

# 全球支付产业标记化发展趋势分析

中国银联股份有限公司 周皓 周明 赵海

支付标记化(Payment Tokenization)采用替代值(称为“标记”)来代替原始信息(如银行卡号)的方式,不仅可以应对在线支付与移动支付的市场竞争与安全问题,同时还兼顾了未来线上支付与线下支付融合的趋势,目前,我国境外已经形成了较为成熟的产品与商业模式。

## 一、支付产业中标记化的概念

标记化指用替代值代替原始信息(银行卡号等),支付标记化是指将标记化应用于跨行交易全环节。根据标记化的覆盖范围与应用目的,可以分为收单端标记、发卡端标记与卡组织标记。

(1) 收单端标记(Acquirer Token): 收单机构维护管理标记; 商户使用标记发起交易, 由收单机构转换为卡号送给卡组织。

(2) 发卡端标记(Issuer Token): 发卡机构维护管理该标记; 商户、收单机构与卡组织均使用标记处理交易, 发卡银行最终与原始卡号对应, 并进行交易处理。

(3) 卡组织标记(Payment Network Token): 卡组织维护管理标记; 商户使用标记发起交易, 经由收单机构系统, 被卡组织转换为卡号送给发卡银行。EMVCo 认为卡组织标记才能称为支付标记。

上述三种不同类型的标记在跨行交易流程中的数据转换如图 1 所示。

## 二、支付产业标记化发展现状

### 1. 收单端标记

在美国, 为收单机构或者商户提供卡号标记化服务(即收单端标记)已经是较为成熟的业务。

由于美国地区接连发生的持卡人账户信息泄露事件(如 2013 年美国零售业巨头 Target 公司发生顾客账户信息泄漏事件, 影响了 4000 万顾客), 商户希望不再保留持卡人卡号与卡有效期; 同时, 支付卡产业数据安全标准(PCI DSS)规定了有关卡号与卡有效期的技术保护措施——强加密与标记化, 如果使用了标记化将缩小 PCI 审计的范围。在业务需要与规范指导的背景下, 收单端标记已经成为美国地区多数收单机构(商户)的选择, 也培育了一批安全厂商(如美国 RSA 公司为 First Data 提供标记化服务, Visa 的子公司 CyberSource 对外提供标记化服务等)。

在美国以外的地区, 由于仅凭卡号与有效期无法完成交易(比如境内的在线支付交易通常需要输入动态口令或者使用安全性更高的 USBKey), 加上商户习惯于保留卡号用于增值业务, 所以收单端标记的需求并不是很迫切。随着互联网支付业务增长以及移动互联网时代的到来, 持卡人一方面追求支付的便捷体验, 另一方面也担心卡号信息等重要账户数据的泄露, 尤其是跨渠道

的滥用，因此，商户出于安全及客户体验考虑也已经提出不存储卡号的需求。

## 2. 发卡端标记

一直以来，发卡银行拥有金融账户管理权利，发出的卡号本质上也是其为持卡人账户建立的一种标记（称之为银行卡号），存放在磁条介质或者芯片介质、或者远程下发在手机安全单元（Secure Element, SE）中，卡号与印制在卡面上的卡号一致。随着二维码、主机卡模拟（Host-based Card Emulation, HCE）等业务技术发展，这一情况正在逐渐改变。

发卡银行认为，如果在二维码中放置卡号与有效期信息，或者通过基于 HCE 下发卡号和有效期信息存放在手机应用中，会面临着这些信息被泄露的风险，而这种风险极有可能演变为系统性风险。所以发卡银行也提出了将卡号标记化（生成临时卡号）的需求，这既能适

应移动互联网时代无卡支付的便捷要求，同时对发卡银行基于卡号的交易处理机制改动也相对较小。

据了解，西班牙、韩国等国家和地区的银行正在探索实践基于发卡端标记的产品；境内第三方机构在二维码产品中尝试脱机方式产生临时账户的方案，境内发卡银行试图借助 HCE 技术实现远程发卡（基于手机软件）。

## 3. 卡组织标记（支付标记）

EMVCo 于 2014 年 3 月发布的《支付标记化规范——技术框架 V1.0》首次在产业中提出了支付标记的概念以及框架体系。EMVCo 规范对于“支付标记化”的定义是：“支付卡号在跨行交易中被替代值（即支付标记）替换的过程，实施支付标记化可提高交易效率，提升交易安全，增加服务透明度”。EMVCo 定义的支付标记与卡号相同，一般由 13~19 位数字组成，而且该数值必须符合卡号的基本验证规则，被分配在一个发卡机构标识码

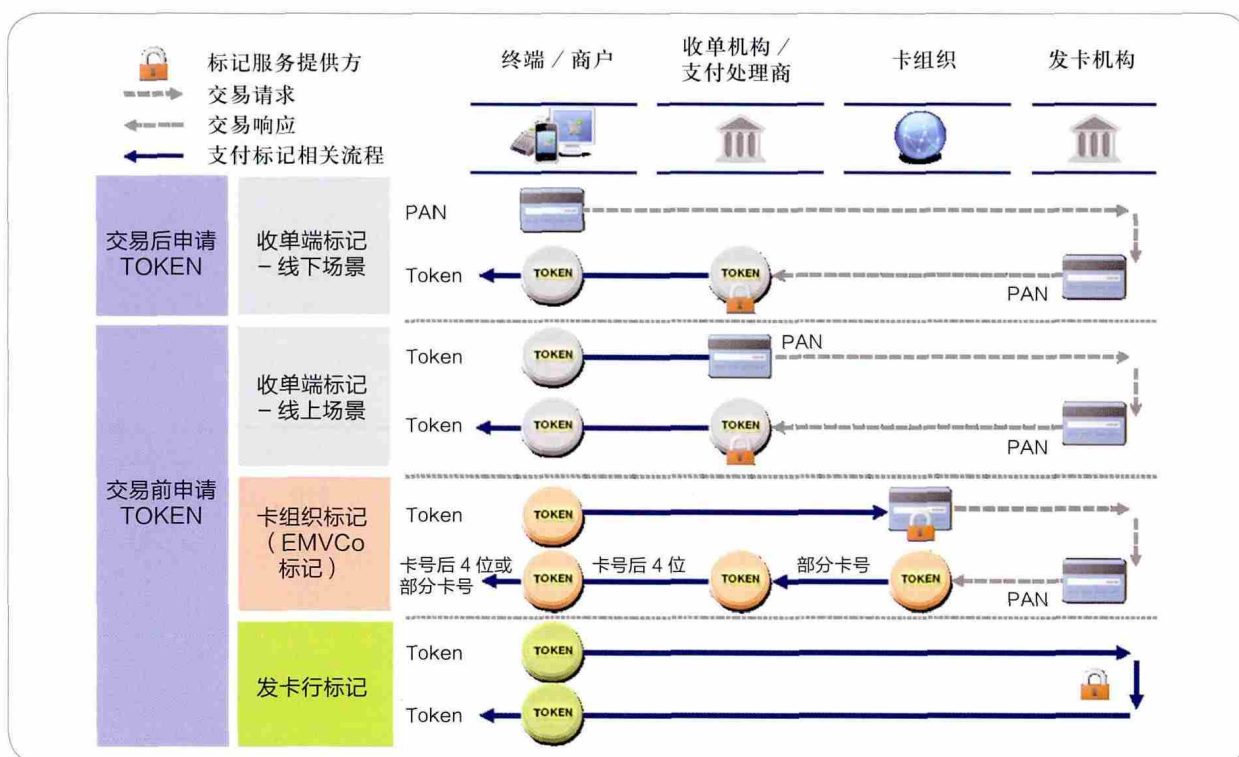


图 1 支付标记化在银行卡跨行交易中的应用流程

(BIN)范围内,且不得与真实卡号数值相同或冲突。除此之外,EMVCo还定义了支付标记的申请与处理流程、API接口,未来还将发布对于标记服务提供方(TSP)的认证要求。

目前,VISA已经率先面向市场推出了相关产品与服务:2014年6月2日,美国地区的全部VISA发卡机构已经按VISA技术标准完成了发卡系统改造,具备了支持支付标记化服务的条件;2014年6月12日,VISA在2014亚洲移动通信博览会上展出了基于云端的移动支付产品,也使用支付标记化技术;2014年9月,VISA开始宣传新的支付标记化服务,并已经在APPLE PAY中应用。

### 三、支付标记化发展趋势

根据对美国市场不同标记化主体需求的分析,并结合EMVCo技术框架对于标记化技术的研究,本文认为卡组织的支付标记化是连接产业全环节的标记化方案,囊括了收单端标记与发卡端标记,未来将与现有产业中的其他标记化方案并存发展。

#### 1. 支付标记化将成为新的安全解决方案、创新支付方案的基础

一方面,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大量持卡人的投诉,发生泄露事件的商户面临巨大的经济损失与法律裁决,美国监管机构对VISA、万事达也施加压力,要求加强对持卡人支付安全的保护。另一方面,VISA、万事达已经推广的3DS(Three Domain Secure)1.0在线支付安全规范,由于涉及发卡机构与收单机构复杂的系统改造,同时持卡人在交易中需要输入辅助认证要素,影响了支付体验,目前在全球(尤其是美国)的普及程度不高。因此,境外卡组织需要在不改变持卡人用卡号与有效期完成交易的前提下,有效提高在线支付与移动支付的安全性。

此外,苹果、Google等国际巨头试图通过变革性技

术进入移动支付领域,催生支付产业在创新领域保持快速发展。据报道,苹果公司正在围绕iPhone为中心打造移动支付系统;Google在新发布的Android4.4奇巧智能操作系统中支持新的主机卡模拟HCE技术,无需SIM卡等安全载体即可为持卡人提供NFC移动支付服务。由于苹果公司与Google均拥有过亿的用户,而且大多数用户已经将登录账户与卡账户绑定,因此在移动支付领域或将分流卡组织交易,VISA、万事达基于支付标记化提出了新的解决方案,如VISA的基于云端支付的方案,正是将HCE技术与支付标记化技术结合使用。

#### 2. 支付标记化角色分工将催生专业化服务商

EMVCo支付标记化框架在不改变现有产业各方分工的基础上,新增加了标记申请方(TR)与标记服务提供方(TSP)两个重要角色(EMVCo关于支付标记的生态系统如图2所示)。其中TR负责搜集持卡人卡号、有效期及相关信息,向TSP申请支付标记并将标记返回相关方;TSP负责产生支付标记、有效期及担保级别,并负责在交易过程中实现支付标记到卡号的转换。

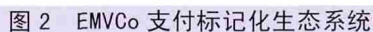
未来,支付产业会出现不同类型的TR,以卡组织为主体建设的TSP也会根据合作需求两两连接。

#### 3. 支付标记化将推动产业各环节的发展

EMVCo支付标记化规范实质提供的不是具体产品方案,而是全球通用的基础性技术框架。此次发布的支付标记化规范,拓宽了EMVCo原有在IC卡与终端领域制定标准的业务范围,开始涉足在线支付与移动支付等创新领域的技术标准制定。支付标记化除了可以有效支撑收单业务与发卡业务,也可以为产业提供增值服务。

##### (1) 对收单业务的支撑

目前收单端标记仅能解决商户存储卡号的风险问题,而卡组织支付标记不仅考虑了该需求,还增加了场景控制、身份认证等功能。比如EMVCo规范里面提到的COF(存储卡信息的大商户)、Digital Wallet(数字钱包)等两类场景。



依据；二是在支付标记应用环节，支付标记首先应在被限定的范围内使用，一旦超出了使用范围，TSP 会进行风险提示，其次，TSP 可以向商户或者收单机构提供标准化工具采集真实交易的环境信息，若环境信息（如持卡人在线支付的 IP 地址、智能手机的硬件序列号等）发生明显变化，TSP 会实时根据上送的环境信息进行风险识别与分析，将分析结果与已分配的担保级别进行对比，再次根据不同的情况进行相应的风险提示，利用云后台的处理能力为商户、收单机构与发卡机构提供相关的交易风险服务，这就是基于风险的身份认证（Risk-based Authentication）。FCC

（本文选自 2015 年金融科技活动周“金融科技惠民”主题征文）

EMVCo 发布的规范中关于担保级别的规定如下：

一是在支付标记申请环节，需要对持卡人与卡片进行双重的身份认证，既确保卡片的真实性，又确保持卡人的真实性，通过担保级别可以有效标识不同级别的身份认证结果，为后续的业务处理与风险职责分担提供重要