PCI 3DS 技术常见问题解答（FAQ）简介

atsec 陈谨运 2023 年 9 月

关键词：技术 FAQ、PCI 3DS、EMV® 3DS、3DS server、ACS、DS、无卡交易（CNP）

1 PCI 3DS 标准简介

为了降低交易欺诈风险，Visa Inc.于 2001 年开发并推出了 3-D Secure（3DS）V1.0 协议。3DS 协议对无卡交易（CNP：card-not-present）电子商务购买过程启用了安全身份验证，以达到降低欺诈交易的风险。3DS 的安全身份验证协议基于三域模型作为协议核心基础，3DS 包含的三个域分别是发卡域、商户/收单域和交互域，详细信息如下：

- 发卡域
  - 持卡人和消费者设备
  - 访问控制服务器（ACS：Access Control Server）
  - 发卡机构（Issuer）
- 商户/收单域
  - 3DS 请求者（3DS Requester）
  - 3DS 客户（3DS Client）
  - 3DS 服务器（3DS Server）
- 交互域
  - 目录服务器（DS：Directory Server）
  - 目录服务器证书颁发机构 （DS-CA：Directory Server Certificate Authority）
  - 授权系统（Authorisation System）

其中收单域和发卡域通过交互域连接，目的是在电子商务交易期间对持卡人进行身份验证或提供身份验证和账户确认。这些额外的安全防护有助于防止未经授权的 CNP 交易，并保护商家免受 CNP 欺诈。随着标准的不断发展和完善，当前最新的协议版本是 3DS V2.3.0。目前 3DS 协议参与的卡品牌包括 American Express、Discover、JCB、Mastercard、UnionPay 和 VISA。

3DS 协议层面的实现由 EMV®维护的文档“EMVCo_3DS_Protocol and Core Functions Specification”和“EMVCo_3DS_SDK Specification”进行定义，而实现 3DS 协议的应用程序所在环境的安全性则通过 PCI SSC（Payment Card Industry Security Standards Council）维护的 PCI 3DS 核心安全标准来保护。从下图我们可以清楚的了解到 PCI 3DS 核心安全标准关注的 3DS 对象主要包括：3DS server、ACS 和 DS。

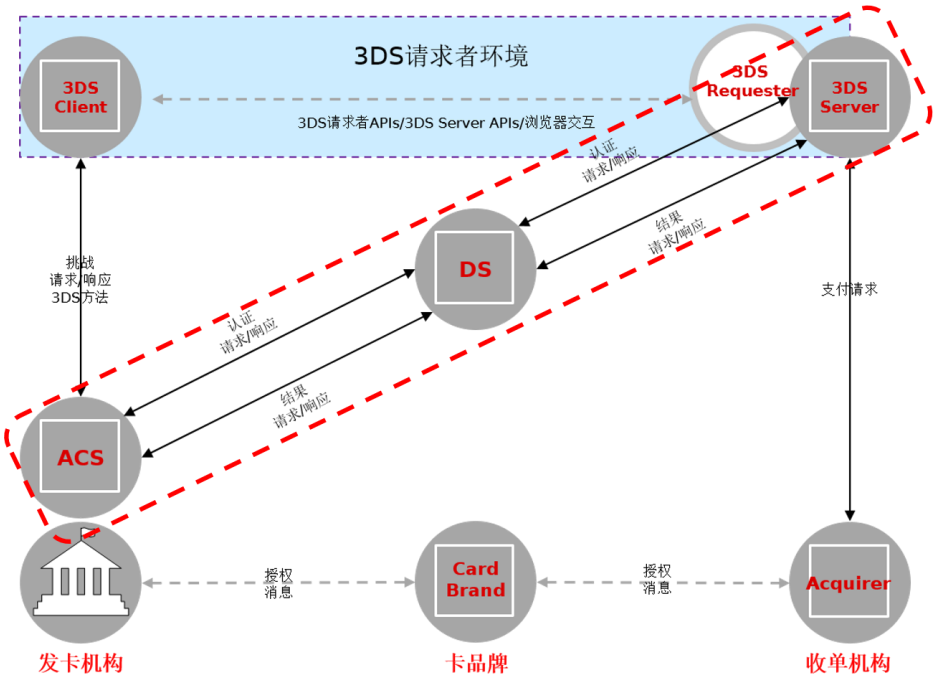

图 1：PCI 3DS 核心标准关注的 EMV® 3DS 对象

2 PCI SSC 维护的 PCI 3DS 标准

PCI SSC 维护了 3DS 协议运行环境相关的安全标准要求和报告模板，并负责授权 PCI 3DS 核心安全标准相关的评估机构和评估人员，以下是 PCI SSC 维护的与 3DS 相关的安全标准：

- PCI 3DS Core Security Standard—重点关注特定 3DS 功能及其所处环境需要注意的安全控制要求。
- PCI 3DS Data Matrix—PCI 3DS 数据矩阵，该文档列举了 3DS 交易过程中被定义为敏感数据的数据元素列表。
- PCI 3DS SDK Security Standard—重点关注 3DS SDK 实施过程需要注意的安全控制要求。

PCI 3DS 核心安全标准分为两个部分。第一部分是用于保护 3DS 数据环境（3DE：3DS Data Environment）的技术和操作安全控制的基线要求。如果机构的 3DE 环境已经完整实现了 PCI DSS 的合规评估，可以采用 PCI DSS 评估结果支持 PCI 3DS 第一部分要求的验证。

- 维护所有人员的安全策略
- 安全网络连接
- 开发和维护安全系统
- 脆弱性管理
- 管理访问
- 物理安全
- 事件响应准备

PCI 3DS 要求的第二部分是 3DS 安全要求，用于保护 3DS 数据和流程。无论机构是否已经 PCI DSS 合规，如果机构执行 3DS 功能，则第二部分的要求必须作为评估的内容被执行。

- 验证范围
- 安全管控
- 保护 3DS 系统和应用
- 针对 3DS 系统的安全逻辑访问
- 保护 3DS 数据
- 密码和密钥管理
- 3DS 系统的物理防护

3 PCI 3DS 技术 FAQ

根据 PCI SSC 的要求，机构在执行 PCI SSC 相关标准合规或者评估的时候，除了要满足标准本身的要求以外，还需要考虑技术常见问题解答（FAQ：Frequently Asked Questions）的内容。技术 FAQ 是 PCI SSC 所维护标准不可或缺的强制性部分，在 PCI SSC 相关标准安全评估过程中必须予以考虑。技术 FAQ 可能包含有关如何解释需求的信息，在某些情况下，还可能添加新的或扩展现有的需求。对于 PCI 3DS 评估，机构除了需要符合 PCI 3DS 核心安全标准的要求，还需要考虑 PCI 3DS 技术 FAQ “3DS Core v1.x Technical FAQs”的内容。

3.1 PCI 3DS 技术 FAQ 包含的内容

PCI SSC 于 2023 年 9 月 27 日对 PCI 3DS 技术 FAQ 进行修订，当前最新版本的 PCI 3DS 技术 FAQ 包含了对如下问题的解答：

- **问题 1： 如果身份验证值（AV）是加密生成的值（例如“密码”），是否需要根据 PCI 3DS 核心要求 P2-5.4.2 对其进行加密？（2021 年 4 月发布）**

  回复：加密生成的身份验证值（AV）是否可以在不加密（再次加密）的情况下存储将取决于每个支付系统（即支付品牌）如何生成 AV 以及如何使用该值。

“EMVCo_3DS_Protocol and Core Functions Specification”并没有规定生成 AV 所需的方法或算法，并使每个支付系统能够确定使用哪种方法和/或算法。PCI 3DS 核心安全标准假设这些值是在 3DS 传输处理过程中直接使用的静态值，因此，在任何允许存储之前，必须根据 PCI 3DS 数据矩阵和 PCI 3DS 核心安全标准要求 P2-5.4.2 与其他 3DS 敏感数据一起进行加密存储。

如果 AV 是一个动态值（比如是一次性的值）在生成后不能重复使用，或者已经使用强加密算法进行了加密，并且需要在使用前对该值进行解密，则可以在允许的情况下存储该 AV 且无需再次加密。3DS 实体应联系相关的卡品牌，以获取有关该支付系统生成和使用的 AV 是否可以不需额外加密而进行存储的更多信息。

- **问题 2：哪种 3DS 组件要求使用硬件安全模块（HSM：hardware security module）保护和管理加密密钥？（2021 年 4 月发布）**

  回复：要求 P2-6 涵盖所有 3DS 组件（包括 ACS、DS 和 3DS 服务器）的加密和密钥管理。P2-6.1.2 明确指出，只有包含 DS 和/或 ACS 系统的环境才需要使用 FIPS 140-2 的 3 级（整体合规）或更高级别认证，或 PCI PTS 批准的 HSM 进行所有密钥管理活动。其他 HSM 相关要求，如要求 P2-6.2 和 P2-6.3，仅适用于 ACS 和 DS 所在的环境。

  对于只有 3DS 服务器的环境，建议但不强制使用 HSM 进行加密和密钥管理。

- **问题 3：是否可以使用补偿控制措施满足 P2-6.2.1 的要求?（2023 年 9 月发布）**

  回复：不可以。要求 P2-6.2.1 要求具有 HSM 逻辑访问权限的人员使用 HSM 控制台或使用非控制台访问解决方案来访问这些 HSM。

  然而，自 2023 年 9 月版本的技术 FAQ 发布生效后，不再专门要求非控制台 HSM 访问解决方案由独立实验室进行评估以验证是否符合 ISO 13491。

  非控制台 HSM 访问解决方案的另一组要求如下。请注意，如果完全满足以下这些要求，则可用于满足当前发布的要求 P2-6.2.1 至 P2-6.2.5。如果使用这些替代要求，请在合规报告（ROC：Report On Compliance）中针对每个相应要求记下此技术 FAQ，并包含适当的评估和文档以验证所规定的要求是否已得到满足。

  - (P2-6.2.1) Non-console HSM access for the purposes of management and configuration requires the use of MFA.
  - (P2-6.2.2) Non-console HSM access for the purposes of management and configuration is performed using a secure channel.
  - (P2-6.2.3) Secret or private cryptographic keys, key components, and/or key shares input to or output from the HSM are secured through dual control and split knowledge.
  - (P2-6.2.4) Non-console access used for the loading of clear-text key components or key shares originates from a Secure Cryptographic Device (SCD), that is either:
    - Listed on the NIST Cryptographic Module Validation Program (CMVP) list and approved to FIPS 140-2 Level 3 or 140-3 Level 3 (overall) or higher. Refer to http://csrc.nist.gov.

    或者，

    - Listed on the PCI SSC website, with a valid PCI SSC listing number, as an Approved PCI PTS Device.
  - (P2-6.2.5) When loaded through a non-console interface, key components and key shares are encrypted using a key encryption key that is specific for the purposes of key transport. Use of encryption provided by a secure channel is not sufficient to meet this requirement.

- **问题 4：3DS 实体是否可以将其 HSM 的托管和管理外包给第三方服务提供商？（2020 年 12 月发布）**

回复：可以。只要满足所有适用要求，3DS 实体可以选择将其 HSM 基础设施的托管和管理外包给第三方服务提供商。3DS 实体应与其服务提供商合作，以确定哪些要求由服务提供商负责合规，哪些要求由 3DS 实体负责合规。3DS 实体仍然最终负责确保满足有关 HSM 托管和管理的所有适用要求。相关更多信息，请参阅 PCI 3DS 核心安全标准中的“使用第三方服务提供商/外包”章节的内容。

- **问题 5：哪些类型的 3DS 组件在 PCI 3DS 核心安全标准要求 P2-7 的范围内？（2020 年 12 月发布）**

  回复：与数据中心和闭路电视（CCTV：closed circuit television）安全相关的要求 P2-7.1 和 P2-7.2 仅适用于 DS 和 ACS 系统。

  如要求 P2-7 概述部分所述，DS 和 ACS 系统是 3DS 基础设施的关键组件，需要具有更高物理安全控制的安全设施来限制、管理和监控所有物理访问。

  对于仅存在 3DS 服务器的位置，建议满足 P2-7 中的要求，但不是必需的。有关不同 3DS 组件的信息，请参阅 PCI 3DS 核心安全标准。

3.2 PCI 3DS 新增技术 FAQ 分析

PCI SSC 于 2023 年 9 月 27 日对 PCI 3DS 技术 FAQ 的更新，新增了对“**是否可以使用补偿控制措施满足 P2-6.2.1 的要求?**”问题的回复。PCI SSC 为 3DS 实体安全管理 HSM 提供额外可选的合规思路。以下是原始合规要求和可选合规要求的对比：

原始合规要求	可选合规要求
6.2.1 Personnel with logical access to HSMs must be either at the HSM console or using an HSM non-console access solution that has been evaluated by an independent laboratory to comply with the following sections of the current version of ISO 13491: ■ Annex A – Section A.2.2: Logical security characteristics. ■ Annex D – Section D.2: Logical security characteristics. (Note: The use of single DEA message authentication codes is not permitted.) ■ Annex E – Section E.2.1: Physical security characteristics, and Section E.2.2: Logical security characteristics. (Note: Only random number generators meeting the requirements ■ of SP 800-90A are allowed.) ■ Annex F – Section F.2.1: Physical security characteristics, and Section F.2.2: Logical security characteristics. ■ If digital signature functionality is provided: Annex G – Section G.2.1: General considerations, and Section G.2.2: Device management for digital signature verification.	(P2-6.2.1) Non-console HSM access for the purposes of management and configuration requires the use of MFA.
6.2.2 All non-console access to HSMs originates from a 3DE network(s).	(P2-6.2.2) Non-console HSM access for the purposes of management and configuration is performed using a secure channel.
6.2.3 Devices used to provide personnel with non-console access to HSMs are secured as	(P2-6.2.3) Secret or private cryptographic keys, key components, and/or key shares

follows: ■ Located in a designated secure area or room that is monitored at all times. ■ Locked in room/rack/cabinet/drawer/safe when not in use. ■ Physical access is restricted to authorized personnel and managed under dual control. ■ Authentication mechanisms (e.g., smart cards, dongles, etc.) for devices with non-console access are physically secured when not in use. ■ Operation of the device requires dual control and multi-factor authentication. ■ Devices have only applications and software ■ installed that are necessary. ■ Devices are verified as having up-to-date security configurations. ■ Devices cannot be connected to other networks while connected to the HSM. ■ Devices are cryptographically authenticated prior to the connection being granted access to HSM functions.	input to or output from the HSM are secured through dual control and split knowledge.
6.2.4 The loading and exporting of clear-text cryptographic keys, key components, and/or key shares to/from the HSM is not permitted over a non-console connection.	(P2-6.2.4) Non-console access used for the loading of clear-text key components or key shares originates from a Secure Cryptographic Device (SCD), that is either: ■ Listed on the NIST Cryptographic Module Validation Program (CMVP) list and approved to FIPS 140-2 Level 3 or 140-3 Level 3 (overall) or higher. Refer to http://csrc.nist.gov. or, ■ Listed on the PCI SSC website, with a valid PCI SSC listing number, as an Approved PCI PTS Device.
6.2.5 Activities performed via non-console access adhere to all other HSM and key-management requirements.	(P2-6.2.5) When loaded through a non-console interface, key components and key shares are encrypted using a key encryption key that is specific for the purposes of key transport. Use of encryption provided by a secure channel is not sufficient to meet this requirement.

原始的 PCI 3DS 核心安全要求允许 3DS 实体采用本地控制台和远程非控制台方式对 HSM 进行管理。但如果 3DS 实体采用远程非控制台的形式对 HSM 进行管理，则 HSM 的非控制台需要经过由独立的实验室根据 ISO 13491 标准进行评估。随着云环境的日益普及，对 HSM 的远程管理变得越来越重要。但对 HSM 非控制台执行额外的 ISO 13491 评估会极大的增加 3DS 实体合规的时间和经济成本。因此 PCI SSC 此时推出备选的 HSM 管理要求显得尤为重要。备选的 HSM 管理要求从如何加强认证操作人员身份（采用多因素认证方式）、采用安全通道、双人操作和知识分离方式、经过安全认证的安全加密设备（SCD：Secure

Cryptographic Device）对密钥进行操作等方面入手确保实现对 HSM 的安全管理，做到了在不降低安全要求级别的前提下，极大的减少对 3DS 实体对 HSM 的操作限制，有效的提供了 3DS 实体的操作效率。

4 结束语

随着新技术的不断出现，PCI SSC 维护的标准也在不断的演进和完善。atsec 作为 PCI SSC 授权的 PCI 3DS 评估机构和全球执行评估机构圆桌会议（GEAR: Global Executive Assessor Roundtable）的成员机构之一，从 2018 年起持续多年积极参与 GEAR 工作并贡献于产业发展，进一步致力于全球支付卡数据的安全保障。atsec 作为战略性合作伙伴，圆桌会议的成员机构将代表评估机构产业，为 PCI SSC 的计划和项目从产业、地域和技术领域提出见解。期待更多的机构参与到 PCI SSC 的参与机构，为标准和产业发展提供宝贵的意见和建议。

5 参考文档和链接

[1] Payment Card Industry 3-D Secure (PCI 3DS) Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server Technical FAQs for use with Version 1.x September 2023: https://docs-prv.pcisecuritystandards.org/3DS/Frequently%20Asked%20Questions%20(FAQ)/PCI_3DS_Core_v1.x_Technical_FAQs_Sep2023.pdf

[2] PCI 3DS Core Security Standard: https://www.pcisecuritystandards.org/documents/PCI-3DS-Core-Security-Standard-v1.pdf

[3] Payment Card Industry 3-D Secure (PCI 3DS) Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server Technical FAQs for use with Version 1.x: https://docs-prv.pcisecuritystandards.org/3DS/Frequently%20Asked%20Questions%20(FAQ)/PCI_3DS_Core_v1.x_Technical_FAQs_Sep2023.pdf

[4] atsec: www.atsec.cn