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

2015-07-01 发布　　2015-07-01 实施

中 国 银 联 股 份 有 限 公 司　发布

目　　录

中国银联股份有限公司（以下简称“中国银联”）对该规范文档保留全部知识产权权利，包括但不限于版权、专利、商标、商业秘密等。任何人对该规范文档的任何使用都要受限于在中国银联成员机构服务平台（http://member.unionpay.com/）与中国银联签署的协议之规定。中国银联不对该规范文档的错误或疏漏以及由此导致的任何损失负任何责任。

未经中国银联书面同意，您不得将该规范文档用于与中国银联合作事项之外的用途和目的。未经中国银联书面同意，不得下载、转发、公开或以其它任何形式向第三方提供该规范文档。如果您通过非法渠道获得该规范文档，请立即删除，并通过合法渠道向中国银联申请。

中国银联对该规范文档或与其相关的文档是否涉及第三方的知识产权（如加密算法可能在某些国家受专利保护）不做任何声明和担保，中国银联对于该规范文档的使用是否侵犯第三方权利不承担任何责任，包括但不限于对该规范文档的部分或全部使用。

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：赵海、周皓、周明、章明、李伟、陈芳。

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，从银联角度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，旨在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。而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。

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。
- 发卡机构，可以通过支付标记化方案发行虚拟卡，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。

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；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，支付标记化系统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，负责支付标记化系统（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。

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。在标记化系统中，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等等，它也会受到标记存储位置等其它因素的影响。

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，是支付标记系统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。

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。

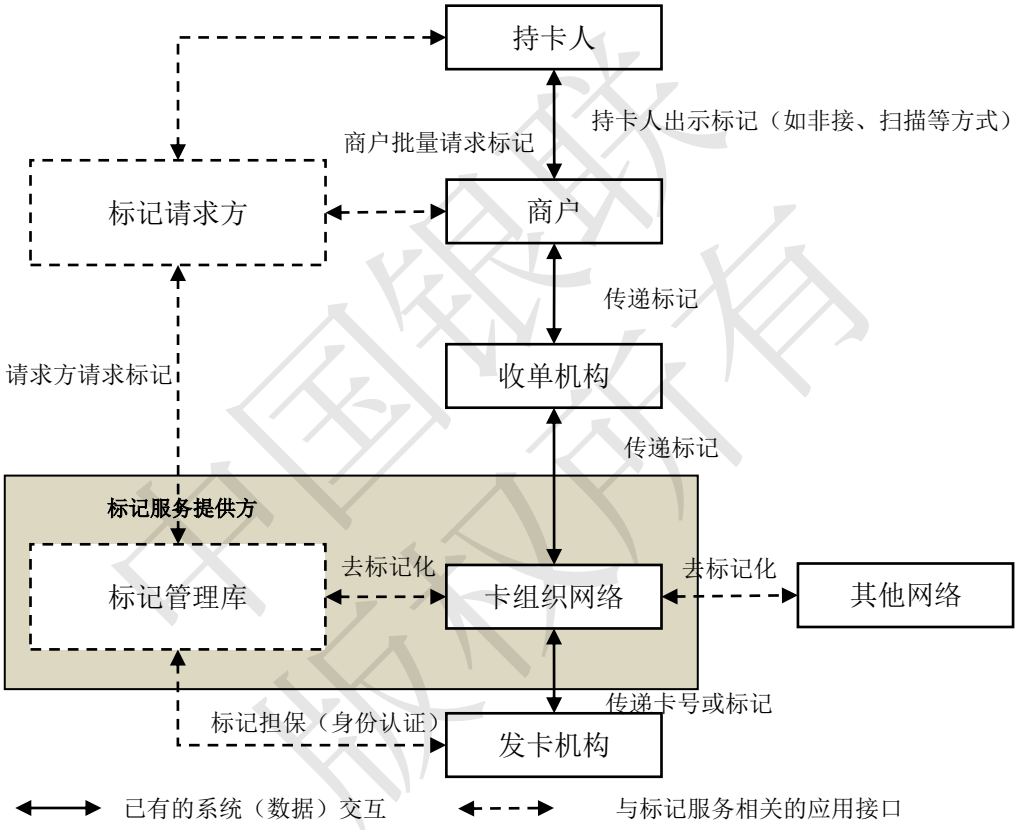

图 1：支付标记化系统架构

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

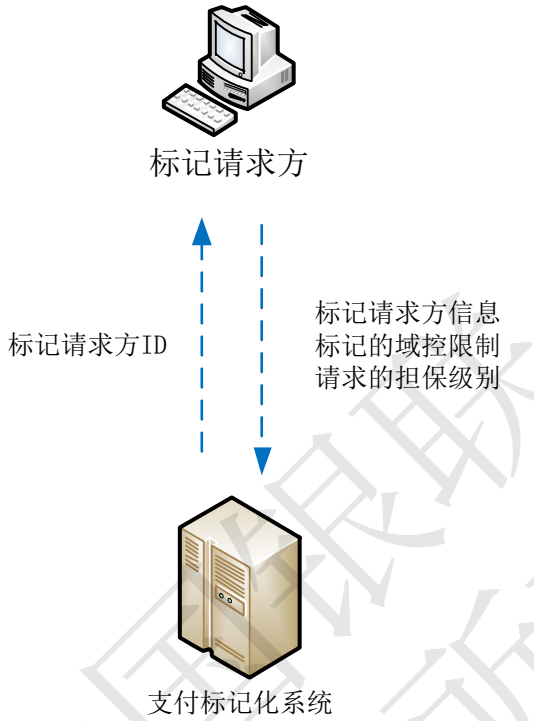

图 2：支付标记请求方注册流程

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：

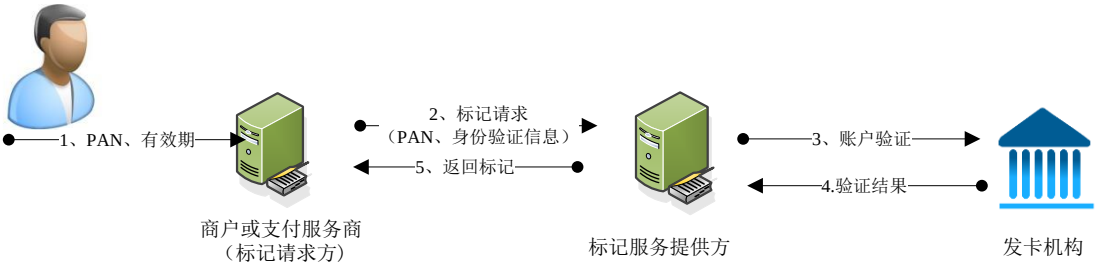

图 3：支付标记化申请流程

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

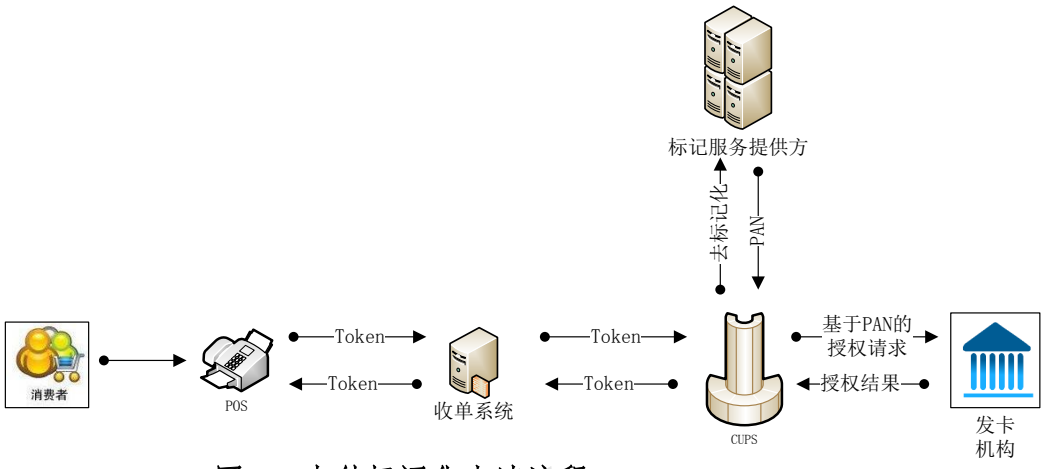

图 4：支付标记化申请流程

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。

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。担保级别的取值从 00 至 99，担保级别取值越高，则说明当前支付标记与卡号的绑定关系越可信；担保级别取值越低，则说明当前支付标记与卡号的绑定关系可信度越弱。此外，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，同时也立足本土市场，努力打造“银联安全认证与风险监控服务”，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 ApplePay 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。

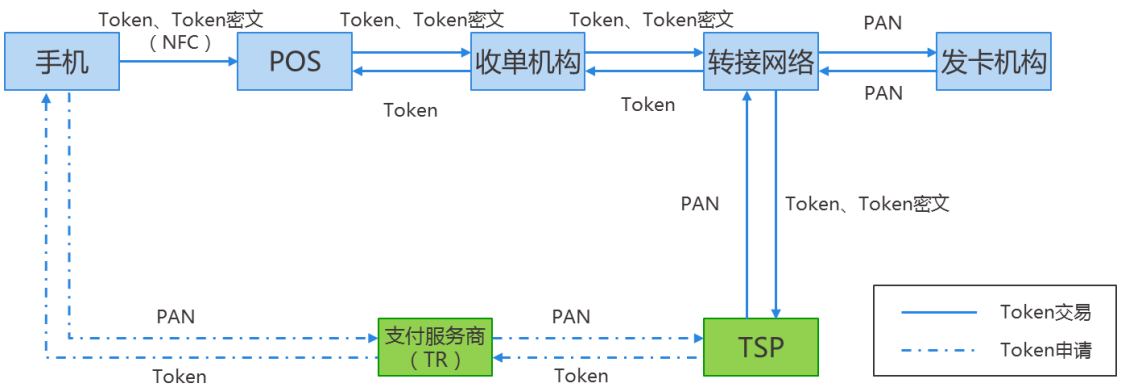

图 5：NFC 支付模式框架图

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。

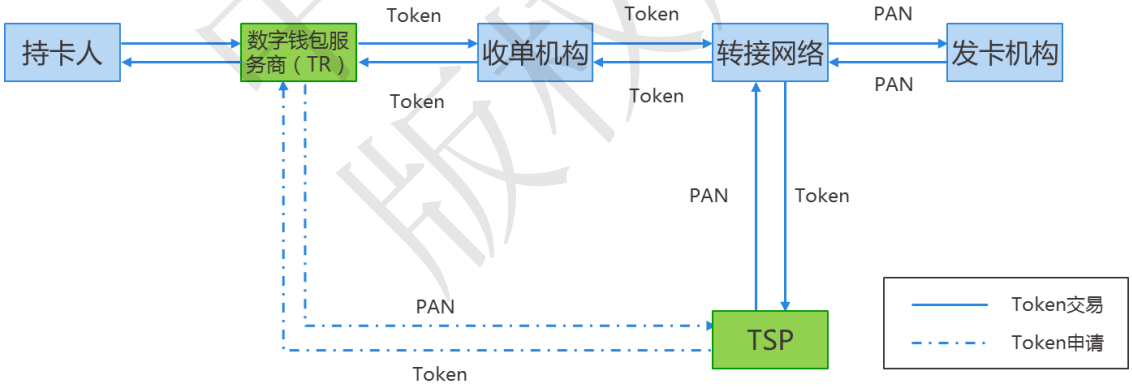

图 6：数字钱包支付模式框架图

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。

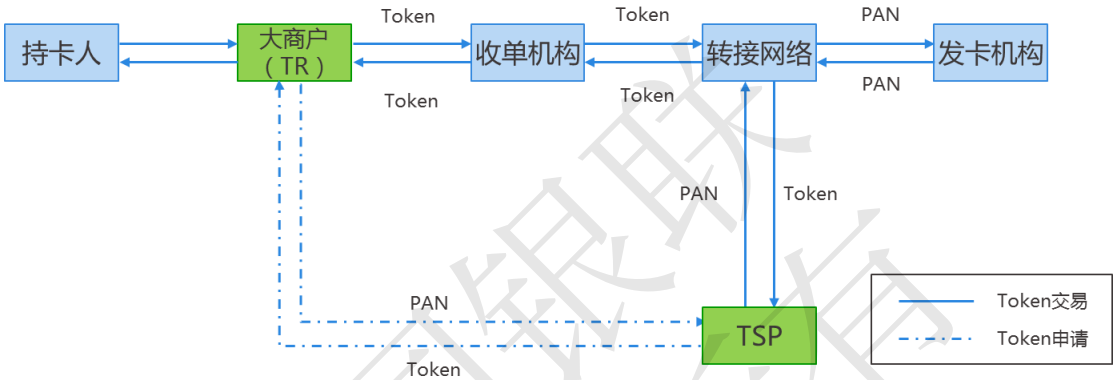

图 7：大商户支付模式框架图

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。

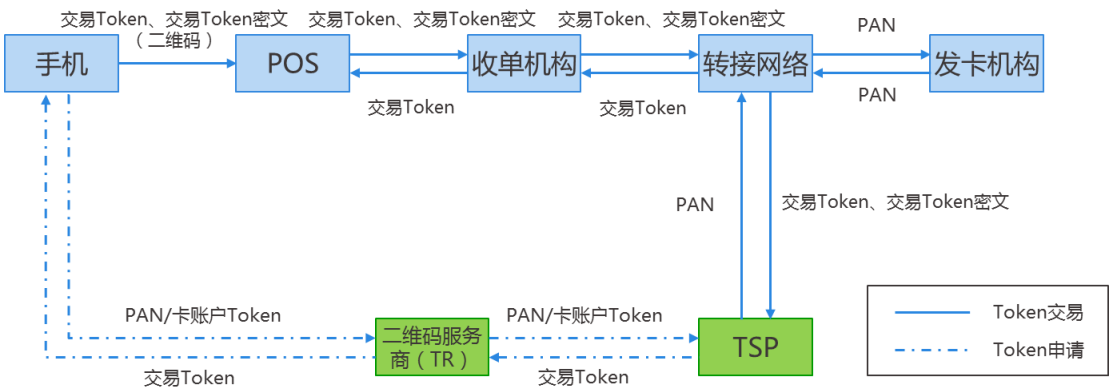

图 8：二维码支付模式框架图

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。目前，银联支付标记化系统已逐步实现对线上、线下交易产品的支持。银联明确了相关产品与技术实施路线图，同步编制了相关的业务规则、技术接口文档等等。

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 3 家大型线上商户试点接入，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。

未来，银联支付标记化服务将在诸如二维码、光子支付等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。

6.3 配套文档发布计划

另外，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支持要点》（向合作伙伴提供）

- ✓ 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管理服务接口技术规范》（2015 年下半年发布）

  《中国银联银联卡交换系统技术规范 Token 支付接口规范》（2015 年下半年发布）

第七章　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。

7.1 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。

7.2 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。

7.3 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。

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，银联正在研究提出账户参考号（PAR）的概念与方案。

7.4 发卡机构

发卡机构将继续保持其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、自建标记化系统。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：

7.4.1 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）

7.4.2 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

7.5 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，但如果支付产业连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。

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。

参考文献

[1] EMVCo Payment Tokenisation Specification Technical Framework 1.0
[2] 中国银联支付标记业务支持要点