Online PIN

Frequently Asked Questions

What is Online PIN?

Online Personal Identification Number (PIN) validation is a Cardholder Verification Method (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.

1. Enabling Online PIN

Q1.1 How are Online PIN and Offline PIN different?

During an Online PIN transaction, the PIN is entered into the terminal, then 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.

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.

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.

All Participants, vendors and processors are recommended to support Online PIN and in some designated countries, support for Online PIN is mandatory. Please refer to the *Business and Operational Policy Manual* for further information.

Q1.2 How 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.

Q1.3 What additional information should be considered prior to finalizing plans to adopt Online PIN?

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

- Business and Operational Policies Manual
    - Participant Data Security Policy (DSP)
    - POS Online PIN Certification and Enablement Program
- PCI Standards which can be found at www.pcisecuritystandards.org

Participants are reminded to frequently review all Network Participant Updates (NPUs) for future announcements.

Participants should contact their American Express Representative for more information.

2. Revised PCI PIN Security Requirements v3.0

Q2.1 What changes has the Payment Card Industry (PCI) announced related to PIN security?

In August 2018, PCI published *PIN Security Requirements and Testing Procedures v3.0*, which outlined a number of changes to strengthen security controls as older technology becomes weak and new threats are introduced. PCI published a revision of this document in March 2021 (v3.1). Participants that are certified for Online PIN should familiarize themselves with the updated procedures

Q2.2 As an Online PIN-certified participant, am I impacted by the updated procedures?

As referenced in the *Business and Operational Policies Manual*, the AEGNS Data Security Policy (DSP) is a set of comprehensive policy requirements designed to protect Account Data whenever such data is stored, processed, or transmitted. AEGNS has endorsed and incorporated Payment Card Industry (PCI) PIN Security Standard Requirements into the DSP. Participants processing Online PIN must therefore adhere to the latest PCI standards.

Q2.3 What changes has PCI mandated?

- Effective January 1, 2023: Fixed Key for Triple Data Encryption Algorithm (TDEA, also known as TDES) PIN encryption in Point-of Interaction (POI) devices is disallowed.
- Effective January 1, 2023: Fixed Key for TDEA (TDES) PIN encryption in host-to-host is disallowed.
- Effective January 1, 2023: Encrypted symmetric keys must be managed in structures called Key Blocks. Refer to *PIN Security Requirements and Testing Procedures v3.1 (requirement 18-3)* for further details.
- PCI did announce effective dates for supporting ISO Format 4 (AES); however, those dates were suspended on March 11, 2021. Revised dates have yet to be announced.

Q2.4 What is a fixed key?

As defined by PCI, a Fixed Key is a transaction key management method whereby the fixed transaction key is either physically loaded from a key-loading device, using components or shares, or remotely loaded using asymmetric techniques. The fixed transaction key is used for transaction processing until a new key is similarly loaded. There is no ability to change this key except by using the same technique that originally loaded the key.
(Source: *PCI PTS PIN Security Requirements—Technical FAQs* for use for Version 3, dated September 2021.)

Q2.5 What is master/session key management?

As defined by PCI, Master/Session Key management is a method for managing transaction keys using a Master Key to encrypt new or replacement Key Encipherment Keys, Derivation Keys, and/or Session
Keys for distribution. (Source: *PCI PTS PIN Security Requirements— Technical FAQs* for use for Version 3, dated September 2021.)

The Master/Session Key management method is used to encrypt Online PIN data. A Master Key is the exchange key, also known as the Zone Master Key (ZMK). Session Key refers to the PIN encryption key, also known as the Zone PIN Key (ZPK). American Express supports both Manual and Dynamic Master/Session Key implementations and will continue to do so after January 1, 2023.

Q2.6 What is derived unique key per transaction?

Derived Unique Key per Transaction (DUKPT) is a key management method that provides unique encryption keys for every transaction using a Base Derivation Key. American Express supports DUKPT and will continue to do so after January 1, 2023.

Q2.7 Who needs to migrate from fixed key?

Any existing participant using Fixed Key will need to migrate to a Master/Session Key – Manual, Master/Session Key – Dynamic, or Derived Unique Key Per Transaction (DUKPT) key management method. Please refer to the latest *Network Specifications and Online PIN Implementation Guide* for details or contact your American Express Representative for further information .

Q2.8 Please elaborate on encrypting keys with key blocks.

As referenced in *PIN Security Requirements and Testing Procedures 3.1*, encrypted symmetric keys must be managed in structures called Key Blocks. PCI has phased dates for the implementation of Key Blocks:

- Phase 1 – Implement Key Blocks for internal connections and key storage within Service Provider Environment – June 1, 2019
- Phase 2 – Implement Key Blocks for external connections to Associations and Networks – January 1, 2023
- Phase 3 – Implement Key Blocks to extend to all merchant hosts, point-of-sale (POS) devices, and ATMs – January 1, 2025

In *PCI Informational Supplement: PIN Security Requirement 18-3 – Key Blocks*, PCI confirmed that all previously established keys can still be used. These keys are not expected to be reissued or changed.

Q2.9 In what scenarios will a key block be required?

After January 1, 2023:

- Any new key exchange with a new Online PIN participant must be encrypted with a Key Wrapping Key (KWK), also referred to as a Key Block Protection Key (KBPK). This includes participants who certify for Dynamic Key Exchange, as session keys are exchanged in the 1804/1814 network messages.
- When an existing Online PIN participant is required to rotate a key, the new key will be encrypted with a Key Wrapping Key (KWK).

Q2.10 What key management methods will American Express support?

American Express will support the following key management methods:

- Master/Session Key – Manual/static
- Master/Session Key – Dynamic Key Exchange (DKE)
- Derived Unique Key per Transaction (DUKPT)

For more information, please refer to the *Global Network Specification Guide* and *Online PIN Implementation Guide or* contact your American Express Representative.

Q2.11 How will American Express support the key management methods?

- American Express will continue to support PIN Encryption in Data Field 52 until Master/Session Manual Keys are disallowed.
- American Express now supports Enhanced PIN Encryption in a newly defined Data Field (DF111). Master/Session Key – Dynamic (DKE) and Derived Unique Key per Transaction (DUKPT) are two key management methodologies supported in Data Field 111.
- American Express strongly recommends migrating to Master/Session Key – Dynamic Key Exchange or Derived Unique Key per Transaction (DUKPT) in DF111 to combat attacks on security.

For more information, please refer to the latest *Network Specifications* and the *Online PIN Implementation Guide* or contact your American Express Representative.

Q2.12 Why was enhanced PIN encryption in data field 111 introduced?

- Enhanced PIN Encryption will support PIN encryption in a newly defined field. The data field will provide longer field lengths to support the migration to ISO Format 4 (AES) and will adhere to the key block requirements as stipulated by PCI.
- American Express strongly recommends migrating to Master/Session Key – Dynamic Key Exchange or Derived Unique Key per Transaction (DUKPT) in DF111 to combat attacks on security.

For more information, please refer to the latest Network Specifications and Online PIN Implementation Guide or contact your American Express Representative.

Q2.13 How do I find out more about Online PIN?

For more information about Online PIN, visit our website or reach out to your American Express Representative.