DON'T *do business* WITHOUT IT™

American Express SafeKey®

FREQUENTLY ASKED QUESTIONS

1. General FAQs

Q1.1 WHAT IS AMERICAN EXPRESS SAFEKEY®?

American Express SafeKey is a security solution that leverages global industry standards to detect and reduce online fraud, adding an extra layer of security when Card Members shop online or on their mobile devices. SafeKey is based on the EMV®* 3-D Secure (3DS) protocol.

Card Member data provided during the purchase experience, such as name, email address, phone number, and shipping address, can help identify legitimate and fraudulent transactions more accurately.

Through an Issuer's use of risk-based authentication methods, SafeKey can reduce friction and offer a more streamlined checkout experience. Card Members can leverage SafeKey and shop on devices most convenient to them, including smart devices to make in-app purchases.

Q1.2 WHAT ARE THE MAIN BENEFITS OF SAFEKEY?

SafeKey can help reduce fraud on Card-not-present transactions. This helps protect the Card Member against their Card being used without permission, enables the Issuer to be involved in the authentication assessment, and can provide fraud liability shift to the Merchant (see FLS section for further details).

Q1.3 HOW DOES SAFEKEY WORK?

SafeKey helps reduce online fraud by asking the Issuer to confirm the Card Member's identity before a transaction is authorized.

1. The authentication flow starts with the Card Member spending online with a Merchant.
2. The Merchant submits a SafeKey transaction via their 3DS Server Provider to the American Express Directory Server (DS).
3. The DS forwards the request to the relevant Issuer's Access Control Server (ACS).
4. The ACS applies sophisticated risk-modeling techniques to confirm the Card Member's identity.
5. In certain circumstances, the Card Member may be asked to confirm their identity by interacting with their Issuer.

Q1.4 WHERE IS SAFEKEY AVAILABLE?

SafeKey is available in any Amex operating market to Acquirers and Issuers who choose to implement it. For a Merchant to benefit from FLS, its Acquirer must be certified for SafeKey.

*EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo.

1. General FAQs

Q1.5 HOW DOES SAFEKEY REFLECT THE EVOLVING EMV 3DS SPECIFICATIONS (e.g., 2.2.0 and 2.3.1)?

SafeKey features and functionalities are updated to reflect each new version of EMV 3DS. SafeKey ACS and 3DS Server Providers need to recertify to the latest version to benefit from all features.

Q1.6 WHAT ARE THE FEATURES OF EMV 3DS?

EMV 3DS aims to meet the evolving requirements of the remote payments environment, including:

- Support and direct integration for browser and in-app shopping needs.
- Improved Issuer risk assessment through enhanced data.
- Support for a variety of authentication methods, including one-time passcodes, biometrics, and out-of-band authentication.
- Token-based transaction support for enhanced security and to account for the expansion of token usage across the industry.
- Enablement of non-payment authentication, such as provisioning a Card to a digital wallet.
- Ability for Merchants to initiate authentications (e.g., for Recurring Billing, Mail Orders, and Telephone Orders).
- Improvements to Card Member user experience and checkout flows.
- Additional support for PSD2.

Q1.7 WHERE CAN I FIND THE SAFEKEY SPECIFICATIONS?

SafeKey specifications and Implementation Guides are available at:

- Issuers/Acquirers: https://network.americanexpress.com/globalnetwork/sign-in/
- ACS and 3DS Server Providers: https://network.americanexpress.com/globalnetwork/amex-enabled/
- Merchants: http://www.americanexpress.com/merchantspecs
- Baseline EMV specs: www.emvco.com

Q1.8 HOW DOES THE 3DS SERVER KNOW WHICH SAFEKEY VERSION TO USE?

The SafeKey service maintains records of the Card (BIN) ranges that are supported by SafeKey and which optional features Issuers and their ACS providers support. These records are made available to every 3DS Server. When a Merchant requests a Card Member authentication, the 3DS Server checks if the specific Card is indicated as SafeKey enabled and sends the appropriate message version.

Note: See Appendix for a detailed feature comparison of each SafeKey version.

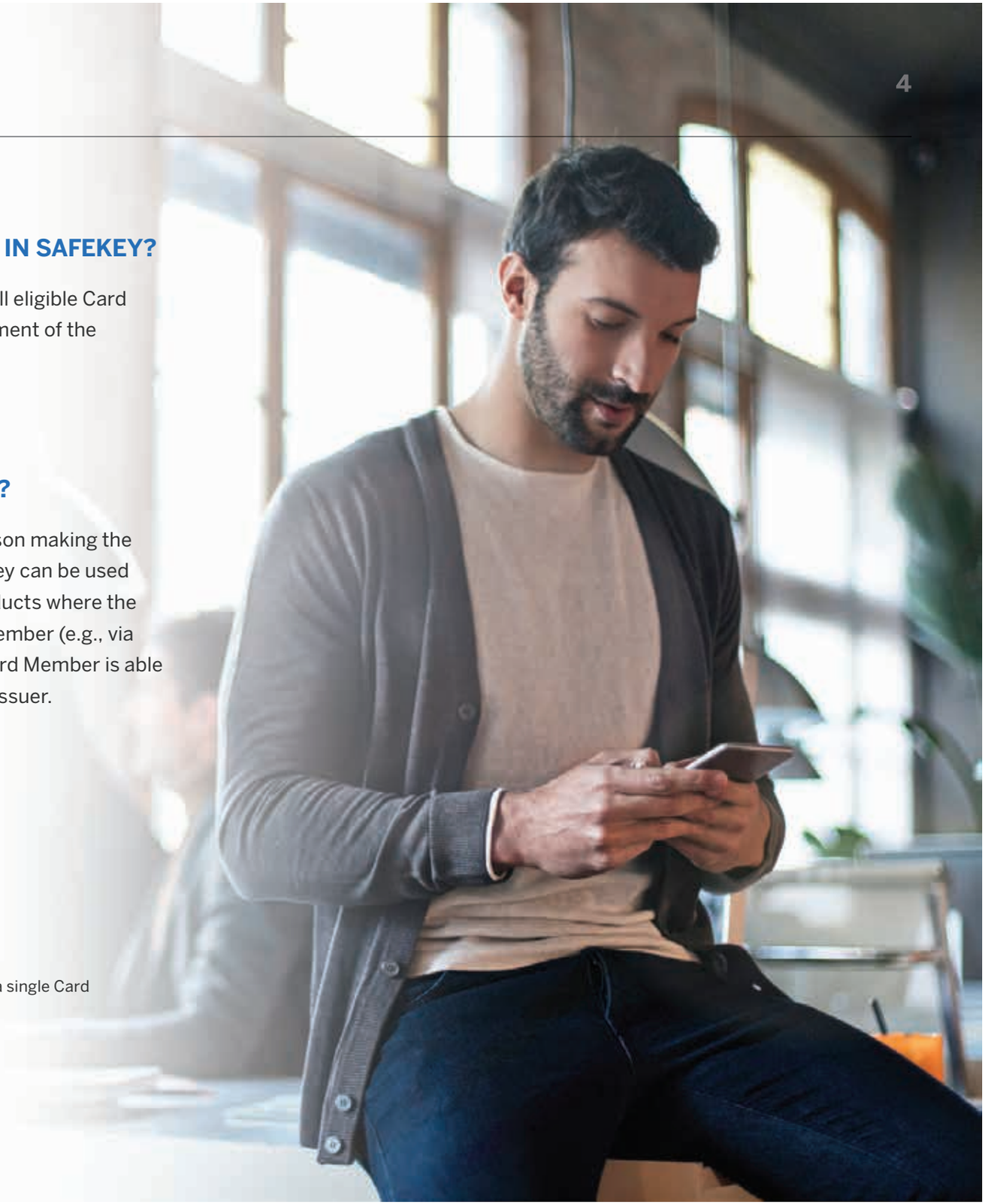
1. General FAQs

Q1.9 DO CARD MEMBERS HAVE TO ENROLL IN SAFEKEY?

Card Members do not have to enroll in SafeKey, since all eligible Card Members* will be pre-enrolled** by Issuers as a requirement of the EMVCo specification.

Q1.10 CAN SAFEKEY BE USED FOR ONLINE TRANSACTIONS ON ALL CARD PRODUCTS?

SafeKey provides the benefit of authenticating the person making the transaction as the Card Member. Consequently, SafeKey can be used only for Card-not-present transactions using Card products where the Issuer is able to communicate directly with the Card Member (e.g., via email, text message, push notification, etc.) and the Card Member is able to receive and respond to a request for input from the Issuer.



*Applicable to Card products for which the Issuer is able to identify a single Card Member and authenticate the Cardholder. See Question 1.10.

**Subject to local market regulations.

2. Fraud Liability Shift (FLS) FAQs

Q2.1 WHAT IS SAFEKEY FRAUD LIABILITY SHIFT (FLS)?

If there is fraud on a qualifying transaction, SafeKey FLS transfers fraud liability from the Merchant to the Issuer.

Q2.2 HOW DOES A MERCHANT OBTAIN FLS?

A Merchant obtains FLS for transactions that have been authenticated by SafeKey, provided they have met FLS policy criteria. Merchants are expected to maintain low fraud rates and meet the requirements of the SafeKey specifications, for example, by provisioning accurate data in SafeKey messages. Merchants should refer to their Acquirer for details of the FLS policy.

Q2.3 WHAT IS AN AUTHENTICATED SAFEKEY TRANSACTION?

An authenticated transaction is one where the Issuer has confirmed the identity of the Card Member as indicated by an Authentication Value in the message provided to the Merchant. Please refer to the SafeKey specifications for details.

Q2.4 WHAT IS AN ATTEMPTED SAFEKEY TRANSACTION?

An attempted transaction is one where the Merchant has tried to perform a SafeKey authentication, but the Issuer does not support the version of SafeKey required by policy, or the Issuer's ACS is not available. SafeKey may grant an attempted authentication as indicated by an Authentication Value in the message provided to the Merchant. Please refer to the SafeKey specifications for details.

3. Merchant FAQs

Q3.1 I AM A MERCHANT NOT CURRENTLY USING SAFEKEY. HOW DO I START USING IT?

Merchants should initially talk to their 3DS Server Provider to enable SafeKey. For a list of 3DS Server Providers who have certified with American Express, please visit the AMEX Enabled website. Merchants also need to talk to their Acquirer or Payment Service Provider (PSP) to ensure SafeKey data can be passed in the Authorization and Submissions messages.

Q3.2 DO I NEED TO ENGAGE DIRECTLY WITH AMERICAN EXPRESS TO USE SAFEKEY?

Merchants do not need to register or enroll directly with American Express to use SafeKey. Your 3DS Server Provider will ensure you are set up for SafeKey authentication messages. Merchants also need to talk to their Acquirer or PSP to ensure SafeKey data can be passed in the Authorization and Submissions messages.

Q3.3 AS A MERCHANT, HOW DO I KNOW WHICH VERSION OF SAFEKEY TO ASK MY 3DS SERVER PROVIDER TO USE?

It is recommended that Merchants ask their 3DS Server Provider to implement the latest version of SafeKey.

Q3.4 HOW DO I KNOW WHICH VERSIONS OF SAFEKEY A 3DS SERVER PROVIDER SUPPORTS?

Merchants should talk to their 3DS Server Provider to understand which versions they support. A list of 3DS Server Providers who are certified for SafeKey, including the version they are certified for, is available on the AMEX Enabled website.

Q3.5 HOW DOES A MERCHANT OR 3DS SERVER KNOW WHICH VERSIONS OF SAFEKEY AN ISSUER SUPPORTS?

All 3DS Servers request Issuer BIN information from American Express each day. This data shows the Issuers that support SafeKey and which versions and features they support. The 3DS Server then uses this information to determine the appropriate type of authentication to be performed.

Q3.6 AS A MERCHANT, HOW CAN I ENABLE MY APP FOR SAFEKEY?

Merchants must integrate a 3DS Software Development Kit (SDK) into the Merchant App in order to enable it for SafeKey. Merchants should engage with their 3DS Server Provider or a 3DS SDK Provider. 3DS SDKs must be tested and approved through EMVCo. Please visit www.emvco.com for a list of approved 3DS SDK Providers.

3. Merchant FAQs

Q3.7 WHAT IS A 3DS SOFTWARE DEVELOPMENT KIT (SDK)?

The 3DS SDK is a component that is incorporated into the Merchant App. The 3DS SDK manages the SafeKey processing on behalf of the app and interfaces with the 3DS Server.

Q3.8 DOES AMERICAN EXPRESS APPLY TRANSACTION FEES FOR USE OF SAFEKEY?

No. Please talk to your 3DS Server Provider to understand any costs related to their services.

Q3.9 WHAT HAPPENS IF THE ISSUER DOES NOT SUPPORT SAFEKEY?

Issuers who do not participate may be liable for transaction fraud where SafeKey authentication was attempted by the Merchant. Please refer to your Acquirer for further details of the SafeKey FLS policy.

Q3.10 CAN I USE SAFEKEY IF MY ACQUIRER IS NOT CERTIFIED?

Yes. You can benefit from SafeKey authentication checks. However, you cannot benefit from FLS unless your Acquirer is certified to ensure that SafeKey data can be passed in the Authorization and Submissions messages.

Q3.11 ARE THERE FEATURES IN SAFEKEY THAT HELP MERCHANTS SUPPORT STRONG CUSTOMER AUTHENTICATION?

Yes, all versions of SafeKey support Strong Customer Authentication, which may be required for transactions in scope of PSD2 or other similar regulatory mandates.

Q3.12 WHERE CAN I FIND AUTHORIZATION AND SUBMISSION SPECIFICATIONS FOR SAFEKEY?

Please refer to your Acquirer for the most recent technical specifications. American Express directly acquired Merchants can visit www.americanexpress.com/merchantspecs.

4. ACS and 3DS Server Provider FAQs

Q4.1 WHERE CAN I FIND A LIST OF CERTIFIED ACS AND 3DS SERVER PROVIDERS?

For a list of certified ACS and 3DS Server Providers who have registered with American Express, please visit the AMEX Enabled website.

Q4.2 CAN I CHOOSE HOW MY CERTIFIED PRODUCT IS LISTED ON THE AMEX ENABLED WEBSITE?

Yes. Providers can choose to list all of their products separately or combine them into a single listing. Either way, the list will indicate which version(s) of SafeKey the product is certified for. Please discuss this with your Certification Analyst if you are unsure.

Q4.3 ARE THERE ANY PREREQUISITES TO STARTING SAFEKEY CERTIFICATION?

Yes. In order to start SafeKey certification, a provider must have obtained an EMV 3DS Letter of Approval (LOA).

Q4.4 HOW SHOULD ACS AND 3DS SERVER PROVIDERS CERTIFY FOR SAFEKEY?

The first step in getting certified for SafeKey is to register with AMEX Enabled; providers should start by completing a company registration form on www.amexenabled.com to gain access to the SafeKey documentation.

Q4.5 HOW DO I REGISTER FOR CERTIFICATION AND TESTING FOR THE FIRST TIME?

After registering with AMEX Enabled, providers need to submit a SafeKey enrollment form to begin their certification. An American Express Certification Analyst will then explain the forthcoming steps, including how to access the SafeKey Test Lab.

Q4.6 HOW DO I UPLIFT TO THE LATEST VERSION OF SAFEKEY?

Providers who are already certified for SafeKey should log in to the AMEX Enabled Dashboard and request an enrollment link.

Q4.7 DO I NEED TO COMPLETE CERTIFICATION FOR EXISTING SAFEKEY VERSIONS BEFORE CERTIFYING FOR THE LATEST VERSION?

No. All previous SafeKey version test cases are included in the latest certification. Every SafeKey participant is expected to certify for the latest version.

4. ACS and 3DS Server Provider FAQs

Q4.8 HOW DO I ADD ANOTHER EMVCo LOA TO MY SAFEKEY ENROLLMENT?

Providers must inform Amex when they receive a new LOA from EMVCo. Amex can support multiple LOAs until certification to the latest version is complete. To add a new or renewed LOA, please contact safekey.certification@aexp.com.

Q4.9 DOES THE SAFEKEY PROGRAM HAVE ONGOING REQUIREMENTS?

Yes, please see the SafeKey Program Guide in AMEX Enabled for more details. Ongoing requirements for providers include: maintaining a valid contract, providing proof of current PCI compliance, renewing certificates before they expire, ensuring contact details are correct, and returning to Amex to test for any new features supported.

5. Issuer and Acquirer FAQs

Q5.1 HOW SHOULD ISSUERS AND ACQUIRERS OBTAIN CERTIFICATION FOR SAFEKEY?

Issuers and Acquirers need to certify with American Express to ensure SafeKey data can be passed in the Authorization and Submissions messages. They should talk to their American Express representative about obtaining certification for SafeKey, or visit www.amexsafekey.com for more information.

Q5.2 DOES IT MATTER WHICH VERSION OF SAFEKEY AN ISSUER OR ACQUIRER CERTIFIES FOR?

Issuers and Acquirers must complete certification to ensure SafeKey data can be passed in the Authorization and Submissions messages. This certification for SafeKey is not version specific.

Issuers must also complete integration testing with their ACS Provider once their ACS Provider has completed certification for a different SafeKey version.

Acquirers do not need to complete additional certification to support discrete SafeKey versions. However, if an Acquirer is also acting as a 3DS Server Provider, additional certification requirements apply.

Q5.3 HOW DO I ACCESS THE SAFEKEY IMPLEMENTATION GUIDES AND SPECS?

- Issuers/Acquirers: Sign in to access the Knowledge Base at https://network.americanexpress.com/globalnetwork/sign-in/
- ACS and 3DS Server Providers: Visit https://network.americanexpress.com/globalnetwork/amex-enabled/
- Prop Merchants: Visit http://www.americanexpress.com/merchantspecs
- Network Merchants: Contact your Acquirer

APPENDIX: Feature Comparison Chart

FEATURE	SAFEKEY 2.2	SAFEKEY 2.3
App-based (in-app) enablement	✓	✓
Non-payment authentication	✓	✓
Token-based transactions	✓	✓
Out-of-band authentication	✓	✓
3DS Requestor-Initiated (3RI) non-payment authentications	✓	✓
3DS Requestor-Initiated (3RI) payment authentications	✓	✓
Decoupled authentication	✓	✓
PSD2 data elements and indicators	✓	✓
Additional support for gaming consoles and headless devices		✓
Support for Secure Payment Confirmation		✓
Automated out-of-band transitions and UI enhancements		✓
Enhanced data for additional payment scenarios		✓

SafeKey specifications can be accessed through AMEX Enabled and Knowledge Base.