American Express SafeKey®
Preguntas frecuentes

SECCIÓN 1: PREGUNTAS FRECUENTES GENERALES

P1.1 ¿QUÉ ES AMERICAN EXPRESS SAFEKEY®?

American Express SafeKey es una solución de seguridad que utiliza los estándares internacionales del sector para detectar y reducir el fraude online. Para conseguirlo, se añade una capa adicional de seguridad en las compras realizadas online o desde dispositivos móviles de los Titulares. SafeKey 2.0 utiliza el protocolo 3-D Secure de EMV®.

Los datos que proporcionan los Titulares durante su experiencia de compra, como el nombre, la dirección de correo electrónico, el número de teléfono y la dirección de envío, pueden ayudar a identificar qué transacciones son legítimas y cuáles son fraudulentas con mayor precisión.

A través del uso de métodos de autenticación basados en reglas de riesgo, SafeKey puede reducir los puntos de fricción y ofrecer una experiencia de compra más sencilla. Además, los Titulares pueden beneficiarse de SafeKey y comprar a través del dispositivo que les resulte más cómodo, incluidas las aplicaciones de compras.

P1.2 ¿CUÁLES SON LAS PRINCIPALES VENTAJAS DE SAFEKEY?

SafeKey puede ayudar a reducir el fraude en las transacciones de comercio electrónico. A su vez, esto ayuda a proteger a los Titulares frente al riesgo de que su Tarjeta sea utilizada sin permiso; también permite al Emisor estar involucrado en la evaluación de la autenticación y a los Establecimientos disponer de delegación de la responsabilidad en caso de fraude (consulte la sección de Delegación de Responsabilidad del Fraude (FLS) para más información).

EMV® es una marca comercial registrada en Estados Unidos y otros países, y una marca no registrada en los demás. La marca EMV es propiedad de EMVCo.

© 2019 American Express. Reservados todos los derechos.

P1.3 ¿CÓMO FUNCIONA SAFEKEY?

Para reducir el fraude online, SafeKey solicita al Emisor la confirmación de la identidad del Titular antes de que se autorice la transacción:

1. El proceso de autenticación se inicia cuando el Titular incurre en un gasto online con un Establecimiento.
2. El Establecimiento envía una transacción de SafeKey al Servidor de Directorios de American Express (DS) a través del proveedor del servidor 3DS (Merchant Plug-In).
3. El DS dirige la solicitud al Servidor de Control de Acceso (ACS) del Emisor correspondiente.
4. A través del ACS, se aplican sofisticadas técnicas de evaluación del riesgo para confirmar la identidad del Titular.
5. En ocasiones, se podrá solicitar al Titular que proporcione una contraseña de un solo uso al ACS.

P1.4 ¿EN QUÉ SECTORES ESTÁ DISPONIBLE SAFEKEY?

SafeKey está disponible para todos los Adquirentes y Emisores que deseen implementarlo, independientemente del mercado con el que trabajen. Para que un Establecimiento pueda utilizar este servicio, el Adquirente debe disponer de la certificación de SafeKey.

P1.5 ¿QUÉ ES 3-D SECURE (3DS) 2.0 Y POR QUÉ ES IMPORTANTE LANZAR UNA NUEVA VERSIÓN?

La solución original SafeKey se basó en el protocolo 3DS 1.0.2 y fue diseñada para respaldar la autenticación de los Titulares para transacciones de comercio electrónico realizadas a través del navegador de un ordenador. La entidad técnica internacional EMVCo, de la que American Express forma parte, ha ampliado su margen de actuación para liderar el sector de pagos, y para ello ha desarrollado la especificación 3DS 2.0 y los programas de prueba y aprobación asociados.

La versión 2.0 de 3DS admite los pagos remotos no procedentes de navegadores, como los pagos realizados en aplicaciones, a través de teléfono móvil y carteras electrónicas. Además, el objetivo ha sido proporcionar nuevas capacidades en cuanto a tecnología, seguridad, rendimiento, experiencia de usuario y flexibilidad con el fin de garantizar la perdurabilidad del servicio.

P1.6 ¿CÓMO REFLEJA SAFEKEY LAS ESPECIFICACIONES CAMBIANTES DE EMV 3DS, COMO LAS VERSIONES 2.1.0 Y 2.2.0?

Las funciones y la funcionalidad de SafeKey 2.0 se actualizan para reflejar cada nueva versión de EMV 3DS. Los participantes de SafeKey deberán volver a obtener el certificado de la versión más reciente para poder beneficiarse de todas las funciones.

P1.7 ¿QUÉ NOVEDADES OFRECE 3DS 2.0?

La versión 2.0 de 3DS de EMV pretende satisfacer las cambiantes necesidades del sector de pagos remotos, incluyendo la capacidad para:

- Soportar y tener una integración directa para las compras realizadas a través de navegadores y aplicaciones
- Mejorar la evaluación del riesgo del Emisor a través de datos adicionales
- Compatibilidad con una gran variedad de métodos de autenticación, como contraseñas de un solo uso, biometría y autenticación fuera de banda
- Compatibilidad con transacciones basadas en tokens para mejorar la seguridad y para fomentar la expansión del uso de tokens en la industria
- Realizar autenticación en transacciones que no llevan asociado un pago, como en casos de aprovisionamiento de una Tarjeta en una cartera digital
- Capacitación de los Establecimientos para iniciar autenticaciones (por ejemplo, Recibos Recurrentes y Pedidos por Correo o por Teléfono)
- Mejoras en la experiencia de usuario y los flujos de pago de los Titulares de tarjetas
- Soporte adicional para PSD2

Nota: Consulte el apéndice para obtener información detallada sobre la comparación de las funciones de cada versión de SafeKey

© 2019 American Express. Reservados todos los derechos.

P1.8 ¿DÓNDE PUEDO CONSULTAR LAS ESPECIFICACIONES DE SAFEKEY 2.0?

Las especificaciones y las guías de implementación de SafeKey 2.0 están disponibles en:

- Emisores/Adquirentes: https://network.americanexpress.com/globalnetwork/sign-in/
- Proveedores de servidor ACS y 3DS (MPI): https://network.americanexpress.com/globalnetwork/amex-enabled/
- Establecimientos: http://www.americanexpress.com/merchantspecs
- Especificaciones de referencia de EMV: www.emvco.com

P1.9 ¿CUÁL ES EL COMPROMISO DE AMERICAN EXPRESS CON SAFEKEY 1.0?

American Express está monitorizando el uso de SafeKey 1.0 en el sector y continuará dando soporte al servicio mientras se vaya expandiendo la implementación de SafeKey 2.0. Además, American Express anunciará el momento en que SafeKey 1.0 sea reemplazado por SafeKey 2.0 y ofrecerá un margen de tiempo adecuado para esta transición.

P1.10 ¿PUEDEN COEXISTIR SAFEKEY 1.0 Y SAFEKEY 2.0?

Sí, SafeKey 1.0 y 2.0 funcionan de manera independiente, de modo que pueden coexistir. Con el tiempo, se espera que SafeKey 2.0 reemplace la versión 1.0. Durante este periodo de transición, se recomienda que los Establecimientos busquen los servicios de un proveedor de servidor 3DS (MPI), que soporte ambos productos. Cuando un Establecimiento solicita la autenticación de una transacción, será responsabilidad del proveedor de servidor 3DS utilizar una versión u otra de SafeKey.

P1.11 ¿CÓMO IDENTIFICA EL SERVIDOR 3DS (MPI) LA VERSIÓN QUE DEBE UTILIZAR?

El servicio SafeKey guarda registros de rangos de tarjetas (BIN) compatibles con SafeKey 2.0, y estos detalles pasan a estar disponibles para cualquier servidor 3DS (MPI). Cuando un Establecimiento solicita la autenticación de un Titular, el servidor 3DS (MPI) comprueba si la tarjeta en cuestión permite utilizar SafeKey 2.0. Si lo permite, deberá utilizarse el servicio SafeKey 2.0; en caso contrario, se debería utilizar la versión 1.0.

P1.12 ¿ES POSIBLE IMPLANTAR SAFEKEY 2.0 SIN LA VERSIÓN SAFEKEY 1.0?

Sí. Con el tiempo, esta será la práctica habitual para quien vaya a utilizar este servicio por primera vez. Los Participantes deberán tener en cuenta que llevará cierto tiempo hasta que SafeKey 2.0 esté implantado en su totalidad.

P1.13 LOS TITULARES, ¿DEBEN INSCRIBIRSE EN SAFEKEY 2.0 SI YA LO HICIERON CON SAFEKEY 1.0?

Los Titulares no tienen que inscribirse en SafeKey 2.0, ya que los Emisores se encargarán de hacerlo por ellos al tratarse de un requisito de la especificación EMVCo.

P1.14 ¿PUEDE UTILIZARSE SAFEKEY PARA TRANSACCIONES ONLINE CON TODO TIPO DE TARJETAS?

SafeKey ofrece la ventaja de autenticar que la persona que realiza la transacción es el propio Titular. Por este motivo, no es posible utilizar este servicio con productos anónimos, como pueden ser las Tarjetas prepago, donde no se registra la identidad del usuario.

SECCIÓN 2: PREGUNTAS FRECUENTES: DELEGACIÓN DE RESPONSABILIDAD EN CASO DE FRAUDE (FLS)

P2.1 ¿QUÉ ES LA DELEGACIÓN DE RESPONSABILIDAD EN CASO DE FRAUDE (FLS)?

Si existe fraude en una transacción cualificada de SafeKey, la responsabilidad de éste se traslada del Establecimiento al Emisor por medio de la delegación de responsabilidad del fraude (FLS) de SafeKey.

© 2019 American Express. Reservados todos los derechos.

P2.2 ¿CÓMO PUEDE OBTENER UN ESTABLECIMIENTO LA FLS?

Los Establecimientos obtienen la FLS por las transacciones que han sido autenticadas por SafeKey y siempre que cumplan los criterios de la política de FLS. Los Establecimientos deben mantener índices de fraude bajos y cumplir los requisitos de las especificaciones de SafeKey, por ejemplo, la entrega de datos correctos en los mensajes de SafeKey. Los Establecimientos deben consultar al Adquirente los detalles de la política de FLS.

P2.3 ¿EN QUÉ CONSISTE UNA TRANSACCIÓN AUTENTICADA DE SAFEKEY?

Una transacción autenticada es aquella en la que el Emisor ha confirmado la identidad del Titular y esta información aparece indicada con un valor de autenticación específico en el mensaje de respuesta. Para obtener más información, consulte las especificaciones de SafeKey.

P2.4 ¿EN QUÉ CONSISTE UN INTENTO DE TRANSACCIÓN DE SAFEKEY?

Un intento de transacción es aquel en el que el Establecimiento ha intentado llevar a cabo la autenticación de SafeKey, pero el Emisor no admite SafeKey o el ACS del Emisor no está disponible. SafeKey podrá conceder un intento de autenticación indicado a través de un valor de autenticación en el mensaje de respuesta; consulte las especificaciones de SafeKey para obtener más información.

SECCIÓN 3: PREGUNTAS FRECUENTES: ESTABLECIMIENTOS

P3.1 ¿CÓMO PUEDO CONOCER LOS PASOS PARA IMPLANTAR SAFEKEY?

Los Establecimientos que deseen utilizar SafeKey deberán ponerse en contacto con su proveedor de servidor 3DS (MPI) o su Adquirente.

P3.2 ¿CÓMO PUEDO INSCRIBIR UN ESTABLECIMIENTO EN SAFEKEY?

Los Establecimientos deben ponerse en contacto con su proveedor de servidor 3DS (MPI) o su Adquirente para inscribirse en SafeKey. También disponen de un portal de inscripción online para ciertos Adquirentes en: www.amexsafekey.com.

P3.3 ¿HAY FORMA DE SABER QUÉ VERSIÓN DE SAFEKEY SE DEBE UTILIZAR COMO ESTABLECIMIENTO?

Se recomienda seleccionar un proveedor de servidor 3DS (MPI) que soporte ambas versiones. Éste seleccionará la versión adecuada, ya que puede saber qué versión de SafeKey admite el Emisor y, en consecuencia, utilizar las funciones mejoradas.

P3.4 ¿ES POSIBLE SABER COMO ESTABLECIMIENTO SI MI PROVEEDOR DE SERVIDOR 3DS (MPI) ADMITE SAFEKEY 2.0?

Los proveedores de servidor 3DS (MPI) colaboran con EMVCo y American Express para obtener la certificación de SafeKey 2.0. Los Establecimientos deberán ponerse en contacto con sus respectivos proveedores para tratar este tema. Para conocer los proveedores de servidor 3DS (MPI) con certificación de American Express y registrados en AMEX Enabled, puede consultar la lista disponible en el sitio web de Amex Enabled (www.amexenabled.com).

P3.5 ¿ES NECESARIO QUE LOS ESTABLECIMIENTOS SE INSCRIBAN EN SAFEKEY 2.0 SI YA ESTÁN INSCRITOS EN SAFEKEY 1.0?

Los Establecimientos deben colaborar con su proveedor de servidor 3DS (MPI) para conocer los procedimientos de SafeKey 2.0 y poder aprovecharlos.

P3.6 ACTUALMENTE NO UTILIZO SAFEKEY EN MI ESTABLECIMIENTO. ¿CÓMO ME INSCRIBO EN SAFEKEY 2.0?

Los Establecimientos deben ponerse en contacto, en primera instancia, con su proveedor de servidor 3DS (MPI) para tramitar la inscripción en SafeKey. Para conocer los proveedores de servidor 3DS (MPI) con certificación de American Express y registrados en AMEX Enabled, puede consultar la lista disponible en el sitio web de Amex Enabled (www.amexenabled.com).

© 2019 American Express. Reservados todos los derechos.

P3.7 ¿CÓMO PUEDE SABER UN ESTABLECIMIENTO O SERVIDOR 3DS (MPI) LAS VERSIONES DE SAFEKEY QUE ADMITE EL EMISOR?

El servidor 3DS (MPI) dispone de la información sobre qué Emisores utilizan SafeKey 2.0 y qué versiones de 2.0 admiten. El servidor 3DS (MPI) utiliza esta información para determinar el tipo de autenticación que se debe realizar.

P3.8 ¿CÓMO PUEDO ACTIVAR LA APLICACIÓN DE MI ESTABLECIMIENTO PARA QUE ADMITA SAFEKEY?

Los Establecimientos deben integrar un Kit de Desarrollo de Software (Software Development Kit o SDK) 3DS en la aplicación del Establecimiento para poder integrar SafeKey 2.0. Para ello, deberán colaborar con su proveedor de servidor 3DS (MPI) o un proveedor de SDK 3DS. Los SDK 3DS deben someterse a pruebas y posterior aprobación de EMVCo. Diríjase a la página www.emvco.com para consultar los proveedores de SDK aprobados.

P3.9 ¿QUÉ ES UN KIT DE DESARROLLO DE SOFTWARE (SDK) 3DS?

El SDK 3DS es un componente incorporado a la aplicación del Establecimiento. Este componente gestiona el procesamiento de SafeKey en nombre de la aplicación y se comunica con el servidor 3DS.

P3.10 ¿SE APLICAN COMISIONES POR TRANSACCIÓN EN AMERICAN EXPRESS POR EL USO DE SAFEKEY?

No. Comuníquese con su proveedor de servidor 3DS (MPI) para conocer el coste de sus servicios.

P3.11 ¿QUÉ SUCEDE SI EL EMISOR NO ADMITE SAFEKEY?

Si bien SafeKey es, actualmente, un servicio opcional para Emisores, aquellos que no participen podrían ser responsables por el fraude de las transacciones en las que el Establecimiento haya llevado a cabo un intento de autenticación de SafeKey. Contraste esta información con su Adquirente para conocer más información sobre la política de FLS de SafeKey.

P3.12 ¿QUÉ SUCEDE SI EL ADQUIRENTE DE UN ESTABLECIMIENTO NO ADMITE SAFEKEY?

El Adquirente del Establecimiento tiene como requisito estar certificado para SafeKey. De esta forma, se garantiza el procesamiento de los mensajes de autorización y envío necesarios, y la correcta atribución de la delegación de responsabilidad en caso de fraude. Nota: El procesador del Establecimiento también debe soportar SafeKey y transmitir los datos necesarios al Adquirente.

P3.13 ¿EXISTEN FUNCIONES DE SAFEKEY QUE AYUDEN A LOS ESTABLECIMIENTOS A ADMITIR UNA AUTENTICACIÓN REFORZADA?

Sí, todas las versiones de SafeKey son compatibles con una Autenticación de cliente reforzada, como los requisitos PSD2.

P3.14 ¿DÓNDE PUEDEN OBTENER LAS ESPECIFICACIONES DE AUTORIZACIÓN Y ENVÍO PARA SAFEKEY LOS ESTABLECIMIENTOS?

Consulte a su Adquirente para conocer las especificaciones técnicas más recientes. Los Establecimientos adquiridos directamente por American Express pueden visitar www.americanexpress.com/merchantspecs.

SECCIÓN 4: PREGUNTAS FRECUENTES: PROVEEDOR DE SERVIDOR ACS Y 3DS (MPI)

P4.1 ¿CÓMO PUEDEN OBTENER LA CERTIFICACIÓN DE SAFEKEY LOS PROVEEDORES DE SERVIDOR ACS Y 3DS (MPI)?

El primer paso para obtener la certificación de SafeKey es registrarse en AMEX Enabled. Los proveedores deben completar el formulario de inscripción de la empresa en la página www.amexenabled.com para acceder a la documentación de SafeKey.

P4.2 ¿DÓNDE PUEDO ENCONTRAR UNA LISTA DE PROVEEDORES DE SERVIDOR ACS Y 3DS CERTIFICADOS?

Para conocer los proveedores de servidor ACS y 3DS (MPI) con certificación de American Express, puede consultar la lista disponible en el sitio web de Amex Enabled (www.amexenabled.com).

© 2019 American Express. Reservados todos los derechos.

P4.3 ¿ES NECESARIA LA CERTIFICACIÓN PARA SAFEKEY 2.0 SI YA SE HA COMPLETADO LA CERTIFICACIÓN DE SAFEKEY 1.0?

Sí. En el caso de los proveedores de servidor ACS y 3DS (MPI), es necesario obtener certificaciones independientes para las distintas versiones de SafeKey 1.0 y SafeKey 2.0. Consulte la página www.amexsafekey.com para más información. EMVCo proporciona un servicio de aprobación EMV 3DS obligatorio dirigido a los proveedores de servidor ACS y 3DS (MPI), que debe completarse antes de la certificación de American Express SafeKey 2.0.

P4.4 ¿CÓMO PUEDO REGISTRARME PARA EL PROCESO DE CERTIFICACIÓN Y LA REALIZACIÓN DE PRUEBAS?

Por favor, regístrese en www.amexenabled.com para iniciar el proceso de certificación de SafeKey. El Analista de certificación de American Express le explicará cómo acceder al SafeKey Test Lab.

SECCIÓN 5: PREGUNTAS FRECUENTES: EMISOR Y ADQUIRENTE

P5.1 ¿CUÁL ES EL PROCEDIMIENTO DE CERTIFICACIÓN DE SAFEKEY PARA EMISORES Y ADQUIRENTES?

Los Emisores y Adquirentes deben ponerse en contacto con sus respectivos representantes de American Express para obtener información para la certificación de SafeKey o visitar la página www.amexsafekey.com para obtener más información.

P5.2 SI UN EMISOR O UN ADQUIRENTE DISPONEN DE LA CERTIFICACIÓN DE SAFEKEY 1.0, ¿ES NECESARIA LA CERTIFICACIÓN DE SAFEKEY 2.0?

Los mensajes de autorización y envío (submission) no han variado entre las versiones 1.0 y 2.0 de SafeKey, por lo que no es necesario volver a obtener la certificación. Sin embargo, el proceso de autenticación para el ACS sí necesitará certificación.

© 2019 American Express. Reservados todos los derechos.

APÉNDICE: TABLA COMPARATIVA DE FUNCIONES

Tabla comparativa de American Express SafeKey®

Función	SafeKey 1.0	SafeKey 2.0	
		SafeKey 2.1 (EMV 2.1.0)	SafeKey 2.2 (EMV 2.2.0)
Basado en el estándar de la industria 3-D Secure	●	●	●
Capa de seguridad adicional al tramitar la compra	●	●	●
Autenticación de pagos	●	●	●
Autenticación basada en navegador	●	●	●
Flexibilidad para que los Emisores puedan utilizar distintos métodos de autenticación (por ejemplo, contraseñas de un solo uso, toma de decisiones basadas en el riesgo, etc.)	●	●	●
Soporte para el cumplimiento de la PSD2	●	●	●
Compatibilidad con más datos para autenticaciones sin fricción	Disponible en EE. UU. y sus territorios	●	●
Activación basada en las aplicaciones (dentro de las aplicaciones)	—	●	●
Autenticación de transacciones que no llevan un pago asociado	—	●	●
Transacciones basadas en token	—	●	●
Autenticación fuera de banda	—	●	●
Autenticaciones iniciadas por los Establecimientos	—	—	●
Autenticación disociada	—	—	●
Indicadores adicionales de la PSD2	—	—	●

Nota: Es posible que algunas de estas funciones requieran certificaciones adicionales.

AMERICAN EXPRESS SafeKey®

© 2019 American Express. Reservados todos los derechos.