PCI PIN 标准近期更新及动态分享

作者：atsec 张志鹏 2025 年 2 月

关键词：PCI PIN，Technical FAQ，2024，Key Block，ISO 13491，受控环境，KMO

对于 PCI PIN 的标准本身，经常关注 atsec 的读者，应该比较熟悉，本文就不再赘述了。对于初步了解的读者，可以参考往期文章“PIN Security 的标准简介（https://www.atsec.cn/pci-pin-security-introduction/）”以及“PCI PIN 标准相关截止时间的解读以及近期重要信息（https://www.atsec.cn/pci-pin-share/）”。

随着支付产业内的技术发展，PCI PIN 标准一直在动态地演进。在 2024 年里，PCI 标委会通过更新 Technical FAQ 文档以及定期召开 QPA 网络研讨会的方式，对出现的新技术方案提出了相应安全要求，对实际评估过程中遇到的具体问题做了相关澄清和解读。笔者将会从如下几个方面来和大家分享相关的更新。

1 Key Block 相关技术问答的解读

1.1 根据 PCI 标委会最新的更新，符合要求的 Key Block 方法有如下几种：

1) 对于使用对称技术存储和分发对称密钥的情况，以下的方法是符合要求的：

- 如果密钥和敏感属性字段使用 AES 加密，则可以使用 ISO 20038、ANSI X9.143 中的方法或 ISO/IEC 19772 的机制 2 中的方法。
- 如果密钥和敏感属性字段使用 TDES 加密，则可以使用 ANSI X9.143 中的方法或 ANSI X9.102 中的 TDKW 方法。

2) 对于使用非对称技术存储和分发对称密钥的情况，以下的方法是符合要求的：

- ASC X9 TR-34。
- 至少要使用 RSA OAEP 算法对对称密钥进行加密，并对加密后的密钥和下面第 3）条中指定的敏感属性字段进行 RSA 签名，以允许密钥接收方 KRD（Key Receiving Device）验证密钥分发方 KDH（Key Distribution Host）的身份。
- 使用 ECDH（Elliptic Curve Diffie-Hellman）协议计算出一个共享密钥，使用 ECDH 协议派生出共享密钥，然后使用此共享密钥对目标密钥做对称加密，并对加密后的密钥和下面第 3）条中指定的敏感属性字段进行 ECDSA（Elliptic Curve Digital Signature Algorithm）签名。

3) 如果其他对称或非对称加密方法未在上面第 1）条和第 2）条中列出，但已经根据 PCI HSM 和 POI 技术常见问题解答中定义的标准（参见 PTS HSM Technical Frequently Asked Questions 和 PTS POI Technical Frequently Asked Questions）被验证为等效，并在该设备的 PCI 批准列表中的“附加信息”中注明，这些方法也可以满足该要求的意图。Key block 中定义了敏感属性字段，通过这些属性可以限制密钥的使用范围，避免滥用或错误使用。所有符合要求的方法必须至少包括以下敏感属性：

- 用于定义预期用途的若干属性，用于限定密钥可以执行的操作。
- 用于定义密钥可以使用的加密算法和操作模式的若干属性。

- 用于定义可导出性的若干属性，即定义受保护的密钥是否可以转移到密钥所在的加密域之外。
- 对加密密钥和敏感属性的身份验证字段（即 MAC（Message Authentication Code）、数字签名或经过身份验证的加密）。

此外，随着行业持续迁移 POI 和 HSM 基础设施，在未来的标准中，对新部署的设备将要求密钥长度混淆填充到算法的最大长度，例如 TDEA 为 192 位，AES 为 256 位。

1.2 在 PCI PIN 标准中定义了关于 Key Block 要求的实施截止日期，可以参考 atsec 往期文章“PCI PIN 标准相关截止时间的解读以及近期重要信息分享（https://www.atsec.cn/pci-pin-share/）”，这并不意味着所有以前建立的密钥都必须更改。所有以前建立的密钥仍然可以使用。在实施截止日期后，密钥块交换密钥（例如，X9.143 密钥块保护密钥（KBPK，Key Block Protection Key），TR34 非对称密钥封装密钥等）必须被建立，以用于加密封装所有的被传输密钥。关于目前用于加密对称密钥的密钥（KEK，Key-encrypting Key）并不强制要求用新的 KBPK 来替换现有的 KEK。如果您的 HSM 或 POI 厂商具有能力支持将现有的 KEK 直接转换为 KBPK 使用，或者您拥有 KEK 的组件来重新创建它作为 KBPK，那么，您可以直接使用现有的 KEK 作为 KBPK。或者您拥有组件或份额来重新创建它作为 KBPK。

1.3 根据 Key Block 第 3 阶段要求，自 2025 年 1 月 1 起，对所有商户主机、销售点（POS）设备和自动取款机实施 Key Block 封装方案。但这并不会影响在该日期之前存在的 POI（POS 和 ATM）设备的部署。对于市场上存量的 POI 设备无需强制转换为使用 Key block，但可选择这样去做。对于新部署的设备，必须对密钥传输和存储实现 Key Block 的封装方式。例如：1）通过本地密钥注入实现 MK/SK（主密钥/会话密钥）密钥管理方案时，设备内必须建立 KBPK（密钥块保护密钥）以支持 X9.143 Key block 的封装，用于后续定期远程更新会话密钥。2）非对称方法（例如 TR-34）可用于远程初始密钥的建立。

1.4 对称密钥在存储或传输时必须使用 Key block 结构进行封装管理。但是，对于直接从密钥加载设备（KLD）经过直连线将对称密钥到注入 POI 或 HSM 设备的情况，该要求并不适用。也就是说，在这种情况下，不需要对密钥做 Key block 封装。但对 POI v5 以上的设备还是需要进行加密传输的。需要说明的是，该要求仅适用于加密存储在 SCD 的篡改保护边界之外的对称密钥和非对称私有密钥，包括：1) 存储在交易主机上，2) 在 KIF 中，或 3) 在 POI 设备的非安全内存中。此外，在受控环境（ISO 13491 定义的受控环境或要求 32-9 中定义的安全环境）以外，通过网络连接传输加密密钥（对称密钥和非对称私有密钥）的情况，必须使用 Key block 封装。如果密钥材料处于受控或安全环境中，则可以在不使用 Key block 封装的情况下对密钥材料进行加密。

请注意，不允许使用非 SCD 键盘输入明文密钥材料。此外，无论设备如何连接，密钥材料在从 SCD 键盘传输到 KLD 时都必须加密。

2 关于 32-9 中定义的 KIF 安全房和 ISO 13491-2 中定义的受控环境

对于什么场景需要实施 KIF 安全房，什么场景需要实施 ISO 13491-2 中定义的受控环境，标准给出了更多的明确要求。

2.1　从 PCI PIN 的标准要求 13-9 和 32-9 中可以看出，明文密钥/密钥组件注入的过程被明确禁止。那么带来一个问题，32-9 中定义的 KIF 安全房的目的就是要预防明文密钥/密钥组件出现在 SCD 设备以外内存中所带来的风险。如果现在整套密钥注入方案中都不涉及明文密钥/密钥组件出现在 SCD 设备以外内存中的情况，那么是否还有必要搭建 32-9 中定义的 KIF 安全房呢？答案是不必要强制搭建 32-9 中定义的 KIF 安全房。但是对于那些仅仅在生产线上执行未经身份验证的加密密钥注入的 KIF/工厂/维修中心，其物理环境至少要满足 ISO-13491-2 标准中定义的受控环境。如果涉及注入明文密钥或明文密钥组件时，才需要要求 32-9 中定义的安全环境。

请注意，受控环境仍然需要物理上的进/出控制（门和门禁控制）以及其他几个要求（参见 ISO 13491-2），但不需要满足双人占用（即禁止环境内只由一人占用）的要求。如果可以保证生成 Key block 的系统在受控环境中运行，则 POI 也可以在非受控环境（ISO 13491-2）中使用经过身份验证的 Key block 进行注入。

2.2　什么情况下可以在 32-9 定义的安全房以外手动（手写的方式）记录生成的关键组件？

当满足以下条件，并且不存在其他兼容的通信方式（如智能卡）时，可以在要求 32-9 中定义的 KIF 安全房以外生成并手动记录密钥分量/组件，以便与其他组织建立共享密钥。

- 仅使用经过认证的安全加密设备（SCD），例如 PCI 或 FIPS 140-2/3 认证的 HSM 或密钥加载设备（KLD），且密钥分量不得以明文形式出现在 SCD 或硬件管理设备（HMD）之外的内存中。
- 过程需在 ISO 13491-2 定义的受控或更高级别的环境中进行。
- 必须遵守双重控制与知识分割原则。
- 监控摄像头不得拍摄明文密钥材料、密码组合锁、PIN 键盘或键盘；否则，密钥保管人员应通过身体遮挡视线。
- 遵守标准中其他相关密钥生成的要求（如要求 6-1）。

2.3　PCI PIN 标准 32-9 中，详细阐述了对 KIF 安全房的安全要求，如需了解详情请参考标准原文“PIN Security Requirements and Testing Procedures v3.1”。在技术问答文档中，多次提及了 ISO 13491-2 定义的受控环境或更高级别的环境，这里做一个简单介绍：ISO 13491-2 中按照安全性由低到高的顺序，定义了四种物理环境，分别是：非受控环境，最小受控环境，受控环境和安全环境。以下是针对受控环境的基本要求：

- 环境入口处设有门锁或监控，仅允许被授权人员进入环境。访客必须由被授权人员陪同进入。
- 必须记录所有访客的访问行为，且访问记录应安全保存并进行定期审查。
- 始终有至少两名被授权人员对关键设备进行持续监视。使用视频摄像头持续监视关键设备。应注意摄像系统的安装要保证不形成偷窥的可能性。
- 所有供人员或设备通过的出入口均应被持续监视。设备进出必须有书面授权。
- 除了受监控的出入口外，没有其他任何途径（比如地板下或天花板上）可以不经授权地进入受控环境，或将设备移进/移出。

3 近期发布的其他技术问答

3.1 对于硬件管理设备（HMD），例如智能卡，在密钥管理方面不能等同于安全加密设备（SCD）。根据 ISO 13491 中的说明，HMD 不被视为等同于 SCD，因为 HMD 是一种非安全加密设备（NSCD），通常是一种专用集成电路卡 ICC（Integrated Circuit Card），具有类似于 SCD 的安全功能，但缺乏篡改响应处理能力。如 ISO 11568 所述，明文密钥组件和分量既包括书面形式，也包括存储在 HMD 中的组件和分量，无论该组件或分量是否在 HMD 或类似设备中加密。因此，PCI PIN 标准中对明文密钥组件和分量的安全要求同样适用于使用 HMD 管理的组件和分量。

3.2 对于已经超过了认证有效期的 PCI PTS 批准的 EPP（Encrypting PIN Pad）、PED（PIN Entry Device）和 SCRP（Secure Card Reader PIN），仍然可以继续使用。前提是，在部署该设备那一刻，该设备仍在 PCI PTS 认证有效期内。然而，在该设备已经超过了认证有效期之后，新的部署（即额外的设备）是被禁止的，除非是替换现有部署的同类设备，如更换坏旧设备。

3.3 超过了认证有效期的 PIN 接受设备（包括 EPP、PED 和 SCRP），在一定条件下可以作为 PCI PIN 评估所认可的设备。在认证到期之前部署的 PIN 接受设备在认证到期后的 10 年内可以作为 PCI PIN 认可的设备。超过该时间长度后继续使用认证过期的 PIN 接受设备，可能会使相关机构承担由于设备在“认证过期”后使用而导致的任何安全漏洞的责任风险。

3.4 在 PCI PIN 的评估过程中，经常会遇到 KIF 厂商自身是符合最小密钥强度的规定（PCI PIN Annex C 中的规定），但是对接的收单机构或商户要求 KIF 厂商向其 POI 设备注入比规定更弱的密钥。这时，作为 KIF 厂商也是可以符合 PIN 安全要求的。前提是 KIF 厂商向评估员证明其具备注入强加密算法密钥的能力。如果弱密钥是根据收单机构的明确要求注入的，则这些密钥的责任由收单机构承担。KIF 厂商必须保留收单机构关于此请求的文件。此外，评估员必须在 PIN ROC 中列出所有 KIF 厂商为其注入了弱密钥的机构。

3.5 在使用非对称技术分发对称密钥时，KDH 不可以使用 KRD 的公钥直接对交易密钥（如 IPEK- Initial PIN Encryption Key 或 TMK- Terminal Master Key）进行加密。如 TR-34 所述，KRD 的公钥应用于加密临时对称封装密钥，该密钥用于加密交易密钥。TR-34 将交易密钥数据、交易密钥使用细节和签名身份包含在加密数据部分中，然后用 KDH 签名密钥对整个加密结构进行签名，以确保 KDH 和 KRD 之间所有数据的认证。对于不符合 TR-34 的实现，必须要考虑按照标准认可的 Key block 封装方法对交易密钥进行加密封装，并使用来自 KDH 的签名私钥对加密的交易密钥以及密钥使用属性进行签名。标准认可的 Key block 封装方法参照本文的第 2.1 节。

4 标委会针对密钥管理的发展动向。

根据 PCI 标委会对支付安全标准的发展计划，新的标准 KMO（Key Management Operations）正在规划和制定中。该标准将结合相关产业标准且专注于密钥管理的安全要求，为产业已有标准（如 PCI PIN 和 P2PE 等）起到积极和推动的作用。atsec 作为 PCI PIN 和 P2PE 评估机构以及 FIPS 140-2/3 测评机构，将持续跟踪 PCI 标准体系的演进动态，为产业合规提供专业技术支持。

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_2024.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 atsec: https://www.atsec.cn/