American Express SafeKey®
Häufig gestellte Fragen (FAQ)

ABSCHNITT 1: FAQ - ALLGEMEIN

F1.1 WAS IST AMERICAN EXPRESS SAFEKEY®?

American Express SafeKey ist eine Sicherheitslösung, die die globalen Industriestandards nutzt, um Online-Betrug im Internet zu entdecken und zu reduzieren – SafeKey dient für zusätzliche Sicherheit, wenn Karteninhaber am PC oder mit dem Mobilgerät online shoppen. SafeKey 2.0 basiert auf dem EMV®-3-D-Secure-Protokoll.

Die während des Einkaufs übermittelten Daten von Karteninhabern, wie beispielsweise Name, E-Mail-Adresse, Telefonnummer und Lieferanschrift, können bei der genaueren Unterscheidung zwischen legitimen und unbefugten Transaktionen hilfreich sein.

Durch risikobasierte Authentifizierungsmethoden auf Seiten des Kartenherausgebers sorgt SafeKey für einen reibungslosen und optimierten Bezahlvorgang. Außerdem können Karteninhaber SafeKey beim Shoppen mit ihren bevorzugten Geräten verwenden – auch für In-App-Käufe auf Smart-Geräten.

F1.2 WAS SIND DIE GRÖSSTEN VORTEILE VON SAFEKEY?

SafeKey trägt zur Reduzierung unbefugter E-Commerce-Transaktionen bei. So werden Karteninhaber vor der unzulässigen Verwendung ihrer Karte geschützt, der Kartenherausgeber ist an der Authentifizierungsauswertung beteiligt und kann die Haftung bei Betrug an den Vertragspartner weiterleiten (Einzelheiten finden Sie im Abschnitt zu FLS).

F1.3 WIE FUNKTIONIERT SAFEKEY?

SafeKey trägt zum Schutz vor Online-Betrug bei, indem der Kartenherausgeber die Identität des Karteninhabers bestätigen muss, bevor eine Transaktion freigegeben wird:

1. Der Authentifizierungsprozess beginnt, sobald der Karteninhaber bei einem Vertragspartner mit Karte bezahlt.
2. Der Vertragspartner übermittelt eine SafeKey-Transaktion über seinen 3DS-Server-Provider (Vertragspartner-Plug-in, kurz „MPI“) an den American Express Directory Server (DS).
3. Der DS leitet die Anfrage an den Access Control Server (ACS) des entsprechenden Kartenherausgebers weiter.
4. Der ACS wendet fortschrittliche Risikomodelltechniken an, um die Identität des Karteninhabers zu bestätigen.
5. In bestimmten Fällen wird der Karteninhaber darum gebeten, ein Einmalkennwort an den ACS zu senden.

F1.4 WO IST SAFEKEY VERFÜGBAR?

SafeKey ist in jedem Markt für Kundenberater und Kartenherausgeber verfügbar, die das System einsetzen möchten. Damit ein Vertragspartner den Dienst nutzen kann, muss sein Kundenberater für SafeKey zertifiziert sein.

F1.5 WAS IST 3-D SECURE (3DS) 2.0 UND WARUM BENÖTIGT DIE BRANCHE EINE NEUE VERSION?

Die ursprüngliche Version von SafeKey, die auf dem Protokoll von 3DS 1.0.2 basiert, wurde entwickelt, um die Authentifizierung von Karteninhabern bei E-Commerce-Transaktionen auf PC-Browsern zu unterstützen. Die globale technische Gesellschaft EMVCo, in der American Express Mitglied ist, hat ihre Aufgaben erweitert, um die Weiterentwicklung der 3DS-2.0-Spezifikation und des damit verbundenen Prüf- und Genehmigungsprogramms in der Zahlungsbranche zu leiten.

3DS 2.0 unterstützt ortsferne Zahlungen außerhalb des Browsers, darunter In-App-Käufe sowie Zahlungen per Mobiltelefon oder Benutzerkonto. Darüber hinaus bestand das Ziel darin, neue Funktionen hinsichtlich Technologie, Sicherheit, Leistung, Benutzerfreundlichkeit und Flexibilität für eine langfristige Realisierbarkeit zu liefern.

F1.6 INWIEFERN BERÜCKSICHTIGT SAFEKEY DIE SICH STÄNDIG WEITERENTWICKELNDEN EMV 3DS-SPEZIFIKATIONEN (Z. B. V2.1.0 UND V2.2.0)?

Die Funktionen und Merkmale von SafeKey 2.0 werden kontinuierlich aktualisiert, um jede neue Version von EMV 3DS zu unterstützen. SafeKey-Teilnehmer müssen sich für die neueste Version rezertifizieren, um von allen Funktionen profitieren zu können.

F1.7 WELCHE FUNKTIONEN BIETET 3DS 2.0?

Das Ziel von EMV 3DS 2.0 ist es, den Anforderungen der sich ständig weiterentwickelnden Umgebung für ortsferne Zahlungen gerecht zu werden. Dazu gehören die folgenden Funktionen:

- Die Unterstützung und direkte Integration für Browser- und In-App-Shopping
- Verbesserte Risikobewertung für Kartenherausgeber durch erweiterte Daten
- Die Unterstützung einer Vielzahl von Authentifizierungsmethoden, einschließlich Einmalkennwörtern, biometrischer Daten und Out-of-Band-Authentifizierung
- Die Unterstützung token-basierter Transaktionen für erhöhte Sicherheit, um der branchenweit steigenden Nutzung von Tokens gerecht zu werden
- Die Nichtzahlungsauthentifizierung, etwa beim Hinzufügen einer Karte zum Benutzerkonto
- Die Möglichkeit für Vertragspartner, Authentifizierungen zu initiieren (z. B. für wiederkehrende Rechnungen, Versandbestellungen und telefonische Bestellungen)
- Verbesserung der Benutzerfreundlichkeit und des Zahlungsprozesses für Karteninhaber
- Zusätzliche Unterstützung für PSD2

Hinweis: Im Anhang finden Sie einen detaillierten Funktionsvergleich für jede SafeKey-Version.

F1.8 WO FINDE ICH DIE SAFEKEY-2.0-SPEZIFIKATIONEN?

SafeKey-2.0-Spezifikationen und Implementierungsanleitungen finden Sie unter:

- Kartenherausgeber/Kundenberater: https://network.americanexpress.com/globalnetwork/sign-in/
- ACS- und MPI- /3DS-Server-Anbieter: https://network.americanexpress.com/globalnetwork/amex-enabled/
- Vertragspartner: http://www.americanexpress.com/merchantspecs
- Baseline EMV-Spezifikationen: www.emvco.com

F1.9 INWIEFERN SETZT SICH AMERICAN EXPRESS FÜR SAFEKEY 1.0 EIN?

American Express überwacht den Einsatz von SafeKey 1.0 und unterstützt den Dienst weiterhin, während allmählich der Umstieg auf SafeKey 2.0 erfolgt. American Express wird mit ausreichend Vorlaufzeit bekannt geben, sobald SafeKey 1.0 vollständig durch SafeKey 2.0 ersetzt wird.

F1.10 KÖNNEN SAFEKEY 1.0 UND SAFEKEY 2.0 GLEICHZEITIG LAUFEN?

Ja. SafeKey 1.0 und 2.0 funktionieren unabhängig voneinander und können somit gleichzeitig laufen. SafeKey 2.0 soll allmählich Version 1.0 ersetzen, und in dieser Übergangsphase sollten sich Vertragspartner MPI- / 3DS-Server-Anbieter suchen, die beide Produkte unterstützen. Wenn ein Vertragspartner die Authentifizierung einer Transaktion anfordert, liegt es in der Verantwortung des MPI- / 3DS-Server-Anbieters, die passende SafeKey-Version zu verwenden.

F1.11 WOHER WEISS DER MPI- /3DS-SERVER, WELCHE SAFEKEY-VERSION VERWENDET WERDEN MUSS?

Der SafeKey-Dienst hält die Kartenbereiche (BIN-Bereiche) fest, die von SafeKey 2.0 unterstützt werden, und diese Details werden jedem MPI- / 3DS-Server zur Verfügung gestellt. Wenn ein Vertragspartner die Authentifizierung eines Karteninhabers anfordert, überprüft der MPI- / 3DS-Server, ob die betroffene Karte mit SafeKey 2.0 kompatibel ist. Falls ja, sollte SafeKey 2.0 verwendet werden, und falls nicht, sollte SafeKey 1.0 verwendet werden.

F1.12 KANN SAFEKEY 2.0 OHNE SAFEKEY 1.0 EINGESETZT WERDEN?

Ja. Das wird im Laufe der Zeit der Standardansatz für alle Neueinsteiger sein. Die Teilnehmer sollten sich darüber im Klaren sein, dass es eine Zeit dauern wird, bis SafeKey 2.0 vollständig eingerichtet ist.

F1.13 MÜSSEN SICH KARTENINHABER FÜR SAFEKEY 2.0 REGISTRIEREN, WENN SIE BEREITS FÜR SAFEKEY 1.0 REGISTRIERT SIND?

Karteninhaber müssen sich nicht für SafeKey 2.0 registrieren, da alle teilnahmeberechtigten Karteninhaber von den Kartenherausgebern als Voraussetzung für die EMVCo-Spezifikation bereits im Voraus registriert werden.

F1.14 KANN SAFEKEY FÜR ONLINE-TRANSAKTIONEN MIT ALLEN KARTENPRODUKTEN VERWENDET WERDEN?

SafeKey bietet gegenüber anderen Produkten den Vorteil, dass es die Person, die eine Transaktion durchführt, als den Karteninhaber authentifiziert. Folglich kann es nicht mit anonymen Produkten wie Prepaidkarten verwendet werden, bei denen die Identität des Nutzers nicht registriert wird.

ABSCHNITT 2: FAQ ZU FRAUD LIABILITY SHIFT (FLS – HAFTUNGSUMKEHR BEI BETRUG)

F2.1 WAS IST SAFEKEY FRAUD LIABILITY SHIFT (FLS)?

Bei einem Betrugsfall mit einer qualifizierenden Transaktion überträgt SafeKey FLS die Haftung für den Betrugsfall vom Vertragspartner auf den Kartenherausgeber.

F2.2 WIE ERHÄLT DER VERTRAGSPARTNER FLS?

Einem Vertragspartner wird FLS für Transaktionen gewährt, die von SafeKey authentifiziert wurden, sofern sie die Kriterien der FLS-Richtlinien erfüllen. Von Vertragspartnern wird erwartet, dass sie die Betrugsraten niedrig halten und die Anforderungen der SafeKey-Spezifikationen erfüllen, beispielsweise die Bereitstellung genauer Daten in SafeKey-Nachrichten. Vertragspartner sollten sich für Einzelheiten zur FLS-Richtlinie an ihren Kundenberater wenden.

F2.3 WAS IST EINE AUTHENTIFIZIERTE SAFEKEY-TRANSAKTION?

Eine Transaktion ist authentifiziert, wenn der Kartenherausgeber die Identität des Karteninhabers gemäß einem Authentifizierungswert in der Antwortnachricht bestätigt hat. Einzelheiten finden Sie in den SafeKey-Spezifikationen.

F2.4 WAS IST EINE VERSUCHTE SAFEKEY-TRANSAKTION?

Bei einer versuchten Transaktion hat der Vertragspartner versucht, eine SafeKey-Authentifizierung durchzuführen, jedoch unterstützt der Kartenherausgeber SafeKey nicht, oder der ACS des Kartenherausgebers ist nicht verfügbar. SafeKey kann eine versuchte Authentifizierung gemäß einem Authentifizierungswert in der Antwortnachricht genehmigen. Einzelheiten finden Sie in den SafeKey-Spezifikationen.

ABSCHNITT 3: FAQ FÜR VERTRAGSPARTNER

F3.1 WIE SCHÄTZE ICH AM BESTEN EIN, WELCHE SCHRITTE ERFORDERLICH SIND, UM SAFEKEY EINZURICHTEN?

Vertragspartner, die SafeKey einrichten möchten, sollten sich an ihren zuständigen MPI- / 3DS-Server-Anbieter oder Kundenberater wenden.

F3.2 WIE MELDE ICH MICH ALS VERTRAGSPARTNER BEI SAFEKEY AN?

Vertragspartner sollten sich an ihren MPI- / 3DS-Server-Anbieter oder Kundenberater wenden, um sich bei SafeKey anzumelden. Ein Online-Anmeldeportal ist zudem für bestimmte Kundenberater unter www.amexsafekey.com verfügbar.

F3.3 WIE WEISS ICH ALS VERTRAGSPARTNER, WELCHE SAFEKEY-VERSION ICH VERWENDEN MUSS?

Es wird empfohlen, einen MPI-/3DS-Server-Anbieter auszuwählen, der alle SafeKey-Versionen unterstützt. Der Anbieter wählt daraufhin die passende Version aus, da er weiß, welche SafeKey-Versionen der Kartenherausgeber unterstützt, und verwendet die erweiterten Funktionen.

F3.4 WOHER WEISS ICH ALS VERTRAGSPARTNER, OB MEIN MPI- / 3DS-SERVER-ANBIETER SAFEKEY 2.0 UNTERSTÜTZT?

MPI- / 3DS-Server-Anbieter arbeiten mit EMVCo und American Express zusammen, um sich für SafeKey 2.0 zu zertifizieren. Vertragspartner sollten sich mit ihrem Provider in Verbindung setzen, um ihre Pläne zu besprechen. Eine Liste der MPI- / 3DS-Server-Anbieter, die durch American Express zertifiziert und bei AMEX Enabled registriert sind, finden Sie auf der AMEX Enabled Website (www.amexenabled.com).

F3.5 MÜSSEN SICH VERTRAGSPARTNER FÜR SAFEKEY 2.0 REGISTRIEREN, WENN SIE BEREITS FÜR SAFEKEY 1.0 REGISTRIERT SIND?

Vertragspartner sollten sich mit ihrem MPI- / 3DS-Server auseinandersetzen, um die Verfahren zu verstehen, die die Nutzung der Vorteile durch SafeKey 2.0 ermöglichen.

F3.6 ICH BIN EIN VERTRAGSPARTNER, DER SAFEKEY DERZEIT NICHT VERWENDET. WIE SCHREIBE ICH MICH FÜR SAFEKEY 2.0 EIN?

Vertragspartner sollten sich zunächst an ihren MPI- / 3DS-Server-Anbieter wenden, um die Einschreibung für SafeKey zu besprechen. Eine Liste der zertifizierten MPI- / 3DS-Server-Anbieter, die bei American Express registriert sind, finden Sie auf der AMEX Enabled Website (www.amexenabled.com).

F3.7 WOHER WEISS EIN VERTRAGSPARTNER ODER MPI-/3DS-SERVER, WELCHE SAFEKEY-VERSIONEN EIN KARTENHERAUSGEBER UNTERSTÜTZT?

Der 3DS-Server (MPI) enthält Informationen darüber, welche Herausgeber SafeKey 2.0 unterstützen und welche Versionen von 2.0 sie unterstützen. Der 3DS-Server (MPI) verwendet diese Daten, um den geeigneten Authentifizierungstyp zu bestimmen.

F3.8 WIE KANN ICH ALS VERTRAGSPARTNER MEINE APP FÜR SAFEKEY FREISCHALTEN?

Vertragspartner müssen ein 3DS-Software-Development-Kit (SDK) in die Vertragspartner-App integrieren, um sie für SafeKey 2.0 freischalten zu können. Vertragspartner sollten sich diesbezüglich an ihren MPI- / 3DS-Server-Anbieter oder einen 3DS-SDK-Provider wenden. 3DS-SDKs müssen von EMVCo geprüft und genehmigt werden. Auf www.emvco.com finden Sie eine Liste zugelassener SDK-Provider.

F3.9 WAS IST EIN 3DS-SOFTWARE-DEVELOPMENT-KIT (SDK)?

Das 3DS-SDK ist eine Komponente, die in die Vertragspartner-App aufgenommen wird. Das 3DS-SDK verwaltet die SafeKey-Verarbeitung für die App und bildet eine Schnittstelle zum 3DS-Server.

F3.10 BERECHNET AMERICAN EXPRESS TRANSAKTIONSGEBÜHREN FÜR DIE VERWENDUNG VON SAFEKEY?

Nein. Bitte sprechen Sie mit Ihrem MPI- / 3DS-Server-Anbieter, um sich über die Kosten für dessen Dienstleistungen zu informieren.

F3.11 WAS PASSIERT, WENN DER KARTENHERAUSGEBER SAFEKEY NICHT UNTERSTÜTZT?

Zwar ist SafeKey derzeit ein optionaler Service für Kartenherausgeber, jedoch haften teilnehmende Herausgeber in eventuellen Betrugsfällen bei Transaktionen nicht, bei denen eine SafeKey-Authentifizierung durch den Vertragspartner versucht wurde. Bitte wenden Sie sich für Einzelheiten zur SafeKey-FLS-Richtlinie an Ihren Kundenberater.

F3.12 WAS PASSIERT, WENN DER KUNDENBERATER EINES VERTRAGSPARTNERS SAFEKEY NICHT UNTERSTÜTZT?

Der Kundenberater eines Vertragspartners muss für SafeKey zertifiziert sein. Damit soll sichergestellt werden, dass die erforderlichen Genehmigungen sowie die Übermittlung von Nachrichten verarbeitet werden können und die Haftungsumkehr bei Betrug ordnungsgemäß zugeteilt werden kann. Hinweis: Der Verarbeiter eines Vertragspartners sollte SafeKey unterstützen und die benötigten Daten an den Kundenberater weiterleiten können.

F3.13 GIBT ES FUNKTIONEN IN SAFEKEY, DIE VERTRAGSPARTNER BEI DER UNTERSTÜTZUNG EINER STARKEN KUNDENAUTHENTIFIZIERUNG UNTERSTÜTZEN?

Ja, alle Versionen von SafeKey unterstützen eine starke Kundenauthentifizierung, z. B. PSD2-Anforderungen.

F3.14 WO ERHALTEN VERTRAGSPARTNER AUTORISIERUNGS- UND EINREICHUNGSSPEZIFIKATIONEN FÜR SAFEKEY?

Die aktuellen technischen Spezifikationen erhalten Sie von Ihrem Kundenberater. Vertragspartner, deren unmittelbarer Kundenberater American Express ist, können www.americanexpress.com/merchantspecs besuchen.

ABSCHNITT 4: FAQ FÜR ACS- UND MPI- / 3DS-SERVER-ANBIETER

F4.1 WIE KÖNNEN SICH ACS- UND MPI- / 3DS-SERVER-ANBIETER FÜR SAFEKEY ZERTIFIZIEREN?

Der erste Schritt für die SafeKey-Zertifizierung ist die Registrierung bei AMEX Enabled. Anbieter müssen das Registrierungsformular für Unternehmen auf www.amexenabled.com ausfüllen, um Zugriff auf die SafeKey-Dokumentation zu erhalten.

F4.2 WO FINDE ICH EINE LISTE MIT ZERTIFIZIERTEN ACS- UND MPI- / 3DS-SERVER-ANBIETERN?

Eine Liste der zertifizierten ACS- und MPI- / 3DS-Server-Anbieter, die bei American Express registriert sind, finden Sie auf der AMEX Enabled Website (www.amexenabled.com).

F4.3 IST EINE ZERTIFIZIERUNG FÜR SAFEKEY 2.0 ERFORDERLICH, WENN DIE ZERTIFIZIERUNG FÜR SAFEKEY 1.0 BEREITS ABGESCHLOSSEN WURDE?

Ja. Für ACS- und MPI-/3DS-Server-Anbieter sind separate Zertifizierungen für die verschiedenen SafeKey-Versionen erforderlich. Einzelheiten finden Sie unter www.amexsafekey.com. EMVCo hat einen verpflichtenden EMV-3DS-Genehmigungsdienst für ACS- und MPI-/3DS-Server-Anbieter eingerichtet, der vor der Zertifizierung durch American Express SafeKey 2.0 durchgeführt werden muss.

F4.4 WIE REGISTRIERE ICH MICH FÜR DIE ZERTIFIZIERUNG UND TESTS?

Registrieren Sie sich unter www.amexenabled.com, um den SafeKey-Zertifizierungsprozess zu starten. Ihr American Express Zertifizierungsanalyst erklärt Ihnen, wie Sie auf das SafeKey Test Lab zugreifen können.

ABSCHNITT 5: FAQ FÜR KARTENHERAUSGEBER UND KUNDENBERATER

F5.1 WIE KÖNNEN SICH KARTENHERAUSGEBER UND KUNDENBERATER FÜR SAFEKEY ZERTIFIZIEREN?

Kartenherausgeber und Kundenberater sollten sich bezüglich Einzelheiten über die Zertifizierung für SafeKey an ihren American Express Vertreter wenden oder www.amexsafekey.com besuchen.

F5.2 MUSS SICH EIN KARTENHERAUSGEBER ODER KUNDENBERATER FÜR SAFEKEY 2.0 ZERTIFIZIEREN, WENN BEREITS EINE ZERTIFIZIERUNG FÜR SAFEKEY 1.0 DURCHGEFÜHRT WURDE?

Die Netzwerknachrichten für SafeKey 1.0 und 2.0 sind einheitlich. Eine erneute Zertifizierung ist daher nicht erforderlich. Für die Authentifizierungsverarbeitung für den ACS ist jedoch eine Zertifizierung erforderlich.

ANHANG: FUNKTIONSVERGLEICHSTABELLE

American Express® SafeKey Vergleichstabelle

Merkmal	SafeKey 1.0	SafeKey 2.0	
		SafeKey 2.1 (EMV 2.1.0)	SafeKey 2.2 (EMV 2.2.0)
Basiert auf der branchenführenden Standardtechnologie 3-D Secure	●	●	●
Zusätzliche Sicherheitsebene an der Kasse / beim Check-out	●	●	●
Zahlungsauthentifizierung	●	●	●
Browserbasierte Authentifizierung	●	●	●
Flexibilität für den Kartenherausgeber durch eine Vielzahl von Authentifizierungsmethoden (z. B. Einmalkennwörter, risikobasierte Entscheidungsfindung etc.)	●	●	●
Unterstützung für PSD2-Compliance	●	●	●
Unterstützung mehrerer Datenelemente zur Förderung reibungsloser Authentifizierungen	Verfügbar in den USA und ihren Territorien	●	●
App-basierte Aktivierung	–	●	●
Nichtzahlungsauthentifizierung	–	●	●
Token-basierte Transaktionen	–	●	●
Out-of-Band-Authentifizierung	–	●	●
Vom Händler initiierte Authentifizierungen	–	–	●
Entkoppelte Authentifizierung	–	–	●
Weitere PSD2-Kenndaten	–	–	●

Hinweis: Für einige dieser Funktionen ist möglicherweise eine zusätzliche Zertifizierung erforderlich.