8 位长度银行卡 BIN 码在 PCI DSS 中的实践

atsec，李迪

2023 年 4 月

1 银行卡号编码现状

现代银行与支付系统很大程度上依赖于银行卡作为用户账户的代表，而银行卡号 PAN（Primary Account Number）则是用户账户的唯一体现。常见的银行卡卡号从 14 位到 19 位数字不等，其编码规则严格遵循国际标准 ISO/IEC 7812。目前最新的标准为 ISO/IEC 7812-1:2017(en)[1]。该标准定义了 PAN 的三个组成部分，分别是发卡行识别码（IIN：Issuer Identification Number，或者 BIN：Bank Identification Number）、个人账户号码（Individual Account Number）、校验码（Check Digit）。

ISO/IEC 7812 从 1989 年首次颁布直到最新标准发布的 2017 年，发卡行识别码（下文使用更常见的简称“BIN 码”）始终保持在 6 个数字长度，可以为最多 1,000,000 家发卡机构提供不同的号码资源。然而在银行卡发行数量极大增加的今天，6 位数字显然已经不能满足当下的需求，因此最新版的 ISO/IEC 7812 标准中将 BIN 码扩展为了 8 位数字，理论上可以支撑多达 100,000,000 发卡机构。发卡机构可以选择仍然保留和目前相同位数的 PAN 长度。例如针对 16 位长度的 PAN，在原有标准下 BIN 码为 6 位，个人账户码为 9 位，校验码为 1 位，而在新标准下，相同的 16 位 PAN 则包含了 8 位 BIN 码，7 位个人账户码和 1 位校验码。图 1 展示了新旧标准下 PAN 编码格式的变化：

图 1：ISO/IEC 7812 标准中 PAN 编码格式的变化

各家卡品牌也在积极推进新标准的实施，目前 VISA[2]、Mastercard[3]等卡品牌已经明确给出了迁移时间点，要求其接入机构完成对 8 位 BIN 码的支持。

然而短短两位数字的变化，却可能对现有的卡片支付系统造成极大的影响，本文主要关注于 8 位 BIN 码对支付系统的支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standard）合规可能造成的影响。

2 针对 PCI DSS 的合规考虑

在最新的 PCI DSS 4.0 标准要求 3.4.1、要求 3.5.1 以及要求 3.5.1.1 中，对 PAN 的掩码和截断做出了详细的规定[4]。其中“掩码（Mask）”指的是对于显示在屏幕上、或者打印在纸质收据或报表中的 PAN 的部分数字进行打码，不展示完整的 PAN；而“截断（Truncate）”指的是对保存在磁盘、数据库或者日志中的 PAN，永久性的删除部分数字，使其无法复原回原始的 PAN[5]。

标准条目如下：

要求 3.4.1：*PAN is masked when displayed (the BIN and last four digits **are the maximum number** of digits to be displayed), such that only personnel with a legitimate business need can see **more than** the BIN and last four digits of the PAN（PAN 在显示时被掩盖（BIN 和最后 4 位数字是显示的**最大数字**），这样只有具有合理业务需求的人员可以看到比 BIN 和 PAN 的最后 4 位数字**更多**的内容）*

图 2 分别展示了屏幕上的掩码 PAN 以及 POS 收据上的掩码 PAN 的例子：

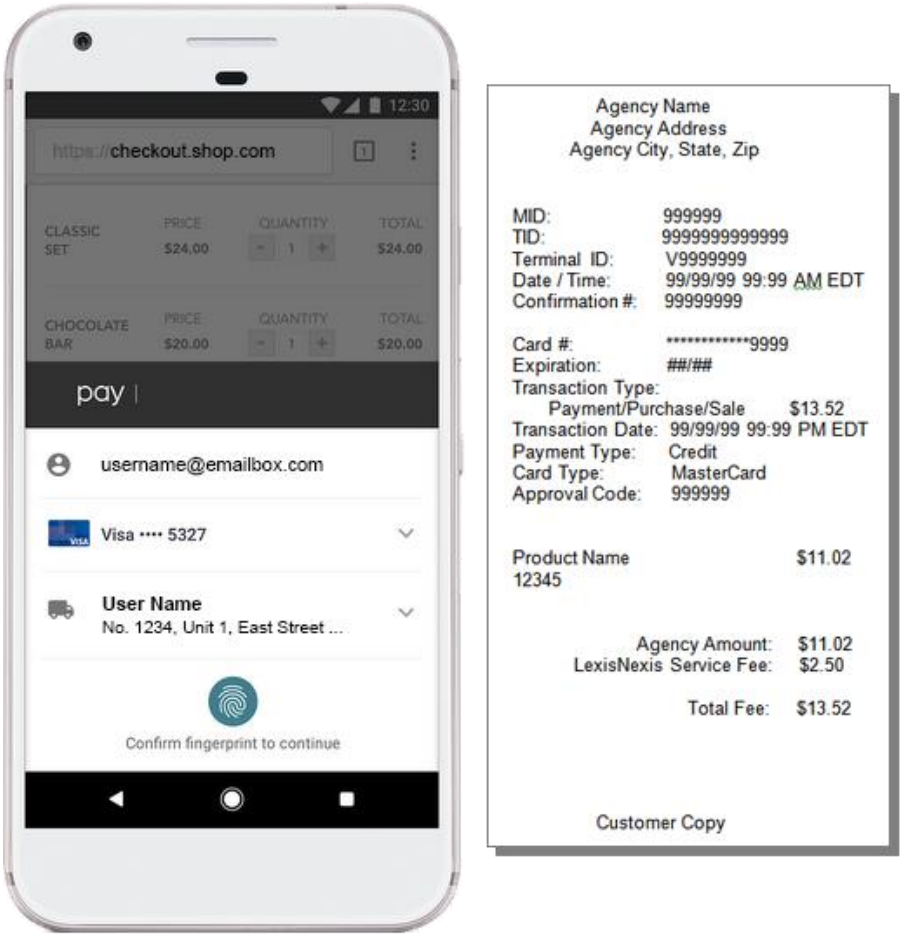

图 2：屏幕上的掩码 PAN（左）以及 POS 收据上的掩码 PAN（右）

要求 3.5.1：*PAN is rendered unreadable anywhere it is stored by using any of the following approaches:（通过使用以下任何一种方法，使 PAN 在任何存储位置都不可读：）*

- *One-way hashes based on strong cryptography of the entire PAN（基于整个 PAN 的强效加密法的单向散列）*
- *Truncation (hashing cannot be used to replace the truncated segment of PAN)（截断（不能使用散列法来替换 PAN 的截断部分））*
  - *If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN（如果相同 PAN 的散列和截断版本，或者相同 PAN 的不同截断格式，存在于一个环境中，则要有额外控制，使不同的版本无法相互关联以重建原始 PAN）*
- *Index tokens（索引令牌）*
- *Strong cryptography with associated key-management processes and procedures（强效加密法以及相关密钥管理流程和程序）*

***要求 3.5.1.1：** Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.（用于使 PAN 不可读的散列（根据要求 3.5.1 的第一条）是整个 PAN 的加密散列，以及符合要求 3 .6 和 3.7 的相关密钥管理流程和程序）*

图 3 展示了数据库存储的截断 PAN 的例子：

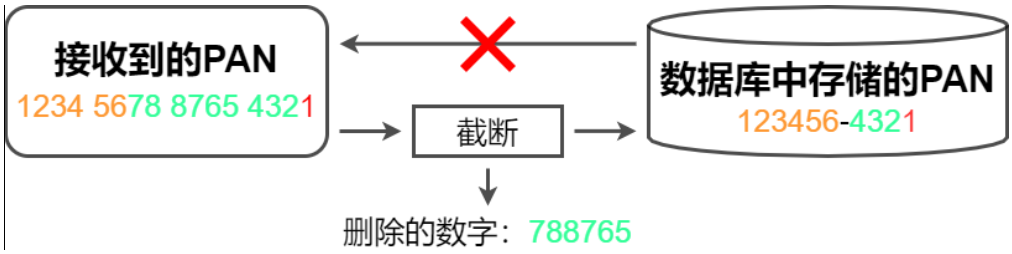

图 3：在数据库中存储的截断 PAN

需要注意的是，目前要求 3.4.1 和要求 3.5.1 都已经正式生效，而要求 3.5.1.1 在 2025 年 3 月 31 日前为最佳实践，在该日期之后转为强制生效。

2.1 掩码或截断安全性的考虑

从上述标准原文中我们可以看到，不论是对展示的 PAN 进行掩码，还是对存储的 PAN 进行截断，目前的要求都指出最多保留 BIN 码和后 4 位数。究其原因， BIN 码通常被用于进行判断发卡机构、交易路由、风控等目的，而后 4 位数字配合 BIN 码则可以供持卡人识别出卡片是否为自己所有，或在较大的系统范围内确认 PAN 的唯一性。中间掩码或截断的 4 位以上数字，则可以确保至少需要猜测 10,000 次才能获取原始 PAN。

因此针对掩码或者截断，作为安全基线的最低要求是，在业务需要或者有明确使用目的的前提下，只有 PAN 的 BIN 码和后 4 位可以进行展示或存储。

针对展示 PAN 的掩码，在明确的业务场景下，部分角色可以通过获得高层书面化的授权形式，展示 PAN 的全部内容而不用进行掩码。比如风控操作人员，在获得来自管理层的业务授权后，可以通过 Web 应用页面显示疑似风险交易的 PAN；或者报表管理员，在获得来自管理层的授权后，可以在交易报表中打印 PAN。

针对存储 PAN 的截断，在上述安全基线要求之外，考虑到 BIN 码升级为 8 位，以及其他业务必要性需要存储更多位 PAN，应严格按照下表中的要求执行：

PAN 长度 **BIN 长度**	**支付卡品牌**	**可接受的 PAN 截断格式**
16 位 PAN （包含 6 位或 8 位 BIN 码）	Discover JCB Mastercard UnionPay Visa	至少 4 位数字需要被截断。 最多可以保留的位数格式： • 前 8 位，任意其他 4 位
15 位 PAN	American Express	至少 5 位数字需要被截断。 最多可以保留的位数格式： • 前 6 位，后 4 位
<15 位 PAN	Discover	最多可以保留的位数格式： • 前 6 位，任意其他 4 位

表 1：可接受的 PAN 截断格式

针对除存储之外其他用途的截断长度、或者判断 BIN 码长度的方式，需要直接咨询对应的支付卡品牌。[6]

2.2 要求 3.5.1.1 中适用的 Keyed Hash 算法

在 PCI DSS 4.0 版本中明确定义可以使用的算法如下：

HMAC: 参考标准 NIST SP 800-107r1 [7]

CMAC: 参考标准 NIST SP 800-38B [8]

GMAC: 参考标准 NIST SP 800-38D [9]

考虑到 PCI DSS 4.0 标准中对有效加密强度应大于等于 128 位的要求，以及结合 NIST SP800-131Ar2 中针对 TDEA 算法 2023 年 12 月 31 日后禁止用于加密计算的要求 [10]，建议选择下表所列的 Keyed Cryptographic Hash 算法：

算法类型	可选择算法长度
HMAC	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/256 HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512
CMAC	AES 128 CMAC, AES 192 CMAC, AES 256 CMAC
GMAC	AES 128 GMAC, AES 192 GMAC, AES 256 GMAC

表 2：建议使用的 Keyed Cryptographic Hash 算法

3 关于 PAN 截断的其他讨论

3.1 截断是否可以用作划分 PCI DSS 持卡人数据环境

如果系统在存储、传输、处理过程中只使用了截断之后 PAN，且其中被截断的部分从该系统中永久删除并无法复原，那么该系统在可靠的网络隔离措施之下，可以被划分在 CDE（持卡人数据环境）之外。

如果该系统被用来提供 PAN 截断功能，由于其一定会在截断过程中传输并处理原始的 PAN，那么该系统将仍被视为 CDE 的一部分[11]。

3.2 多种不同截断措施共存

如果系统中同时存在一个 PAN 的不同截断版本，例如针对同一个 16 位 PAN：

- 系统 1 截断后保留前 6 位后 4 位
- 系统 2 截断后保留前 4 位和中间 8 到 11 位

我们可以看到上述系统的两个截断版本可以恢复出前 6 位、中间 8 到 11 位、后 4 位，和原始 PAN 只有两位数的差别，显著的增加恢复原始 PAN 的可能性。

在这种情况下，系统需要通过额外的设计和评估，确保不同的截断版本不能互相关联起来用于恢复原始 PAN，或者这些关联性最多能够将截断版本恢复至表 1 第三列中要求的长度。否则的话该系统必须被纳入到 CDE 环境中，并对截断版本的 PAN 进行额外的保护，如使用强加密保护截断之后的 PAN 等。[11]

3.3 截断和散列共存

部分支付系统在设计时同时使用同一个 PAN 的截断形式以及散列形式，并将二者储存在相同位置，如同一个数据库的不同表中，甚至于同一张数据表中。在这种情况下，如果攻击者获取到了这个信息，那么它可以通过截断的帮助极大的缩减散列比对的时间，用来恢复原始的 PAN。

以常见的 16 位 PAN 为例：

- 当系统中只储存前 6 位后 4 位截断，那么攻击者没有可比对的对象，无法恢复出原始 PAN
- 如果系统中只储存 PAN 的散列值，攻击者需要执行 10^{16} 次散列计算才能和散列值进行比对恢复出原始 PAN
- 而当系统中同时存储前 6 位后 4 位截断，以及对应 PAN 的散列结果时，攻击者仅需要恢复出被截断的 6 位数字，再考虑到最后一位是校验位，可以通过 Luhn 算法排除明显不符合校验的结果，攻击者可能最多需要执行 10^5 次散列计算

因此在 PCI DSS 要求 3.5.1 中明确指出：“*如果在实体环境中出现同一个 PAN 的散列版本和截断版本，则须采取额外控制措施，确保散列版本和截断版本不能被相互关联，用于重建原始 PAN。*”

可行的控制措施例如：

1. 将同一个 PAN 的散列版本和截断版本分开进行保存，并确保消除两者之间的关联性，使得攻击者无法同时获取散列版本和截断版本的数据，或者即使获取了数据也不能将其关联起来。例如分别存储在两个不同的数据库或者不同的系统，且针对性的设置强效访问控制策略等。
2. 在对 PAN 进行散列之前填充足够长度的盐值，并确保盐值和散列版本或截断版本的 PAN 保存在不同地方。如使用 HSM 生成并保存盐值，而将散列版本和截断版本的数据保存在数据库中。盐值的长度需要满足表 1 中第三列的要求，也就是通过填充盐值，使得散列之前的 PAN 恢复其原始长度。盐值的生成尽可能使用随机数据，在可行的情况下针对每一个 PAN 使用唯一盐值等。

以上补偿控制措施只是参考性信息。如果机构使用了补偿控制措施，需要评估人员（QSA）每年度参考实际的部署和环境情况，并结合系统需要应对的风险进行确定和验证。

各家机构在实施过程中如果有针对 PCI DSS 标准以及相关安全合规的问题和探讨，可以随时联系 atsec。

参考文档：

1. ISO/IEC 7812-1:2017(en)
2. Preparing for the Eight-Digit BIN
3. 8-Digit BIN Expansion and PCI Standards
4. 8-digit BINs and PCI DSS: What You Need to Know
5. What is the difference between masking and truncation?
6. What are acceptable formats for truncation of primary account numbers?
7. Recommendation for Applications Using Approved Hash Algorithms
8. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
9. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
10. Transitioning the Use of Cryptographic Algorithms and Key Lengths
11. Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?