AMERICAN EXPRESS

Frequently Asked Questions

American Express Online PIN & PIN Security Requirements

Contents

Participants not yet Online PIN Enabled

1 How does Online PIN differ from Offline PIN?

During an Offline PIN transaction, the Card Member enters the PIN into the terminal and the PIN is verified by the Chip Card or mobile device, without going to the Issuer for verification.

With an Online PIN transaction, the PIN is entered into the terminal where it is encrypted and sent to the Issuer for PIN verification.

From a Merchant, Acquirer, and Issuer perspective, implementing Online PIN impacts a number of areas, 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.

2 Is support of Online PIN a mandatory requirement?

For Acquirers: Yes. American Express is updating its Business and Operational Policies (BOP) to mandate Acquirers' support of Online PIN in all countries in phases over the next few years. This reflects developments within the card payment industry. Acquirers are advised to refer to the Business and Operational Policies (BOP) and to contact their American Express representative for more information.

Issuers are advised to contact their American Express representative for more information.

3 When must planning begin to support Online PIN?

Acquirers should start planning now. Acquirers should refer to the October 2018 Network Participant Updates for a list of countries and the associated dates to support Online PIN.

4 What are the main considerations for Online PIN compared to Offline PIN?

The main considerations are listed under Question 1 within this FAQ document. In addition, the changes to the PCI PIN Security Standards should also be considered by all Participants when planning their approach to support Online PIN.

5 How do the new PCI PIN Security Requirements impact plans to support Online PIN?

Representatives from Participants Information Security and IT teams should be engaged to determine the best approach to move to Online PIN, carefully considering the new standards and associated timelines. Contact your American Express representative for more information.

6 How can we help?

Participants planning to migrate to Online PIN for the first time should contact their American Express representative for more information about our migration program and the support which is available.

In addition, it is crucial that all Participants are aware of the new PCI PIN Security Standards and should read the questions which follow.

PCI PIN Security Standards

1 Why did PCI update the PIN Security Standards?

Security controls must evolve as older methods of security become weak and new threats are identified. PCI announced that version 3.0 of their PIN standards will ensure the future integrity of PIN by minimizing future risk to the key generation and operations.

2 As an Online PIN enabled Participant, how do the new PCI PIN Security requirements impact my processes?

American Express policy requires the PIN to be protected in accordance with the PCI PIN Security Standards. The following areas should be reviewed in light of the PCI PIN Security Standards:

- Acquirers should consider the impact on POS terminal device hardware and configurations
- Decide on the Key Management Scheme you will implement to migrate away from static keys. American Express supports both Master/Session (Dynamic Key Exchange) and Derived Unique Key Per Transaction (DUKPT) for host-to-host and terminal-to-host key 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
- All areas referenced in PCI Standards Security Council publications on this subject

Issuers should consider the impact on their issuing infrastructure including chip card personalization.

3 Which documents from the PCI should I refer to?

Participants should start to become familiar with the documents listed below. Please remember to refer to the PCI website as further documentation is likely to be published in future:

Description	Link
PCI Press Release, 1st August 2018	PIN Security Standard Press Release
PCI Modifications – Summary (v2.0 to v3.0)	PCI SSC Modifications—Summary
PCI Revised Standard	PCI PIN Security Requirements & Testing version 3.0: Aug 2018

4 Will the content of the Authorization message change?

Yes. The extent of the change will depend on which key management scheme you choose for terminal-to-host and host-to-host PIN encryption. The American Express Network Specifications – Authorizations document will be published to reflect the changes required.

5 When do these changes have to be completed?

PCI has published a set of deadlines for compliance. These can be found in the PCI PIN Security Requirements & Testing version 3.0. Some of the key dates are in the table below – please refer to the PCI publication for most accurate dates. American Express will be publishing its own program dates in due course.

Standard	Description	Deadline
Key Blocking	Mandated to reduce hacking and protect the integrity of the PIN	1 June 2021: Implement Key Blocks for external connections to Associations and Networks 1 June 2023: Implement Key Block to extend to all Merchant Hosts, point-of-sale (POS) devices and ATMs.
Fixed Key Decommission	Fixed key disallowed for Triple Data Encryption Algorithm (TDEA) PIN in point-of-interaction devices and host-to-host connections	1st January 2023
AES to replace TDEA/TDES	Applies to AES decryption capability – impacts Issuers	1st January 2023
AES to replace TDEA/TDES	Applies to AES encryption capability – impacts Acquirers	1st January 2025

Participants should contact their American Express representative for more information.

6 What Key management methods will American Express support?

American Express will support both Dynamic Key Exchange (DKE) and Derived Unique Key Per Transaction (DUKPT). Further information will be provided by the end of 2019.

7 What is Dynamic Key Exchange (DKE)?

DKE is a form of master/session key management in which PIN session keys are exchanged using an automated process in the Network using standard Network management messages.

8 How is DKE used by American Express?

After an initial manual exchange of transport keys which are used to encrypt the PIN session keys, the encrypted PIN session keys are exchanged in messages between American Express and the partner.

9 What messages are used to support DKE?

1804/1814 Network Management Messages:

PIN session keys are requested and exchanged using 1804/1814 Network management messages. Partners can request PIN session keys as needed, and the Network will provide the encrypted session keys in an 1814 Network management response message.

Partners receiving the PIN session keys and their identifying key check value in those messages will use the PIN session key to encrypt the PINs.

The PCI requirement for key blocks are required when passing PIN session keys in the Network Management messages.

1100 Authorization Request Message:

1100 Authorization requests are used to send the encrypted PIN data with the key check value associated with the PIN session key used for the PIN encryption.

10 What is Derived Unique Key per Transaction (DUKPT)?

DUKPT is a key management PIN encryption scheme where every transaction is provided with a different PIN key based on a derivation key. A derivation key is used to cryptographically compute other keys, e.g. for use in DUKPT.

11 How does American Express use DUKPT?

American Express supports DUKPT encryption in two different scenarios:

- In terminal-to-host scenarios, where the terminal has a DUKPT key injected into it, and that key is used to encrypt the PIN for each transaction sent into the Network.
- In host-to-host scenarios American Express also allows and supports DUKPT, where a DUKPT key is exchanged between American Express and a Participant. In these cases, the sending host sends DUKPT PIN-encrypted transactions to the receiving host, which will use the DUKPT PIN key to decrypt the PIN data. DUKPT PIN encryption is enabled with a manual exchange for the base derivation key, and then DUKPT is systematically enabled by using DUKPT encryption of PIN data in 1100 Authorization Request messages.

12 Do key blocks impact DUKPT transactions?

Not for messages in the Network. The DUKPT metadata (key set identifier) for PIN transactions, which are passed through the Network via messages, are not impacted by PCI requirements for key blocking. However, there are impacts unrelated to data in Network Messages. For example, data-at-rest key storage requirements for secure cryptographic devices, such as host security modules, are impacted by key blocking requirements when using DUKPT.