour utiliser SafeKey, y compris la version pour laquelle ils ont une certification, est présentée sur le site Web AMEX Enabled.

Q3.5 COMMENT UN MARCHAND OU SERVEUR 3DS PEUT-IL SAVOIR QUELLES VERSIONS DE SAFEKEY SONT PRISES EN CHARGE PAR UN ÉMETTEUR?

Chaque jour, tous les serveurs 3DS demandent à American Express le numéro d'identification des émetteurs. Ces données indiquent les émetteurs qui prennent SafeKey en charge, ainsi que les versions et les caractéristiques prises en charge. Les serveurs 3DS utilisent ensuite ce renseignement pour déterminer le type d'authentification qui doit être réalisée.

3. Questions des marchands

Q3.6 EN TANT QUE MARCHAND, COMMENT PUIS-JE ACTIVER SAFEKEY DANS MON APPLICATION?

Les marchands doivent intégrer une trousse de développement de logiciel pour 3DS (« 3DS SDK ») dans leur application de marchand afin d'activer SafeKey. Les marchands doivent s'adresser à leur fournisseur de serveurs 3DS ou à un fournisseur de trousses de développement de logiciel pour 3DS. Les trousses de développement de logiciel pour 3DS doivent être testées et approuvées par EMVCo. Veuillez visiter www.emvco.com pour une liste de fournisseurs approuvés de trousses de développement de logiciel pour 3DS.

Q3.7 QU'EST-CE QU'UNE TROUSSE DE DÉVELOPPEMENT DE LOGICIEL (SDK) POUR 3DS?

Une SDK pour 3DS est un composant qu'on intègre à l'application des marchands. La SDK pour 3DS gère le traitement de SafeKey pour l'application, et transmet des renseignements aux serveurs 3DS.

Q3.8 American Express FACTURE-T-ELLE DES FRAIS DE TRANSACTION POUR L'UTILISATION DE SAFEKEY?

Non. Veuillez vous adresser à votre fournisseur de serveurs 3DS pour connaître les coûts associés à ses services.

Q3.9 QU'ARRIVE-T-IL SI L'ÉMETTEUR NE PREND PAS SAFEKEY EN CHARGE?

Les émetteurs non participants pourraient être tenus responsables des transactions frauduleuses pour lesquelles une authentification par SafeKey a été tentée par les marchands. Veuillez vous adresser à votre banque administratrice pour en savoir plus sur la politique de transfert de la responsabilité pour les fraudes de SafeKey.

Q3.10 PUIS-JE UTILISER SAFEKEY SI MA BANQUE ADMINISTRATRICE N'A PAS LA CERTIFICATION?

Oui. Vous pouvez bénéficier des vérifications d'authentification de SafeKey. Toutefois, vous ne pouvez pas bénéficier du transfert de la responsabilité pour les fraudes si votre banque administratrice n'a pas la certification assurant que les données de SafeKey peuvent être transmises dans les messages d'autorisation et de soumission.

3. Questions des marchands

Q3.11 Y A-T-IL DES CARACTÉRISTIQUES DANS SAFEKEY QUI AIDENT LES MARCHANDS À PRENDRE EN CHARGE LA NORME « AUTHENTIFICATION FORTE DU CLIENT »?

Oui, toutes les versions de SafeKey prennent en charge l'authentification forte du client, qui peut être requise pour les transactions relevant de la DSP2 ou d'un autre mandat réglementaire semblable.

Q3.12 OÙ PUIS-JE TROUVER LES SPÉCIFICATIONS D'AUTORISATION ET DE SOUMISSION POUR SAFEKEY?

Veuillez vous adresser à votre banque administratrice pour connaître les plus récentes spécifications techniques. Les marchands recrutés directement par American Express peuvent visiter www.americanexpress.com/merchantspecs.

4. Questions sur fournisseurs de serveurs de contrôle d'accès et de serveurs 3DS

Q4.1 OÙ PUIS-JE TROUVER UNE LISTE DE FOURNISSEURS DE SERVEURS DE CONTRÔLE D'ACCÈS ET DE SERVEURS 3DS?

Pour obtenir une liste de fournisseurs de serveurs de contrôle d'accès et de serveurs 3DS inscrits auprès d'American Express, veuillez visiter le site Web AMEX Enabled.

Q4.2 PUIS-JE CHOISIR COMMENT MON PRODUIT CERTIFIÉ FIGURE SUR LA LISTE DU SITE WEB AMEX ENABLED?

Oui. Les fournisseurs peuvent choisir de présenter sur la liste tous leurs produits séparément, ou les combiner dans une seule entrée. Dans les deux cas, la liste indique pour quelles versions de SafeKey chaque produit est certifié. Veuillez en discuter avec votre analyste de certification en cas d'incertitude.

Q4.3 Y A-T-IL DES PRÉREQUIS POUR COMMENCER LA CERTIFICATION POUR SAFEKEY?

Oui. Afin de commencer la certification pour SafeKey, un fournisseur doit avoir obtenu une lettre d'approbation EMV 3DS.

Q4.4 COMMENT LES FOURNISSEURS DE SERVEURS DE CONTRÔLE D'ACCÈS ET LES FOURNISSEURS DE SERVEURS 3DS DOIVENT-ILS PROCÉDER POUR OBTENIR LA CERTIFICATION POUR SAFEKEY?

La première étape pour obtenir la certification pour SafeKey est de s'inscrire auprès d'AMEX Enabled. Les fournisseurs doivent commencer par remplir un formulaire d'inscription d'entreprise sur www.amexenabled.com pour gagner accès à la documentation sur SafeKey.

Q4.5 COMMENT PUIS-JE M'INSCRIRE POUR LA CERTIFICATION ET LES TESTS POUR LA PREMIÈRE FOIS?

Après s'être inscrits auprès d'AMEX Enabled, les fournisseurs doivent soumettre un formulaire d'adhésion à SafeKey pour commencer leur certification. Un analyste de certification d'American Express expliquera ensuite les prochaines étapes, y compris comment accéder au laboratoire de tests de SafeKey.

Q4.6 COMMENT PUIS-JE PASSER À LA PLUS RÉCENTE VERSION DE SAFEKEY?

Les fournisseurs qui ont déjà la certification pour SafeKey doivent accéder au tableau de bord d'AMEX Enabled pour demander un lien d'adhésion.

4. Questions sur fournisseurs de serveurs de contrôle d'accès et de serveurs 3DS

Q4.7 DOIS-JE OBTENIR LA CERTIFICATION POUR LES VERSIONS PRÉCÉDENTES DE SAFEKEY AVANT D'OBTENIR LA CERTIFICATION POUR LA PLUS RÉCENTE VERSION?

Non. La certification pour la plus récente version de SafeKey comprend les tests pour toutes les versions précédentes. Tous les participants à SafeKey doivent obtenir la certification pour la plus récente version.

Q4.8 COMMENT PUIS-JE AJOUTER UNE AUTRE LETTRE D'APPROBATION D'EMVCo À MON ADHÉSION À SAFEKEY?

Les fournisseurs doivent aviser Amex lorsqu'ils reçoivent une nouvelle lettre d'approbation d'EMVCo. Amex peut prendre en charge plusieurs lettres d'approbation jusqu'à ce que la certification pour la plus récente version soit obtenue. Pour ajouter une nouvelle lettre d'approbation ou une lettre d'approbation renouvelée, veuillez téléverser votre document de lettre d'approbation d'EMCo dans la section Messages d'AMEX Enabled. Attention : n'apportez pas de changements à votre système tant qu'Amex n'a pas confirmé que les changements reliés à la lettre d'approbation ont été traités sans ses systèmes.

Q4.9 LE PROGRAMME SAFEKEY COMPORTE-T-IL DES EXIGENCES CONTINUES?

Oui, veuillez consulter le guide du programme SafeKey sur AMEX Enabled pour plus de détails. Les exigences continues pour les fournisseurs comprennent : maintenir un contrat valide, fournir une preuve de conformité actuelle aux normes de l'industrie des cartes de paiement, renouveler les certificats avant leur expiration, tenir à jour les coordonnées et retourner à Amex pour tester toute nouvelle caractéristique prise en charge.

5. Questions pour émetteurs et banques administratrices

Q5.1 COMMENT LES ÉMETTEURS ET LES BANQUES ADMINISTRATRICES DOIVENT-ILS OBTENIR LA CERTIFICATION POUR SAFEKEY?

Les émetteurs et les banques administratrices doivent obtenir la certification auprès d'American Express pour assurer que les données de SafeKey peuvent être transmises dans les messages d'autorisation et de soumission. Ils doivent discuter à leur représentant d'American Express au sujet de l'obtention de la certification pour SafeKey, ou visiter www.amexsafekey.com pour obtenir de plus amples renseignements.

Q5.2 LA VERSION DE SAFEKEY POUR LAQUELLE UN ÉMETTEUR OU BANQUE ADMINISTRATRICE A OBTENU UNE CERTIFICATION EST-ELLE IMPORTANTE?

Les émetteurs et les banques administratrices doivent obtenir la certification pour assurer que les données de SafeKey peuvent être transmises dans les messages d'autorisation et de soumission. Cette certification pour SafeKey n'est pas propre à une version.

Les émetteurs doivent également effectuer des tests d'intégration avec leur fournisseur de serveurs de contrôle d'accès une fois que leur fournisseur de serveurs de contrôle d'accès a obtenu la certification pour une version différente de SafeKey.

Les banques administratrices n'ont pas besoin d'obtenir une certification supplémentaire pour prendre en charge les versions discrètes de SafeKey. Cependant, si une banque administratrice agit aussi comme fournisseur de serveurs 3DS, d'autres exigences de certification s'appliquent.

Q5.3 COMMENT PUIS-JE ACCÉDER AUX GUIDES DE MISE EN ŒUVRE ET AUX SPÉCIFICATIONS DE SAFEKEY?

- Émetteurs et banques administratrices : ouvrez une session pour accéder à la section « Knowledge Base » (Base de connaissances) au https://network.americanexpress.com/globalnetwork/sign-in/
- Fournisseurs de serveurs de contrôle d'accès et de serveurs 3DS : visitez le https://network.americanexpress.com/globalnetwork/amex-enabled/
- Marchands exclusifs : visitez le http://www.americanexpress.com/merchantspecs
- Marchands de réseau : communiquez avec votre banque administratrice

ANNEXE : Tableau de comparaison des caractéristiques

CARACTÉRISTIQUE	SAFEKEY 2.2	SAFEKEY 2.3
Activation basée sur les applications (dans les applications)	✓	✓
Authentification autre que pour paiements	✓	✓
Transactions basées sur des jetons	✓	✓
Authentification hors bande	✓	✓
Authentifications autres que pour paiement amorcées par demandeur 3DS (3RI)	✓	✓
Authentifications pour paiement amorcées par demandeur 3DS (3RI)	✓	✓
Authentification découplée	✓	✓
Éléments de données indicateurs de la DSP2	✓	✓
Prise en charge supplémentaire pour consoles de jeu et appareils « headless »		✓
Prise en charge de confirmation de paiement sécurisé		✓
Transactions hors bande et améliorations d'interface d'utilisation automatisées		✓
Données rehaussées pour plus de situations de paiement		✓

Les spécifications de SafeKey se trouvent sur AMEX Enabled et dans la base de connaissances.