PCI PIN 标准相关截止时间的解读以及近期重要信息分享

作者：atsec 张志鹏 2024 年 3 月

关键词：PCI PIN，Technical FAQ，截止时间，Fixed Key，Key Block，Modified PED，HSM，密钥组件/分量，Visa PIN Security Program，MPOC

众所周知，PIN（个人识别码）数据用于在终端发出的授权请求中对持卡人进行身份验证。PIN 仅由十进制数字组成。PIN 码也经常被大家俗称为信用卡的密码。因此，PIN 码属于机密性最高的支付认证数据。PCI 标委会针对 PIN 数据保护专门出台了用于保护 PIN 数据以及相关密钥数据的安全标准“PCI PIN 安全要求和测试程序（PCI PIN Security Requirements and Testing Procedures）”。该标准包含一套完整的安全要求，用于在 ATM 和销售点（POS）终端进行联机和脱机支付卡交易处理期间，对 PIN（个人识别码）数据进行安全管理、处理和传输。该标准适用的机构包括但不限于：收单机构、收单机构的商户、收单机构的代理服务商、处理 PIN 交易的机构、提供相关密钥管理功能的机构、支持 PIN 输入设备的机构等。对于 PCI PIN 标准的介绍，可以参考之前文章“PCI PIN Security 标准简介”。

本文重点对 PCI PIN 标准提及的一些安全要求点的截止时间进行了解读，并介绍了近两年来产业内关于 PCI PIN 标准的一些重要信息。

一、 PCI PIN 标准中几个安全要求点截止时间的解读

当前遵循的 PCI PIN 的标准现行版本是 2021 年 3 月所发布的安全标准“PCI_PIN_Security_Requirements_Testing_v3_1_202103”，虽然主标准近三年没有做更新，但是主标准中有些安全要求提及的截止时间点（例如 2023 年 1 月 1 日、2024 年 1 月 1 日），导致在执行 PCI PIN 评估中的评估标准也发生了变化。此外，PCI 标委会通过不定期的更新 Technical FAQ 文档“PCI_PIN_Technical_FAQs_v3_December_2023“，对产业内持续产生的一些疑问做了澄清和解答。Technical FAQ 文档在这三年里更新了 13 次。当前最新版本的 FAQ 是 2023 年 12 月发布的 v3 版本。这里笔者综合上述两篇文档以及产业内的最佳实践，针对近两年的产业内常见问题，给出了以下解读。

1. 关于 2-2 的解读，标准原文如下：

2-2 Online PIN translation must only occur using one of the allowed key-management methods: DUKPT, fixed key, master key/session key.

Note:	
Effective 1 January 2023:	*Fixed key for TDEA PIN encryption in POI devices is disallowed.*
Effective 1 January 2023:	*Fixed key for TDEA PIN encryption in host-to-host connections is disallowed.*

结合 PCI PIN 的 Technical FAQ 中对该要求的答疑，有以下解读：

- 自 2023 年 1 月 1 日起，不允许 POI 设备使用基于 TDEA 算法的固定密钥方案进行 PIN 加密保护。

- 自 2023 年 1 月 1 日起，不允许针对主机到主机的 PIN 加密保护，使用基于 TDEA 算法的固定密钥方案。
- 固定密钥方案是一种交易密钥管理方法，是指固定的交易密钥用于交易处理，所有的交易都使用同一个密钥，直到加载新的固定密钥。除非使用最初加载密钥的相同技术，否则无法更改此密钥。固定交易密钥可以物理加载（使用 KLD 加载或使用密钥组件/分量加载），也可以使用非对称技术远程加载。
- 主密钥/会话密钥管理方案（MK/SK），是一种使用密钥加密密钥（也称为主密钥）管理交易密钥的方法，主密钥用于加密以分发新的或替换的密钥加密密钥、派生密钥和/或会话密钥（例如，PIN 加密密钥）。该方法也称为主密钥/交易密钥方法。

基于当前的行业实践，强调一下，对于那些用于机构和机构之间的 PIN 保护密钥也要注意此问题。如果 PIN 保护密钥还在使用基于 TDEA 算法的固定密钥方案，那么需要升级 TDEA 算法到更强的算法（如 AES128），或者废除固定密钥方案，使用主密钥/会话密钥方案。

2. 关于 13-9 的解读，标准原文如下：

> **13-9** Key-injection facilities that use PC-based key-loading software platforms or similar devices (e.g., modified PEDs) that allow clear-text secret and/or private keys and/or their components to exist in memory outside the secure boundary of an SCD must minimally implement the following additional controls:
>
> ***Note: Effective 1 January 2021,*** *entities engaged in key loading on behalf of others shall not be allowed to use PC based key-loading methodologies where clear-text secret and/or private keying material appears in the clear in memory outside the secure boundary of an SCD.*
>
> ***Effective 1 January 2023****, entities only performing key loading for devices for which they are the processor shall no longer have this option.*

结合 PCI PIN 的 Technical FAQ 中对该要求的答疑，有以下解读:

- 自 2021 年 1 月 1 日起，对于那些基于 PC 的密钥加载方法，如果该方法导致明文密钥和/或私钥材料会以明文形式出现在 SCD 安全边界之外的内存中，则不再允许实体使用此类方法。该截止日期是针对代表其他机构进行密钥注入的场景。
- 自 2023 年 1 月 1 日起，以上同样的限制生效于支付处理机构自身进行密钥注入的场景。
- 针对在密钥生成过程中，使用了 PC 设备并且明文密钥材料通过了 PC 内存中的场景，在 2023 年 1 月 1 日后，也是禁止使用的。
- 使用了修改的 PED 设备（Modified PED）作为密钥加密设备时，修改的 PED 设备也被视为 PC 同类设备。即使 PED 设备曾经通过了 PCI 认证，修改的 PED 设备也不视为 SCD 设备。明文密钥材料也不可以通过其内存。此类修改的 PED 设备不被作为是 SCD，除非它通过了 KLD 级别的 PCI-PTS 验证。
- 对于那些通过 PC 上的终端模拟软件来加载/注入明文密钥或私钥的组件/分量的场景，在 2023 年 1 月 1 日后，也是禁止使用的。
- 关于在安全房以外，手动抄写明文密钥组件/分量的情况，标准是允许的，但是需要满

足以下要求：

- ✓ 明文密钥组件/分量仅允许显示在 PCI 批准或 FIPS 批准的 SCD（例如 HSM 或 KLD）的集成显示屏上。密钥组件/分量绝不能出现在 SCD 或硬件管理设备 (HMD) 防篡改边界之外的内存中。
- ✓ 该过程在 ISO 13491-2 定义的受控或更高环境中执行。
- ✓ 必须遵循双重控制和分裂知识的原则。
- ✓ 监控摄像机的安装位置必须确保它们不会监控任何用于输入密码/验证码或其他验证凭证的明文密钥材料、密码锁、密码键盘或键盘；否则，密钥保管员必须将其身体放置在遮挡监控的位置。

- 自 2024 年 1 月 1 日起，在对生产中使用的任何 HSM（即使位于满足标准 6-3 要求的安全房中）加载明文密钥和私钥的密钥组件/分量时，必须使用 SCD 通过以下方式之一进行加载：

1) 使用 SCD 设备对 HSM 做相关加载，例如 PCI 批准的 KLD，
2) PCI 批准的远程管理解决方案，或
3) 通过集成键盘输入密钥材料，该键盘专为某些 HSM 型号上可能存在的安全输入而设计。

在方法 2)和 3)适用的情况下，明文密钥和私钥的密钥组件/分量的加载还可能涉及与方法 2)和 3)结合使用硬件管理设备 (HMD)，如 Smart card。

3. 关于 18-3 的解读，标准原文如下：

18-3 Encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods.

The phased implementation dates are as follows:

- **Phase 1 –** 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 (HSM). Effective date: **1 June 2019.**
- **Phase 2** – Implement Key Blocks for external connections to Associations and Networks. Effective date: **1 January 2023.**
- **Phase 3** – Implement Key Block to extend to all merchant hosts, point-of-sale (POS) devices and ATMs. Effective date: 1 **January 2025**.

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, e.g., TR-31
- A digital signature computed over that same data, e.g., TR-34
- 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*.

结合 PCI PIN 的 Technical FAQ 中对该要求的答疑，有以下解读：

- 对于 Phase2 的情况，涉及和外部机构之间的配合。服务提供商必须在截止日期 2023

年 1 月 1 日之前为所有支持 Key block 的外部机构实施 Key block 方案。当其他机构改造为支持 Key block 时，服务提供商必须有能力及时为其实施 Key block 方案。

- “ASC X9 TR 31: Interoperable Secure Key Exchange Key Block Specification”（简称 TR-31）已被 ANSI 归类为“历史”，“X9.143 Retail Financial Services: Interoperable Secure Key Block Specification”（简称：X9.143）是较新的版本。所有对 TR-31 的引用都已更新为 X9.143。简单理解就是使用 X9.143 的说法代替了 TR-31 的说法。目前在 FAQ 的新版本中已经使用 ANSI X9.143 代替了 TR-31 的说法。这样就带来一个问题，生成支持 TR-31 的 SCD 是否还符合规范要求。笔者认为此类情况仍可以视为合规情况，原因有两点：一是因为 X9.143 是 TR-31 规范的新版，其中对于 Key block 部分的定义没有大的调整，二是 PCI PIN 标准中说明了对于 Key block 的实现，X9.143 并不是唯一的实现，可以使用 ANSI X9.143 或任何等效方法。基于前几年业界普遍认可 TR-31 的格式，因此认为支持 TR-31 的 SCD 仍然是符合规范要求的。

4. **关于 32-9 的解读，标准原文如下：**

> **32-9** The KIF must implement a physically secure room for key injection where any secret or private keys or their components/shares appear in memory outside the secure boundary of an SCD during the process of loading/injecting keys into an SCD.
>
> The secure room for key injection must include the following:
>
> - **Effective 1 January 2024,** the injection of clear-text secret or private keying material shall not be allowed for entities engaged in key injection on behalf of others. This applies to new deployments of POI v5 and higher devices. Subsequent to that date, only encrypted key injection shall be allowed for POI v5 and higher devices.
> - **Effective 1 January 2026**, the same restriction applies to entities engaged in key injection of devices for which they are the processors.
>
> ***Note:*** *This does not apply to key components entered into the keypad of a secure cryptographic device, such as a device approved against the* PCI PTS POI Security Requirements. *It does apply to all other methods of loading of clear-text keying material for POI v5 and higher devices.*

结合 PCI PIN 的 Technical FAQ 中对该要求的答疑，有以下解读：

- 自 2024 年 1 月 1 日起，针对新部署的 POI v5 以及更高版本设备的密钥注入，只能使用密文密钥注入的方式。该截止日期是针对代替其他支付处理机构进行密钥注入的场景。

- 自 2026 年 1 月 1 日起，以上同样的限制生效于支付处理机构自身进行密钥注入的场景。

- 对于 POI v4 及更早版本的设备，将继续允许将明文密钥注入设备，直到支付品牌强制要求停止使用任何此类设备。

- 对于针对那些在 2024 年 1 月 1 日前已经部署的 POI v5 设备，并且该设备不满足密文密钥注入的功能要求的，如果是次要版本更新，该设备可以继续不满足密文密钥注入的功能要求。如果是主要版本更新部署到设备上，则必须将密文密钥注入的功能更新进该设备。

- 针对现有商家已部署的 POI v5 或以上的设备，如果该设备尚不支持密文密钥注入，也尚未对其软件进行必要更新以支持加密密钥加载，则仍然可以使用非加密方法进行明

文密钥注入。如果服务提供商在新商家/合法实体合作时或现有商家进行主要软件更新时，展示出 POI v5 及更高版本设备的加密密钥加载能力，则视为满足标准 32-9 的要求。此外，QPA 必须在 PIN 的 ROC 报告中写明相关加密密钥加载的解决方案。

- 对于先前部署的设备进行维修或类似更换，以及扩展现有部署等场景，仍然可以使用明文密钥注入的方案。对于新的商家或实体，不允许采用明文密钥加载的方案。

二、 行业重要信息分享

除了 PCI PIN 标准本身的解读，在此也更新行业内的两个重要信息。

1. MPOC 标准中提出 PCI PIN 的相关需求

在 PCI 标委会发布的 MPOC 标准中说明，如果 MPOC 所使用的 Back-end system 涉及了 PIN 数据处理或 PIN 加密密钥管理，那么该系统必须符合 PCI PIN 的安全要求。原文如下：

5A-3 Security of Back-end Systems

Back-end environments used as part of an MPoC Solution are secure and maintained in compliance with relevant standards or requirements.

Security Requirements	Test Requirements	Guidance
Objective: Back-end environment are implemented and operated securely and in ways that maintain compliance to other applicable standards.		
5A-3.1 Environments that store, process, or transmit account data must comply with the requirements of PCI DSS.	**5A-3.1.a** The tester must confirm through examination that a valid Attestation of Compliance (AOC) outlining compliance of any environment within the MPoC Solution that stores, processes, or transmits account data with the PCI DSS requirements.	Environments that are PCI DSS compliant demonstrate that the minimum set of industry-expected security controls have been applied to that environment, which reduces risk compared to environments that do not apply security controls. This includes any payment processing backends directly implemented by the MPoC Solution, or where there is the ability for the MPoC Solution systems to have access to cleartext account data, or the cryptographic keys that can be used to decrypt any encrypted account data.
5A-3.2 Environments performing PIN processing, or manage PIN related cryptographic keys, must comply with the requirements of PCI PIN.	**5A-3.2.a** The tester must confirm through examination that a valid AOC outlining compliance of any PCI PIN-processing environment included in the MPoC Solution exists and is current and up to date with the features provided. **5A-3.2.b** The tester must confirm through examination that the key-loading facilities used for any PCI PTS devices implemented in the MPoC Solution are included in the PCI PIN compliance scope.	Environments that are PCI PIN compliant demonstrate that the minimum set of industry-expected security controls have been applied to that environment, which reduces risk compared to environments that do not apply security controls. Specific non-compliances raised as part of PCI PIN validation, due to the use of an MPoC Solution, need to be considered when assessing this requirement.
5A-3.3 All remote kernel environments implemented by the solution must comply with PCI DSS requirements.	**5A-3.3.a** The tester must confirm through examination that a valid Attestation of Compliance (AoC) outlining compliance of the remote kernel environment(s) with the PCI DSS requirements. This AOC must cover the scope of the remote kernel processing environment.	Environments that are PCI DSS compliant demonstrate that the minimum set of industry-expected security controls have been applied to that environment, which reduces risk compared to environments that do not apply security controls.

2. Visa PIN 安全体系的完结（Sunset）

2023 年 8 月 1 日，VISA 发布声明“Visa PIN Security Program Will Be Sunset”，宣布了自 2023 年 10 月 1 日起，Visa 取消 Visa PIN 安全计划“Visa PIN Security Program Guide”，并且不再主动验证 PCI PIN 安全要求。需要强调的是，Visa 更新合规计划的决定并不是对 PCI PIN 标准重视程度的降低。Visa 作为卡品牌之一，不再单独提出详细的 PIN 安全计划，更多的是从整体产业提出相关安全合规要求，比如产业监管机构、各个收单机构或者合作机构，以及 PCI 安全标准委员会。产业机构应一如既往达到相关标准合规，从而呈现 PIN 处理的安全性。

客户、处理商和服务提供商仍需要按照产业相关机构的要求和最佳实践遵守 PCI PIN 安全要求。PCI PIN 安全合规性证明需要合格的 PIN 评估员 (QPA)来测试和评估要求和控制，并且应至少每 2 年进行一次。请查看 Visa PIN 安全计划更新备忘录以了解更多详细信息。参考链接为：Visa PIN Security Program Update Memo。

附录：参考文档和链接

1 PIN Security Requirements and Testing Procedures v3.1: https://docs-prv.pcisecuritystandards.org/PIN/Standard/PCI_PIN_Security_Requirements_Testing_v3_1.pdf

2 PTS PIN Technical Frequently Asked Questions v3.0: https://docs-prv.pcisecuritystandards.org/PIN/Frequently%20Asked%20Questions%20(FAQ)/PCI_PIN_Technical_FAQs_v3_December_2023.pdf

3 PIN Security Rqmt 18-3 Key Blocks Information Supplement：https://docs-prv.pcisecuritystandards.org/PIN/Supporting%20Document/PIN_Security_Rqmt_18-3_Key_Blocks_2022_v1.1.pdf

4 Visa PIN Security Program Update：https://usa.visa.com/content/dam/VCOM/global/partner-with-us/documents/visa-pin-program-memo.pdf

5 Mobile Payments on COTS Security and Test Requirements v1.0.1 ： https://docs-prv.pcisecuritystandards.org/MPoC/Standard/Mobile_Payments_on_COTS-v1-0-1.pdf

6 atsec: www.atsec.cn