VISA PIN SECURITY BULLETIN **31 July 2020**

Key Block Effective Dates Extended

Distribution: Validating PIN Security Program Participants and Sponsoring Acquirers

Intended Audience: PIN Program Mgrs., Security, Compliance & Risk Personnel

Summary *– The Payment Card Industry Security Standards Council (PCI SSC) has extended the effective dates of the PCI PIN Key Block Requirements for Phase 2 and Phase 3. The PIN Security Program and Visa's requirement to exchange keys in the key block format will align with the revised effective dates. A Visa Business News (VBN) article will be published the first week of August to all Visa stakeholders. The following information aligns with the VBN but contains additional considerations specific to the Visa PIN Security Program.*

Key Block Effective Dates Extended

In December 2014, the Payment Card Industry (PCI) PIN Security Requirements introduced requirement 18-3, Key Blocks. The requirement, sometimes referred to as "key bundling," greatly improved the protection of symmetric keys that are shared among payment system participants to protect PINs and other sensitive data. The key block requirement in PCI PIN Security Requirements standard is applicable to all PIN program participants.

Due to a number of factors, including impacts to organizations due to COVID-19 pandemic, PCI SSC has extended the effective dates for key block implementations. A PCI SSC bulletin published on 17 July 2020, communicates the revised dates as follows:

> **Phase 1:** Implement key blocks for internal connections and key storage within service provider environments. This includes all applications and databases connected to hardware security modules (HSMs). Phase 1 became effective 1 June 2019; this date will not be extended.
>
> **Phase 2:** Implement key blocks for external connections to associations and networks. **New effective date: 1 January 2023** (replaces previous effective date of 1 June 2021).
>
> **Phase 3:** Implement key blocks to extend to all merchant hosts, POS devices and ATMs.

New effective date: 1 January 2025 (replaces previous effective date of 1 June 2023).

The PIN Security Program will recognize the revised PCI dates, meaning organizations that are unable to exchange PIN keys with another organization in the key block format will continue to be compliant until 1 January 2023. After this date organizations not meeting the requirement will be found not compliant. Since the Phase 1 date did not change, all PIN participants are expected to be compliant as of 1 June 2019.

PIN Participants must continue their efforts to implement Key Blocks per PCI PIN Security Requirements and Visa Requirements. Refer to previously published information for additional information. *Note: PCI SSC and Visa will update existing documentation in the coming months to reflect the revised effective dates.*

Available on Visa Online:

Visa Business News:

- 4 May 2017 - Implementation Date Change for PCI PIN Security Key Bundling Requirement
- 19 July 2018 - Support for Key Exchange in Key Block Format
- 27 June 2019 - Supplementary Information to Support Key Block

Visa Tech Letter articles regarding exchanging symmetric keys with Visa:

- Static Key: October 2018 GTLIG: Article 4.4
- Dynamic Key: April 2019 GTLIG: Article 4.17
- Key Block Header Definitions: April 2020 GTLIG Article 3.14

Available from the PCI SSC Document Library:

PCI PIN Security Requirements and Testing Procedures, Version 3.0
Information Supplement: PIN Security Requirement 18-3—Key Blocks
Information Supplement: Cryptographic Key Blocks
PCI blog articles:

- Key Blocks 101 – Basic questions about the key block method and how it helps secure payment data.
- Key Blocks 102 – Addresses questions about Key Block Applicability
- Key Blocks 103 - Addresses the 3 phases for implementing the Key Blocks requirement
- Key Blocks 104 - Covers basic questions about the Advanced Encryption Standard (AES) and the Triple Data Encryption Standard (TDES) block ciphers and how they relate to key blocks.

Client Responsibilities

Clients must continue to:

- Ensure that all agents are appropriately registered in the Visa Third Party Agent (TPA) Registration Program. Contact your regional Visa representative to obtain information about the registration process.
- Ensure that their acquiring TPAs that process or handle PIN data comply with the PCI PIN security requirements and adhere to the Visa Rules and Visa PIN Security Program.
- Ensure that their own processing environments that handle PIN data comply with the PCI PIN security requirements.
- Perform the necessary due diligence prior to engaging any TPA, and maintain policies and procedures to provide the correct level of oversight and control of the agent.
- Clients that use agents identified as Validating PIN Participants that have not performed an on-site PIN assessment or have areas of non-compliance may be subject to non-compliance assessments as defined in the Visa PIN Security Program Guide.

For More Information

For more information on Visa's support for the key block requirement, contact your Visa representative. Merchants and third party agents should contact their issuer or acquirer.

For more information on the Visa PIN Security Program, visit the PIN Security website or contact your regional PIN program manager:

AP: pinsec@visa.com

CEMEA: pcicemea@visa.com

Europe: visaeuropepin@visa.com

LAC: pinlac@visa.com

North America: pinna@visa.com

Global: pin@visa.com