American Express SafeKey®
Veelgestelde vragen

DEEL 1: ALGEMENE VRAGEN

V1.1 WAT IS AMERICAN EXPRESS SAFEKEY®?

American Express SafeKey is een beveiligingsoplossing die gebruikmaakt van wereldwijde industriestandaarden om online fraude op te sporen en te verminderen, door een extra beveiligingsverificatie toe te voegen wanneer kaarthouders online of met hun smartphone aankopen doen. SafeKey 2.0 is gebaseerd op het EMV® 3-D Secure-protocol.

Gegevens van de kaarthouder die tijdens de aankoop worden verstrekt, zoals naam, e-mailadres, telefoonnummer en verzendadres, kunnen helpen bij het nauwkeuriger identificeren van legitieme en frauduleuze transacties.

SafeKey maakt gebruik van de op risico's gebaseerde verificatiemethoden van de kaartuitgever en vereenvoudigt en vergemakkelijkt het online betalen. Bovendien kunnen kaarthouders op apparaten die zij het handigst vinden, gebruikmaken van SafeKey en winkelen, inclusief in-app aankopen op smartphones.

V1.2 WAT ZIJN DE BELANGRIJKSTE VOORDELEN VAN SAFEKEY?

SafeKey helpt fraude bij e-commerce-transacties te verminderen. Dit helpt de kaarthouder te beschermen tegen situaties waarin hun kaart zonder toestemming wordt gebruikt, betrekt de kaartuitgever bij de verificatie-evaluatie en kan de aansprakelijkheid bij fraude bij het kaartaccepterend bedrijf leggen (zie FLS-sectie voor meer details).

V1.3 HOE WERKT SAFEKEY?

SafeKey helpt online fraude te verminderen door de kaartuitgever te vragen om de identiteit van de kaarthouder te bevestigen voordat een transactie wordt geaccepteerd:

1. Het authenticatieproces start zodra de kaarthouder online een aankoop doet bij een kaartaccepterend bedrijf.
2. Het kaartaccepterende bedrijf dient een SafeKey-transactie via hun 3DS Server (MPI) Provider in bij de American Express Directory Server (DS).
3. De DS stuurt het verzoek door naar de betreffende Access Control Server (ACS) van de kaartuitgever.
4. De ACS hanteert geavanceerde risicomodeltechnieken om de identiteit van de kaarthouder te bevestigen.
5. In bepaalde gevallen kan de kaarthouder worden gevraagd om een eenmalig wachtwoord terug te sturen aan de ACS.

V1.4 WAAR IS SAFEKEY BESCHIKBAAR?

SafeKey is beschikbaar op elke markt voor betalingsverwerkers en kaartuitgevers die ervoor kiezen om het te implementeren. Als een kaartaccepterend bedrijf gebruik wil maken van de service, moet hun betalingsverwerker gecertificeerd zijn voor SafeKey.

V1.5 WAT IS 3-D SECURE (3DS) 2.0 EN WAAROM HEEFT DE INDUSTRIE EEN NIEUWE VERSIE NODIG?

De originele SafeKey, gebaseerd op het 3DS 1.0.2-protocol van de industrie, is ontworpen om verificatie van kaarthouders te ondersteunen voor pc-browser-gebaseerde, e-commerce-transacties. De wereldwijde technische instantie, EMVCo, waarvan American Express een lid is, heeft de toepassing uitgebreid om de betalingsindustrie te leiden in de verdere ontwikkeling van de 3DS 2.0-specificatie en het bijbehorende test- en goedkeuringsprogramma.

3DS 2.0 ondersteunt niet-browser-gebaseerde externe betalingen, zoals in-app, mobiele en digitale portemonnees. Daarnaast zijn er nieuwe mogelijkheden op het gebied van technologie, beveiliging, prestaties, gebruikerservaring en flexibiliteit om een lange levensduur te garanderen.

V1.6 HOE GEEFT SAFEKEY DE VERANDERENDE EMV 3DS-SPECIFICATIES WEER (BIJV. V2.1.0 EN V2.2.0)?

De functies en functionaliteit van SafeKey 2.0 zijn bijgewerkt voor elke nieuwe versie van EMV 3DS. SafeKey-deelnemers moeten zich opnieuw certificeren voor de nieuwste versie om van alle functies te kunnen profiteren.

V1.7 WAT ZIJN DE FUNCTIES IN 3DS 2.0?

EMV 3DS 2.0 streeft ernaar om aan de veranderende behoeften bij externe betalingen te voldoen, met inbegrip van:

- Ondersteuning en directe integratie voor browser- en in-app-winkelbehoeften
- Verbeterde risicobeoordeling van de kaartuitgever door extra gegevens
- Ondersteuning voor diverse verificatiemethoden, zoals eenmalige wachtwoorden, biometrie en out-of-band-verificatie
- Ondersteuning voor tokengebaseerde transacties voor betere beveiliging, vanwege de uitbreiding van het tokengebruik in de sector
- Maakt verificatie van niet-betaling mogelijk, zoals het verstrekken van een kaart aan een digitale portemonnee
- Mogelijkheid voor kaartaccepterende bedrijven om verificaties te initiëren (bijv. voor terugkerende facturering, postorderbedrijven en telefoonorderbedrijven)
- Verbeteringen in de gebruikerservaring en betaalprocessen voor kaarthouders
- Aanvullende ondersteuning voor PSD2

Opmerking: Zie de bijlage voor een gedetailleerde vergelijking van elke SafeKey-versie

V1.8 WAAR VIND IK DE SAFEKEY 2.0-SPECIFICATIES?

SafeKey 2.0-specificaties en implementatiegidsen zijn beschikbaar op:

- Kaartuitgevers/betalingsverwerkers: https://network.americanexpress.com/globalnetwork/sign-in/
- ACS & 3DS Server (MPI) Providers: https://network.americanexpress.com/globalnetwork/amex-enabled/
- Kaartaccepterende bedrijven: http://www.americanexpress.com/merchantspecs
- Basisspecificaties EMV: www.emvco.com

V1.9 HOE IS AMERICAN EXPRESS BETROKKEN BIJ SAFEKEY 1.0?

American Express houdt toezicht op het gebruik van SafeKey 1.0 in de industrie en zal de service blijven ondersteunen naarmate het gebruik van SafeKey 2.0 toeneemt. American Express zal aankondigen wanneer de SafeKey 1.0 volledig vervangen zal worden door SafeKey 2.0 en een passende tijdslijn geven.

V1.10 KUNNEN SAFEKEY 1.0 EN SAFEKEY 2.0 NAAST ELKAAR WORDEN GEBRUIKT?

Ja, SafeKey 1.0 en 2.0 werken onafhankelijk van elkaar, zodat ze naast elkaar kunnen worden gebruikt. In de loop van tijd wordt verwacht dat SafeKey 2.0 versie 1.0 zal vervangen en tijdens deze overgangsperiode wordt aanbevolen dat kaartaccepterende bedrijven kiezen voor 3DS Server (MPI) Providers die beide producten ondersteunen. Wanneer een kaartaccepterend bedrijf vraagt om een transactie-authenticatie, dan is het de verantwoordelijkheid van de 3DS Server (MPI) Provider om gebruik te maken van de juiste SafeKey-versie.

V1.11 HOE WEET DE 3DS SERVER (MPI) WELKE VERSIE MOET WORDEN GEBRUIKT?

De SafeKey-service houdt gegevens bij van de kaartreeksen (BIN) die worden ondersteund door SafeKey 2.0 en deze gegevens zijn beschikbaar voor elke 3DS Server (MPI). Wanneer een kaartaccepterend bedrijf vraagt om een kaarthouderverificatie, controleert de 3DS Server (MPI) of de specifieke kaart is aangemerkt als geschikt voor SafeKey 2.0. Als dit het geval is, moet de SafeKey 2.0-service worden gebruikt, indien niet dan moet SafeKey 1.0 worden gebruikt.

V1.12 KAN SAFEKEY 2.0 WORDEN GEÏMPLEMENTEERD ZONDER SAFEKEY 1.0?

Ja. Na verloop van tijd zal dit de standaard aanpak voor nieuwe gebruikers worden. Deelnemers moeten zich ervan bewust zijn dat het nog even duurt voordat SafeKey 2.0 volledig is geïmplementeerd.

V1.13 MOETEN KAARTHOUDERS ZICH AANMELDEN VOOR SAFEKEY 2.0 ALS ZE AL AANGEMELD ZIJN VOOR SAFEKEY 1.0?

Kaarthouders hoeven zich niet aan te melden voor SafeKey 2.0, aangezien alle in aanmerking komende kaarthouders vooraf door kaartuitgevers worden aangemeld zoals vereist in de EMVCo-specificatie.

V1.14 KAN SAFEKEY VOOR ONLINE TRANSACTIES OP ALLE KAARTPRODUCTEN WORDEN GEBRUIKT?

SafeKey biedt het voordeel van verificatie dat de persoon die de transactie uitvoert, ook de kaarthouder is. Het kan dus niet worden gebruikt met anonieme producten, zoals prepaid kaarten, waarbij de identiteit van de gebruiker niet is geregistreerd.

DEEL 2: VRAGEN FRAUD LIABILITY SHIFT (FLS)

V2.1 WAT IS SAFEKEY FRAUD LIABILITY SHIFT (FLS)?

Als er sprake is van fraude bij een kwalificerende transactie, wordt de aansprakelijkheid door SafeKey FLS overgedragen van het kaartaccepterende bedrijf naar de kaartuitgever.

V2.2 HOE VERKRIJGT EEN KAARTACCEPTEREND BEDRIJF FLS?

Een kaartaccepterend bedrijf verkrijgt FLS voor transacties die zijn geverifieerd door SafeKey, mits deze voldoen aan de criteria van het FLS-beleid. De kaartaccepterende bedrijven dienen een laag fraudepercentage te hebben en te voldoen aan de vereisten van de SafeKey-specificaties, bijvoorbeeld het verstrekken van accurate gegevens in SafeKey-berichten. Kaartaccepterende bedrijven kunnen voor meer informatie over het FLS-beleid terecht bij hun betalingsverwerker.

V2.3 WAT IS EEN GEVERIFIEERDE SAFEKEY-TRANSACTIE?

Een geverifieerde transactie is een transactie waarbij de kaartuitgever de identiteit van de kaarthouder heeft bevestigd, zoals aangegeven door een verificatiewaarde in het antwoordbericht. Raadpleeg de SafeKey-specificaties voor meer informatie.

V2.4 WAT IS EEN GEPOOGDE SAFEKEY-TRANSACTIE?

Een gepoogde transactie is een transactie waarbij het kaartaccepterende bedrijf heeft geprobeerd om een SafeKey-verificatie uit te voeren, maar de kaartuitgever geen SafeKey ondersteunt of de ACS van de kaartuitgever niet beschikbaar is. SafeKey kan een gepoogde verificatie toestaan, zoals aangegeven door een verificatiewaarde in het antwoordbericht; raadpleeg de SafeKey-specificaties voor meer informatie.

DEEL 3: VRAGEN KAARTACCEPTERENDE BEDRIJVEN

V3.1 HOE KAN IK BEOORDELEN WAT IK MOET DOEN OM SAFEKEY TE GAAN GEBRUIKEN?

Kaartaccepterende bedrijven die SafeKey willen gebruiken, dienen contact op te nemen met hun 3DS Server (MPI) Provider of betalingsverwerker.

V3.2 HOE MELD IK MIJ ALS KAARTACCEPTEREND BEDRIJF AAN VOOR SAFEKEY?

Kaartaccepterende bedrijven dienen contact op te nemen met hun 3DS Server (MPI) Provider of betalingsverwerker om zich aan te melden bij SafeKey. Er is ook een online aanmeldingsportal beschikbaar voor bepaalde betalingsverwerkers op www.amexsafekey.com.

V3.3 HOE WEET IK ALS KAARTACCEPTEREND BEDRIJF WELKE VERSIE VAN SAFEKEY IK MOET GEBRUIKEN?

Het wordt aanbevolen om een 3DS Server (MPI) Provider te selecteren die alle versies van SafeKey ondersteunt. Zij zullen de juiste versie selecteren omdat zij weten welke versies van SafeKey de kaartuitgever ondersteunt en zullen de bijbehorende verbeterde functies gebruiken.

V3.4 HOE WEET IK ALS KAARTACCEPTEREND BEDRIJF OF MIJN 3DS SERVER (MPI) PROVIDER SAFEKEY 2.0 ONDERSTEUNT?

3DS Server (MPI) Providers werken samen met EMVCo en American Express om te certificeren voor SafeKey 2.0. Kaartaccepterende bedrijven dienen contact op te nemen met hun provider om hun plannen te bespreken. Een lijst van 3DS Server (MPI) Providers die zijn gecertificeerd met American Express en geregistreerd met AMEX Enabled is beschikbaar op de AMEX Enabled-website (www.amexenbled.com).

V3.5 MOETEN KAARTACCEPTERENDE BEDRIJVEN ZICH AANMELDEN VOOR SAFEKEY 2.0 ALS ZIJ AL ZIJN AANGEMELD VOOR SAFEKEY 1.0?

Kaartaccepterende bedrijven dienen met hun 3DS Server (MPI) Providers samen te werken om de procedures voor het profiteren van SafeKey 2.0 te begrijpen.

V3.6 IK BEN EEN KAARTACCEPTEREND BEDRIJF DAT MOMENTEEL GEEN SAFEKEY GEBRUIKT. HOE KAN IK MIJ AANMELDEN VOOR SAFEKEY 2.0?

Kaartaccepterende bedrijven moeten in eerste instantie contact opnemen met hun 3DS Server (MPI) Provider over aanmelding voor SafeKey. Voor een lijst met gecertificeerde 3DS Server (MPI) Providers die zijn geregistreerd met American Express, raadpleegt u de AMEX Enabled-website (www.amexenbled.com).

V3.7 HOE WEET EEN KAARTACCEPTEREND BEDRIJF OF 3DS SERVER (MPI) WELKE VERSIES VAN SAFEKEY EEN KAARTUITGEVER ONDERSTEUNT?

De 3DS Server (MPI) ontvangt informatie over welke kaartuitgevers SafeKey 2.0 ondersteunen en welke versies van 2.0 ze ondersteunen. De 3DS Server (MPI) gebruikt deze gegevens om te bepalen welk type verificatie moet worden uitgevoerd.

V3.8 HOE KAN IK ALS KAARTACCEPTEREND BEDRIJF MIJN APP GESCHIKT MAKEN VOOR SAFEKEY?

Kaartaccepterende bedrijven dienen een 3DS Software Development Kit (SDK) in hun app te integreren om het geschikt te maken voor SafeKey 2.0. Kaartaccepterende bedrijven kunnen hiervoor contact opnemen met hun 3DS Server (MPI) Provider of een 3DS SDK Provider. 3DS SDK's moeten worden getest en goedgekeurd door EMVCo; raadpleeg www.emvco.com voor een lijst met goedgekeurde SDK Providers.

V3.9 WAT IS EEN 3DS SOFTWARE DEVELOPER KIT (SDK)?

De 3DS SDK is een component die is opgenomen in de Merchant App. De 3DS SDK beheert de SafeKey-verwerking namens de app en communiceert met de 3DS Server.

V3.10 BRENGT AMERICAN EXPRESS TRANSACTIEKOSTEN IN REKENING VOOR GEBRUIK VAN SAFEKEY?

Nee. Neem contact op met uw 3DS Server (MPI) Provider voor de kosten van hun services.

V3.11 WAT GEBEURT ER ALS DE KAARTUITGEVER GEEN SAFEKEY ONDERSTEUNT?

Hoewel SafeKey momenteel een optionele service voor Kaartuitgevers is, zijn Kaartuitgevers die niet deelnemen wel aansprakelijk voor transactiefraude waar door het kaartaccepterende bedrijf een poging tot SafeKey-verificatie is gedaan. Raadpleeg uw betalingsverwerker voor meer informatie over het SafeKey FLS-beleid.

V3.12 WAT GEBEURT ER ALS DE BETALINGSVERWERKER VAN EEN KAARTACCEPTEREND BEDRIJF SAFEKEY NIET ONDERSTEUNT?

Het is een vereiste dat de betalingsverwerker van een kaartaccepterend bedrijf gecertificeerd is voor SafeKey. Dit is om ervoor te zorgen dat de noodzakelijke autorisatie- en indieningsberichten kunnen worden verwerkt en de fraude-aansprakelijkheid correct kan worden toegewezen. Opmerking: de verwerker van een kaartaccepterend bedrijf moet ook SafeKey ondersteunen en de benodigde gegevens doorgeven aan de betalingsverwerker.

V3.13 ZIJN ER FUNCTIES IN SAFEKEY DIE KAARTACCEPTERENDE BEDRIJVEN HELPEN UITGEBREIDE KLANTVERIFICATIE TE ONDERSTEUNEN?

Ja, alle versies van SafeKey ondersteunen uitgebreide klantverificatie, zoals PSD2-vereisten.

V3.14 WAAR KUNNEN KAARTACCEPTERENDE BEDRIJVEN AUTORISATIE- EN INDIENINGSSPECIFICATIES VOOR SAFEKEY VERKRIJGEN?

Raadpleeg uw betalingsverwerker voor de meest recente technische specificaties. Rechtstreeks bij American Express verwerkte kaartaccepterende bedrijven gaan naar www.americanexpress.com/merchantspecs.

DEEL 4: VRAGEN ACS & 3DS SERVER (MPI) PROVIDER

V4.1 HOE MOETEN ACS EN 3DS SERVER (MPI) PROVIDERS ZICH CERTIFICEREN VOOR SAFEKEY?

De eerste stap in de certificering voor SafeKey is registratie bij AMEX Enabled. Providers dienen het bedrijfsregistratieformulier op www.amexenbled.com in te vullen om toegang tot de SafeKey-documentatie te krijgen.

V4.2 WAAR VINDT MEN EEN LIJST MET GECERTIFICEERDE ACS EN 3DS SERVER (MPI) PROVIDERS?

Voor een lijst met gecertificeerde ACS en 3DS Server (MPI) Providers die zijn geregistreerd met American Express, raadpleegt u de AMEX Enabled-website (www.amexenbled.com).

V4.3 IS CERTIFICERING VOOR SAFEKEY 2.0 NOODZAKELIJK ALS SAFEKEY 1.0-CERTIFICERING IS VOLTOOID?

Ja. Voor ACS en 3DS Server (MPI) Providers zijn afzonderlijke certificeringen vereist voor de verschillende versies van SafeKey. Zie www.amexsafekey.com voor meer informatie. EMVCo levert een verplichte EMV 3DS-goedkeuringsservice voor ACS en 3DS Server (MPI) Providers, die vóór de American Express SafeKey 2.0-certificering moet worden voltooid.

V4.4 HOE REGISTREER IK MIJ VOOR CERTIFICERING EN TESTEN?

Registreer u op www.amexenabled.com om het certificeringsproces voor SafeKey te starten. Uw American Express-certificeringsanalist zal u uitleggen hoe u toegang krijgt tot het SafeKey Test Lab.

DEEL 5: VRAGEN KAARTUITGEVERS EN BETALINGSVERWERKERS

V5.1 HOE MOETEN KAARTUITGEVERS EN BETALINGSVERWERKERS ZICH CERTIFICEREN VOOR SAFEKEY?

Kaartuitgevers en betalingsverwerkers dienen contact op te nemen met hun American Express-vertegenwoordiger over certificering voor SafeKey of naar www.amexsafekey.com te gaan voor meer informatie.

V5.2 ALS EEN KAARTUITGEVER OF BETALINGSVERWERKER IS GECERTIFICEERD VOOR SAFEKEY 1.0, IS CERTIFICERING VOOR SAFEKEY 2.0 DAN VEREIST?

De netwerkberichten voor SafeKey 1.0 en 2.0 komen overeen, zodat hercertificering niet is vereist. De authenticatieverwerking voor de ACS is echter wel onderworpen aan certificering.

BIJLAGE: VERGELIJKINGSTABEL VAN FUNCTIONALITEITEN

Vergelijkingstabel American Express SafeKey®

Kenmerk	SafeKey 1.0	SafeKey 2.0	
		SafeKey 2.1 (EMV 2.1.0)	SafeKey 2.2 (EMV 2.2.0)
Gebaseerd op industriestandaard 3-D Secure	●	●	●
Extra beveiligingslaag bij het afrekenen	●	●	●
Verificatie van betaling	●	●	●
Browsergebaseerde verificatie	●	●	●
Flexibiliteit voor kaartuitgevers met betrekking tot verificatiemethoden (bijv. eenmalige wachtwoorden en risicogebaseerde besluiten, etc.)	●	●	●
Ondersteuning voor PSD2-conformiteit	●	●	●
Ondersteuning voor meer gegevenselementen voor probleemloze verificaties	Beschikbaar in de VS en haar deelstaten	●	●
App-functionaliteit (in-app) mogelijk	—	●	●
Verificatie van niet-betaling	—	●	●
Tokengebaseerde transacties	—	●	●
Out-of-band-verificatie	—	●	●
Door kaartaccepterende bedrijven geïnitieerde verificaties	—	—	●
Ontkoppelde verificatie	—	—	●
Aanvullende indicatoren PSD2	—	—	●

Opmerking: Voor sommige van deze functies is mogelijk aanvullende certificering vereist.

AMERICAN EXPRESS SafeKey®