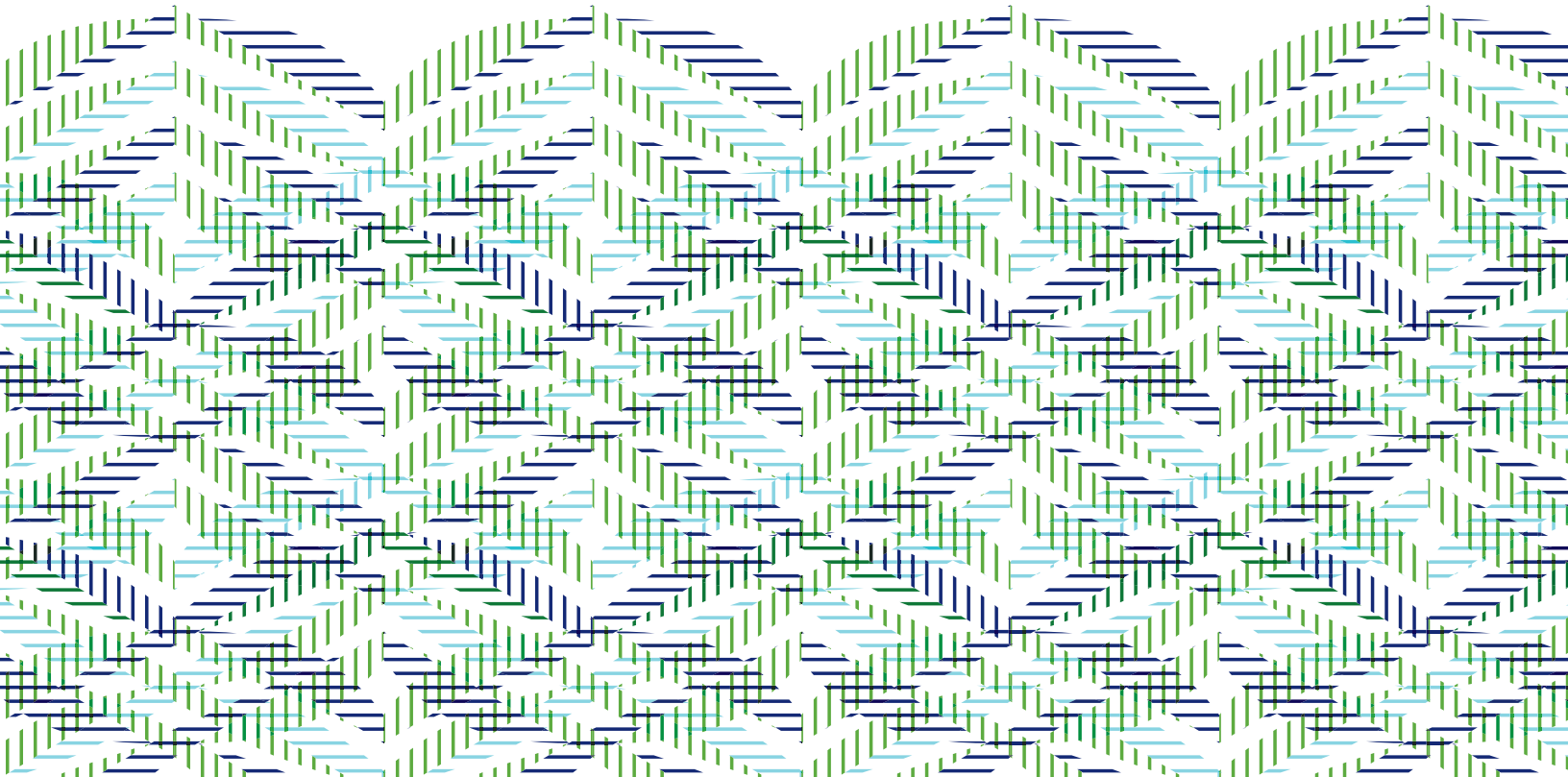
AMERICAN EXPRESS SAFEKEY®

PREGUNTAS FRECUENTES

NOVIEMBRE DE 2016



¿QUÉ ES AMERICAN EXPRESS SAFEKEY®?

El programa American Express SafeKey (en adelante, "SafeKey") es una herramienta de autenticación que añade un nivel adicional de seguridad cuando los Titulares participantes realizan compras online. SafeKey puede ayudar a reducir el uso online no autorizado antes de que ocurra, ya que valida la identidad del Titular a través de diversos métodos de autenticación, incluidas la autenticación basada en el riesgo y las contraseñas dinámicas de un solo uso.

¿DÓNDE ESTÁ DISPONIBLE SAFEKEY?

A partir del 15 de abril de 2016, American Express amplió la política de delegación de la responsabilidad derivada del fraude (FLS) SafeKey a todos los mercados.

¿QUÉ ES 3-D SECURE®?

3-D Secure es un protocolo para la prevención del fraude en el comercio electrónico aceptado como un estándar en el ámbito de la autenticación interoperativa de pagos en todo el mundo. American Express ha adquirido una licencia del protocolo 3-D Secure y ha lanzado una solución propia denominada SafeKey.

¿QUÉ TIPO DE MÉTODOS DE AUTENTICACIÓN ADMITE SAFEKEY?

SafeKey se basa en el protocolo 3-D Secure y admite varios métodos de autenticación, incluidas la autenticación basada en el riesgo y las contraseñas dinámicas de un solo uso.

¿SE AJUSTA SAFEKEY A LOS ESTÁNDARES DEL SECTOR?

Sí.
SafeKey se ajusta a los estándares del sector para facilitar la certificación y minimizar los costes de desarrollo en la medida de lo posible. Los Emisores, Adquirentes y Proveedores descubrirán que la solución 3-D Secure de American Express es prácticamente igual a otras utilizadas en el sector de medios de pago.

¿QUÉ OTRAS HERRAMIENTAS HAY DISPONIBLES PARA LA PREVENCIÓN DEL FRAUDE?

SafeKey complementa otras soluciones y herramientas de American Express para la prevención del fraude, como la comprobación automatizada de direcciones (AAV) y la autorización mejorada (EA). SafeKey debería utilizarse junto con otras soluciones para la prevención del fraude, para incorporar un nivel adicional de seguridad.

¿QUÉ SE ENTIENDE POR DELEGACIÓN DE LA RESPONSABILIDAD DERIVADA DEL FRAUDE ("FLS") SAFEKEY?

En las transacciones SafeKey que cumplen los requisitos, la delegación de la responsabilidad derivada del fraude (FLS) SafeKey transfiere la exposición del fraude del Establecimiento o Adquirente al Emisor, cuando un Establecimiento participante en SafeKey autentica con el Emisor una transacción sin tarjeta física. Si el Establecimiento intenta realizar una transacción de SafeKey o un Emisor es capaz de autenticar una transacción de SafeKey, el emisor no podrá presentar una retrocesión de cargo por fraude contra el Establecimiento elegible.

¿PUEDE UTILIZARSE SAFEKEY PARA TRANSACCIONES ONLINE CON TODOS LOS PRODUCTOS DE TARJETA?

SafeKey no puede habilitarse ni utilizarse para autenticar productos de Tarjeta que sean anónimos, como algunas Tarjetas prepago en las que la identidad de los usuarios no se registra. Esto incluye productos de Tarjeta que podrían tener varios usuarios, como Tarjetas de compras de empresa.

PREGUNTAS FRECUENTES PARA ESTABLECIMIENTOS

¿CÓMO PUEDE UN ESTABLECIMIENTO INSCRIBIRSE EN SAFEKEY?

Los Establecimientos podrán inscribirse en el programa SafeKey en el portal de inscripción de SafeKey amexsafekey.com. Asimismo, los Establecimientos pueden dirigirse a su Merchant Plug-In (MPI) o Proveedor de servicios de pago.

¿QUÉ ESFUERZO EXIGE PARA UN ESTABLECIMIENTO IMPLEMENTAR SAFEKEY?

Los niveles de desarrollo técnico necesarios para integrar SafeKey pueden variar en función del modelo de procesamiento. Los Establecimientos deben considerar los costes asociados al desarrollo técnico interno y a los enlaces externos con terceros.

¿EL ESTABLECIMIENTO PUEDE DESACTIVAR SAFEKEY TRAS SU IMPLEMENTACIÓN?

Técnicamente, el Establecimiento puede desactivar SafeKey. Sin embargo, el objetivo de SafeKey es reducir los casos de fraude en transacciones sin tarjeta física. Por este motivo, American Express recomienda no desactivar SafeKey en ningún momento conforme a las directrices de implementación de SafeKey.

¿CÓMO SE AUTENTICA Y AUTORIZA UNA TARJETA CUANDO EL ESTABLECIMIENTO Y EL TITULAR ESTÁN INSCRITOS EN SAFEKEY?

- ☐ Al tramitar el pedido, el Titular selecciona como método de pago American Express y proporciona el número de la Tarjeta.
- ☐ El componente MPI (Merchant Plug-in) integrado con el sitio web del Establecimiento se comunicará con el Servidor de directorio de SafeKey para determinar si la Tarjeta American Express está inscrita en SafeKey.
- ☐ El Servidor de directorio de SafeKey se comunicará con el Emisor de la Tarjeta para determinar si la Tarjeta es válida para el servicio.
- ☐ El Emisor responderá con el estado "Y" si la Tarjeta es elegible, junto con una URL a la que deberá dirigirse al Titular para autenticarse (el Sitio de autenticación).
- ☐ La aplicación del Establecimiento redirigirá automáticamente al Titular al Sitio de autenticación.
- ☐ En el Sitio de autenticación, el Emisor mostrará la página con el diálogo de autenticación en la que el Titular intentará realizar la autenticación. El Emisor enviará una respuesta al Establecimiento con el resultado de autenticación. Por razones de seguridad, el mensaje se enviará firmado digitalmente.
- ☐ El MPI (Merchant Plug-in) validará la firma y notificará al Establecimiento el resultado de la autenticación.
- ☐ El Establecimiento puede aprobar o rechazar la transacción en función del resultado de la autenticación.

¿SERÁ NECESARIO MODIFICAR LOS TÉRMINOS Y CONDICIONES PARA ESTABLECIMIENTOS CON EL FIN DE ACOMODAR EL PROGRAMA SAFEKEY?

Sí.
Los Términos y Condiciones de aceptación de la tarjeta American Express pueden modificarse o volver a emitirse para incluir la delegación de la responsabilidad derivada del fraude SafeKey.

¿QUÉ SE ENTIENDE POR "TRANSACCIÓN INTENTADA"?

Un intento de autenticación de SafeKey tiene lugar cuando un Establecimiento solicita autenticar al Titular, pero el Titular o el Emisor no están inscritos en el programa SafeKey. En este caso, se requerirán datos de autenticación válidos (p. ej., el valor de verificación de American Express ["AEVV"] y el indicador de comercio electrónico ["ECI"]) en los mensajes de Autorización y Envío como prueba del intento.

¿OBTENDRÁ UN ESTABLECIMIENTO PARTICIPANTE LA DELEGACIÓN DE RESPONSABILIDAD DERIVADA DEL FRAUDE SAFEKEY EN TODAS LAS TRANSACCIONES SIN TARJETA FÍSICA?

No.
Los Establecimientos solo podrán obtener la delegación de la responsabilidad derivada del fraude SafeKey en transacciones SafeKey intentadas o totalmente autenticadas. En el caso de cargos estándar de comercio electrónico, se aplicará la política habitual de aceptación para operaciones sin tarjeta física y el Establecimiento será responsable si el Titular reclama posteriormente el cargo.

¿DÓNDE PUEDE OBTENER UN ESTABLECIMIENTO LAS ESPECIFICACIONES DE AUTORIZACIÓN Y ENVÍO DE SAFEKEY?

Las especificaciones técnicas más recientes para Establecimientos están disponibles en americanexpress.com/merchantspecs. Para obtener información adicional sobre las especificaciones estándar de los mercados en los que se admite SafeKey, los Establecimientos pueden ponerse en contacto con su Responsable de cuenta en American Express o con su Proveedor de servicios de pago (PSP).

¿QUÉ CRITERIOS DEBE SATISFACER UN ESTABLECIMIENTO PARA ACOGERSE A LA DELEGACIÓN DE LA RESPONSABILIDAD DERIVADA DEL FRAUDE SAFEKEY?

Para acogerse a la delegación de la responsabilidad derivada del fraude SafeKey, un Establecimiento deberá:

- ☐ Utilizar SafeKey.
- ☐ En mercados fuera de Estados Unidos, utilizar el resto de herramientas de prevención del fraude online de American Express disponibles en su mercado.
- ☐ Mantener un índice de fraude sobre las ventas brutas del 1 % o menos en todas las transacciones de SafeKey. En el mercado de Estados Unidos, mantener la integridad de los datos y los umbrales de calidad por encima del 85 %.

En Reino Unido, por ejemplo, el Establecimiento necesitaría participar en AVS y recopilar o enviar el Código de seguridad impreso en la tarjeta (PCSC), además de utilizar SafeKey y mantener el nivel de fraude sobre las ventas brutas correspondiente.

¿QUÉ OCURRE SI UN EMISOR DECIDE NO PARTICIPAR EN SAFEKEY?

Si bien SafeKey es un servicio opcional para Emisores, los Emisores que no participen podrían ser responsables por las transacciones en las que el Establecimiento haya intentado una autenticación SafeKey. Consulte la sección 7.9 del manual Políticas empresariales y operativas disponible en GNSweb.

¿QUÉ COSTES CONLLEVA LA UTILIZACIÓN DE SAFEKEY?

Además de los costes de obtener un servicio ACS, los costes relativos a la certificación de red y los certificados pueden confirmarse a través de su representante de American Express.

¿CÓMO PUEDE UN EMISOR AVERIGUAR QUÉ PROVEEDORES DE ACS CUENTAN CON CERTIFICACIÓN PARA SAFEKEY?

Para obtener información específica sobre los proveedores de ACS certificados para SafeKey, póngase en contacto con el representante local de AEGNS. Si ya participa en los programas 3-D Secure de otras asociaciones y desea utilizar el mismo proveedor de ACS para SafeKey, solicite a su proveedor de ACS que visite el sitio web de inscripción de SafeKey para completar la certificación correspondiente.