Frequently Asked Questions

Online PIN with American Express

Contents

Enabling Online PIN

1 What is Online PIN?

Online Personal Identification Number (PIN) validation is a Card Member Verification (CVM) used to authenticate the Card Member at the Point of Sale (POS).

Issuers and Acquirers can use Online PIN as an acceptable CVM to complete a card present EMV® chip or an Expresspay Contactless transaction.

2 How is Online PIN and Offline PIN different?

During an Online PIN transaction, the PIN is entered into the terminal, encrypted and sent to the Issuer for PIN verification. An Offline PIN transaction is validated between the terminal and chip card or mobile device with no Issuer validation.

Implementing Online PIN has considerations for Merchants, Acquirers and Issuers, including but not limited to:

- The POS device hardware and configuration must be Online PIN enabled.
- Issuers must enable the Online PIN capability within their EMV Chip cards.
- There are differences in the Authorization messages passed between the POS terminal and the Issuer's host, which are required to pass PIN data in a securely encrypted form.
- All Participants, their vendors, processors, and the American Express host platforms must be upgraded to support Online PIN and recertified by American Express. Please refer to the Business and Operational Policy for more information and mandate dates.

3 Does American Express mandate the use of Online PIN?

American Express Network Participants are advised to refer to the Business and Operational Policies manual (BOP) for more information regarding Online PIN and their obligations. Participants can contact their American Express Representative for more information.

Note: Acquirers should refer to section **POS Online PIN Certification and Enablement Program** for more information regarding the program and associated timelines.

4 What considerations should be made prior to finalizing Online PIN enablement plans?

American Express Network Participants should familiarize themselves with the following information as this may assist in determining plans and timelines:

- Business and Policies manual (BOP): Participant Data Security Policy.
- Business and Policies manual (BOP): POS Online PIN Certification and Enablement Program.
- PCI PIN Security Requirements v3.0 (discussed in the next section of the FAQs).
- Network Participant Update (NPU) dated April 2020: Dynamic Key Exchange (DKE) – Acquirer Enablement.
- Review future Network Participant Updates (NPU) for future announcements.

Participants should contact their American Express Representative for more information.

Revised PCI PIN Security Requirements v3.0

1 What changes has PCI announced in relation to PIN security?

In August 2018, PCI published an updated PIN security requirements document PIN Security – Requirements and Testing Procedures v3.0.

The changes will strengthen security controls as older technology becomes weak and new threats are introduced.

2 As an Online PIN certified AEGN Participant, am I impacted by the updated PCI PIN Security V3.0 requirements?

As documented in the Business and Operational Policies Manual, all American Express Participants must comply with the Participant Data Security Policy that includes Payment Card Industry (PCI) PIN Security Requirements.

Any new and existing American Express Participant will need to review the updated Payment Card Industry (PCI) PIN Security Requirements v3.0 and determine how these new changes may impact their PIN processing procedures.

3 How could the changes to the Payment Card Industry (PCI) PIN Security Requirements v3.0 impact current processing? What are some considerations?

American Express requires American Express Network Participants who process PIN transactions must do so in accordance with the Payment Card Industry (PCI) PIN Security Requirements. The following considerations should be made when determining their obligations:

- Acquirers should consider the impact on POS terminal device hardware and configurations.
- If processing using static keys, decide on the key management scheme that is most suitable. American Express supports Master/Session (Dynamic Key Exchange) and Derived Unique Key Per Transaction (DUKPT) for host to host and terminal to host encryption.
- Host systems to support revised Authorization message formats.
- Vendors and agents providing services e.g. merchants, issuers, acquirers, aggregators, payment processors, key injection facilities, certificate processors.
- Requirements outlined in the PCI Standards Security Council announcements and publications related to PCI PIN Security.
- Issuers should consider the impact on their issuing infrastructure including chip card personalization.

4 Where can I find more information?

Participants should familiarize themselves with the documentation listed below and regularly refer to the PCI website for future announcements. American Express Network Participants should also refer to all Network Participant Updates (NPU) for future announcements.

- August 2018: PCI PIN Security – Requirements and Testing Procedures v3.0.
- August 2018: PCI SSC Modifications – Summary of Significant Changes from v2.0 to v3.0.
- June 2019: PCI Information Supplement – PIN Security Requirement 18-3 Key Blocks.
- April 2020: Network Participant Update (NPU) – Dynamic Key Exchange (DKE) – Acquirer Enablement.
- July 2020: PCI Bulletin – Key Block Implementation Revision FINAL.

5 Will the layout of the Authorization message change?

Yes, to support the PCI PIN Security v3.0 requirements the layout of the Authorization message will need to change. The extent of the change depends on the chosen key management scheme for terminal-to-host or host-to-host PIN encryption.

The changes will be updated in the Network Specifications Authorization document and Online PIN Implementation Guide.

American Express Network Participants are reminded to review the NPU articles for further announcements.