PCI 3DS 核心安全标准助力线上交易为支付安全保驾护航

atsec 陈谨运、刘岩，2021 年 11 月

关键词：PCI 3DS、EMVCo 3DS、3DS server、ACS、DS、无卡交易（CNP）

1 背景

传统的线上交易一般通过信用卡的持卡人数据（姓名，卡号，有效期）和敏感的认证数据（安全校验码，如 CVV2/CVC2/CID2/CAV2/CVN2）完成支付授权。随着信息泄漏日益严重，交易欺诈大幅攀升，如何防护交易欺诈，尤其是如何验证消费者的合法身份成为支付行业各机构日益严峻的挑战。此外，随着越来越多的消费者使用各种设备进行在线购物，传统的线上支付授权要素很难满足消费者希望获得安全、快速和方便的电子商务结账体验。

2 标准历史

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，三域模型包括收单域、发卡域和交互域，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。随后 VISA 将 3DS 协议授权给其他主要支付卡品牌，包括 American Express（SafeKey），Discover 和 DinersClub（ProtectBuy），JCB（J/Secure)）和万事达卡（SecureCode）。上述支付卡品牌均创建了各自的 3DS 程序，其目标都是为了减少生态系统内的欺诈活动。2015 年 1 月 8 日，由 American Express，Discover，JCB，MasterCard，UnionPay 和 Visa 共同成立的 EMVCo 组织正式宣布将由其对 3DS 协议标准进行开发和维护。EMVCo 于 2016 年 1 月 16 日正式发布了 3DS V2.0 协议，并于 2017 年 10 月，2018 年 12 月和 2021 年 9 月进行了版本更新，当前最新的协议版本是 3DS V2.3.0。目前主要卡品牌对应的 3DS 程序如下：

- AMERICAN EXPRESS（SafeKey）
- Discover（ProtectBuy）
- JCB（J/Secure）
- Mastercard（ID Check）
- UnionPay（UnionPay 3DS）
- VISA（Verified by VISA）

3 3DS 简介

3DS 英文全称 3-D Secure 或者 Three Domains Secure，翻译成中文为三个域安全。3DS 描述了由 EMVCo 开发和维护用于支持 CNP 交易中的消费者卡片认证的一系列技术要求。3DS 包含的三个域分别是：

- 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）

透过 EMV 3DS 交易流程图，我们能够更直观的了解上述三个域之间的关联关系。

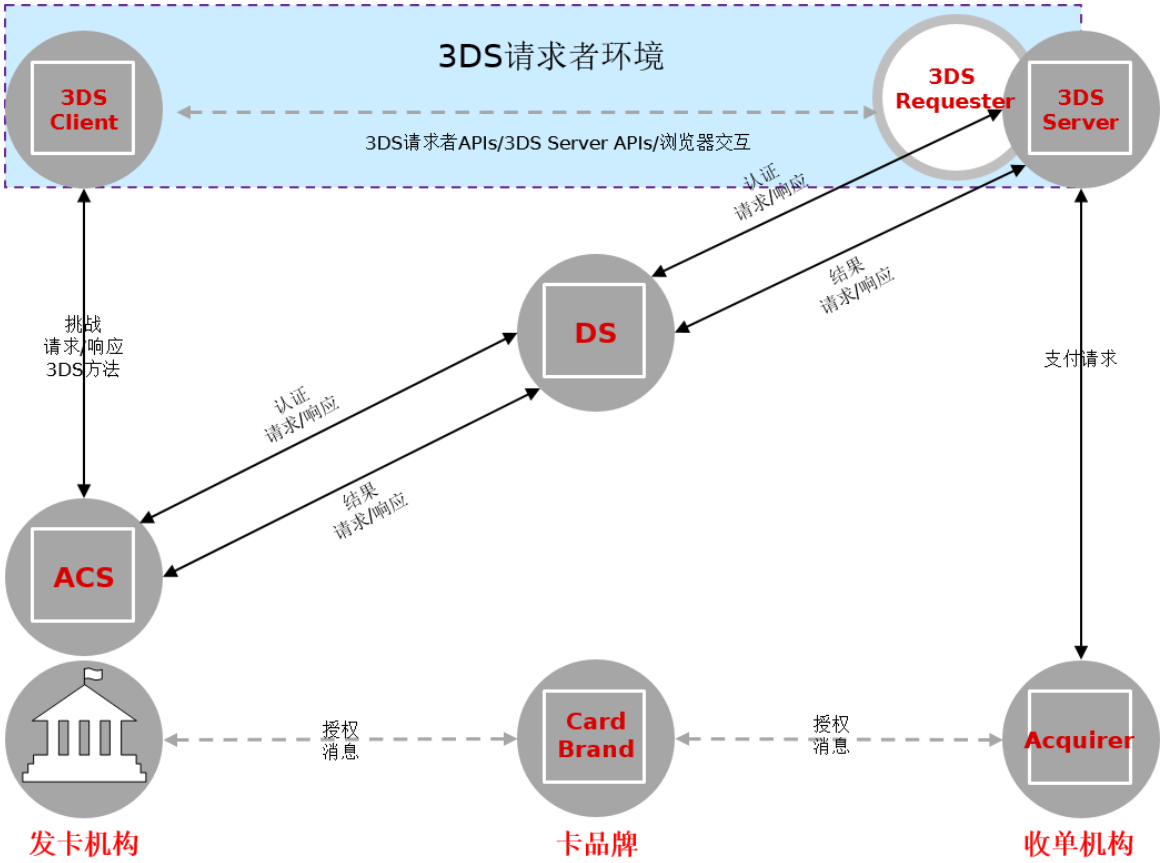

图 1：EMVCo 3DS 交易流程

3.1 EMVCo 维护的 3DS 相关标准

从 EMVCo 官网我们了解到，EMVCo 负责开发和维护 3DS 协议相关的技术标准，授权 EMVCo 相关的 3DS 评测实验室和测试平台，对符合 3DS 技术标准实现的产品进行认证并维护 EMVCo 相关的 3DS 合规产品列表。以下是 EMVCo 维护的 3DS 相关的技术标准：

- EMV® 3-D Secure Protocol and Core Functions Specification
- EMV® 3-D Secure Split-SDK Specification
- EMV® 3-D Secure—SDK Specification

最新的 3DS 协议支持移动终端和传统浏览器的安全认证和身份识别，从而可以更加方便持卡人在移动终端（如智能手机、平板电脑）或者传统 PC 上完成操作。新版本的 3DS 协议规范所支持的持卡人身份识别方式更加全面，包括但不限于在线 PIN、离线 PIN、挑战响应（Challenge-response）、共享密钥、静态密码、生物识别、一次性密码等。

3.2 PCI SSC 维护的 3DS 相关标准

PCI SSC（Payment Card Industry Security Standards Council）是由 American Express，Discover，JCB，MasterCard 和 Visa Inc.作为创始成员，于 2006 年创立的关注支付产业安全的组织。UnionPay 于 2021 年正式成为 PCI SSC 的战略成员，与创始成员一起共同领导 PCI SSC 的发展。PCI SSC 维护了不同支付环节相关的安全标准，以下是 PCI SSC 维护的安全标准图示[1]：

[1] *注：图 2 引自 https://www.pcisecuritystandards.org/pci_security/standards_overview*

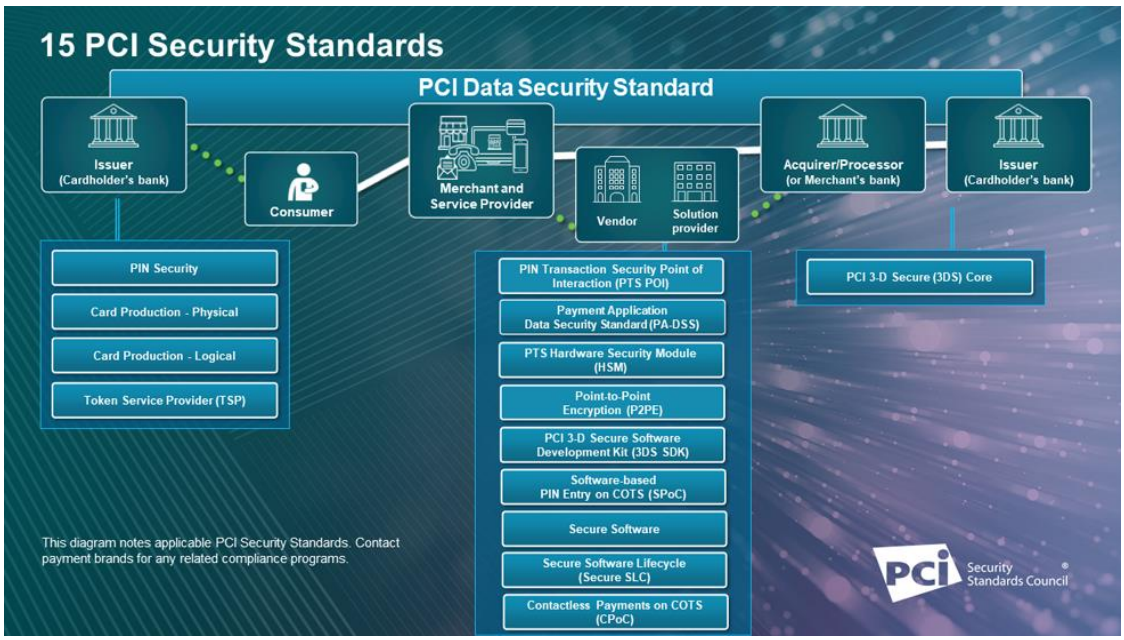

图 2：PCI SSC 维护的安全标准

从 PCI 标准委员会官网我们了解到，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
- PCI 3DS SDK Security Standard -- 重点关注 3DS SDK 实施过程需要注意的安全控制

PCI 3DS 核心安全标准合规机构可以通过 PCI SSC 官网地址查询授权机构和评估人员的资质信息。以下是 atsec 被授权的 PCI 3DS 核心安全标准评估的资质页面。

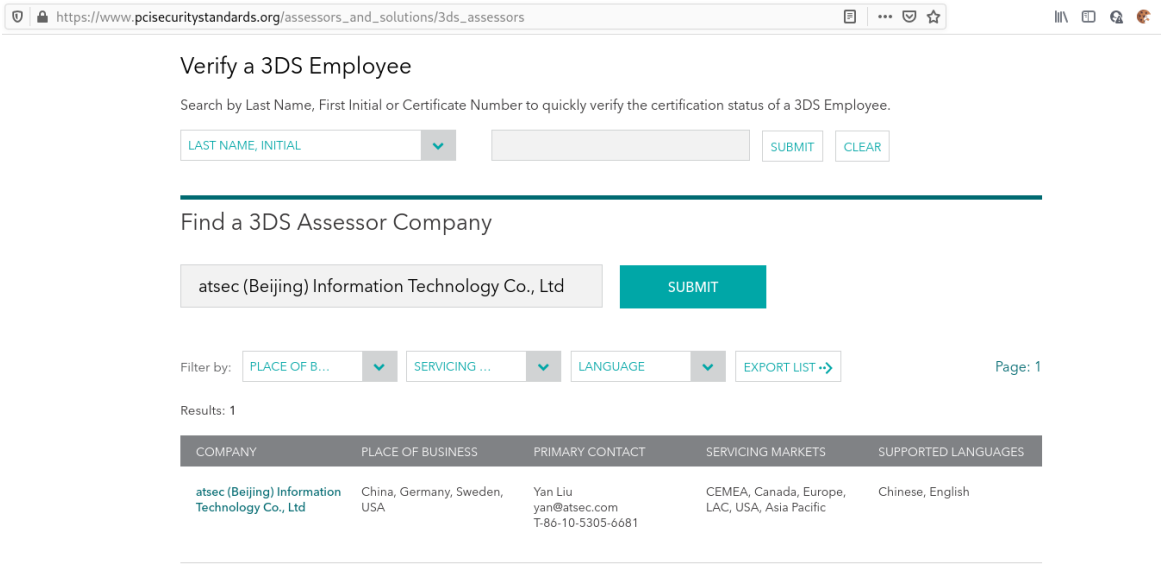

图 3：atsec PCI 3DS 服务资质

4 PCI 3DS 核心安全标准简介

与 EMVCo 关注 3DS 标准功能实现不同，PCI SSC 维护的 PCI 3DS 核心安全标准为执行特殊 3DS 功能的机构定义了安全要求和评估流程。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。

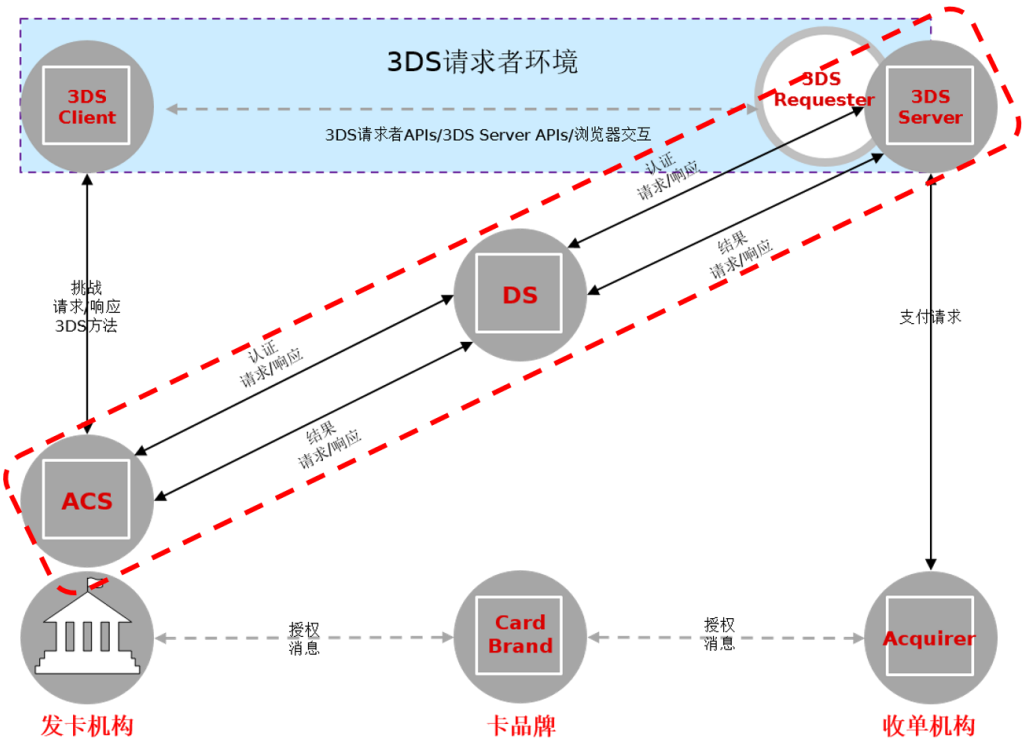

图 4：PCI 3DS 核心标准关注的 EMVCo 3DS 对象

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

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环节被执行。

- 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

5 3DS 好处

3DS 协议作为有效降低 CNP 交易欺诈的技术能够为支付产业带来如下益处[2]：

[2] *内容引用自 https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_-EMV-3DS-for-E-Commerce.pdf*

- 对于发卡机构，3DS 交易能够增强身份认证和欺诈管理，并提供更好的数据和灵活的身份验证方法改进发卡机构确定交易合法性的决策过程，从而：
  - 提高交易批准率
  - 减少电子商务欺诈
  - 增强消费者对交易不会被错误拒绝的信心
- 对于商户：3DS 交易提供更高的安全性，从而减少纠纷。另外额外的安全防护可帮助商家更好地防止欺诈并为客户提供便利，从而：
  - 提高交易安全性
  - 转移欺诈交易的责任
  - 更少的错误拒绝
  - 降低结账放弃的风险
- 对于消费者：3DS 提供更好、更安全的结账体验，消费者可以使用他们喜欢的设备在线购物并期望：
  - 更快、更轻松的身份验证
  - 更少的错误拒绝购买
  - 对交易安全的信心

根据 VISA 发布的调查数据[3]统计显示，3DS 交易在如下方面有得到很大的提升：

- 交易时间：购物者加快结账速度——时间减少了 85%。
- 购物车放弃：更多购物者完成购买——退货率下降 70%。

6 结束语

支付系统安全建设与管理的工作应做到事前防御，而不是等待事后再去弥补。作为第三方独立的合规安全评估机构，atsec 一直被视为各个金融支付机构的朋友和战略伙伴。虽然支付机构从安全建设的角度会面临各种难题，也存在因安全建设带来的工作量和各种成本，但是我们的目标是共同抵御黑客的入侵，共同避免安全事件的发生。

安全工作重在实施的过程和控制，而安全建设工作也需要多方努力。我们也期待着有更多的参与和合作，使得整个支付产业能够以构建“安全和风险”为根基，而不是仅仅去应对“泄露与黑客”。atsec 期待着为中国的整体支付安全做出我们的贡献。

7 参考文档和链接

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

[2] EMV® 3DS for E-Commerce:Fighting Fraud and Friction: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_-EMV-3DS-for-E-Commerce.pdf

[3] New and improved 3-D Secure: https://usa.visa.com/content/dam/VCOM/global/visa-everywhere/documents/visa-3d-secure-2-program-infographic.pdf

[4] atsec: www.atsec.cn

[3] *此内容统计数据引自 https://usa.visa.com/content/dam/VCOM/global/visa-everywhere/documents/visa-3d-secure-2-program-infographic.pdf*