针对云加密机 PCI PIN 标准要求及其实践

作者：atsec 张志鹏 2025 年 1 月

关键词：PCI PIN，Technical FAQ，HSM as a Service，云加密机，多租户

近年来，随着云计算技术的深入应用，多家云服务提供商和加密机制造商推出了“HSM as a Service”的服务，通常也会被称为云加密机服务。其带来的便利性和灵活性吸引着越来越多支付行业内的厂商（包括支付交易处理厂商，终端制造商等）考虑使用“HSM as a Service”方案来实现 PIN 交易系统、密钥注入系统等。

厂商在利用这些优势的同时，一定要清楚的意识到此类“HSM as a Service”服务是由云加密机提供商面向多租户提供的云加密机服务，在 PCI PIN 合规过程中要满足额外安全要求点。如果一个厂商在 PCI PIN 合规过程中使用到了云加密机服务，那么关于加密机部分的 PCI PIN 合规工作就需要由云加密机提供商和云加密机使用者共同协作完成。这个场景非常类似于云租户利用公有云服务搭建一个符合 PCI DSS 要求的支付系统。合规的思路也是一致的，一部分安全要求点由云加密机提供商作为 TPSP（Third-Party Service Provider）来负责完成，如：作为多租户云加密机要保证租户之间的完全隔离性、加密机硬件设备本身的生命周期管理流程、确保加密机是在 FIPS 140-2/3 或 PCI-PTS HSM 认证有效期内的设备、加密机所在物理环境本身的安全要求、由云加密机提供商管理的密钥/密钥组件的安全管理流程、云加密机提供商对加密机逻辑访问控制、由云加密机提供商管理的加密机 HMD（Hardware Management Device，例如智能卡）的安全管理、支持符合要求的 Key block 格式等等。其他所有的安全要求点由云加密机使用者来负责完成，如：云机密机的日常使用流程、对云加密机访问权限控制流程、方案中确保没有明文密钥和密钥组件出现在 SCD（Secure Cryptographic Device）设备以外的内存、以及其他所有云加密机提供商责任范围以外的安全要求点。因此，以下是针对云加密机提供商以及云加密机使用者两个角度来解读 PCI 标委会发布的相关 FAQ 技术问答以及评估方法。

1 对于云加密机提供商

云加密机提供商提供的多租户云加密机服务在 PCI PIN 评估中，需要注意以下几点要求：

提供多租户（即同时多个组织使用）HSM 服务的服务提供商禁止在租户之间使用共享的对称密钥或非对称密钥的私钥。针对那些用于支持每个 HSM 租户（客户）并且由 HSM 服务提供商管理或拥有的密钥，必须为每个 HSM 租户分配唯一的密钥。但对于那些用于 HSM 虚拟化系统的密钥（例如，设备认证密钥、固件完整性密钥等），该要求并不适用。

1.1 提供多租户 HSM 服务的提供商禁止在不同的 HSM 实例上使用相同的本地主密钥/主文件密钥（“Local Master Key”或“Master File Key”）。当提供多租户 HSM 服务时，不由 HSM 租户直接拥有或管理的 “主密钥/存储密钥” 在每个 HSM 实例中必须是唯一的。除非该租户实例集群是明确指派用于负载平衡或热备份的目的，才可以出现多个 HSM 实例使用相同的主密钥/存储密钥。

1.2 针对多租户 HSM 的额外要求。为多个租户提供加密密钥存储和操作的云加密机提供商必须使用具有多租户功能的加密机以及程序化的控制措施，来确保满足以下要求：

- 任何一个租户的密钥层次结构中的任何密钥泄露都不会影响其他租户的加密密钥的安

全性。

- 任何一个租户的加密密钥不能被其他租户以任何方式加载、删除、访问、或用于加解密操作处理。
- HSM 租户必须能够查询 HSM 配置以确定设置是否符合 PCI PIN 要求。如果要对设置进行变更，首先确认该变更是否可能对 PCI PIN 的合规要求造成影响。如果可能有影响，必须在变更之前，将该变更通知到 HSM 租户。
- 云加密机提供商必须始终满足所有相关的 PCI PIN 要求。

1.3 不同的云加密机提供商的解决方案是不一样的。因此，HSM 实例对加密密钥材料的保护方式也是不同的。云加密机提供商可能采用的两种（但不限于）解决方案如下：

- 解决方案 1：在单个物理 HSM 设备中实现两个或多个虚拟 HSM，每个虚拟 HSM 都拥有其独立的防篡改密钥，例如由 HSM 租户控制的主密钥/存储密钥；
- 解决方案 2：通过某种实现方式，HSM 设备将 HSM 租户的主密钥以加密形式存储在更高级别的防篡改密钥下，类似于工作密钥本身以加密形式存储在 HSM 租户的主密钥下的方式。

无论采用哪种实现方式，保护用户密钥所有权和安全性的要求依然适用，并且任何 HSM 防篡改密钥（无论是否由用户直接管理）都应是每个 HSM 唯一的，且不得导致其保护的用户密钥被暴露或未经授权使用。

1.4 云 HSM 硬件设备中的一个逻辑隔离区域，一般称作一个租户分区。云加密机提供商（HSM 拥有者）在将分区移交给租户的过程中，云加密机提供商必须具备并遵循的流程包括：

- 需要使用密码学意义上的解耦功能：通过密码学技术将 HSM 分区的管理权从服务提供商转移到租户。初始情况下，服务提供商拥有分区的管理权。通过解耦功能确保服务提供商无法访问或控制租户的分区管理密钥。分区的控制权（如密钥创建、分区操作权限）只属于租户。即使服务提供商拥有对云 HSM 硬件设备的物理访问权，也无法干预租户的分区管理。
- 确保分区清洁：确保分配给租户的分区不包含云加密机提供商的先前租户的任何密钥或痕迹，除了默认的管理密钥（用于租户初始化），且这些默认密钥必须在初始化过程中被新租户定义的密钥所替换。
- 限制云加密机提供商的操作权限：确保云加密机提供商在租户分区上仅允许执行暂停或终止分区的操作。请注意，具体流程的细节可能因 HSM 平台供应商和/或型号（包括固件版本）的不同而有所变化。

1.5 在终止一个租户分区的过程中，云加密机提供商必须执行哪些程序？对于租户分区的终止，云加密机提供商必须制定并遵循的书面程序包括，确保完全擦除密钥材料、终止租户对该分区的管理访问和配置的能力。这些文件化的程序必须规定关键材料的销毁速度，无论是立即销毁还是在合同规定的销毁时间表内销毁，并确保向租户传达销毁通知。此外，当租户关系终止时，该租户拥有的所有实例上的所有密钥（例如，在备份或外部存储中）都应被安全地销毁/擦除。在所有情况下，分区的安全日志文件应在终止后继续保留。根据服务协议，谁负责分区内的密钥管理活动，就由谁来维护终止后的安全日志。负责维护日志的租户可以将此日志维护责任委托给云加密机提供商。

1.6 当租户使用云加密机时，经常会使用远程（非控制台）连接将密钥远程加载到 HSM 上。针对这种情况，标准有以下额外要求：

- 对称密钥、私钥以及密钥组件必须以确保其保密性和完整性的方式运输。如使用 Key block 方式对密钥进行加密封装。
- 所有加密密钥（包括公钥），都必须保证其真实性。例如使用可信证书做签名。
- 使用公钥技术远程（非控制台）加载的加密密钥不能依赖于未认证的公钥或在密钥协议过程中建立的不保证密钥真实性的密钥。对于远程连接需要安全通道，但该安全通道不能作为提供机密性或真实性控制机制的方法。

从上面的要求可以看出，当通过远程方式将对称密钥、私钥以及密钥组件加载到 HSM 中时，需要对密钥、密钥组件本身做保密性和完整性等保护，根据 PCI PIN 标准的要求，此类密码学运算必须由 SCD 设备（比如 KLD（Key-Loading Device））来完成，再通过安全通道将密钥远程加载到 HSM 中。在行业实践中，经常会出现使用 KLD 设备来配合云加密机服务的方案。这样才可以保证在 SCD 设备以外的内存中不存在明文的密钥材料（对称密钥、私钥以及密钥组件），才能符合 PCI PIN 的标准要求。因此，作为云加密机提供商，需要考虑支持相关的接口方案，比如提供可信公钥，支持 TR-34 封装的密钥导入等等。

1.7 云加密机提供商也可以使用第三方托管的数据中心设施来容纳 HSM 设备。但是前提是必须满足以下条件：

- 云加密机提供商必须控制所有逻辑访问。数据中心运营人员不得对 HSM 拥有任何逻辑访问权限（管理员或操作员）。
- 云提供商必须适当放置符合 PIN 要求 Annex B 32-9.7 的闭路电视摄像头，并将图像发送到云提供商控制的服务器，该服务器位于托管 HSM 的数据中心以外的地点，例如云提供商自己的地点。
- 访问容纳云提供商 HSM 和/或外围设备（如防火墙）的机柜必须是：
  - 由云加密机提供商员工直接控制，通过徽章或同等方式进行双重控制；或
  - 在需要物理访问的情况下，仅限于通过徽章或等效机制双重控制的已知预先授权的数据中心员工，才可以访问机柜。在任何访问期间，始终监控对设备机柜的访问，监控活动包括以下内容：
    - 在特定时间窗口内，为批准的目的做访问授权，
    - 在访问时和访问期间，验证数据中心员工的身份，以及

- 监控在维护窗口期间内的所有活动。

2 针对云加密机使用者

如果一个云加密机服务的使用者（租户）要通过 PCI PIN 的评估，租户有责任确保选择或合作的云加密机提供商满足有关 HSM 管理的所有适用要求。那么，在 PCI PIN 的评估中，租户和云加密机提供商，二者的责任又应该如何分配？基于 atsec 作为独立第三方 PCI PIN 的评估机构的经验，当云加密机提供商作为 TPSP 参与到被评估者的审核时，通常有二种情况。一是云加密机提供商本身通过了 PCI PIN 评估，二是云加密机提供商本身未通过 PCI PIN 评估。

2.1 云加密机提供商本身已经通过了 PCI PIN 评估

这种情况下，评估者会承认云加密机提供商 PCI PIN 评估的结果，并且检查租户使用的相关云加密机的服务是否都覆盖在了这个评估范围之内。此时，需要云加密机提供商配合提供的材料包括：

- PCI PIN 的合规证明（AOC，Attestation of Compliance）：针对该云加密机服务产品，云加密机提供商有责任向租户提供在有效期内（二年以内）的 PCI PIN 的合规证明（AOC）。
- PCI PIN 合规责任的归属说明：在 PCI DSS 的标准中明确提及了多租户的服务提供商应该提供合规责任矩阵来明确划分合规责任的归属。虽然 PCI PIN 标准目前并没有对此做明确的规定，但是根据 PCI DSS 的标准思路，建议可以提供此类的官方材料来说明合规责任的归属。
- 云加密机服务的产品使用手册：为租户提供此类文档以说明如何配置和使用云加密机服务才能符合 PCI PIN 的要求。防止租户在不知晓的情况下，不安全使用云加密机服务。

此外，租户应该定期检查云加密机提供商的 PCI PIN 的 AOC 文档的有效性，并考虑此 PCI PIN 评估范围是否覆盖了租户需要的所有产品功能。在配置和使用云加密机产品时，应该遵循 PCI PIN 的相关标准要求。在基于云加密机设计整体方案时，应该保证密钥的保密性、完整性和真实性。

2.2 云加密机提供商本身未通过 PCI PIN 评估

这种情况下，评估者会把云加密机提供商也纳入到 PCI PIN 评估中。这时云加密机提供商需要配合评估员的访谈、观察、取证等工作。所有关于云加密机的技术实现，人员管理，和安全策略流程都会被全面评估。

2.3 针对常见的业务场景适用性的思考

适用于 PCI PIN 评估的常见业务场景包括 PIN Transaction Processing Operations，RKD（Remote Key Distribution），LKI（Local Key Injection），CA/RA（Certification and Registration Authority Operations）。这几个场景是否都适合使用云加密机服务来实现其中的密钥管理呢？笔者根据审核实践，给出以下的分析。

- PIN Transaction：在制定合理的系统设计方案的基础上，是可以使用云加密机来满足 PCI PIN 标准中提到的安全要求点。系统设计方案一定保证在 SCD 设备以外的内存中

不存在明文的密钥材料（对称密钥、私钥以及密钥组件）。比如，需要考虑如何将收单机构的明文密钥组件以安全的方式加载到云加密机中。通常会涉及在本地使用 KLD 设备参与明文密钥组件的合成以及相关密钥加解密工作。

- RKD：请注意，这里的 RKD 方案并不包括 CARA 部分，只是针对 Annex A1 的部分。也就是针对已经下载好凭证（如可信证书）的 POI 设备做远程密钥分发的方案。对于这类 RKD 方案，其结论和要求与 PIN Transaction 是类似的。在制定合理的系统设计方案的基础上，是可以使用云加密机来满足 PCI PIN 标准中提到的安全要求点。
- CA/RA:如果租户想使用云加密机服务结合云主机或云平台以外的主机来实现一套 CARA 中心，要满足 PCI PIN 标准是不可行的或难度极大的。原因是在 PCI PIN 标准 Annex A2 中对很多关键操作要求必须是离线操作（包括对离线证书签发操作以及 CA 应用软件的离线更新等）。这些离线操作以及相关的系统组件（Offline CA HSM，Online CA HSM，防火墙，服务器，数据库等）需要放在离线的 CA 安全房（Annex A2 32-2 中定义的安全房）中进行的。这和云加密机本身的灵活性和远程执行的特点也是不一致的。因此不建议使用云加密机来搭建满足 PCI PIN 标准要求的 CA/RA 中心。
- LKI：不适用，因为本地密钥注入的方案指的就是在 KIF 设施以内实施，注入密钥设备和被注入设备在同一个地点通过线缆直连的方式进行密钥注入。这和云加密机远程执行的特点是相矛盾的。

3 总结

综上所述，使用面向多租户的云加密机服务来实现密钥管理方案是可行的。前提是云加密机提供商自身环境以及其使用者的环境都必须满足 PCI PIN 的安全要求。多租户的云加密机服务带来的隔离问题（包括租户间隔离以及提供商和租户之间的隔离）以及远程管理使用加密机的问题，是需要重点关注的。在 PCI PIN 的评估中，云加密机提供商和云加密机使用方各自的合规责任需要明晰，双方共同配合来完成完整的合规评估。另外，在不同的业务场景中，需要具体分析是否适合使用云加密机来实现密钥管理方案，并且要制定合理的设计方案。

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. atsec: www.atsec.cn