Implementation Date Change for PCI PIN Security Key Bundling Requirement

In December 2014, Version 2.0 of the *Payment Card Industry (PCI) PIN Security Requirements* introduced a requirement: 18-3, Key Bundling. The requirement, sometimes referred to as "key blocks" or "key bundling," greatly improved the protection of symmetric keys that are shared among payments system participants to protect PINs and other sensitive data.

Mark Your Calendar:

- Phase 1 takes effect **(June 2019)**
- Phase 2 takes effect **(June 2021)**
- Phase 3 takes effect **(June 2023)**

The requirement states:

> "Effective 1 January 2018, encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods.
>
> Acceptable methods of implementing the integrity requirements include, but are not limited to:
>
> - A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the key block, which includes the key itself.
> - A digital signature computed over that same data.
> - An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102."

Industry participants have communicated concerns about the complexity and effort required to meet the January 2018 date. Therefore, based on industry feedback, the PCI Security Standards Council (SSC) has issued a bulletin that communicates revisions to the implementation date associated with the 18-3, Key Bundling, requirement.

The new implementation dates have been broken into three phases, each with its own effective date. This will allow organizations to focus their resources to address implementation tasks specific to their environment and support a smooth migration across the payments network.

The phases and revised effective dates are as follows:

- **Phase 1—Effective June 2019:** Implement key blocks for internal connections and key storage within service provider environments; this would include all applications and databases connected to hardware security modules (HSMs).
- **Phase 2—Effective June 2021:** Implement key blocks for external connections to associations and networks.
- **Phase 3—Effective June 2023:** Implement key blocks to extend to all merchant hosts, POS devices and ATMs.

The PCI SSC is preparing an informational supplement that will be published in the coming weeks on cryptographic key blocks, providing additional information on what key bundling is, why this requirement is important, and implementation guidance. Visa will communicate the availability of the supplement when it is published.

Stakeholder Impact

Payments stakeholders that exchange PIN data with other entities are affected by this requirement.

Visa has reviewed the phases and associated effective dates for 18-3, Key Bundling, and preparations are underway to be compliant with all phases of the requirement.

Note: Visa will apply the key block requirement to **all** keys that Visa transmits between itself and payment stakeholders. This includes keys that protect PIN data, as well as keys that protect other data. Examples include Cardholder Verification Value (CVV) and Cardholder Authentication Verification Value (CAVV) data.

To help stakeholders prepare for these changes, Visa plans to allow for key exchanges to be sent in the existing format and the key block format for a period of time leading up to the June 2021 implementation date for Phase 2. After June 2021, Visa will only send or receive keys in the key block format.

Additional information for Dynamic Key Exchange (DKE) participants, as well as information about how and when all Visa stakeholders can begin exchanging keys in key block format, will be published in the 2018 Global Technical Letter.

Additional Resources

Documents & Publications

PCI SSC Bulletin—Revision to the Implementation Date for PCI PIN Security Requirements 18-

3 PCI PIN Security Requirements, Version 2.0

Online Resources

Visa PIN Security website

For More Information

For more information on supporting the Key Bundling requirement, contact your Visa representative.

For information on the Visa PIN Security Program, contact your regional Visa Risk representative:

- **AP and CEMEA:** pinsec@visa.com
- **Canada and U.S.:** pinna@visa.com
- **LAC:** pinlac@visa.com
- **Global:** pin@visa.com