American Express SafeKey® Frequently Asked Questions

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. And 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 authorised:

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 modelling 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 programme.

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.

Q1.6 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
- Improve Issuer risk assessment through enhanced data
- Support a variety of authentication methods, including one-time passcodes, biometrics and out-of-band authentication
- Support token-based transactions for enhanced security and to account for the expansion of token usage across the industry
- Enable non-payment authentication, such as provisioning a card to a digital wallet
- Enable Merchants to initiate authentications (e.g. for Recurring Billing, Mail Order and Telephone Order)
- Improve Card Member user experience and checkout flows
- Offer 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 is monitoring the industry's use of SafeKey 1.0 and will continue to support the service while adoption of SafeKey 2.0 grows. American Express will announce when the SafeKey 1.0 service will be fully succeeded by SafeKey 2.0 and give an appropriate lead time.

Q1.10 CAN SAFEKEY 1.0 AND SAFEKEY 2.0 CO-EXIST?

Yes, SafeKey 1.0 and 2.0 operate independently so they can co-exist. Over time it is expected that SafeKey 2.0 will supersede 1.0 and during this transitional period it is recommended that Merchants seek the services of 3DS Server (MPI) Providers who support both products. When a Merchant requests a transaction authentication it is the 3DS Server (MPI) Provider's responsibility to utilise the appropriate SafeKey version.

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. If it is, then the SafeKey 2.0 service should be used, if not then SafeKey 1.0 should be utilised.

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

Yes. Over time this will become the standard approach for new adopters. Participants should be aware that there will be a period of time before SafeKey 2.0 is fully established.

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

Card Members do not have to enrol 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 UTILISED 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 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 SafeKey or the Issuer's ACS is not available. SafeKey may grant an attempted authentication as indicated by an authentication value in the Response message; please refer to the SafeKey specifications for details.

SECTION 3: MERCHANT FAQs

Q3.1 HOW DO I ASSESS WHAT I NEED TO DO IN ORDER TO ADOPT SAFEKEY?

Merchants wishing to adopt SafeKey should talk to their prospective 3DS Server (MPI) Provider or Acquirer.

Q3.2 AS A MERCHANT, HOW DO I ENROL IN SAFEKEY?

Merchants should contact their 3DS Server (MPI) Provider or Acquirer to enrol in SafeKey. An online enrolment portal is also available for certain Acquirers at www.amexsafekey.com.

Q3.3 AS A MERCHANT, HOW DO I KNOW WHICH VERSION OF SAFEKEY TO USE?

It is recommended to select a 3DS Server (MPI) Provider who supports all versions of SafeKey. They will select the appropriate version as they know which versions of SafeKey the Issuer supports and will use the enhanced features accordingly.

Q3.4 AS A MERCHANT, HOW DO I KNOW IF MY 3DS SERVER (MPI) PROVIDER SUPPORTS SAFEKEY 2.0?

3DS Server (MPI) Providers are working with EMVCo and American Express to obtain certification for SafeKey 2.0. Merchants should contact their provider to discuss their plans. A list of 3DS Server (MPI) Providers certified with American Express and registered with AMEX Enabled is available on the AMEX Enabled website (www.amexenabled.com).

Q3.5 ARE MERCHANTS REQUIRED TO ENROL IN SAFEKEY 2.0 IF THEY HAVE ALREADY ENROLLED IN SAFEKEY 1.0?

Merchants should work with their 3DS Server (MPI) to understand the procedures for benefitting from SafeKey 2.0.

Q3.6 I AM A MERCHANT NOT CURRENTLY USING SAFEKEY. HOW DO I ENROL IN SAFEKEY 2.0?

Merchants should initially talk to their 3DS Server (MPI) Provider about enrolment in SafeKey. For a list of certified 3DS Server (MPI) Providers who have registered with American Express, please see the AMEX Enabled website (www.amexenabled.com).

Q3.7 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.

Q3.8 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.

Q3.9 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.

Q3.10 DOES AMERICAN EXPRESS APPLY TRANSACTION FEES FOR USE OF SAFEKEY?

No. Please talk to your 3DS Server (MPI) Provider to understand the cost of their services.

Q3.11 WHAT HAPPENS IF THE ISSUER DOES NOT SUPPORT SAFEKEY?

Though SafeKey is currently an optional service for Issuers, Issuers that 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.

Q3.12 WHAT HAPPENS IF A MERCHANT'S ACQUIRER DOES NOT SUPPORT SAFEKEY?

It is a requirement for a Merchant's Acquirer to be certified for SafeKey. This is to ensure the necessary authorisation and submission messages can be processed and fraud liability shift can be attributed correctly. 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 AUTHORISATION AND SUBMISSION SPECIFICATIONS FOR SAFEKEY?

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

SECTION 4: ACS & 3DS SERVER (MPI) PROVIDER FAQs

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

The first step in obtaining certification 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 (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, authentication processing for the ACS will be subject to certification.

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 U.S. and its territories	●	●
App-based (in-app) enablement	—	●	●
Non-payment 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.