# Token移动支付

## 一、与传统支付的差别

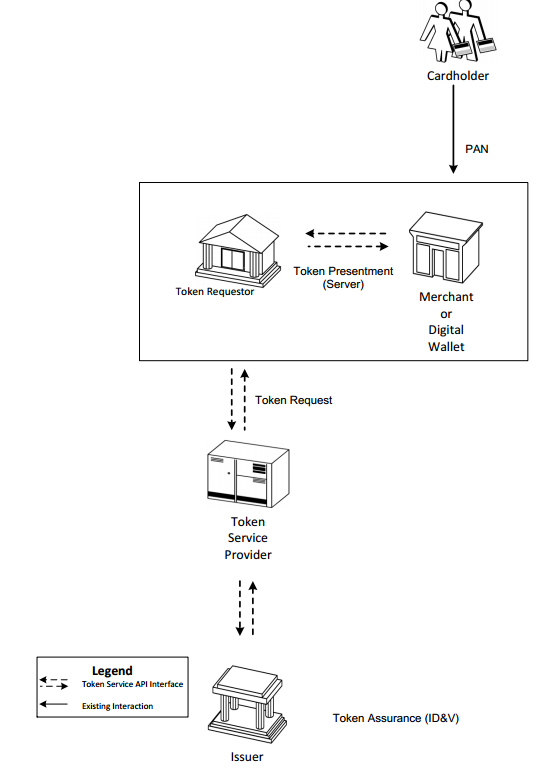
Token体系中，除了传统电子支付参与方外，新增了2个参与方，如下图所示：

|  |  |  |
| --- | --- | --- |
| Token系统参与方 | | 角色实例 |
| 传统电子支付参与者 | 持卡人（Cardholder） | 手机，移动终端 |
| 商户（Merchant） | 超市A |
| 收单方（Acquirer） | 银行B |
| 支付网络转接方（Payment Network） | 银联 |
| 发卡方（Card Issuer） | 银行B |
| 新增参与方 | 令牌请求方（Token Requestor） | 终端支付应用 |
| 令牌服务提供方（Token Service Provide） | 银联 |

Token的应用原理：Token SP根据Token Requestor提供的PAN(主账号)生成Token后，将Token作为PAN的取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Token SP、转接方、发卡方间传递，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。

## Token应用的典型流程

### 2.1 Token的申请流程



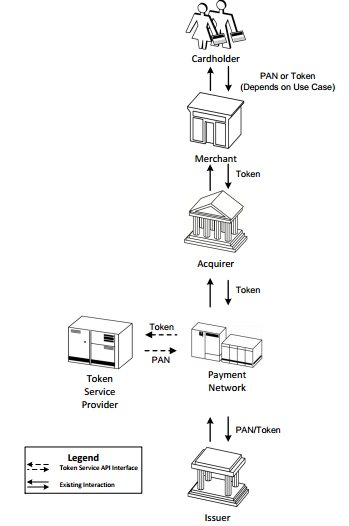
1)、 终端传递PAN至Token Requestor;

2)、 Token Requestor向Token SP发起Token申请，发送PAN;

3)、 Token SP根据PAN，生成对应的Token并返回至Token Requestor，同时建立PAN至Token的映射并存储在Token库中，与发卡方共享此Token库;

4)、 Token Requestor将返回的Token传递至终端。

### 2.2 Token交易流程



1)、 Token从终端开始，依次传递至POS、收单方、转接方;

2)、 转接方通过与Token SP的接口，发送Token至Token SP;

3)、 Token SP对Token执行去令牌化操作，并将PAN传递至转接方;

4)、 转接方将Token&PAN传递至发卡方，发卡方用Token库进行验证，验证通过后，再将PAN传递至转接方;

5)、 验证后的Token从转接方开始，依次传递至收单方和POS，之后Token作为PAN的替代值继续后续的交易流程。

可以看到，在交易过程中，PAN传递且仅传递在Token SP、发卡方和转接方三者之间。

## 三、各个环节的职能

1、Token Service Provider

被授权的实体，为已经注册的令牌请求者提供支付令牌。主要功能包括但不局限于一下几点：

a维护和管理令牌库

b生成并发行令牌

c为令牌请求者提供注册

d处理令牌申请

令牌服务提供者负责建立和管理自己私有的令牌请求APIs、令牌库、令牌申请平台、和注册服务。

1. Cardholder

持卡者扮演的角色并没有发生变化，并且他们也并不用知道自己交易过程中是使用Token代替卡号进行交易的，相应的，为了给令牌提供保障，令牌请求者（例如电子钱包，支付宝钱包）会要求持卡者参与到身份识别和验证的过程。

1. Card Issuer

卡发行者扮演的角色也没有变化。与持卡者保持这账户关系，并进行授权和风险管理。

4、Merchant

商户将使用支付令牌取代个人卡号。其他过程保持不变，为了增加互操作性，商户需要添加标准中规定的数据元素。

5、Acquire

收款方职能不变，但是需要添加标准中规定的额外数据域。

6 、Payment Network

支付网络转接方，Payment Network可以充当Token Service Provider。如果不充当Token Service Provider，则Payment Network必须补充相应方法能同Token Service Provider进行交互处理Token。

7、Token Requestor

令牌请求者（可以是传统支付产业、包括电子钱包，支付宝等等），令牌请求者必须在令牌提供者处注册，成功注册后会获得一个Token Requestor ID，获得ID后，请求者还需要补充相应的Token API，这样之后才能发起令牌请求。

## 四、Token与PAN绑定中的身份认证以及信用评级

### 4.1 身份认证信用评级

Tokenisation标准中对Token和PAN(银行卡账号)映射的过程，提供了不同认证方法对应不同信用评级的绑定过程（根据不同认证方法从00最低保障到99最高保障级别）。该过程一般由Token sp 进行。在这个过程中，Token sp需要维护两个必要的新数据元素：Token 验证级别和Token验证数据。并且无论级别高低都需要和发卡行交互这两个数据元素。标准定义的常用绑定时认证方法从低级别到高级别依次有如下方法：

1. 没有进行任何身份验证的绑定；
2. 账户验证，主要验证账户有效性；
3. Token sp对账户进行的风险评估（依据自身维持的账户授权信息）
4. 根据Token发出的请求数据，请求数据一般包括：账户年限和历史记录，账户联系人地址和联系方式，Ip地址，设备ID和设备信息，GPS定位信息，交易频率等；
5. 发卡行直接对持卡者的验证，例如邮件验证，短信验证码等一次性密码验证，手机银行验证；

以上五种方法从认证级别来依次加强。认证方法作用于Token的发行、申请和交易场景控制中。Token SP负责维护这个信用评级，在Token的使用过程中，持卡者也可以申请提升信用等级。

### 4.2 Token的生命周期管理

Token SP需要负责支付Token持续不断的进行管理和更新，因此Token SP需要提供接口来处理Token在生命周期中可能面对的各种事件。标准中明确指明的可能发生的Token事件包括一下几点：

1. 失去关联的Token。可能的事件导致：设备丢失或失窃，银行卡丢失或者失窃，银行卡号存在欺骗警告，Token存在欺骗警告等，这些情况时Token会失去与卡号的关联。
2. Token暂定服务。可能的事件导致：临时的暂定服务因为设备丢失。
3. Token服务激活。可能的事件导致：首次激活Token，Token从2)中的暂定状态回复正常服务。
4. Token信用等级更新。可能的事件导致：因为身份认证方法的改变或者内部操作导致的Token信用等级的改变。
5. 银行卡号的更新：可能的事件导致：更新了原始卡号的信息例如使用截至日期。

## 五、例子：苹果apple pay基于Tokenisation标准流程

Apple pay整个支付流程：

1. 添加一个银行卡：在passbook应用中选择一张已有的银行卡，或者添加通过拍摄或者手动输入添加一个新的银行卡号。
2. 验证银行卡：目前美国银行和苹果提供的唯一验证方式为电话验证。需要提供姓名、卡号、验证码、生日和银行卡关联地址等信息，进行验证。
3. 验证成功后，即可使用了。必须在支持tokenisation的商户使用。将手机贴上具有nfc功能的pos，手机自动点亮并要求指纹输入验证，验证后即完成付款。

流程分析：可以看到apple pay支付中，token码与银行卡号的绑定的过程是发生在电话验证阶段（位于标准中定义的第四级别）。类似与中国快捷支付的开通过程。身份认证过程则是通过指纹验证进行的，代替了传统的手写签名方式。

## 六、6种身份认证方式

用户身份认证是安全的第一道大门，是各种安全措施可以发挥作用的前提。随着互联网的不断发展，越来越多的人们开始尝试在线交易。然而病毒、黑客网络钓鱼以及网页仿冒诈骗等恶意威胁，给在线交易的安全性带来了极大的挑战。近些年国内外网络诈骗事件层出不穷，给银行和消费者带来了巨大的经济损失。层出不穷的网络犯罪，引起了人们对网络身份的信任危机，如何证明“我是谁？”及如何防止身份冒用等问题是必须要解决的问题。目前，身份认证的方式基本有以下这六种。

### 5.1．基于静态口令的认证

用户名+密码的方式，密码即静态口令。容易被猜测，暴力破解，或者诱骗到手，属于单因素认证方式，已经无法适合互联网环境

### 5.2．基于动态口令的认证

包括动态短信，动态令牌。

1)动态短信：短信密码以手机短信形式请求包含6位随机数的动态密码，身份认证系统以短信形式发送随机的6位密码到客户的手机上。客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全性。

2)动态令牌：包括硬件令牌和手机软件令牌。硬件令牌是一个用来生成动态密码的终端，采用基于时间同步的方式，每60秒变换一次口令，口令一次有效，硬件令牌产生6位动态数字进行一次一密的方式认证。手机软件令牌是利用智能手机软件基于时间产生动态密码，且过程中不需要连接任何网络来达到模拟硬件令牌的方式。

### 5.3．基于USBKey的认证

内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用USBKey内置的公钥算法实现对用户身份的认证

### 5.4．基于智能IC卡的认证

智能卡认证是通过智能卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此也存在安全隐患。

### 5.5．基于数字证书的认证

数字证书是一种权威性的电子文档，由权威公正的第三方机构即CA中心签发的证书。以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性。使用了数字证书，即使发送的信息在网上被他人截获，甚至在丢失个人的账户、密码等信息的情况下，仍可以保证账户资金安全。

### 5.6．基于生物识别技术的认证

人类身上独一无二的特征来验证，身体特征包括：指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和DNA等。可以看到苹果apple pay即采用的生物指纹来进行身份验证。

## 七、基于NFC令牌的认证

在以上六种身份认证方式中，美国国家标准局根据根据安全保障水平将他们分为四个等级。从1到4安全保障水平级别依次增强，基于静态口令的认证方式归为2级，基于动态口令或软件证书的认证方式归为3级别，基于USBKey硬件证书的认证方式归为4级。可以看到基于硬件证书的认证方式在安全上是目前最有保障的。NFC标准组织制定的NFC标准中有专门针对数字签名记录类型的定义。而数字签名技术其实就是数字证书的基础，因此可以考虑采用基于NFC的数字证书方式进行身份认证。

### 6.1数字签名

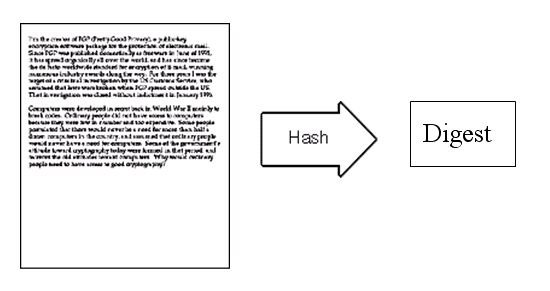
其实，无论是数字签名还是数字证书，它们的最重要的基础理论应该是非对称加密算法。非对称加密即加密信息和解密信息的过程采用不同的密钥。

一个最简单的应用例子就是：假设A生成了自己的公钥和私钥。他把公钥公布出来给大家，例如B，C，D都得到了这个公钥，这时B要给A写一封信，写完后他就用A的公钥对信加密发送给A，而对于这份加密的信是只有用A的私钥才能解开的。也就是只要A的私钥不丢失，信息就不会被泄漏。这样做的好处是，不涉及到真正解密密钥的网络传输！

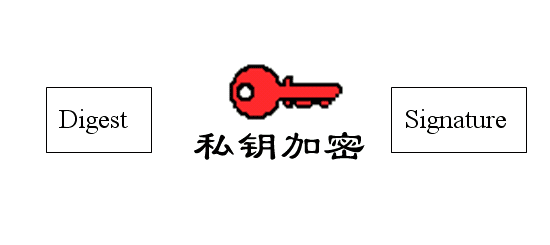
接下来，A需要给回复B一封信，他决定采用数字签名的方法发送这封信。他首先将信采用HASH函数处理产生一个信的摘要，这个摘要满足，一旦信的内容有任何改变，重新对它HASH处理产生的摘要将不同。他用自己的私钥对摘要加密就产生了一个签名并随同信件一起传送给B，B用公钥解开摘要并对原文做HASH处理看结果是否与解密的结果相同，若相同，则证明完全没经过其他人修改过。这就是数字签名技术。

可以用如下图流程清楚的解释这个过程：

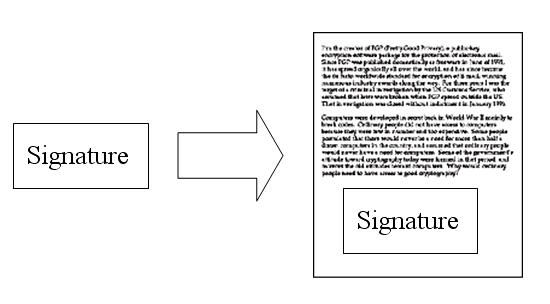
首先，对文件进行HASH处理产生摘要。



然后用私钥对摘要加密，形成加密后的摘要，也就是签名。



最后，将签名随同原始信息一同发送给其他人，这就是一份带有签名的文件。跟现实纸质文件手写签名有异曲同工之妙。



### 6.2数字证书

接着引用上面的例子，如果在上面的例子中，C把B的公钥偷偷的换成了B自己的公钥，并用自己的私钥进行发送信件，C收到的信件可以正常被解密，他却无法意识到有人在冒充A，因为B根本不知道自己的公钥到底有没有人被替换。于是就产生了一个新的机构证书认证中心CA。CA利用自己的私钥对A的公钥和其他个人信息进行加密。生成数字证书。

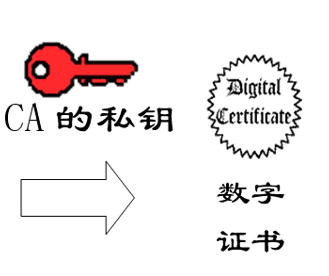


**A的公钥**

**A的个人信息**

**证书的信息等等**

**…………发 发**



这样A拿到证书后就可以安心的写信了，他会将自己的签名和证书一起发送给收件人。



这样其他人收信后，用CA的公钥解开数字证书，就可以拿到A真实的公钥了，然后就能证明"数字签名"是否真的是A签的。

## 八、关于Tokenisation标准的思考

首先基于Token的支付是以现有银行卡为基础和前提的条件的，即必须绑定现有的银行卡，作为一种副账户。我们可以理解Token是银行卡支付的场景的缩减版。一个银行卡可以拥有多个Token来扩大支付场景。这好比现在的快捷支付，同一张银行卡在支付宝申请了一个快捷支付，而在微信支付中要快捷支付是需要重新在申请的。所以一个Token从某一方面起到了作用域控制的效果，这样的好处是Token即使在家是最坏的条件下丢失了，用户的损失也是很小的，我们可以很快废弃这个Token。

Token的存储位置，银行卡号对于用户来说是存在银行卡中（还包括有效期，发卡行等等信息）。其实Token的存储除了Token码也有类似银行卡里必要信息。所以Token存储过程其实等同于银行卡的制卡过程。只不过银行卡制卡标准是非常固定的。而Token是比较灵活的，我们可以他把存在手机安全单元，也可以存在单独的一个孤立设备。

整个Token流程的身份认证，我觉得大体可以分为两部分，一个是绑定过程的认证，一个使用过程的认证。如果撇开绑定过程的认证不谈，其实Token的使用过程中身份认证跟现在的传统银行卡是完全没有区别，只不过是把银行卡号变成了Token码，而这在使用者是完全不知道的，也不需要了解这些细节。这样的好处是用户的支付习惯和支付方式是并没有改变的。