



AMER EXP



American Express SafeKey[®] Frequently Asked Questions

SECTION 1: GENERAL FAQs	1
SECTION 2: FRAUD LIABILITY SHIFT (FLS) FAQs	4
SECTION 3: MERCHANT FAQs	4
SECTION 4: ACS & 3DS SERVER (MPI) PROVIDER FAQs	6
SECTION 5: ISSUER & ACQUIRER FAQs	6
APPENDIX: FEATURE COMPARISON CHART	7

SECTION 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 upon EMV[®] 3-D Secure 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).

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

Q1.3 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 return a One Time Password to the ACS.

Q1.4 WHERE IS SAFEKEY AVAILABLE?

SafeKey is available in any market to Acquirers and Issuers who choose to implement it. For a Merchant to use the service, its Acquirer must be certified for SafeKey.

Q1.5 WHAT IS 3-D SECURE (3DS) 2.0 AND WHY DOES THE INDUSTRY NEED A NEW VERSION?

The original SafeKey, based upon the industry's 3DS 1.0.2 protocol, was designed to support Card Member authentication for PC browser-based, e-commerce transactions. The global technical body, EMVCo, of which American Express is a member, has expanded its scope to lead the payments industry in further developing the 3DS 2.0 specification and its associated testing and approvals program.

3DS 2.0 supports non-browser-based remote payments including in-app, mobile and digital wallets. In addition, the approach has been to deliver new capabilities in terms of technology, security, performance, user experience, and flexibility to ensure longevity.

Q:1.6 HOW DOES SAFEKEY REFLECT THE EVOLVING EMV 3DS SPECIFICATIONS (E.G. V2.1.0 AND V2.2.0)?

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

Q1.7 WHAT ARE THE FEATURES IN 3DS 2.0?

EMV 3DS 2.0 aims to meet the evolving requirements of the remote payments environment, including the ability to:

- 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
- Enable for 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 detailed feature comparison for each SafeKey version

Q1.8 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 & 3DS Server (MPI) Providers: <https://network.americanexpress.com/globalnetwork/amex-enabled/>
- Merchants: <http://www.americanexpress.com/merchantspecs>
- Baseline EMV specs: www.emvco.com

Q1.9 WHAT IS AMERICAN EXPRESS' COMMITMENT TO SAFEKEY 1.0?

American Express has announced the withdrawal of SafeKey 1.0 by October 2022, and advises all users to migrate to the latest version of SafeKey 2.0.

Q1.10 IS IT STILL POSSIBLE TO CERTIFY FOR SAFEKEY 1.0, GIVEN THAT IT WILL NO LONGER BE SUPPORTED BEGINNING OCTOBER 2022?

Yes, 1.0 testing and certification remain supported. American Express will announce when these services will be withdrawn.

Q1.11 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, and these details 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.

Q1.12 CAN SAFEKEY 2.0 BE DEPLOYED WITHOUT SAFEKEY 1.0?

Yes.

Q1.13 DO CARD MEMBERS HAVE TO ENROLL IN SAFEKEY 2.0 IF THEY HAVE ALREADY ENROLLED IN SAFEKEY 1.0?

Card Members do not have to enroll in SafeKey 2.0 as all eligible Card Members will be pre-enrolled by Issuers as a requirement of the EMVCo specification.

Q1.14 CAN SAFEKEY BE UTILIZED FOR ONLINE TRANSACTIONS ON ALL CARD PRODUCTS?

SafeKey provides the benefit of authenticating that the person making the transaction is the Card Member. Consequently, it cannot be used with anonymous products, such as prepaid cards, where the user's identity is not registered.

SECTION 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, provision of 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 Response message. Please refer to the SafeKey specifications for details.

Q2.4 WHAT IS AN ATTEMPTED SAFEKEY TRANSACTION?

An attempted transaction is 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 Response message. Refer to the SafeKey specifications for details.

SECTION 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 see 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. Most providers are likely to support multiple versions of SafeKey, which will give broader coverage depending on the services individual Issuers support.

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 I AM ALREADY USING SAFEKEY 1.0. SHOULD I MOVE TO SAFEKEY 2.0?

Yes. SafeKey 2.0 has strong benefits over SafeKey 1.0 including additional data that improves an Issuer's risk based analysis and can reduce checkout friction. See Appendix for a feature comparison between SafeKey 1.0 and SafeKey 2.0. American Express has announced the withdrawal of SafeKey 1.0 by October 2022, and advise all users to migrate to the latest version of SafeKey 2.0.

Q3.6 HOW DOES A MERCHANT OR 3DS SERVER (MPI) KNOW WHICH VERSIONS OF SAFEKEY AN ISSUER SUPPORTS?

The 3DS Server (MPI) is provided 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.

Q3.7 AS A MERCHANT, HOW CAN I ENABLE MY APP FOR SAFEKEY?

Merchants have to 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 refer to www.emvco.com for a list of approved SDK providers.

Q3.8 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.

Q3.9 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.

Q3.10 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.

Q3.11 AS A MERCHANT, I ONLY SUPPORT SAFEKEY 2.0, BUT THE ISSUER ONLY SUPPORTS SAFEKEY 1.0. WHAT WILL HAPPEN?

Beginning January 2022, Merchants who support SafeKey 2.0 may be eligible for Attempts against Issuers who have not yet uplifted to SafeKey 2.0.

Q3.12 CAN I USE SAFEKEY IF MY ACQUIRER IS NOT CERTIFIED?

Yes. You can benefit from SafeKey authentication checks. However, in order to benefit from FLS, your Acquirer does need to be certified. Note: a Merchant's processor should also be able to support SafeKey and pass the necessary data to the Acquirer.

Q3.13 ARE THERE FEATURES IN SAFEKEY THAT HELP MERCHANTS SUPPORT STRONG CUSTOMER AUTHENTICATION?

Yes, all versions of SafeKey support Strong Customer Authentication, such as PSD2 requirements.

Q3.14 WHERE CAN A MERCHANT OBTAIN 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.

SECTION 4: ACS & 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 A LIST OF CERTIFIED ACS AND 3DS SERVER (MPI) PROVIDERS BE FOUND?

For a list of certified ACS and 3DS Server (MPI) Providers who have registered with American Express, please see the [AMEX Enabled website](http://www.amexenabled.com).

Q4.3 IS CERTIFICATION FOR SAFEKEY 2.0 NECESSARY IF SAFEKEY 1.0 CERTIFICATION HAS BEEN COMPLETED?

Yes. For ACS and 3DS Server (MPI) Providers, separate certifications are required for the different versions of SafeKey. Please see www.amexsafekey.com for more information. EMVCo provides a mandatory EMV 3DS approval service for ACS and 3DS Server (MPI) Providers, which must be completed prior to American Express SafeKey 2.0 certification.

Q4.4 HOW DO I REGISTER FOR CERTIFICATION AND TESTING?

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

SECTION 5: ISSUER & 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 IF AN ISSUER OR ACQUIRER HAS OBTAINED CERTIFICATION FOR SAFEKEY 1.0, IS CERTIFICATION FOR SAFEKEY 2.0 REQUIRED?

The Network messages for SafeKey 1.0 and 2.0 are consistent so re-certification is not required. However, Issuers wishing to support SafeKey 2.0 will need their ACS provider to be certified for SafeKey 2.0 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 to SafeKey and are version agnostic.

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. You may want to choose a solution that supports legacy versions of SafeKey until they are withdrawn to maximize coverage.

APPENDIX: FEATURE COMPARISON CHART

American Express SafeKey® Comparison Chart

Feature	SafeKey 1.0	SafeKey 2.0	
		SafeKey 2.1 (EMV 2.1.0)	SafeKey 2.2 (EMV 2.2.0)
Based on industry-standard 3-D Secure	●	●	●
Extra layer of security at checkout	●	●	●
Payment authentication	●	●	●
Browser-based authentication	●	●	●
Flexibility for Issuers to use a variety of authentication methods (i.e. one-time passcodes, risk-based decisioning, etc.)	●	●	●
Support for PSD2 compliance	●	●	●
Support for more data elements promoting frictionless authentications	Available in the US and its territories	●	●
App-based (in-app) enablement	—	●	●
Nonpayment authentication	—	●	●
Token-based transactions	—	●	●
Out-of-band authentication	—	●	●
Merchant initiated authentications	—	—	●
Decoupled authentication	—	—	●
PSD2 additional indicators	—	—	●

Note: Some of these features may require additional certification.



SafeKey®