DON'T do business WITHOUT IT™

AMERICAN EXPRESS SAFEKEY®

FREQUENTLY ASKED QUESTIONS

Contents

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 2.0 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 in-app purchases on smart devices.

Q1.2 WHAT ARE THE MAIN BENEFITS OF SAFEKEY?

SafeKey can help reduce fraud on e-commerce 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 (Merchant Plug-In) 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.

Q1.5 HOW DOES SAFEKEY REFLECT THE EVOLVING EMV 3DS SPECIFICATIONS (E.G. V2.1.0 AND V2.2.0)?

SafeKey 2.0 features and functionalities are updated to reflect each new version of EMV 3DS. SafeKey participants need to re-certify to the latest version to benefit from all features.

Q1.6 WHAT ARE THE FEATURES OF 3DS 2.0?

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 Order, and Telephone Order)
- Improvements to Card Member user experience and checkout flows
- Additional support for PSD2

NOTE: SEE APPENDIX FOR A DETAILED FEATURE COMPARISON OF EACH SAFEKEY VERSION.

Q1.7 WHERE CAN I FIND THE SAFEKEY 2.0 SPECIFICATIONS?

SafeKey 2.0 specifications and Implementation Guides are available at:

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

Q1.8 IS SAFEKEY 1.0 STILL AVAILABLE?

SafeKey 1.0 is available to Merchants in India until October 2023. All other Merchants should be using SafeKey 2.1 or higher.

1. General FAQs

Q1.10 HOW DOES THE 3DS SERVER (MPI) KNOW WHICH SAFEKEY VERSION TO USE?

The SafeKey service maintains records of card (BIN) ranges, which are supported by SafeKey 2.0. These records are made available to every 3DS Server (MPI). When a Merchant requests a Card Member authentication, the 3DS Server (MPI) checks if the specific card is indicated as SafeKey 2.0 enabled.

Q1.11 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.

Q1.12 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 ecommerce transactions using card products where the Issuer is able to communicate directly with the Card Member (i.e., 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

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 (MPI) Provider to enable SafeKey. For a list of 3DS Server (MPI) Providers who have certified with American Express, please visit the AMEX Enabled website. Merchants also need to talk to their Acquirer or 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?

Your 3DS Server (MPI) 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 USE?

It is recommended that Merchants implement the latest version of SafeKey.

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

Merchants should talk to their 3DS Server (MPI) Provider to understand which versions they support. A list of 3DS Server (MPI) Providers who are certified with American Express is available on the AMEX Enabled website.

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

The 3DS Server (MPI) is provided with information as to which Issuers support SafeKey 2.0 and which versions of 2.0 they support. The 3DS Server (MPI) uses this data 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 2.0. Merchants should engage with their 3DS Server (MPI) 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.

Q3.7 WHAT IS A 3DS SOFTWARE DEVELOPER 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 (MPI) 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. Merchants also need to talk to their Acquirer or PSP to ensure 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 (MPI) Provider FAQs

Q4.1 HOW SHOULD ACS AND 3DS SERVER (MPI) PROVIDERS CERTIFY FOR SAFEKEY?

The first step in certifying for SafeKey is to register with AMEX Enabled. Providers should complete the company registration form on www.amexenabled.com to gain access to the SafeKey documentation.

Q4.2 WHERE CAN I FIND A LIST OF CERTIFIED ACS AND 3DS SERVER (MPI) PROVIDERS?

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

Q4.3 HOW DO I REGISTER FOR CERTIFICATION AND TESTING?

Please register with www.amexenabled.com to start the SafeKey certification process. Your American Express Certification Analyst will explain how to access the SafeKey Test Lab.

5. Issuer and Acquirer FAQs

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

Issuers and Acquirers 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?

The Network messages for different versions of SafeKey are consistent, so certification is only required once. However, Issuers wishing to support the latest version of SafeKey will need their ACS provider to be fully certified and will need to complete integration testing with their ACS.

Q5.3 AS AN ACQUIRER NOT CURRENTLY CERTIFIED FOR SAFEKEY, WHICH VERSION SHOULD I IMPLEMENT?

Acquirers certify for SafeKey and are version agnostic. However, Acquirers should make sure that any 3DS Server (MPI) Providers they work with are certified for the latest SafeKey version.

Q5.4 AS AN ISSUER NOT CURRENTLY CERTIFIED FOR SAFEKEY, WHICH VERSION SHOULD I IMPLEMENT?

American Express recommends certifying to the latest version of SafeKey.

Q5.5 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 (MPI) 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 2.1	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			✓

*Note: SafeKey 2.3 specifications can be accessed through AMEX Enabled and Knowledge Base. Certification for this latest version will be available in 2023.