硕 士 研 究 生 读 书 报 告





题目 浅析支付标记化技术

作者姓名 肖梦婷

作者学号 21651161

指导教师 李启雷

学科专业 软件工程

所在学院 软件学院

提交日期 二○一七 年 一 月

Research on Payment Tokenization Technology

A Dissertation Submitted to

Zhejiang University

in partial fulfillment of the requirements for

the degree of

Master of Engineering

Major Subject: Software Engineering

Advisor: Li Qilei

By

Xiao Mengting

Zhejiang University, P.R. China

2017

摘要

随着移动互联和大数据等技术的兴起与发展，支付行业面临着全新的机遇和挑战。支付的快捷方便对用户来说是不可降低的可用性标准，可是用户的敏感信息的安全性亦是需要保证的。目前，支付产业的各方参与者通过多种手段对交易中存在的欺诈行为提供了保护，如卡片伪造和账户滥用等。有卡交易的形式中，银联芯片卡规范在一定程度上确保了安全。但无卡交易逐渐普及，那么该如何对其进行支付安全保护，最大程度地减少用户账户数据被非法使用，并防止跨渠道的交易欺诈行为呢？支付标记化技术与系统有望解决这些问题。支付标记可以运用在银行卡交易的各个环节，并且适用于线上线下多种交易场景。

**关键词**：移动互联，支付安全，支付标记化

Abstract

With the development of mobile Internet and big data technology, the payment industry is facing new opportunities and challenges. Fast and convenient payment for users is not to reduce the availability of standards, but the user's sensitive information security is also required to ensure that. At present, the participants in the payment industry through a variety of means to protect the existence of fraud in the transaction, such as card forgery and account abuse, etc.. In the form of card transactions, UnionPay chip card specification to a certain extent to ensure the safety. But with the gradual spread of non card transactions, then how to pay for their security protection, to minimize the user account data is illegal use, and to prevent cross channel fraud? Payment Tokenization technology and systems is expected to solve these problems. Payment Tokenization can be used in all aspects of bank card transactions, and applies to a variety of online and offline trading scenarios.

**Keywords：**mobile Internet, payment security, Payment Tokenization

1背景

中国银行业协会于7月28日发布《中国银行卡产业发展蓝皮书(2016)》，称截至2015年底，中国银行卡累计发卡量达56.1亿张，人均持卡数为4.09张，2015年全国的银行卡交易金额为1420.8万亿元人民币。

报告同时指出，随着互联网行业的快速发展，银行卡欺诈风险逐渐向线上交易转移。在以往的线下交易中，银行卡被复制盗刷是高发案件，而在线上交易中，尽管不存在银行卡被复制盗刷的风险，但是交易仍需提供卡号和有效期，很容易给欺诈团体带来可乘之机。

除此之外，移动支付的兴起带来了新的支付技术和模式，尤其是第三方快捷支付，在给人们提供便利的同时，也给风险管控带来了新的挑战。据悉，目前市场上一些第三方支付机构在完成授权时，只需提供银行卡号和预留手机号码就可以办理，犯罪分子可以通过骗取验证码或者挂失手机号等方式获得支付授权，把钱转走。

今年以来，监管层加紧了对支付业务的监管。央行7月初下发了《中国人民银行关于进一步加强银行卡风险管理的通知》，要求各商业银行、第三方支付公司在今年底要使用支付标记化技术进行交易数据处理。支付标记化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，原理在于使用唯一的一个支付标记（与主卡号保持一致，一般由13至19位的数字组成）来替代银行主账号进行交易验证，从而避免卡号信息泄露带来的风险。支付标记化具有以下显著特征：降低敏感信息泄露可能性，具备兼容性和互操作性，促进行业创新的发展。

与传统基于卡号的交易传递过程相比，支付标记化方案替代了原始卡号和有效期，根本上杜绝了敏感信息泄露的可能。同时，通过域控属性限定交易场景（如交易类型、使用次数、交易金额、有效期、支付渠道、商户名称等），既便支付标记本身被泄露，其影响范围也大大降低。此外，收单机构还可以借助支付标记的担保级别实现对交易风险的控制，进一步降低风险。

支付标记化技术作为全球支付领域的最新[前沿技术](http://wiki.mbalib.com/wiki/%E5%89%8D%E6%B2%BF%E6%8A%80%E6%9C%AF" \o "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](http://wiki.mbalib.com/wiki/%E4%BA%A4%E6%98%93" \o "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](http://wiki.mbalib.com/wiki/%E6%A6%82%E7%8E%87" \o "概率)。

2简介

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。

## 2.1基本概念

（1）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。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）Tokenization

将银行卡号替换成Token，以及相关的支付处理过程称为Tokenization。当前Tokenization有多种译法，我们将其翻译为“标记化”，表明银行卡号被替换为Token(支付标记)，以作为支付凭证。标记化替换了银行卡号，但是没有替换银行卡生态系统。从这个意义上 而言，Tokenization是一个生态系统，而非具体的技术或产品。

（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。

（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。

（4）标记服务提供方

标记服务提供方（Token Service Provider，以下简称TSP）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。

（5）标记请求方

标记请求方（Token Requester ，以下简称TR）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。

（6）身份识别和验证

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。

（7）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。

（8）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。

（9）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:

1、远程存储，例如大商户的服务器；

2、SE存储，例如芯片，手机中的SE；

3、本地安全环境存储：例如TEE;；

4、远程安全环境存储：如云SE；

（10）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标记化的使用



图2.1 标记化的四种典型使用场景

标记化的全球性技术框架由EMVCo标准化组织于2014年3月发布。EMVCo在规范中仅描述了四种典型场景:在线商户、数字钱包、非接NFC支付、二维码支付，包括了线上支付场景与线下支付场景，但是其生命力远不止于此。如上述分析，标记化生态系统确保替换银行卡号后，支付得以顺利开展，因此只要应用银行卡号的支付场景，都可以实现标记化，相关的安全技术以及业务方式都可以在其中体现。

## 2.3移动支付安全性

随着智能手机和移动网络的迅猛发展，移动支付进入了千万人的生活，支付标记化技术的推出为支付业务提供了一个相对安全且便捷的解决方案。标记化在四个方面提升了移动支付的安全性：

一是交易处理依靠Token而不是卡号，也就是说卡号信息得以保护，要泄露的也只能是Token。Token和卡号不会同时用于交易路由判读，商户与收单机构仅存有Token，实现了对卡号信息的保护，防范了卡号泄露风险。掌握 Token和卡号绑定关系的机构称为TSP(也就是Token服务提供方)，比如卡组织，或者发卡银行，它负责Token的发行与验证，为从Token到卡号的还原提供相关的验证服务。

二是Token被限定在特定的应用场景。Token即使被泄露也往往没有用武之地。Token的发行需要可信的机构向TSP申请，申请方称为TR(Token请求方)，可以提交Token的限定场景(比如说苹果公司发起Token申请，希望限定Token在某台iPhone使用，再比如某网站发起Token申请，希望限定Token在该网站使用)。这一措施降低了Token泄露后的影响范围。

三是标记化提出分层次的验证机制。发行Token类似发行银行卡，银行在发卡时会对持卡人开展身份核实与信用风险评估，TSP在发行Token时也要开展身份验证，根据不同的验证手段与可信程度，对验证结果分层描述，可分为高安全、中等安全、低安全以及无身份验证等层级，甚至可以用数值精准地描述。验证结果返回给TR，并出现在交易过程中，供参与交易的各方开展交易风险监控时参考。

四是标记化兼容现有的技术以及业务模式。比如说应用Token以后，不用担心持卡人无法选择正确的卡支付，因为卡号的后四位仍然会出现在商户网站，用于提示。再比如IC卡的身份认证机制，包括联机认证与脱机认证，这两种认证方式均可以结合Token使用。因此，Token应用无需持卡人感知并做出改变。

3 技术方案

## 3.1系统架构

支付标记化系统架构(如图3.1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。

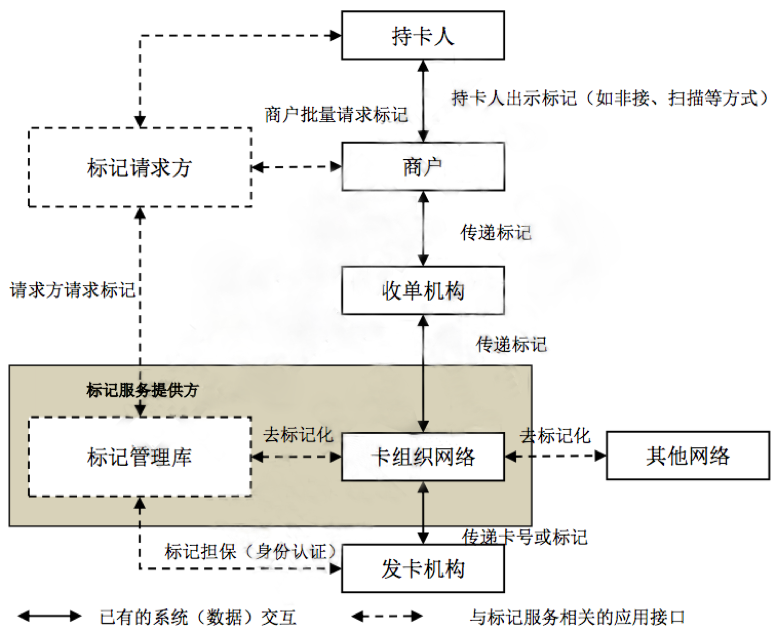


图3.1 支付标记化系统架构

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

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3.2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。

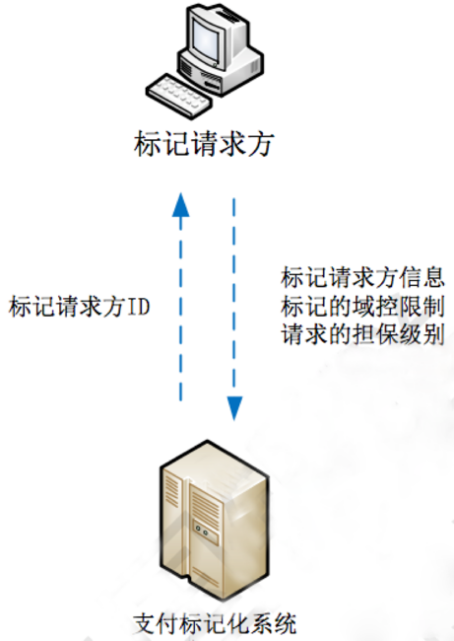


图3.2 支付标记请求方注册流程

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

图3.2概括性地描述了支付标记的申请流程。

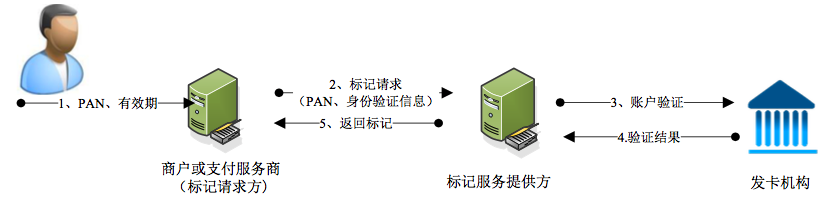


图3.3 支付标记化申请流程

标记申请流程如下：

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标记交易流程

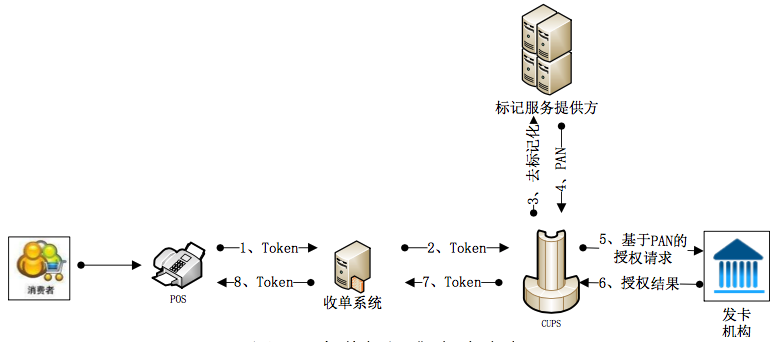


图3.4 支付标记化交易流程

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 应用模式

## 4.1四种支付模式

（1）大商户支付模式

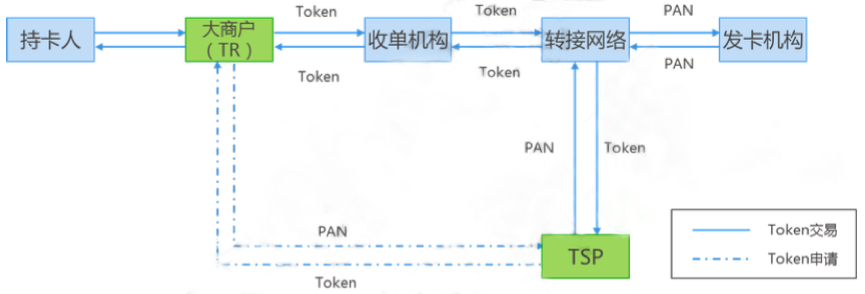


图4.1 大商户支付模式框架图

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。

（2）数字钱包支付模式

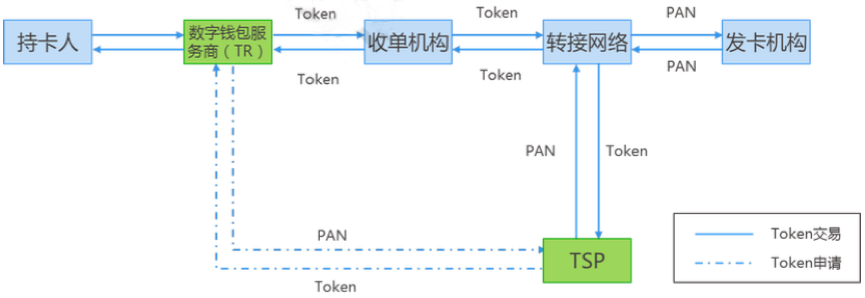


图4.2 数字钱包支付模式框架图

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。

（3）二维码支付模式

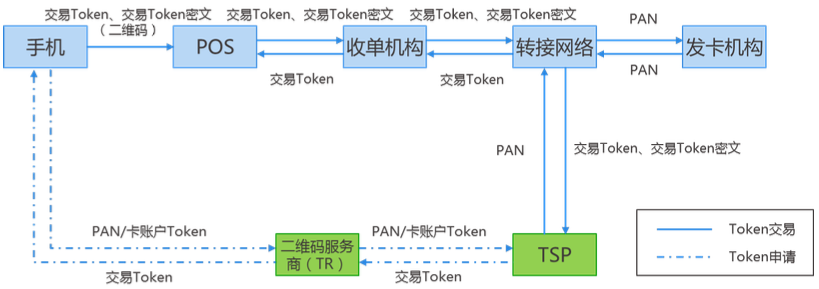


图4.3 二维码支付模式框架图

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4.3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。

（4）NFC支付模式

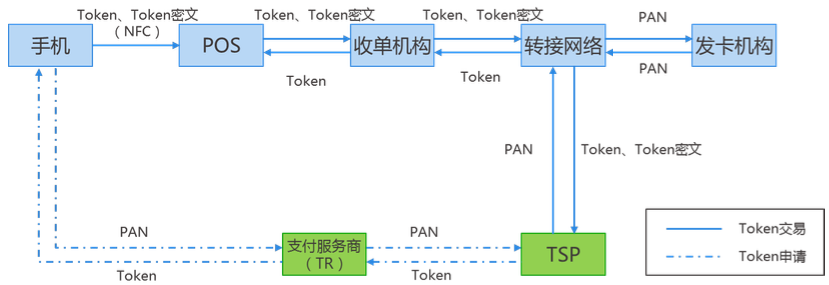


图4.4 NFC支付模式框架图

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。

## 4.2苹果支付（Apple Pay）应用模式

2014年9月9日，苹果公司在发布会上提出了新的支付方式Apple Pay。Apple Pay由NFC近场通信技术、Touch ID指纹识别、安全控件以及Passbook(电子票券管理工具)组成，使用时只须手指按在 home键的指纹识别上，手机靠近支付POS终端，即可完成支付。

想使用Apple Pay，首先要绑定信用卡，在iPhone输入信用卡信息，Apple Pay把信用卡信息发送到卡组织处验证，卡组织验证通过后，会为这张信用卡生成一个Token，并将Token发送到Apple Pay，Apple Pay再把这个加密的Token发送到iPhone。iPhone上不直接存储信用卡信息，而是将Token存放在iPhone中的独立安全芯片中 (SE芯片)，用它代替信用卡的卡号，可以理解为Token和信用卡的卡号等价，但即使Token泄漏，也无法逆向还原出信用卡信息。Token的格式其实是一个16位字符串，它与传统POS机协议里的格式是兼容的，这意味着Apple Pay兼容整个传统信用卡支付网络。无论是刷信用卡，还是用Apple Pay，在整个传统支付体系中都是透明的。在使用时，还有关键一环“Touch ID”，只有指纹认证通过的时候，iPhone才允许利用NFC读取Token出来。

Apple Pay可以看作是基于Token技术的典型应用，在这个新型的支付模式中有几个新的参与方使得这种模式的推广充满新的机遇。TSP（Token服务方）根据TR（Token申请方）提供的用户主账号(PAN)与发卡行协商生成Token后，将Token作为PAN的替代值，流转在支付的各个环节，使得在支付流程中独一无二的PAN只在TSP、转接方、发卡方之间传递，由于三者专线连接且彼此互信，且当Token被检测到风险或到期时，将再次生成新Token替代，从而大幅降低支付过程中PAN泄漏的可能性，极大地提高了PAN的安全性。

由此可以得出，Apple Pay本质上还是一种联机刷卡的解决方案，没有改变传统的支付模式，虽然支付过程参与方增加，但增加的参与方仍是之前的各方，所做的改变是增加了安全保障和提升了用户体验，利益方并没有大的改变，对于使用者来说，这种改变是安全和高科技带来的便捷。

## 4.3Android平台的HCE技术与Token应用

2013年Google公司发布了Android 4.4 KitKat版本，新增一种系统服务HCE技术，即基于主机的卡仿真 (Host-based Card Emulation)，这是一种以App或云端实现安全认证的NFC接口，可以取代基于SWP协议的NFC应用，改变了必须使用电信运营商SIM卡作为SE的模式。

在国内智能手机领域，Android平台是首屈一指的，Token技术是否适用 Android平台呢?接下来我们以高安全度的HCE云端认证方式来探讨Token技术的应用。

HCE模式的支付系统由手机端App、TSP(Token ServiceProvider，Token服务方)、TSM (TrustedService Manager，可信服务管理)、发卡行、商户等几部分组成，核心是手机端App和TSP、TSM间的安全通讯。这个过程可以由非对称密钥体系来保护。非对称密钥体系可以采用国密算法SM9，手机端和TSP端采用指定公钥的方式生成密钥对，其中公钥包含了三个部分:用户密码、随机数和 IMEI(International Mobile Equipment Identity，移动设备国际识别码)。

交易过程中的数据采用加密通讯，加密密钥由TSP端每次随机生成，使用公钥加密后传递给手机App，由手机App解密后在内存中暂存。Token由私钥加密后保存在App的安全域(SandBox)中，在交易过程中，手机App不解密， 直接经由通讯加密密钥加密后传输给TSP。TSP使用通讯加密密钥解密后，再使用公钥解密获取Token原文，再将Token转换为用户信用卡卡号，由TSP通过专用网络与发卡行进行通讯，完成交易。TSP 获取到交易成功或失败的信息后，再将此信息经由加密通讯密钥加密传送给手机端，从而完成全部交易流程。

在这个交易过程中，NFC的安全脱离了电信运营商的SIM提供的SE，APP的安全认证由HCE在云端采用非对称密钥体系完成，Token保存在APP 中，Token的交换过程与Apple Pay相同，差别在于从手机中Token的获取过程，Apple Pay通过Touch ID来实现，而Android的HCE则由非对称密钥体系保护在云端完成，从使用的安全性来说相差不多，但从国内的金融环境和智能手机形态来说，这种方式即摆脱了电信运营商的限制，又极大的减化了安装部署的工作，提升了使用的便捷性。

5 小结

随着移动互联网的进一步发展，以及众多移动支付产品在全球范围内的加速推广，Token和Tokenization注定将频繁出现在业内外的关注焦点中，也必将与各类创新支付相结合。这一枚Token为移动支付产业描绘了一个更加美好的明天，也为监管部门以及银行卡组织提出了新的课题。如何建立完善一套开放、统一、公平、合理的技术标准与业务规则，以及认证检测体系，将是下阶段产业各方需合力优化完善的重点。

参考文献

[1] 中国银联股份有限公司. 中国银联支付标记化技术指引[M]. 2016.07.

[2] 梁丽雯. 支付标记化技术:防盗防泄密利器[J]. 金融科技时代, 2016(8):84-84.

[3] 周明. 支付标记化技术解读[J]. 金卡工程, 2015(9):54-56.

[4] 赵懿. 探析基于Token的“商户-卡组织”线上支付模式[J]. 金融电子化, 2015(9):47-51.

[5] 陆水. 二维码支付——电子银行3.0时代的利器[J]. 金融电子化, 2016(9):49-50.

[6] 周皓, 周明, 赵海. 全球支付产业标记化发展趋势分析[J]. 中国金融电脑, 2015(6):45-48.

[7] 张慧琳, 赵云辉. 浅析基于支付标记化技术的移动支付安全方案[J]. 信息安全与技术, 2015, 6(7).

[8] 罗锦莉. 支付风控新术上线[J]. 金融科技时代, 2016(9):80-83.

[9] 佚名. 华为牵手银联推出Huawei Pay[J]. 中国信息安全, 2016(4):104-104.