支付标记化技术解读

■ 中国银联　周明

1. 概述

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(Payment Tokenization)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。

简单来说，支付标记化(Payment Tokenization) 技术是由国际芯片卡标准化组织EMVCo于2014年正式发布的一项最新技术，原理在于通过支付标记(token)代替银行卡号进行交易验证，从而避免卡号信息泄露带来的风险。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的过程，同时确保该值的应用被限定在一个特定的商户、渠道或设备。支付标记可以运用在银行卡交易的各个环节，与现有基于银行卡号的交易一样，可以在产业中跨行使用，具有通用性。

支付标记化技术作为全球支付领域的最新前沿技术，其优势体现在三个方面：

第一，敏感信息无需留存，持卡人卡号与卡片有效期在交易中不出现；

第二，支付标记仅可在限定交易场景使用，使得支付更安全；

第三，支付标记灵活性更高，与传统银行卡验证功能相比较，支付标记综合了个人身份与设备信息验证、支付信息附加验证、风险等级评估等功能进行交易合法性识别和风险管控。因此，支付标记化不仅可防范交易各环节的持卡人敏感信息泄露，同时也降低了欺诈交易的发生概率。

其实早在2013年，中国银联就启动了支付标记化(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；并同步完成了配套的技术实施指引的编制，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。

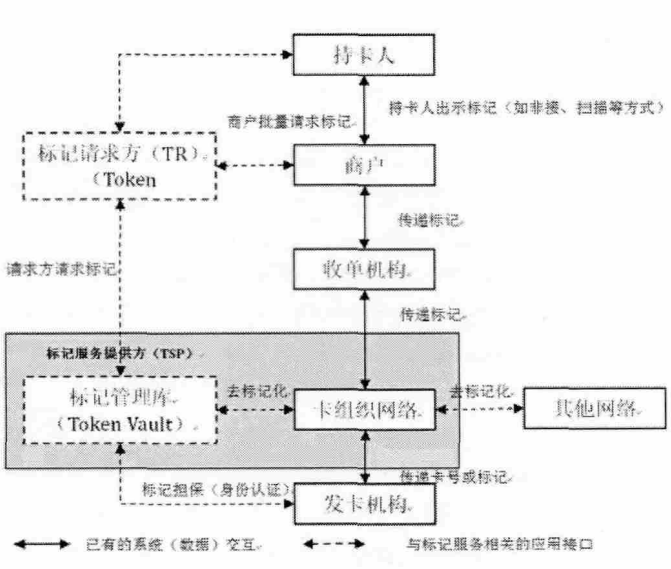

图1　支付标记化系统架构

2. 相关概念

2.1　什么是支付标记?

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　什么是标记服务提供方?

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。

2.3　什么是标记请求方?

标记请求方是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。

2.4　TR、TSP 的职责分工如何划分?

标记请求方是由标记服务提供方认证授权的实体(如商户、收单机构、发卡机构等)，作为授权的一部分，TSP 会制定TR 应遵守的规则和承担的责任。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，该号码由11 位数字组成，其中前三位为标记服务提供方的代码，后8位则有标记服务提供方分配。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。

而标记服务提供方必须得到支付网络(卡组织)授权，以便实现标记化的执行和报文交换。

2.5　什么是身份识别和验证?

身份识别和验证是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。

2.6　担保级别如何应用?

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。

2.7　标记的域控是什么，如何使用?

标记的域控表示标记被限定的使用场景，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。一个简单的例子就是线上商户，可以为该商户定义一个单独的域控，这样即使支付标记被攻击或者泄露，也不能用在其他支付交易场景中。

3. 技术框架

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主体及关系，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。

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。

3.1　标记请求方注册

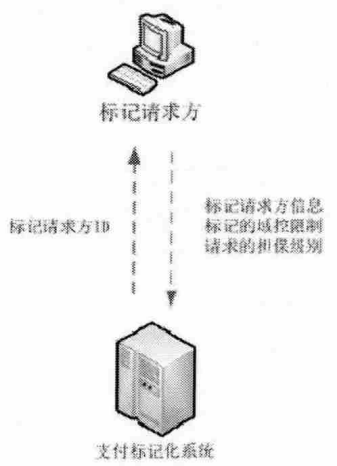

图2　支付标记请求方注册流程

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。

3.2　标记申请流程

图3概括性地描述了支付标记的申请流程：

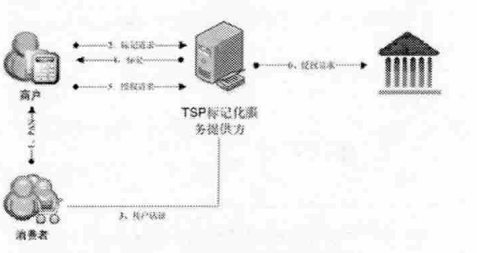

图3　支付标记化申请流程

(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。

3.3 标记的交易流程

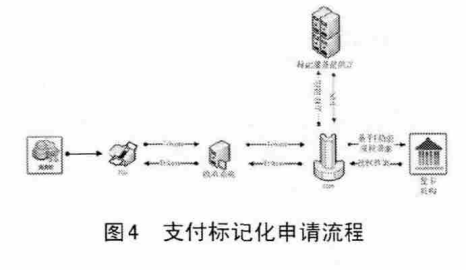

图4 支付标记化申请流程

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。

4. 推广思路

在学习了支付标记化技术的技术框架之后，我们再来一起了解一下支付标记化技术的推广思路及其主要应用。

传统基于卡片的支付方式中，已通过多种因素的验证和措施提升了支付的安全性和便利性。但随着互联网、移动支付的快速发展，现有的线上支付模式(基于卡号)尽管提供了快捷的支付体验，但其安全性也备受诟病。虽然诸如地址验证服务(AVS)、3DS认证以及动态短信码等方式的认证服务在一定程度上降低了交易欺诈的发生概率，但卡号的传递和存储仍然给交易欺诈提供了生存的空间。

而基于Token的支付框架为无卡支付、移动创新支付提出了一个新的思路：在不影响正常业务处理的前提下，消除了商户，甚至是收单机构系统中的敏感数据，并实现了交易场景的验证。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。

(来源：银行卡检测中心)

(上接第53页)

证书的安全载体，无线蓝牙mToken K5基于安全无线蓝牙通讯，多种加密算法防护，确保各种网银终端如智能手机、平板电脑、笔记本电脑安全；

(2) 通讯层包含Internet和无线网络应用，通过加密安全网络传输，对银行业务的中敏感数据进行保护，结合龙脉科技mToken身份认证锁，强双因子认证，为银行以及用户提供了转账、投资、缴费、个人账户管理等网上银行服务。

4. 解决方案

本方案采用龙脉科技设计研发的双界面无线蓝牙mToken K5身份认证锁，龙脉科技mToken K5是专门为金融行业如网上银行，手机银行如智能手机、平板电脑等研制的用于网络安全认证和通讯加密的智能卡双界面KEY，以网上银行以及手机银行平台作为基础，基于PKI/CA安全体系，为银行以及用户提供身份认证、身份识别和信息加密等服务。

龙脉科技mToken K5同时支持USB接口和蓝牙无线两种通讯方式，支持Windows, Linux, Android, IOS等多种操作系统，适用于PC机及各种移动终端，如手机、PDA、平板电脑等，可用作基于公钥体系(PKI, Public Key Infrastructure)的各种应用，如电子邮件加密、数字签名、安全证书、VPN、SSL等等，并可提供多种产品形态，并且，因其提供蓝牙接口，可支持短距离无线通讯，所以无需外接连线且便于携带，为用户提供极大的便利。

5. 方案总结

随着无线通信技术的发展，将会有越来越多的应用从传统的PC机平台向无线终端平台转移，手机银行将会有更广泛的应用。而基于PKI/CA技术体系的安全防护手段将能有效促进这些应用的安全使用，采用身份认证锁作为证书的安全载体，通过在关键业务中引入符合电子签名法要求的可信数字签名，将会更好地为网上银行以及手机银行提供安全保障。