Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

中国银联支付标记化
技术指引

China UnionPay Payment Tokenisation

Technical Guidelines

2016-07-01 发布　　2016-07-01 实施

中 国 银 联 股 份 有 限 公 司　发布

目　　录

前　　言

本标准由中国银联股份有限公司提出。
本标准由中国银联股份有限公司制定。
本标准起草单位：中国银联股份有限公司。
本标准主要起草人：鲁志军、周皓、蒋慧科、章明、赵海、李伟、于晓滨、陈芳、周明。

摘要

移动互联、大数据等新兴技术的发展为支付行业带来全新的挑战和机遇，如何在为用户提供便利、快捷支付体验的同时，确保用户的敏感数据的安全，而又不降低其可用性？支付产业链的各参与方通过多种手段针对交易中的卡片伪造、账户滥用及其他形式的欺诈交易提供了安全保护。虽然银联芯片卡规范在一定程度上确保了有卡交易的安全，但针对逐渐普及的无卡交易及新兴（创新）交易，同样需要对交易进一步的安全保护，从而最大程度地减少持卡人账户数据被非法使用，并防止跨渠道的交易欺诈行为。支付标记化技术与系统在很大程度上有望解决这些问题，并可应用于线上与线下多种交易场景。

自 2013 年，中国银联启动了支付标记化（Payment Tokenization）技术研究和产品实施工作，完成了支付标记化系统（以下简称 TSP）的框架设计规划、系统开发与测试、产品试点应用以及产业影响性分析等多方面的工作。本指引基于 EMVCo Payment Tokenization 技术框架，重点阐述了支付标记化的基本概念、技术框架以及应用场景，旨在为商户、收单机构、发卡行等产业相关方在应用支付标记技术时提供指导性的建议和参考。同时，本指引提出了银联支付标记化建设路线图，为希望与银联合作共建支付标记化产品与服务的合作伙伴提供参考。

第一章　支付标记化提出背景

1.1 支付行业现状

当前，信息化与移动化已经成为全球金融服务创新发展的重要特征。在这样的趋势下，用户一方面将更倾向于利用碎片化的时间，移动、跨屏幕、跨设备地接入互联网;另一方面其碎片化、多元化、虚拟化的网络活动对金融服务，特别是对移动金融服务提出了更高要求，需要金融服务通过网络深入渗透到其生活的方方面面。

据报道,2017 年全球移动支付市场规模将高达 900 亿美元，移动支付服务这种新的支付形态必将成为黑客攻击的新目标。目前业界普遍采用的账户信息保护手段，例如账户安全保护（如数据加密）、系统定期渗透性测试以及端到端加密，都存在一定的局限性，并不能彻底解决问题。而在为用户提供便利、快捷支付体验的同时，如何确保用户的敏感数据的安全？如果可以改变传统基于主账号和相应敏感信息的交易认证方式，那么用户的敏感信息将从根本上得到保护。

1.2 支付行业面临的问题

越来越多的不法分子将支付卡信息视为攻击目标，诸如美国某零售商巨头遭曝光可直接获取大规模账户信息、境内某航旅类商户被曝光明文存储账户信息等，接连发生的持卡人账户信息泄露事件，使得卡组织与发卡机构收到持卡人的大量投诉，发生泄露事件的商户面临巨大的经济风险，甚至在某些地区，面临法律

诉讼。支付卡信息泄露带来的风险主要有两类：

- 伪卡欺诈类，如果磁条卡被侧录，很容易复制成一张伪卡，用于欺诈交易，给持卡人带来资金损失；
- 无卡欺诈类，如果卡号与有效期被泄露，很容易在部分电子商务中挪用于欺诈交易，给持卡人带来资金损失。

在线支付与移动支付环境中，卡组织更加希望能够不改变持卡人用卡号与有效期完成交易的使用习惯，同时有效提高支付的安全性。

1.3 支付标记化方案的意义

支付标记化是使用一个唯一的数值来替代传统的银行卡主账号及有效期的过程，既确保该数值的应用被限定在一个特定的范围，如商户、渠道或设备，又可以应用在银行卡产业全环节，确保国际通用性。支付标记化具有以下显著特征：

1.3.1 降低敏感信息泄露可能性

目前，基本上所有的支付系统均会接触以及处理持卡人的账户敏感数据，尽管部分系统通过了符合国际标准化组织制定的安全标准和认证，如 PCI DSS（账户信息安全认证），但仍然存在被恶意攻击，获取主账号数据的风险。支付标记化方案由于替代了原始卡号与有效期，根本上杜绝了卡号信息泄露的可能；另外，由于在支付标记产生时，对标记应用的范围进行了限定，进一步降低了支付标记泄露后的影响范围。特别强调，只靠支付标记化并不能消除所有交易欺诈。

1.3.2 具备兼容性和互操作性

为了确保支付标记的互操作性，即可以兼容现有的跨行交换网络，支付标记在格式上与主账号保持一致，也是由 13-19 位数字组成，而且该数值符合卡号的基本验证规则，被分配在一个发卡机构标识码（BIN）范围内，且不得与真实的卡 BIN 相同或冲突，这样确保了支付标记可以像卡号一样在跨行网络中正常处理。

需要说明的是，支付标记的申请和交易过程，对持卡人都是无感知的，持卡人并不需要了解在交易过程中用的是支付标记还是主账号。

1.3.3 促进行业创新的发展

对于采用支付标记框架的支付生态系统，相关参与方将获得以下收益，而这些收益也有助于支付标记的推广和使用：

- 持卡人，在不改变现有用户习惯的同时，降低主账号信息在多个交易系统存储并被黑客攻击的风险。支付标记泄漏或存储支付标记的设备丢失时，通过挂失或注销单个支付标记，减少了重新发卡的麻烦，不影响其他标记的交易，可体验到更便利的消费体验。
- 发卡机构，可以通过支付标记化方案发行附属卡，或开展其他方式的移动支付业务，与现有基于卡号的线上支付相比，可提高交易授权级别，并减少了数据泄露事件所带来的欺诈风险。
- 收单机构（商户），可削弱遭受线上攻击和数据泄露后产

生问题的严重性，由于支付标记数据被限定在某一特定的应用范围，因此一方面对攻击者来说，即使攻击成功，也无法获取主账户信息，获取的支付标记配合持卡人认证后才能在特定的范围使用，其影响范围大大降低，另一方面即便可能被应用，也可通过挂失支付标记来消除影响，且不会影响到原始卡片的使用。收单机构（商户）还可以借助支付标记的担保级别实现对交易风险的控制。支付处理网络，通过采用一个开放性标准，既促进交易报文的互操作性，又有助于加强对支付网络及其参与者的系统级数据安全保护。

1.4 支付标记化与其他安全技术

1.4.1 附属卡

虚拟卡是支付标记的一种特殊类型，是一种和主卡关联的、一次一变的动态标记。虚拟卡能进行线上和线下交易，没有使用范围的限制。

1.4.3 芯片安全技术

芯片技术在有卡场景中为持卡交易提供了最全面的安全保障。随着行业升级移动支付系统，基于芯片的设备依然是非常重要的基础设施，因为移动 NFC 支付同样需要利用已有的芯片卡受理设备。当支付标记分发到芯片卡和 NFC 设备中时，能防范对交易中传输的卡片数据的侧录攻击和数据破坏，有效防止潜在的伪卡交易和账号滥用。

支付标记是一种防范攻击的安全和便利的手段。支付标记为电子交易的各参与方提供担保，帮助潜在的欺诈行为能被有效识别、限制和管理。

芯片安全技术和支付标记技术互为补充，共同为线下和线上交易提供一个安全、稳定的支付环境。

第二章　支付标记化基本概念

2.1 概述

早期,业界提出的非支付标记化(Non-Payment Tokenization)方案主要是为商户提供的位于收单侧的卡号替代方案；但由于该方案面向商户或收单机构的受理环境，从收单机构向卡组织、发卡机构发起交易处理请求时仍采用了卡号信息，因此意味着收单机构仍存留卡号信息，且该方案在通用性和互操作性上存在不足，使其在全产业链的应用推广上存在一定的难度。

2014 年， EMVCo 标准化组织发布的支付标记化（Payment Tokenization)技术框架在充分考虑互操作性、兼容性的基础上，解决了卡号信息泄露、支付场景认证等方面的问题。与非支付标记化方案不同,支付标记在确保与现有的支付流程进行融合的同时,有效加强了身份认证与风险监控。具体表现在以下两个方面：

- 交易融合方面：基于 ISO8583（现有银联跨行转接系统报文使用的应用协议）协议与 EMVCo 芯片卡标准，支付标记化扩展了报文域的用途，尽量使得与支付标记化相关的数据元素最大程度复用现有报文域，格式不变仅在含义和取值上发生变化。比如在原有存放卡号的域使用了支付标记替代，而卡号和支付标记在形式上完全类似，因此对任意系统的处理都可透明化；支付标记扩展了数据域，能关联更丰富的交易场景信息。这不仅提升了消费者和商户的使用体验，而且可以作为预防和限制欺诈

交易的有效措施。在芯片卡的应用中，发卡行联机应用密文校验的数据域仍然存在，但这是基于支付标记的应用密文。

- 身份认证与风险监控方面：支付标记申请时，该标记被限定在某一特定范围，且身份认证手段作为支付标记申请过程中的重要步骤被执行。而其担保级别表明了该支付标记与卡号绑定关系的可信程度；交易发生时，TSP 将验证支付标记的应用场景，同时借助担保级别的相关要素进行风险监控。

2.2 概念解析

2.2.1 支付标记

是指主账号（PAN） 的一个替代值，一般由 13 至 19 位的数字组成，该数值必须符合主账号的基本验证规则，其中包括 LUHN 算法校验。在银行卡支付交易中用支付标记替换卡号，用支付标记的有效期替换卡号有效期，不影响交易处理，增强了交易安全。

2.2.2 标记 BIN

标记 BIN 与卡 BIN 类似，主要用于在支付网络中交易路由，但不能和主账号 PAN 的 BIN 冲突，仅用于支付标记的发行，且属于特定的 BIN 范围，并在 BIN 表格中被相应标识。

2.2.3 标记有效期

标记的有效期类似卡号有效期，在报文传输中替代卡号有效

期的报文域，标记有效期一般情况下小于或等于卡号有效期。

2.2.4 标记服务提供方

标记服务提供方是负责产生、维护标记的主体，它也负责管理标记请求方，并向其提供标记的相关服务。标记服务提供方作为支付标记的发行机构，负责 TSP 的建设、维护以及运营，有责任履行以下职责：

- 标记库的持续运行和维护
- 支付标记的生成与发布
- 安全应用和控制
- 支付标记相关数据准备
- 标记请求方的注册功能
- 支付标记生命周期管理
- 去标记化操作
- 建立及管理其自身的标记请求者 API
- 确保标记 BIN 或标记 BIN 范围与传统卡号 BIN 或卡号 BIN 范围不同，以防止 PAN 与标记的冲突。

EMVCo 已制定了一套 TSP 注册机制，通过为不同的 TSP 分配编号，确保在全球范围内每个 TSP 编号对应一家机构。这对于标记请求方了解哪一个 TSP 是合适的支付标记申请对象非常重要，同时确保 TSP 能和传统支付系统交互操作，不发生冲突。

2.2.4 标记请求方

向标记服务提供方提交标记申请的机构。该机构可以是传统

支付行业的参与者或者某类专业化服务提供方。在 TSP 中，标记服务提供方管理并唯一标识标记请求方。标记请求方的实体可以是以下参与方：

- 存留卡号信息的商户
- 数字钱包服务商
- 收单机构、收单机构的外包服务方以及提供商户支付的网关系统服务方
- 移动设备或芯片的制造商
- 发卡机构

标记请求方需遵循标记服务提供方的管理标准、技术规范和入网申请流程。在成功注册后，标记请求方将被分配一个唯一的 ID 号码。结合不同的交易场景，一个标记请求方可以申请多个 ID 号码。

2.2.5 身份识别和验证（ID&V）

用于验证持卡人及其账户的有效性的方法，ID&V 作为支付标记申请时一个重要环节，其结果直接决定了所申请的支付标记和原始主账号 PAN 之间的可信程度。

2.2.6 担保级别

担保级别用于表示所申请的支付标记和其绑定的主账号 PAN 的可信程度，该值受很多因素的影响，包括账户验证的结果、身份认证的结果、风险监控系统的评分、标记存储位置等。

担保级别在标记产生时由标记服务提供方根据一系列控制

要素和验证结果综合判定；在标记产生之后，如果对该标记进行额外的 ID&V 操作，标记的担保级别也可进行更新。

2.2.7 标记的域控

表示标记绑定的使用场景，比如特定的交易类型、使用次数、支付渠道（例如仅 NFC）、商户名称、数字钱包服务提供方或者以上限定场景的任意组合。

2.2.8 标记的存储位置

支付标记位置的安全性将会影响该支付标记的担保级别。标记服务提供方需要定义标记的存储位置，并且负责对相关的标记请求方申请的存储位置执行检查。建议包括以下存储类型：

- 远程存储，例如大商户的服务器；
- SE 存储，例如芯片，手机中的 SE；
- 本地安全环境存储：例如 TEE；
- 远程安全环境存储：如云 SE；

2.2.9 去标记化操作

去标记化操作，是 TSP 根据当前的交易场景在判断支付标记的有效性、域控以及交易金额限制等措施后，将其转换为原始主账号 PAN 的操作。

去标记化操作可能包括交易验证功能。

2.2.10 支付账户参考号（PAR）

支付账户参考号（PAR）是用于关联同一卡号衍生出的不同 Token 的数据元素。相同的 PAN 及其相关的 Token 应具有相同的

PAR。PAR 由 4 位 BIN 管理方标识符（BCI）加 25 位数字和大写字母的组合构成。商户和收单机构利用 PAR 可识别同一主账号的不同支付标记，满足营销分析、风险识别等要求。

第三章　支付标记化技术方案

3.1 系统架构

支付标记化系统架构（如图 1 所示）描述了现有支付产业中主要角色及关系，标记请求方与标记服务提供方两个角色与现有传统支付流程的关系和数据交互接口，明确了支付标记如何共同为持卡人和商户提供标记服务。

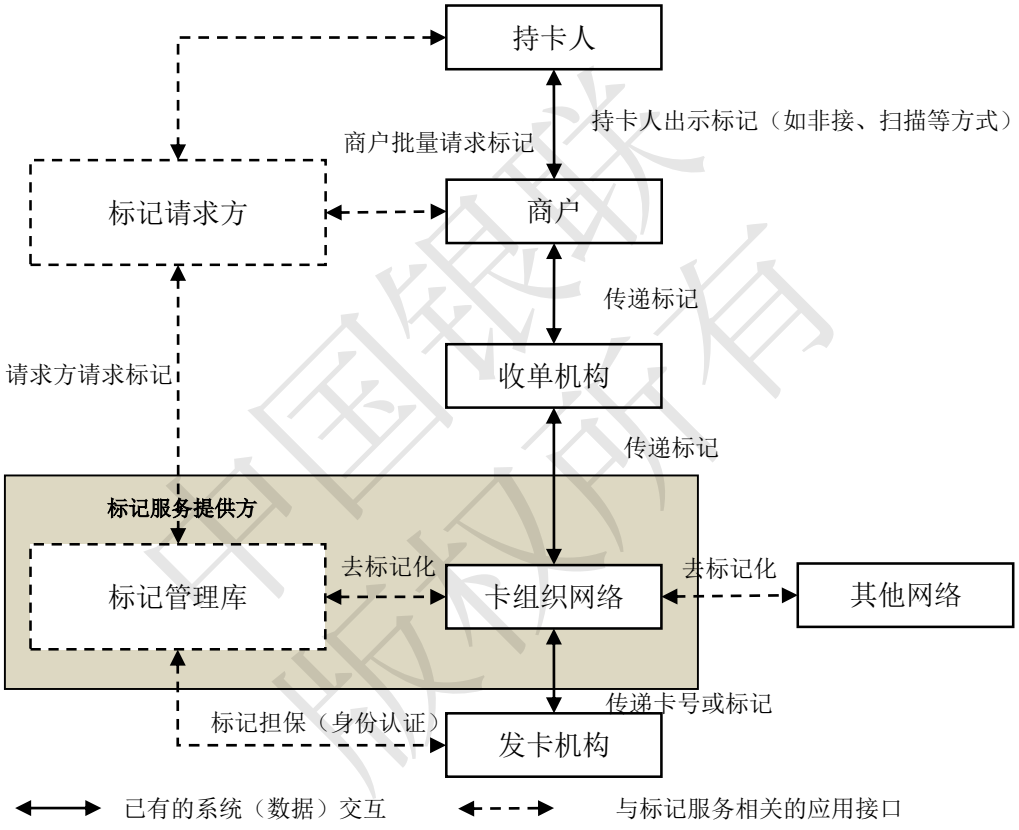

图 1：支付标记化系统架构

其中，标记服务提供方是该标记化框架的核心角色，它提供了标记的申请、生成、管理、去标记化等功能，包括标记请求方（TR）的注册和管理职责。根据不同的业务场景、受理渠道以及标记的应用域控，标记服务提供方会制定与之配套个性化参数和控制措施，最终达到标记交易控制和风险监控。而标记请求方则

作为标记请求的实体向标记服务提供方申请标记，并同步管理需要应用标记的实体，如商户、持卡人等。

3.2 标记请求方注册

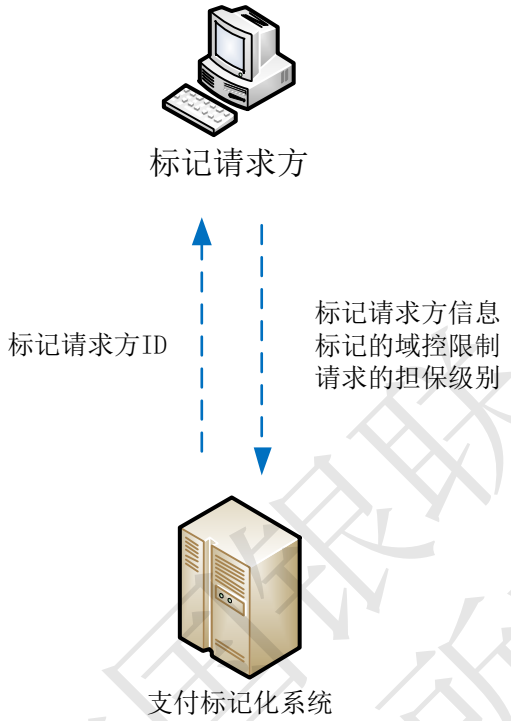

图 2：支付标记请求方注册流程

标记服务提供方应根据自己的业务需求制定所管辖的标记请求方的申请和注册流程（如图 2 所示）。拟注册为标记请求方的实体可以在多个标记服务提供方分别进行注册。

标记服务请求方在申请注册时，标记服务提供方自主决定所需要收集的信息，可能包括持卡人账户验证信息、标记请求方所支持的用户场景、以及标记的域控等。一旦标记请求方注册成功，那么标记请求方被分配一个唯一的 ID，对应该 ID 下的支付标记域控和其他交易控制措施将同步记录在标记服务提供方的系统中，用于后续的交易验证。

3.3 标记申请流程

下图概括性的描述了支付标记的申请流程：

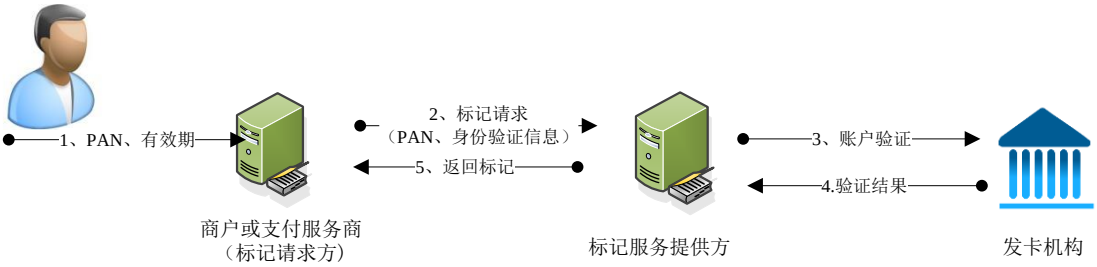

图 3：支付标记化申请流程

1）支付数据标记化的过程对持卡人而言是一个绑卡的操作，需要用户在商户或者支付服务商的页面提交账户信息；在用户绑卡时，采集用户账户信息的主体可作为标记请求方向标记服务提供方申请支付标记；

2）由支付标记请求方（商户或支付服务商）向标记服务提供方申请 Token；

3）标记服务提供方在收到标记申请时，需要与发卡机构共同验证持卡人的身份信息以及部分附加信息；

4）在完成账户验证之后，标记服务提供方生成 Token，并下发给标记请求方；

3.4 标记的交易流程

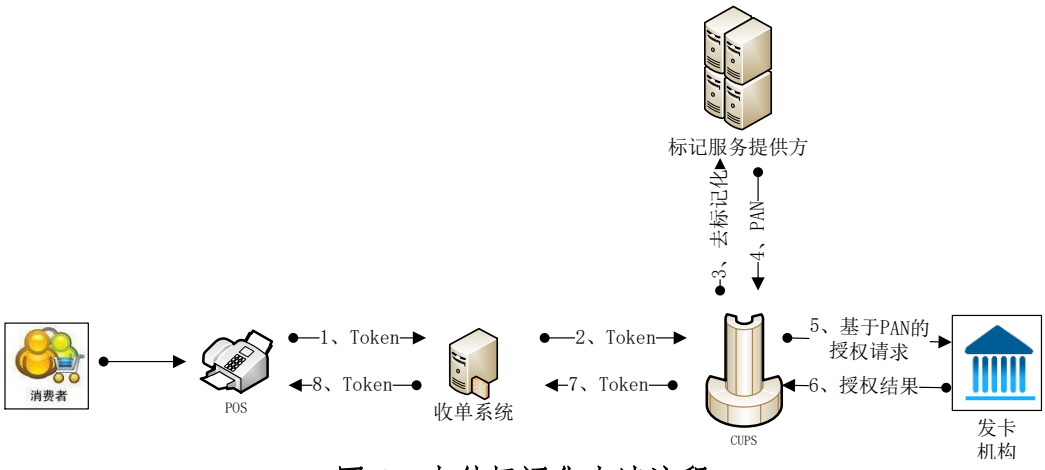

图 4：支付标记化申请流程

支付标记化交易的处理流程与现有基于主账号的交易处理流程完全一致，仅在去标记化操作时需要支付标记服务提供方完成支付标记的交易验证和还原卡号操作。而支付标记的交易路由与主账号的交易路由一致，均是由转接组织根据 BIN 表来进行路由控制以及交易分发。TSP 作为支付标记服务提供方的处理系统，完成支付标记化与原始卡号的转换操作。

3.5 支付标记生命周期管理

银联 TSP 提供支付标记的持续性生命周期管理功能，包括：激活标记、临时挂失标记、更新标记担保级别、更新主账号属性、解除标记关系等。

银联 TSP 支持三种方式对 Token 的属性、状态等要素更新和管理：一是 Token 管理页面，提供给卡组织内部用户对 Token 进行管理，功能包括以上类型，且记录操作日志；二是 TSP 标记管理接口，提供给相应可信发起方对于其权限范围内的 Token 进行管理；三是批量文件接口，提供给相应可信发起方对于其权限范围内的 Token 进行管理。

对于自建TSP的银行,银联TSP可以获取卡号信息变化情况,实现Token号不变情况下更新卡号信息。

3.6 PAR的生成与应用

引入的支付标记增强了数字支付的基础安全,限制了账户泄漏和滥用带来的风险。然而，由于标记交易中不会出现卡号，商户和收单机构不能获得消费者的完整交易记录。

2015年初，EMVCo开始研究制定“支付账户参考号（PAR)”的相关标准,以满足商户、收单关联同一卡号不同Token的需求,用于开展营销分析、增值服务、风险识别（如反洗钱）和关联特殊交易。银联内部在推广基于Token的产品时，市场和产品前端也相继提出了对同一卡号生成的不同Token进行关联的需求(互联网打车类商户、HCE云闪付、银联钱包等)。

PAR是用于关联同一卡号衍生出的不同Token的数据元素,在不使用卡号的情况下,商户和收单机构可通过PAR建立持卡人的Token号和卡号的联系。PAR具备两个重要特征：一是相同的PAN及其相关的Token(包括由不同TSP产生)应具有相同的PAR;二是PAR不能被反向推导出与其相关的卡号和Token号信息。

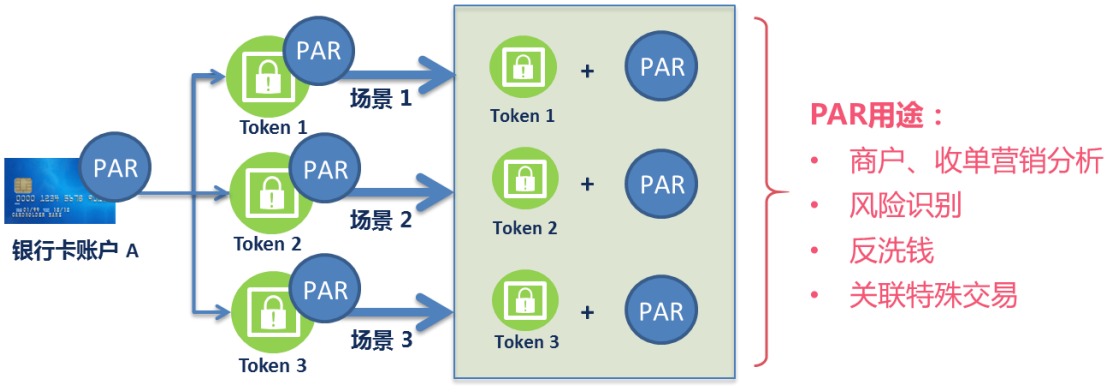

图 5：PAR

3.6.1 管理要求

根据 EMVCo 标准，银联负责管理基于银联卡 Token 的 PAR，确保 PAR 的唯一性，保证银联卡号的 PAR 不会发生冲突。原则上，发卡机构自行建设 TSP 开展银联卡 Token 业务的，应向银联 TSP 查询相关的 PAR，特殊情况下，经银联的业务授权，可以根据银联的规则，自行产生符合银联要求的 PAR。

3.6.2 生成方法

PAR 由 4 位 BIN 管理方标识符（BCI）加 25 位数字和大写字母的组合构成。银联将使用基于哈希算法的生成方法。

图 6：基于 HASH 的 PAR 生成方法 （举例）

3.6.3 PAR 的申请流程

图 7：PAR 的申请流程

3.5.4 PAR 的交易流程

本节涉及的跨行系统处理交易环节的具体报文，参照后续发布的银联交换系统技术规范。

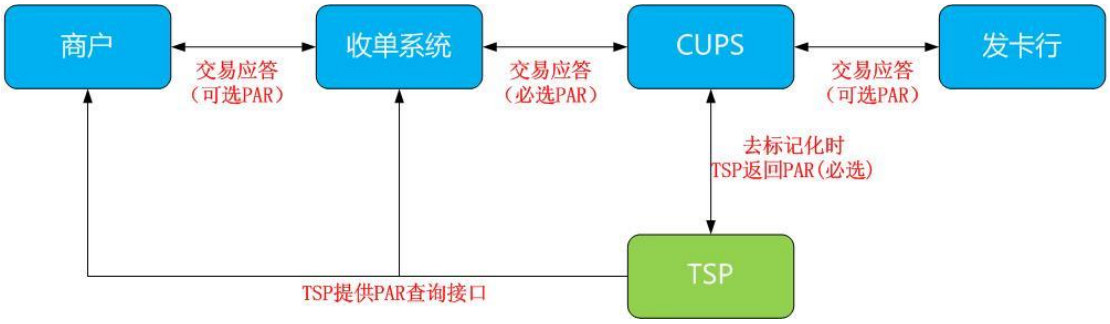

图 8：PAR 的交易流程（举例）

3.7 标记信息同步

根据 EMVCo 发布的标准，银行卡组织、发卡银行都可以承担 TSP 的职责，提供 Token 相关的管理与服务。其中，卡组织 TSP 主要面向本品牌下所有发卡银行发行的卡，发卡银行 TSP 则面向本行卡提供 Token 服务。

目前有多家银行为满足自身个性化的业务需求以及对系统掌控力的诉求，以“自建 TSP”的模式与银联开展 Token 业务合作。在此模式下，Token 与卡号的绑定关系只有发卡机构掌握，银联支付网络无法直接判断一个用于支付的银行卡号是真实银行卡号还是发卡行分配的 Token 号，对业务一致性有一定影响，也给风险控制和商户营销带来难题。

为此需要在不同的 TSP 之间实现 Token 信息的同步，使银联 TSP 可以维护 Token 与卡号映射关系全集，实现 Token 业务风险监控、赔付的统筹管理及针对卡号的精准营销支持。

同时，对于使用银联 TSP 代发 Token 的发卡机构，也可以通过 Token 信息同步通道，从银联 TSP 获取本行卡生成的 Token 信息。

3.8 国际化支持

在传统银联卡交易中，境外交易（境外发行银联卡在境外受理）和跨境交易（境外发行银联卡在境内受理或境内发行银联卡在境外受理）相对于银联卡境内交易需要额外支持多种特殊的业务要素传递，如多币种、本地化时间信息等。在银联支付标记化业务中，也同样存在这样的情况。

银联 TSP 系统服务于境内外银联卡的支付标记化处理。对于境外支付标记化业务或跨境支付标记化业务，在标记申请过程 TR 与银联 TSP 之间需要传递交易限额币种、交易发生的本地时间、交易发生地等信息。交易去标记化过程中，交易限额的检查也会涉及到币种转换过程。

3.9Token 远程管理服务

支付标记化方案在不改变用户习惯的前提下，有效解决了敏感信息泄漏的问题，越来越多的发卡银行采用这一方案并选择使用银联 TSP 服务开办 Token 相关业务。对于这些银行，存在查询及管理本行卡关联 Token，以提升对持卡人的服务水平的需求（例如银行在办理卡片挂失、解挂、换卡、注销等相关业务时，需要对本行卡相关的 Token 进行关联操作）。为此银联将建立基于 Web 的远程管理服务平台，提供 Token 的远程信息查询及生命周期管理等功能。从而帮助发卡银行实现对与本行卡相关的 Token 数据的访问及远程管理，满足持卡人通过发卡银行渠道发起的 Token 数据操作需要。银联 Token 远程管理服务平台提供以下功能：

1、Token 信息查询

根据PAN或Token号查询Token信息，其中包括Token状态、关联银行卡号、失效时间等信息。

2、Token状态管理

根据业务场景修改选定 Token 的状态。Token 共有未激活、已激活、已挂失、已注销四种状态。

Token的状态转换如下图所示：

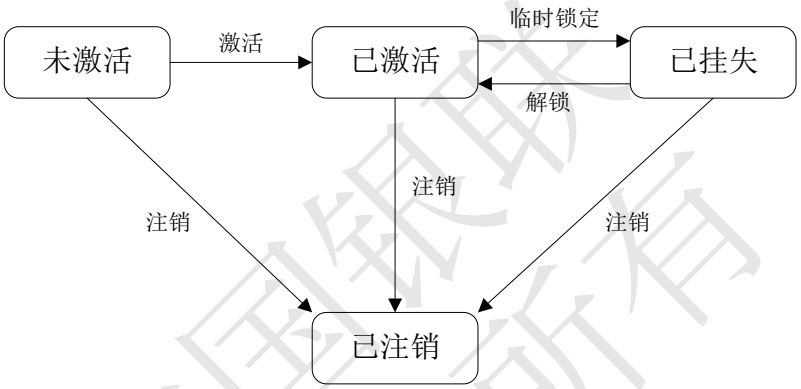

图 13：Token 状态转换

3、卡片信息变更

当用户更换卡号或有效期时，修改原Token和卡号的对应关系，并更新有效期。

4、Token信息变更查询

查询选定Token的信息变更历史，其中包括状态更变、卡号和有效期变更。

5、历史交易查询

查询选定Token最近一段时间内的历史交易信息。

第四章　担保级别与身份认证方法

4.1 担保级别的作用

担保级别用于表示支付标记与卡号之间绑定关系的可信程度，由标记服务提供方在支付标记申请环节根据前端采集的信息、标记请求方注册时已记录的信息、以及持卡人身份识别与认证的结果，并结合担保级别评分模型综合判定后确定。如有需要，担保级别还可以在后续交易环节中进行更新。

担保级别是支付标记化技术中的重要概念之一，虽然是在支付标记申请环节确定，但其使用贯穿于后续的交易环节，因此正确理解和使用担保级别对卡组织、发卡机构和收单机构都有着重要的意义。担保级别至少具备以下三个方面的价值：

一是在支付标记申请环节，实现类似银行发卡时的“信用评估”，作为支付标记是否申请成功，以及该支付标记所可以应用的交易场景范围的凭据；

二是在支付标记交易环节，与风险监控模型相结合，丰富和扩充其信息输入的维度，优化其规则和模型，进而提高识别欺诈交易的效率和准确性；

三是获取更为广泛的用户设备信息和环境信息，用于建立持卡人交易行为数据库，通过大数据分析技术为更广泛的身份认证和交易授权决策提供基础支撑。

4.2 身份认证的方法

身份认证的方法与结果是确定支付标记担保级别的关键步

骤。一方面不同的支付场景需要使用不同的身份认证方法，另一方面不同的身份认证方法将影响担保级别的高低。通常来说，欺诈发生可能性越高的场景越需要高安全等级的身份认证方法，同时认证强度越高的身份认证方法将决定更高的担保级别。当身份认证不被执行时，则申请的是一个担保级别为 0 的支付标记。

与现场有卡交易相比，远程无卡交易在通过支付标记化技术减少敏感信息泄露的同时，还应该提高对持卡人身份认证的强度，因此，在单纯账户信息验证（卡号、有效期、CVN2 等信息的验证）的基础上，应叠加使用多因素认证。除了我们所熟知的数字证书、OTP 令牌、生物特征识别等身份认证手段外，一种被称为“基于风险的身份认证”（RBA，Risk-Based Authentication）技术正在快速崛起，通过建立用户行为分析和识别的数学模型，在用户行为匹配的情况下，简化身份认证，从而在保证安全性的同时提升用户体验。

中国银联一方面积极参与国际标准化组织，力争为国内的支付产业带来最前沿的安全技术，另一方面也立足本土市场，努力打造“银联安全验证与风险监控服务”，通过前端安全组件采集设备信息，实现设备指纹分析、可信设备认证、基于设备信息的欺诈评分等服务，这将是一个可以面向商户、成员机构提供增值服务的基础平台，既可以为商户提供其客户可信度的评分，也可以协助收单或发卡机构判断一笔交易的风险高低。

第五章　支付标记化典型应用场景

在不同交易场景下，支付标记的交易会依据不同的交易流程、用户习惯以及系统交互等方面设计与之对应的交易报文，并增加相应的交易要素，针对每一个应用场景，均需要对现有字段的使用、标记数据在当前字段中的出现情况、以及新数据字段(必要和可选）进行检查。

结合目前支付行业发展趋势，中国银联目前制定了四种不同应用场景下支付标记的技术解决方案。主要包括 NFC 支付（分 HCE 模式和 SE 模式)、数字钱包支付、大商户支付以及二维码支付，同时正在对基于芯片卡的支付标记化方案进行研究。

5.1　NFC 支付模式

在此应用场景中，支付标记可能存储在一个具有 NFC 功能的移动设备 SE 中（如 Apple Pay 模式）或在一个远端的安全服务器上（如 HCE 模式)。以 HCE 为例，支付标记是在用户首次进行绑卡时，由 HCE 支付服务商系统向标记服务提供方申请标记。发起交易时，移动设备（或本地 SE 环境内获取或由远端服务器下发）与 POS 终端交互，将一个含有标记、标记有效期、标记密文以及其他芯片数据元素的报文通过非接通讯方式完成数据交换，并在现有的支付网络中完成交易的授权操作。

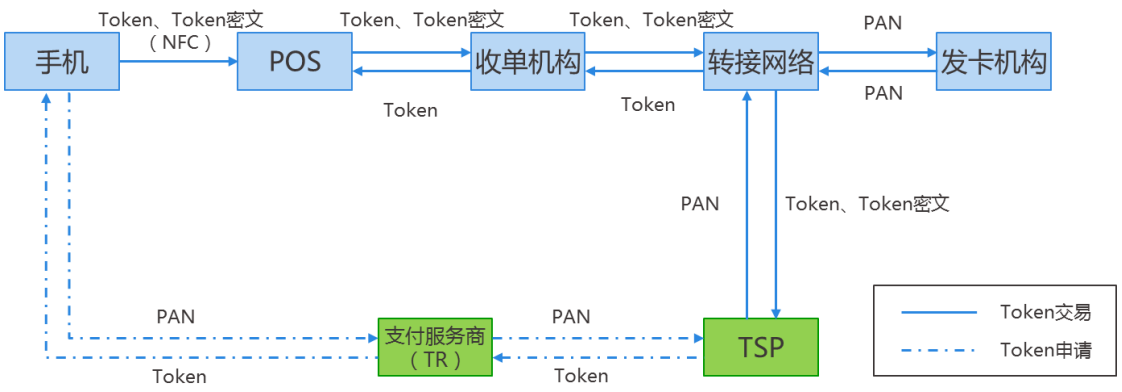

图 9：NFC 支付模式框架图

5.2 数字钱包支付模式

在数字钱包支付中，持卡人在某个支持移动/数字钱包的电子商务网站发起支付请求，该数字钱包服务商可以由发卡机构、支付网络或第三方专业化机构运营；一般情况下数字钱包运营商作为标记请求方申请支付标记。在此应用场景中，钱包运营商出于安全的考虑或者业务的需要，使用支付标记替代主账号，从而不再需要将主账号存储在钱包平台中。另外，在支付标记发行及其生命周期内，通过使用数字钱包用户的信息可以提高身份认证的准确性。

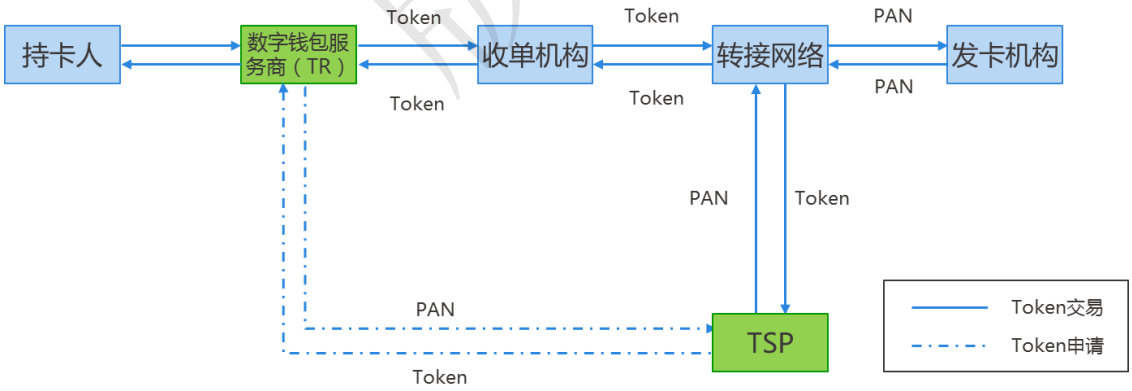

图 10：数字钱包支付模式框架图

5.3 大商户支付模式

大商户支付模式下，目前商户需要在数据库中存储持卡人的

主账号、有效期等敏感信息，以便在后续交易中减少持卡人重复输入账户信息的操作。由于存储卡片数据中可能会导致商户系统被攻击、泄露敏感信息等安全事件。采用支付标记化方案后，商户可以通过支付标记来替换主账号 PAN 信息，且该支付标记可限定在该商户下单独使用，从而消除相应的风险。该应用场景中，商户很可能是标记请求方。一旦标记被返回给这些留存卡号信息的商户，所有后续的电子商务交易都会使用标记和标记有效期（而不是主账号和主账号的有效期）字段来处理。

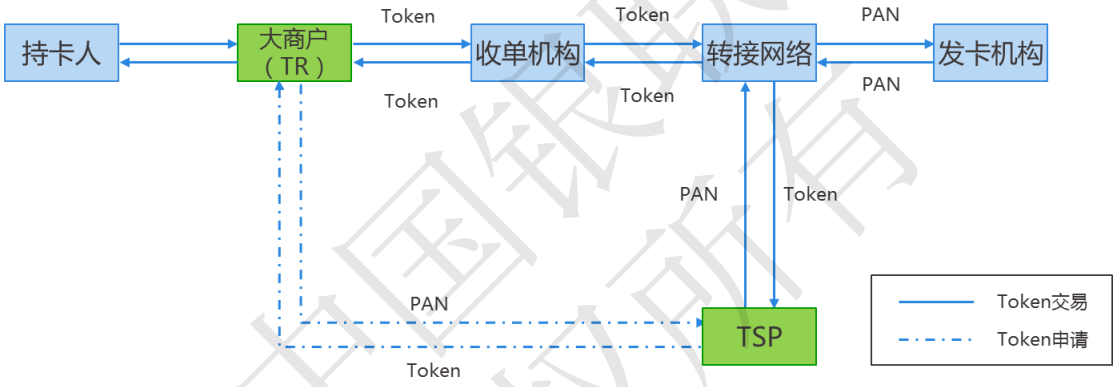

图 11：大商户支付模式框架图

5.4 二维码支付模式

作为支付创新的一种，二维码支付为用户、商户带来快捷支付体验的同时，但由于二维码易复制、安全性弱等特点使其存在一定的风险。而通过支付标记同样可以将敏感信息进行替代，从而确保支付的安全。在该应用场景中，移动设备上的应用程序以安全的方式，生成一个含有支付标记,标记有效期以及其它来自于二维码的数据（如交易 token 密文，指保护 token 数据的校验码），该支付标记（图 8 中的交易 token）被限定为一次有效，且有效时间也被严格控制。交易时，二维码数据被商户的终端读

取，并由商户端向后台发起交易授权请求。

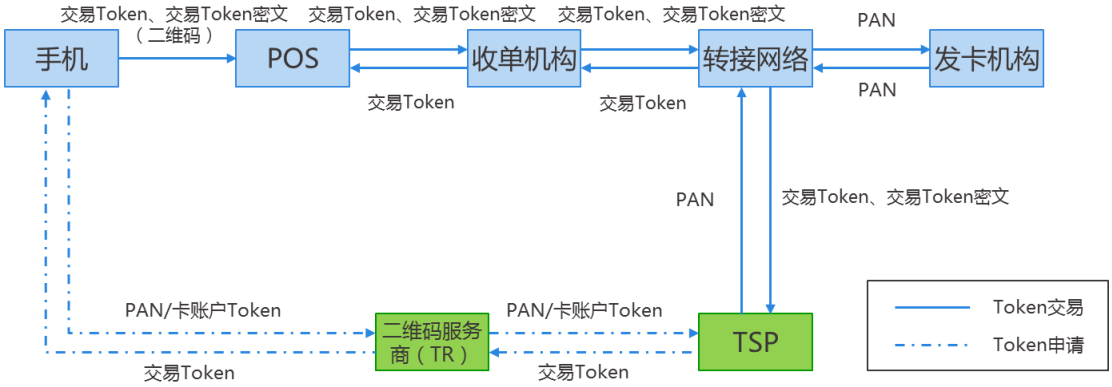

图 12：二维码支付模式框架图

第六章　银联的支付标记化建设路线图

2014 年，中国银联启动了支付标记化的相关工作，结合境内市场的发展现状以及用户习惯，深入研究分析支付标记化的市场需求，明确了相关产品与技术实施路线图。目前，银联 TSP 已逐步实现对线上、线下交易产品的支持，国际化支持以及 Token 远程管理服务。

6.1　产品路线图

6.1.1线上支付

结合线上无卡交易的特点，银联将对线上交易全面采用支付标记化方案，以帮助商户、收单机构在消除支付系统的敏感信息、实现交易场景的认证等。

- ✓ 大商户模式，目前已有 55 家大型线上商户接入，为持卡人提供更加安全、快速的支付体验；
- ✓ 数字钱包模式，该模式下商户端无需额外改造，仅需银联支付网关的适当改造，从而为接入银联支付网关的所有商户提供支付标记化服务。目前，支付标记已经支持跳转 PC 网关、移动端 WAP 进行首次 Token 申请，非首次支付报文传递 Token 号的方式；丰富相关产品支持，后续将重点加强商户端的推广和完善工作。

6.1.2线下支付

针对线下支付产品，将采用“立足创新，逐步过渡”的实施路线实现支付标记化的应用。

在移动支付应用领域，通过支付标记实现远程发卡，一方面，

一定程度上弥补了移动支付远程发卡流程长、涉及关联方多的不足，提升了便利性；另一方面将支付标记而不是卡号下发到手机中，提升了安全性，有效防范了账户信息泄露。银联目前正在开展代发卡银行远程发卡的产品方案，一方面对银行屏蔽了前端复杂的业务处理逻辑、形成了统一规范的银行系统间接口、有效避免了银行系统的重复改造，另一方面可以借助 Token 适应各种创新场景（如 NFC 场景、磁条类辐射模拟交易等），为持卡人提供了安全、快速的支付体验。目前已在云闪付移动支付产品中（包括 Apple Pay、HCE、Samsung Pay 等）集成了支付标记化技术。

未来，银联支付标记化服务将在其他创新性支付解决方案中得到长足发展。

6.2 技术路线图

6.2.1线上支付

发卡机构可在线上无卡交易的场景中，完全不改造其发卡系统实现支付标记化交易的无缝衔接。

如果发卡机构希望获取更多 token 相关的交易信息，可适当改造系统支持数据处理；一方面可获取更多支付标记的控制信息，如生命周期管理、交易域控、担保级别，另一方面可获取与担保级别相关的辅助信息（如部分交易设备认证信息）。

6.2.2线下支付

关于线下交易，发卡机构需要适当的系统改造实现对支付标记化交易的支持，详见对应的技术规范。

第七章　银联基于支付标记化的创新产品

银联已在各类移动支付“云闪付”产品中集成了支付标记化处理，包括目前已上线的 HCE 云端支付、Apple Pay、Samsung Pay,以及即将推出的华为 Pay、小米 Pay 等产品。

7.1 云端支付（HCE）

云端支付是基于 NFC 技术的移动支付产品，与 NFC SIM、全手机方案等需要安全芯片的移动支付不同，通过 Android 的 HCE 技术，云端支付可将手机银行等客户端直接**模拟成一张银行卡**，与非接 POS 终端执行闪付联机交易，并通过云端下载临时密钥，结合 Token 技术保证安全性。

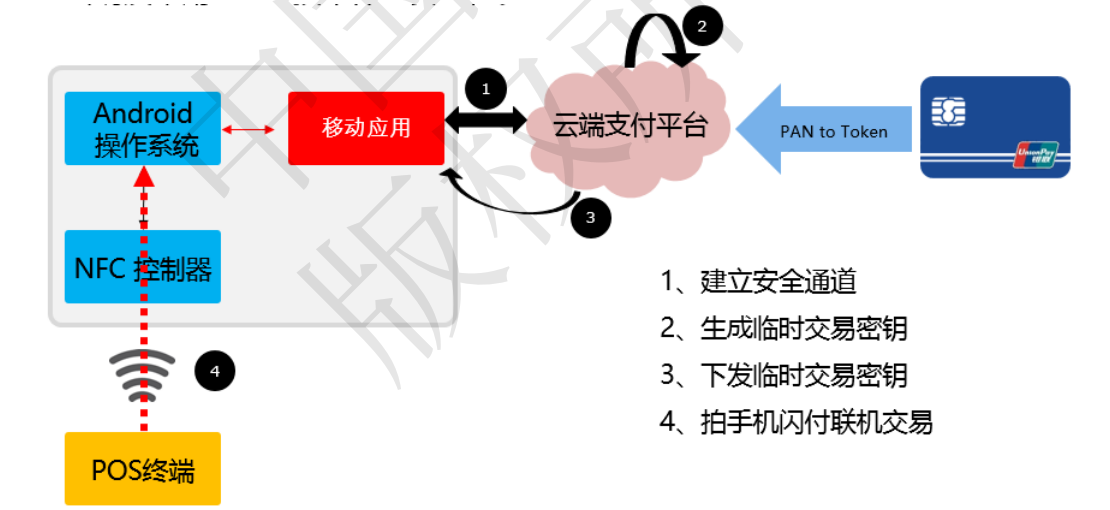

图 14：云端支付示意图

不同于 SE 方案依靠安全芯片对交易凭证和敏感数据的保护，云端支付产品没有安全芯片，因此其安全机制的重点在于平台对欺诈交易的实时监测以及在欺诈发生时迅速进行处理使得欺诈难以获利。云端支付产品采用多重安全保护手段用于安全防护，

包括账户风险控制、身份认证、通信数据安全和安全数据存储等多个方面。在账户风险控制方面，运用 Token 技术将真实卡号转换为基于 Token 的云闪付卡后再存储在手机设备操作系统中，将交易风险限制在可控范围之内。

7.2 Apple Pay

Apple Pay 通过银行、银联及 Apple 公司三方 TSM 系统互联，使用户通过移动终端实现实体银行卡的远程加载。加载至移动终端的设备卡可用于近场和远程支付。

在 Apple Pay 中，一个重要的概念是“设备卡（DPAN)”，即加载于特定移动设备上的 eSE 内，与申请使用的实体卡后台主账户相关联，借助移动设备相关功能共同完成资金支付功能的金融应用。Apple Pay 的设备卡是基于支付标记的真实卡的替代，对于采用银联提供支付标记服务方案的，设备卡即银联 Token。

设备卡的生成过程，关键的步骤是生成设备卡号和芯片个人化数据，生成设备卡号的就是支付标记申请过程。银联可信服务管理平台 TSM 将用户申请基于 Token 的 DPAN 卡的请求转发给银行，包含用户所提供的持卡人及卡片验证信息，以及全手机厂商提供的风险信息；发卡行将申请授权结果告知银联 TSM。如银行通过用户申请，则由银联生成 DPAN（Token）卡个人化数据并下载到安全芯片中。设备卡生命周期管理过程中的激活、暂停、恢复注销等操作，也与支付标记生命周期管理中的同名操作相匹配。在上述整个过程中，银联 TSM 承担了 TR 的角色，向银联 TSP 系

统发起 Token 申请以及 Token 生命周期管理类的交易。

对于金融交易，POS、ATM 等支付终端上发起的基于设备卡的交易，在传递到银联后，会被传递到银联 TSP 系统实施去标记化处理（仅限银联生成 Token 模式），转换为基于真实卡号的交易，送交发卡行进行交易授权处理。而对于“银行自发 Token 模式”，整个跨行交易处理过程与普通银行卡交易无任何差别，银联系统将设备卡交易直接传递到发卡银行，由发卡行自行去标记化并进行授权处理。

7.3 Samsung Pay

韩国 Samsung 公司与银联在移动支付领域的合作内容是 Samsung Pay。该支付产品的本质与 Apple Pay 类似，都是在手机设备的安全区域加载一张与持卡人真实银行卡片关联的设备卡，从而使手机变成了银行卡账户的载体。对于 Samsung Pay，设备卡也采用了支付标记化技术，通过支付标记替代真实卡号在手机设备上的存储。

需要特别说明的是，Samsung Pay 产品支持两种设备卡，其一是芯片卡，其二是模拟磁条卡。芯片卡模式与 Apple Pay 类似，需要在基于支付标记生成设备卡号之后，再生成与之匹配的芯片个人化数据并加载到手机设备上，使手机变成一张芯片卡。

模拟磁条卡模式称为“MST 功能”，即通过磁辐射技术向 POS 机发射磁道信息，模拟完成磁道刷卡交易。在该模式下，基于支付标记生成设备卡号后，再生成与之匹配的模拟磁道数据并加载

到手机上，使手机变成了磁条卡。不同于 IC 卡交易，MST 模式中没有芯片卡验证机制，虽然采用了支付标记化技术，可以防止卡号和卡号有效期泄露，但仍然存在磁道信息被侧录后发起欺诈交易的风险，因此，需要在磁道信息中增加 MST 验证码，实现磁道信息的动态变化。

第八章　支付标记化的影响性分析

中国银联支付标记化技术框架为无卡支付、移动创新支付提供了进一步的支撑和促进。由于标记请求方可能是传统交易流程中的参与者，如线上商户、收单机构、专业化服务机构或者发卡行，甚至是设备制造商（手机制造商），银联作为卡组织，可以更加方便地融合各参与方，提供更加有效、便捷的支付标记服务。该技术框架在不影响正常业务处理的前提下，避免了商户甚至是收单机构留存敏感数据带来的风险隐患，并实现了交易场景的验证，而银联也将致力于建设一个开放、平台化系统，更好为支付产业链的相关方提供综合的支付服务。

8.1 持卡人

在多数情况下，持卡人无需知道生成的支付标记和其账户的关系以及相关操作。但标记请求方（TR）也可以选择让持卡人知悉，并让持卡人参与标记申请过程中的 ID&V 流程。支付标记的后四位可能显示在商户的收据中，持卡人可据此感知支付标记的存在。另外，持卡人使用 Apple Pay 等产品时，绑定卡片后支付标记的后四位会显示在手机上，持卡人可通过与真实卡号比对，感知支付标记的存在。

8.2 商户

对商户而言，与基于主账号的交易流程类似，商户始终作为支付标记的受理方，商户将按现有的支付流程继续处理所有交易，包括授权和获取。对于部分特定的应用场景，商户可能作为标记

的请求方，例如在存留卡号信息的线上商户应用场景中。在这种情况下，商户需要依据银联接口标准采集和处理必要的数据要素。

通过支付标记，商户端不再处理或留存持卡人的敏感数据，更好的实现了账户数据的安全保护。相关机构需制定安全管理规范，禁止商户存储卡号。需要强调的是，支付标记不能消除交易风险，商户或收单机构仍需使用风险管理工具保护其他业务领域的安全。

8.3 收单机构

收单机构与现有交易流程中的处理方式一样处理所有支付标记交易，包括标记获取、授权、清算和差错处理。相关机构需制定安全管理规范，禁止收单机构存储卡号。

考虑到收单机构目前对持卡人的忠诚度分析、优惠券承兑以及风险监控等业务，均依赖卡号进行管理，在应用支付标记化后，会出现同一主账户派生出不同支付标记，收单机构无法关联的问题。因此，为了满足上述收单机构的需求，协助收单机构识别对应同一主账号的不同支付标记，银联研究支付账户参考号(PAR)的概念并提出了技术方案。(参见章节 3.6)

8.4 发卡机构

发卡机构将继续保持当前角色并维护持卡人和对应的账户关系，并在支付标记生态系统进行授权和持续的风险管理。发卡机构可能需要通过系统的改造，实现对支付标记交易的识别和处理。

另外，发卡机构既可以成为标记请求方，向标记服务提供方申请标记；也可以成为标记化服务提供方、自建 TSP。如果发卡行成为标记服务提供方需遵循以下要求或业务规则的要点，详细内容见相应业务规则：

8.4.1 EMVCo 的基本要求

- 负责支付标记的发行、生命周期管理和去标记化操作
- 建立完善的支付标记域控机制
- 支持 ID&V 验证接口
- 提供一套完善的标记请求方的注册、管理规范
- 为商户、收单机构、数字钱包服务商等提供标记请求的接口（根据业务需求）

8.4.2 银联相关要求

- 支付标记 BIN 号由银联分配

（1）支付标记不用于跨行业务，建议发卡机构基于银联已分配的卡 BIN 号进一步细分为支付标记专用 BIN,开展相关业务，并将支付标记专用 BIN 号报备银联，用于相关业务处理。

（2）支付标记用于跨行业务，发卡机构优先基于银联已分配的卡 BIN 号进一步细分为支付标记专用 BIN，并将支付标记专用 BIN 号报备银联；若发卡机构现有卡 BIN 号资源不足以支撑支付标记业务，可向银联申请新专用 BIN，承诺仅用于支付标记业务，并遵循银联的相关业务要求。

●支付标记 BIN 号明确区分借贷记账户属性，发卡机构不得改变该 BIN 号的借贷记属性

●同步支付标记与主账号的绑定关系至银联，用于后续差错业务

8.5 产业实施通用性标记化方案的意义

为使支付标记化服务更具通用性和互操作性，方案在系统交互、数据报文、交易路由以及授权处理上均应遵循互联互通的原则，尽量避免对现有支付处理系统的改造，并尽可能的使各参与方透明化的处理支付标记。结合支付标记的应用分析，可以提供支付标记化服务的主体主要包含卡组织和发卡机构，但如果支付产业链的相关方违背甚至破坏了相关原则，其影响性也会给产业带来更多的问题和困扰：

●银行卡组织负责提供支付标记 BIN，才能确保支付标记的通用性，支付标记 BIN 与卡 BIN 一样，是跨行交易的重要依据，涉及业务定价、品牌管理以及交易处理等方面。如果支付标记服务提供方未向卡组织申请支付标记 BIN，将对现有基于卡号的跨行通用体系造成冲击，违背了“谁的卡品牌，谁负责标记化管理”的原则，对行业监管造成不良影响。

●发卡机构若作为支付标记服务方，在开展跨行交易过程中，需要将卡号与支付标记的对应关系告知银联，否则对后续差错处理交易会造成影响。

●收单机构不应作为支付标记服务方，支付标记的主要目的是替换卡号，使得收单机构与商户不再保存卡号信息，如果收单机构作为

支付标记服务方，同时掌握卡号与支付标记，违背了提出支付标记化的初衷。

第九章　配套文档发布计划

为了让各参与方更好的了解和应用中国银联支付标记化服务，银联编制了相关技术文档以及参考资料供产业各方查阅，具体包括：

- ✓ 业务规则

  《中国银联支付标记业务指引》（2016 年发布）

- ✓ 技术文档

  《中国银联全渠道接口规范》（已发布）

  《中国银联支付标记化服务接口技术规范》（2016 年发布）

  《中国银联银联卡交换系统技术规范 Token 支付接口规范》（已发布）

总结

作为一项既全面创新又与现有支付产业很好融合的技术，支付标记化技术框架将促进支付创新，尤其是移动支付创新的不断发展。

中国银联基于支付标记化的产品与服务也朝着一个开放的、互操作性的方向发展，其目的是为持卡人提供更安全与便捷的移动支付与互联网支付服务。

附录：中国银联支付标记化 Q&A

1、什么是支付标记化？

支付标记化是指用唯一的支付标记替换传统卡号的过程。支付标记被限制在特定的设备、商户、交易类型或者交易通道内。利用支付标记化技术，商户和数字钱包运营商不再存储用户的卡号，取而代之的是，具有指定用途的支付标记。支付标记化的过程发生在交易背后，对消费者来说是透明的。

支付标记扩展了数据域，能存储更丰富的交易信息，这些信息详细描述了交易发起的具体场景，有助于提升交易效率。这不仅提升了消费者和商户的使用体验，而且可以作为预防和限制交易欺诈的有效措施。

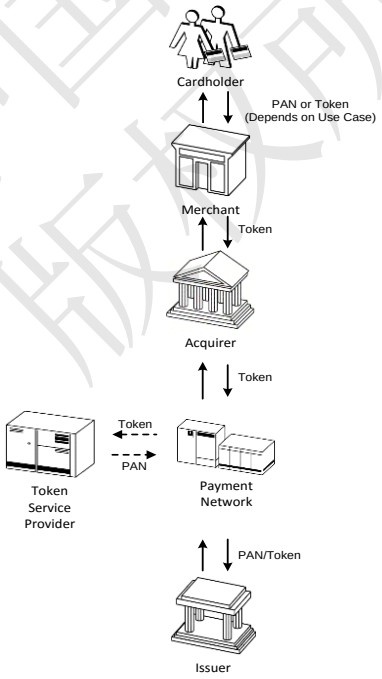

图 1：支付标记化过程示例

2、使用支付标记化技术的意义？

由于支付标记被限制在特定范围内使用，比如特定商户、支

付通道、数字钱包或特定的设备，在限制范围外欺诈交易的可能被大大降低。不仅如此，如果某个标记不再被使用（如消费者在某商户注销账户）或消费者丢失存有标记的设备（如手机），可解除该标记与原卡号的绑定关系。此外，支付标记化使商户或数字钱包运营商不再需要存储卡号。

因此，支付标价提升了交易安全性，一是大大降低电子商务等多种渠道的欺诈风险，二是有效减轻潜在的商户数据泄漏风险，三是进一步增强发卡行管理风险和提供个性化服务的能力。

3、支付标记和虚拟卡的区别？

虚拟卡是支付标记的一种特殊类型，通常被认为是一种和主卡关联的、一次一变的动态标记。采用特定的技术，虚拟卡能进行线上和线下交易，一般来说没有使用范围的限制，即虚拟卡没有被限制在特定的商户内使用，也没有细粒度的控制措施来限制其使用或保证其完整性。支付标记化规范同时支持动态标记（虚拟卡）和可用于多次交易的静态标记。

4、支付标记化和 3D-Secure(3DS)的关系？

3DS 是一种在传统的基于卡号和有效期验证之外，提供增强验证服务的线上身份认证工具。该技术保证用户在交易时获得进一步的反欺诈保护。支付标记化和 3DS 能够协同为用户提供服务。支付标记服务提供方在发行支付标记的过程中，还能够通过 3DS 协议为发卡行提供身份识别和认证的通道。

所有技术（支付标记、虚拟卡、3DS）都能协同交互且与卡

片共存。每种技术都代表支付领域为保证安全交易的一次演变。

注意：在发卡行的访问控制系统验证前，支付标记需执行去标记化操作，因此 3DS 协议需要进行修订。

5、支付标记化和数字钱包的关系？

支付标记化技术为数字钱包运营商和商户带来许多益处。不仅减少了潜在的数据泄漏范围，降低了消费者重新申请银行卡的风险，潜在地，在支付标记发行及其生命周期内，通过使用数字钱包用户的信息可以提高身份认证的准确性。

6、采用支付标记化技术，电子商户是否不再需要自建风险管理工具？

支付标记能降低电子商务中卡片交易的风险，但电子商务中存在广泛的与卡片信息无关的风险。因此即使支付标记能消除所有的支付风险（几乎不可能达到），商户仍然需要使用风险管理工具保护其他业务领域的安全。

7、支付标记化能解决哪些欺诈类型？如果得到广泛使用，能多大程度的消除欺诈交易？

支付标记化技术能够减少卡片数据泄漏后被用于欺诈交易的可能。因为支付标记仅能用于其生成时确定的交易场景，这样，即使标记信息泄漏，也不能用于其他交易场景，因此，欺诈交易的风险得到控制。

支付标记化技术不能完全消除欺诈交易，而是作为商户和收单机构分层安全防御体系的一部分，以减少和遏制针对无卡交易

的攻击。通过增强对恶意滥用卡片信息的防范措施，支付行业正在持续加强对欺诈交易的防范。

8、支付生态系统各参与方可从中获得哪些益处？

支付标记化技术增强了发卡行、收单机构、商户的数据保护能力，减少了潜在的欺诈交易和数据泄漏的影响。

持卡人可获得多方面的益处：支付标记的使用能减少数据泄漏的影响。一张主卡可生成多个标记，其中任何一个标记发生泄漏或者存储该标记的设备丢失，该标记可被禁用，减少了重新发卡的麻烦和可能引起的交易中断。此外，使用动态验证技术，持卡人可体验到更方便的购物体验，在某些情况下，持卡人不再需要输入敏感信息执行身份验证。

如果支付标记的生成属于支付凭证的发行环节。（即在芯片卡中或 NFC 设备中），对各参与方有如下益处：

●发卡行。对于移动数字支付方案，可以获得风险管理数据实现的一致性。此外，发卡行在部署创新支付方案时可以有更多的选择，通常创新支付方案比传统的卡片支付采用更强的验证方式。

●商户。商户可复用现有的支付设备，不需要建立专用系统保护支付信息。商户可以在更广泛的支付生态中复用现有的交易处理过程。一些交易场景中，比如由 NFC 设备在商户的非接触式 POS 机发起的标记交易，商户完全不需要参与支付标记的处理过

程。此外，支付标记可使商户为交易提供更好的担保，减少欺诈和高风险交易的可能性。

●收单机构。当前的收单系统可兼容最新的支付标记化规范。

9、持卡人的支付体验如何？

与现有体验相比，持卡人并不需要增加额外的操作。大多数交易过程中，支付标记对持卡人是透明的。持卡人只需正常发起交易，支付标记化的处理过程则在后台完成。然而，由于标记的最后四位可能显示在商户的收据中，持卡人可能借此感知到芯片卡或 NFC 设备中包含了支付标记。

10、支付标记的用途有哪些？

目前，支付标记和卡号的使用情形相同，可以发起线上或线下交易、兑现付款、支付账单、识别身份和人到人支付。通常情况下，卡片信息在交易链中被“标记化”以保证持卡人的信息安全，甚至持卡人都不知道卡号已被替换为支付标记。

11、支付标记化技术对支付生态的意义？

越来越多的消费者选择使用数字支付，并希望确保他们的卡片信息得到保护。与此同时，商户也在采用新的支付技术，寻求能持续保护持卡人信息的方式。

支付标记化技术不仅能增强数字支付的安全性，同时简化了在移动手机、平板、个人电脑和其他智能终端的购物体验。因此，支付标记提升了“安全性”和“购物体验”。

12、为什么支付行业需要支付标记化规范？

支付标记化的全球通用规范能为数字支付的各参与方提供一致、安全、可靠、互通的环境。对消费者来说，更高的安全性可以增强使用数字支付的信心。对商户来说，将更有信心采用一种基于通用框架并且适用于未来行业需求的新兴支付技术。

支付行业认为，支付标记化规范将保证一致性、提供产品的互操作性，并建立统一的安全等级。EMV 芯片规范已经在有卡交易中提供防欺诈保护，支付标记规范将在无卡交易和移动支付环境下提供类似的保护。

13、支付标记在何种情况下使用？

支付标记可在下列场景中使用：

- 大商户
  - 支付标记可替换大商户系统中的卡号。
  - 支付标记仅限在指定商户中发起交易。
  - 如果支付标记被用在其他范围，如另一家商户，支付标记服务提供方将识别出未授权的交易环境，拒绝此交易，并将其标记为欺诈交易。
  - 支付标记可用于分期付款。
- 数字钱包
  - 支付标记可替换数字钱包运营商系统中的卡号。
  - 支付标记仅限在指定数字钱包中发起交易。
  - 由于一个数字钱包可在多家商户使用，可通过生成密文以确保交易发起方的可信。

- NFC
  - 支付标记存储在 NFC 手机的安全芯片（SE）中。
  - 支付标记发起该类交易时，应选择 NFC 非接交易方式，并进行密文验证，其他交易发起方式将被拒绝。
- 二维码或条形码
  - 支付标记可在二维码或条形码支付中作为账户信息的标识。
  - 支付标记发起该类交易时，将被限制在 POS 的芯片交易模式中，并且可能需要密文验证。

14、建立 TSP 编号注册机制的目的是什么？

EMVCo 已开发出一套 TSP 注册流程。该流程能确保在全球范围内记录各个 TSP 分别代表的发卡机构。这对于标记请求方了解哪一个 TSP 是合适的支付标记申请对象非常重要，同时确保支付标记系统能和传统支付系统的交互操作，不发生冲突。

实现了 EMV 支付标记规范的机构都可以选择向 EMVCo 注册其 TSP，申请全球唯一的 TSP 编号。TSP 编号是由 EMVCo 分配的三位数字编号，可以唯一标识标记请求方和标记控制域间的关联关系。这有助于体现 EMV 支付标记服务机构的透明性。

15、支付标记化规范是否支持所有类型的卡，比如借记卡、信用卡、预付卡等？

是的。该规范可以支持所有卡片类型。

16、EMVCo 的支付标记规范是否只支持线下或线上交易？

EMVCo 支付标记化框架同时考虑了这两种场景。该规范与支付形式无关，一般认为诸如 NFC 支付的线下交易场景将从中获益。然而值得注意的是，支持有卡交易的商户至少在短期内将继续同时接受标记和非标记的交易。

17、EMVCo 的现有规范如何与支付标记规范互为补充？

芯片技术在有卡场景中为持卡交易提供了最全面的安全保障。预计安全芯片技术将继续为支付提供坚实的保护。随着行业升级移动支付系统，基于芯片的设备依然是非常重要的基础设施，因为移动 NFC 支付同样需要利用已有的芯片卡受理设备。更详细地说，当支付标记分发到芯片卡和 NFC 设备中时，能防范对交易中传输的卡片数据的侧录攻击和数据破坏，有效防止潜在的伪卡交易和账号滥用。

由于芯片卡技术能保护线下支付免受攻击，攻击者将攻击目标转移到交易过程最薄弱的地方。在许多地区，就是无卡交易。支付标记是一种防范攻击最安全和便利的手段。支付标记为电子交易的各参与方提供担保，确保潜在的欺诈行为能被有效识别、限制和管理。

这两种规范互为补充，共同为线下和线上交易创建一个完整、稳固的支付环境。该规范在兼容当前支付框架的同时，支持市场创新。更重要的是，该规范促进了全球互操作性，能提供一个使用便利、市场有序、产品最佳的市场环境。

18、支付账户参考号（PAR）的目标是什么？

PAR 重新引入了一种对应关系，这是目前已经存在于支付生态圈中关于主账号（PAN）和 EMVCo Token 间的。 PAR 可用于关联 Token 交易和卡号交易，从而支持原先依赖于卡号的各种支付处理和增值服务需求。

19、为什么 EMVCo 标准引入 PAR？

PAR 的引入是为了解决目前受理侧（包括商户、收单机构、支付处理商）面临的如何关联 Token 交易和卡号交易的问题。PAR 将用于支持各种支付处理和增值服务。

20、PAR 是否可以用来发起金融交易或授权请求？

仅仅只有 PAR 本身不能用来发起金融交易，授权请求或任何其他报文，如请款，清算或退单。

21、对于卡号或支付账户，PAR 是唯一的吗？

支付账户是持卡人和金融机构之间对具体财务资金来源（例如信用卡，借记卡，商务卡，预付卡）所建立的一对一关系，可以通过一个或多个卡号来表示。对于每一个卡号，PAR 是唯一的。当一个支付账户拥有多个不同的卡号时，需要确保为每个卡号产生唯一的 PAR。

22、PAR 属于 PCI 数据范围吗？

请参阅 PCI 安全标准委员会的网站。 PAR 的使用和保护应按照国家，地区和当地的法律法规，包括隐私法。

23、PAR 可以作为消费者身份标识吗？

PAR 不会作为消费者身份标识，同样的， EMVCo Token 或卡

号也不旨在成为消费者身份标识。

24、按照隐私法律法规，PAR 是否属于个人身份信息（PII）或个人数据？

PAR 明确的不被用来识别持卡人，因此应最大限度地减少被归类为 PII（个人身份信息）/个人资料。但是，隐私法因司法管辖区不同而有差异，PAR 的分类也可能取决于实现方式。由于 PAR 被用于关联卡号，因此 PAR 可能需要满足法律和 BIN 管理方的相关要求。

25、PAR 是否可以被存放在磁条卡中？

一磁和二磁上没有足够的存储空间在已有的数据之外再存放 PAR。

26、PAR 如何影响定期付款？

PAR 对定期付款没有影响，因为仅仅只有 PAR 本身不能发起金融交易。

27、PAR 是否会在授权响应中传递？

根据 BIN 管理方的管理要求和支付网络在报文中对 PAR 的支持，PAR 可能会在交易授权的响应报文中传递。用于传递 PAR 的报文域是 ISO8583（1987 年）的 56 域， ISO8583（1993）的 112 域，和 ISO8583（2003 年）的 51 域。

28、谁可以产生 PAR？

BIN 管理方负责管理 PAR 的生成，并确保 PAR 的唯一性。

29、PAR 的生成和发布是否通过 TSP?

PAR 的管理，包括指定具有资格产生 PAR 的实体，都是 BIN 管理方的责任。TSP 可能会了解 PAR 从而支持业务处理，如 Token 申请和参与 PAR 的产生。

30、PAR 是否同时适用于 EMVCo Token 和卡号?

PAR 被分配给一个卡号，以及与该卡号相关的所有 Token。

31、PAR 是否是唯一的?

PAR 在由 BIN 管理方管辖的 PAR 生态系统中是唯一的。其中，BIN 管理方应拥有 EMVCo 分配的 BIN 管理方标识符（BCI）。BIN 管理方负责确保与其 BCI 相关 PAR 的唯一性。

32、谁分配 BCI?

EMVCo 分配和维护 BCI 的列表。各实体可以通过 EMVCo 的注册表和相关流程来注册 BCI。

33、PAR 有多少个字符，谁决定它的唯一值?

PAR 由 29 个字符组成，包含了 EMVCo 分配的 4 位 BCI 以及根据 BIN 管理方要求产生和分配的 25 个具有唯一性的字符。

34、根据 PAR 是否可以确定或预测 Token 和卡号?

PAR 的生成方法应保证其不能通过逆向计算来确定或预测卡号和任何相关的 Token。

35、终端如何在芯片卡交易中识别 PAR?

EMVCo 为 PAR 分配了 EMV 标签'9F24'。终端应能通过 55 域向支付处理机构或收单机构传递 PAR。

36、谁负责管理 PAR 具体的实现方式？

PAR 实现方式的管理属于 BIN 管理方的职责。

37、谁负责提供 PAR 的查询机制？

PAR 的查询机制应由符合 BIN 管理方要求的主体来支持。商户、收单机构、支付处理机构和 TSP 等主体可以将 PAR 的查询机制作为在交易处理中获得 PAR 以外的一种补充或替代方案。

38、PAR 允许的用途包括哪些？

PAR 的使用仅限于以下功能：

• 利用 PAR 和 Token 或 PAR 和卡号完成反向交易（如退货和退单）

• 满足监管要求（如反洗钱（AML））

• 执行风险分析（如识别欺诈）

• 执行其他 BIN 管理方定义的非支付类操作需求（例如在法律许可范围内，支持消费者自愿加入的忠诚度项目）

所有 PAR 的实现都不能与任何国家，地区或地方的法律法规，包括那些涉及隐私的条款产生冲突。BIN 管理方应在支付生态中定义所有与 PAR 用途相关的管理要求。

39、持卡人是否会感受到 PAR 的存在？

持卡人通常不会知道 PAR 的存在。持卡人对 PAR 的无感知不应以任何方式影响持卡人的交易能力。 PAR 的长度和格式一般无需对消费者友好。

40、当卡号改变后，同一个 PAR 能否继续使用？

当支付账户的生命周期发生变化，如丢失、被盗或换卡，相关 PAR 可以被同一支付账户中的后续卡号所使用。在这些情况下，是否继续使用相同的 PAR，BIN 管理方拥有自由裁量权。

41、PAR 是否只涉及 Token？

PAR 的目的是为了关联 Token 交易和相关的卡号交易。虽然 PAR 也可以有更广泛的用途，如 PAR 被分配给某一未执行支付标记化的卡号，但是，对于这样的底层细节问题，BIN 管理方拥有自由裁量权，这类实施层面的问题是在 EMVCo 标准范围之外的。

42、PAR 是否需要被包含在签名数据中？

对该问题，BIN 管理方拥有自由裁量权，这类实施层面的问题是在 EMVCo 标准范围之外的。

43、消费者账户停止使用后，PAR 可以被重复使用吗？如果是这样，在账户停止使用后多久可以再使用？

对该问题，BIN 管理方拥有自由裁量权，这类实施层面的问题是在 EMVCo 标准范围之外的。

44、仅仅只有 PAR 本身是否可以用于退单、退货和冲正？

仅仅只有 PAR 本身不能发起金融交易。只有 Token 或者卡号可以发起交易。

参考文献

[1] EMVCo Payment Tokenisation Specification Technical Framework 1.0

[2] EMVCo_Payment_Account_Reference（PAR）

[3] PCI Tokenization_Product_Security_Guidelines

[4] 中国银联支付标记业务指引