

支付令牌申请方法、设备、系统和服务器

技术领域

本申请属于支付安全技术领域，具体涉及一种支付令牌申请方法、设备、系统和服务器。

背景技术

随着互联网的快速发展，人们的支付方式也发生了巨大的变革，消费者从原先使用银行卡在 POS 机上进行支付，逐渐演变为使用二维码、手机应用（APP）、物联网设备等多种途径进行支付。而支付敏感信息也从单纯的卡号等变得复杂多样，这些敏感信息无论从传递方式、存储位置、加密手段等，都比以前面临着更加严峻的安全风险，如果没有一个安全的支付保障措施，消费者的支付行为将面临不可预估的风险。与此同时，用户越来越频繁地使用手机进行购物和支付。目前，各大银行、第三方支付机构等均推出了自己的钱包应用（例如是云闪付®）。用户使用这些钱包应用时，均需要在各个钱包应用中绑定银行卡进行支付。在一些场景中，用户也会在一些购物应用上绑定银行卡。在各个应用中绑定银行卡的过程，增加了银行卡信息泄露的风险。

发明内容

本申请的目的在于针对现有技术的不足之处，提供一种支付令牌申请方法、设备、系统和服务器。

为解决上述技术问题，本申请采用如下技术方案。

本申请的实施例提供一种支付令牌申请方法，应用于终端设备中的第

二应用模块，所述方法包括：接收第一应用模块的调用指令后，展示已绑定的支付账户，以供用户从已绑定的支付账户中选择一个支付账户，其中，所述调用指令携带所述第一应用模块的商户信息；向服务器发送绑定令牌授权请求，以供所述第一应用模块根据请求到的绑定令牌授权码向所述服务器申请支付令牌，其中，所述绑定令牌授权请求携带所述第一应用模块的商户信息、以及用户所选取的支付账户。

可选地，所述绑定令牌授权请求还携带交易控制参数。

可选地，所述交易控制参数包括：所述支付令牌的有效期、所述支付令牌的单日交易限额和所述支付令牌的单日交易次数中的至少一项。

可选地，还包括：提供设置界面，以供用户设置所述交易控制参数。

可选地，还包括：从服务器接收绑定令牌授权码，并将接收到的绑定令牌授权码转发至所述第一应用模块。

可选地，将接收到的绑定令牌授权码转发至所述第一应用模块的同时，还将所述支付账号的提示信息和/或用户的身份信息的提示信息发送给所述第一应用模块。

本申请的实施例提供一种支付令牌申请方法，应用于终端设备的第一应用模块，所述支付令牌申请方法包括：调用第二应用模块，并向所述第二应用模块传递第一应用模块的商户信息，以供所述第二应用模块向服务器发送绑定令牌授权请求，所述绑定令牌授权请求携带所述第一应用模块的商户信息、以及用户在所述第二应用模块选取的支付账户，其中，所述第一应用模块为调用所述第二应用模块的软件，用户在所述第二应用模块能够选取的支付账户为用户在所述第二应用模块已经绑定的支付账户；接收绑定令牌授权码，所述绑定令牌授权码为所述服务器根据所述绑定令牌

授权请求而生成的；向所述服务器发送支付令牌请求，所述支付令牌请求携带所述绑定令牌授权码；从所述服务器接收支付令牌。

可选地，所述绑定令牌授权码是所述服务器经所述第二应用模块转发至所述第一应用模块的；从所述第二应用模块接收绑定令牌授权码的同时，还从所述第二应用模块接收所述支付账户的提示信息和/或用户的身份信息的提示信息；所述方法还包括：展示所述支付账户的提示信息和/或用户的身份信息的提示信息，以供用户确认所述提示信息是否正确；在用户确认所述提示信息正确的情况下，执行所述向所述服务器发送支付令牌请求的步骤。

可选地，还包括选取第二应用模块的步骤，包括：向所述服务器发送查询请求，以查询所述服务器所支持的应用；展示查询到的应用列表，以供用户从中选取一个应用作为所述第二应用模块。

可选地，在调用所述第二应用模块的情况下，还将加密判别码和所述第一应用模块的商户信息，所述加密判别码为所述第一应用模块在所述服务器进行注册时获取的其商户信息的密文。

可选地，还包括：从服务器接收第一加密数据、第二秘钥和时钟信息，所述第一加密数据为所述绑定令牌授权码经第一秘钥加密得到的密文；根据接收到的时钟信息同步时钟，采用所述第二秘钥以及同步后的时钟信息对自身的商户信息加密得到第二加密数据；在调用所述第二应用模块的情况下，还将所述第二加密数据以及所述第一加密数据发送至所述服务器。

本申请的实施例提供一种支付令牌申请方法，应用于服务器，所述方法包括：从第二应用模块接收绑定令牌授权请求，所述绑定令牌授权请求

携带第一应用模块的商户信息、以及用户在所述第二应用模块的已绑定支付账户中所选取的支付账户；在所述绑定令牌授权请求验证通过的情况下，生成绑定令牌授权码，并将所述绑定令牌授权码发送至所述第一应用模块；从所述第一应用模块接收支付令牌请求，所述支付令牌请求携带所述绑定令牌授权码；在所述支付令牌请求验证通过的情况下，生成支付令牌，并将所述支付令牌发送至所述第一应用模块。

可选地，所述绑定令牌授权请求还携带所述第一应用模块的商户信息；在所述绑定令牌授权码携带的商户信息为已注册的商户信息的情况下，所述绑定令牌授权请求验证通过。

可选地，还包括：对所述第一应用模块提供注册服务；对所述第一应用模块的商户信息进行加密得到加密判别码；将所述加密判别码发送至所述第一应用模块；从所述第一应用模块接收加密判别码和商户信息；对所述加密判别码进行解密，并将解密得到的明文与接收到的商户信息进行比较，如二者一致则所述绑定令牌授权请求验证通过。

可选地，所述支付令牌请求还携带所述第一应用模块的商户信息；对所述支付令牌请求进行验证的步骤包括以下三种验证方式中的至少一种：如所述绑定令牌授权码存在，则验证通过；如所述商户信息与所述绑定令牌授权码申请时的商户信息一致，则验证通过；如所述绑定令牌授权码在有效期内，则验证通过。

可选地，生成所述绑定令牌授权码的同时，还向所述第一应用模块发送第一加密数据、第二密钥和时钟信息，所述第一加密数据为所述绑定令牌授权码经第一密钥加密得到的密文；

所述方法还包括：

从所述第一应用模块接收第二加密数据以及第一加密数据；所述方法还包括：采用自身的第二密钥和自身的时钟信息对自身保留的所述第一应用模块的商户信息加密，得到第三密文，判断所述第三密文与从所述第一应用模块接收的第二密文是否一致，并且判断接收到的第一加密数据经所述第一密钥解密后得到的绑定令牌授权码与自身保留的绑定令牌授权码是否一致，如均一致则所述支付令牌请求验证通过。

可选地，将所述支付令牌发送至所述第一应用模块，包括：经所述第二应用模块转发而将所述绑定令牌授权码发送至所述第一应用模块。

本申请的实施例提供一种支付令牌申请方法，包括：在终端设备，第一应用模块调用第二应用模块，并向所述第二应用模块传递所述第一应用模块的商户信息；在所述终端设备，所述第二应用模块接收第一应用模块的调用指令后，展示在所述第二应用模块已绑定的支付账户，以供用户从已绑定的支付账户中选择一个支付账户，向服务器发送绑定令牌授权请求，其中，所述绑定令牌授权请求携带所述第一应用模块的商户信息、以及用户所选取的支付账户；在所述服务器，在所述绑定令牌授权请求验证通过的情况下，生成绑定令牌授权码，并将所述绑定令牌授权码发送至所述第一应用模块；在所述终端设备，所述第一应用模块向所述服务器发送支付令牌请求，所述支付令牌请求携带所述绑定令牌授权码；在所述服务器，在所述支付令牌请求验证通过的情况下，生成支付令牌，并将所述支付令牌发送至所述第一应用模块。

本申请的实施例提供一种终端设备，所述终端设备具有第一存储器和第一处理器，所述第一存储器存储第一指令和/或第二指令，所述第一指令在所述第一处理器运行时用于执行前述第一应用模块的支付令牌申请方

法，所述第二指令在所述第一处理器运行以执行前述第二应用模块的支付令牌申请方法。

本申请的实施例提供一种服务器，所述服务器包括第二存储器和第二处理器，所述第二存储器存储支付令牌管理程序，所述第二处理器运行所述支付令牌管理程序以执行前述应用在服务器的支付令牌申请方法。

本申请的实施例提供一种支付令牌申请系统，包括前述的终端设备以及前述述的服务器。

与现有技术相比，本申请的有益效果为：用户只需要在第二应用模块上绑定支付账户（例如是绑定银行卡），当其需要在第一应用模块绑定支付账户时，可以通过这个已经绑定支付账户的第二应用模块进行操作，第一应用模块不会接触到诸如银行卡号这样的支付敏感信息，增加了支付账户绑定过程中的安全性。

附图说明

图 1 是本申请的实施例提供的支付令牌申请方法的流程图。

图 2 是本申请的又一实施例提供的支付令牌申请方法的流程图。

图 3 是本申请的又一实施例提供的支付令牌申请方法的流程图。

图 4 是本申请的又一实施例提供的支付令牌申请方法的流程图。

图 5 是本申请的又一实施例提供的支付令牌申请方法的交互流程图。

图 6 是本申请的实施例提供的支付账户管理系统的结构框图。

具体实施方式

在本申请中，应理解，诸如“包括”或“具有”等术语旨在指示本说

说明书中所公开的特征、数字、步骤、行为、部件、部分或其组合的存在，并且不旨在排除一个或多个其他特征、数字、步骤、行为、部件、部分或其组合存在的可能性。

另外还需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

本申请的实施例中，终端设备例如是智能手机、平板电脑、或者个人电脑这样的供终端用户操作的设备。第二应用模块例如是云闪付[®]、手机银行、具有支付功能的购物 APP 这样的进行支付的应用模块，当然也可以是这些应用模块的 HTML5 页面。第一应用模块指的是需要绑定支付账户（例如是需要绑定银行卡）的软件，同样例如是云闪付[®]应用、具有支付功能的购物 APP，或者它们的 HTML5 页面。第一应用模块和第二应用模块标号的区分仅在于在应用过程中，第二应用模块已经绑定了支付账户，第一应用模块需要通过第二应用模块的协助申请支付令牌。第一应用模块可和第二应用模块可以完全由软件实现、完全由硬件实现、或者软硬结合的方式实现。服务器提供支付令牌的管理服务。支付令牌（payment token）也称令牌或支付令牌，它是用一段代码代替诸如银行卡号这样的支付敏感信息。

下面结合附图所示的实施例对本申请作进一步说明。

参考图 1，本申请实施例所提供的支付令牌申请方法，应用于终端设备的第二应用模块。从软件角度看，执行主体是已经绑定支付账户的软件，例如是云闪付[®]应用、或者云闪付[®]HTML5 页面；从硬件角度看，执行主体可以是运行这些软件的终端设备或者为终端设备提供 HTML5 页面服务

的服务器。该方法包括以下步骤。

步骤 S101、接收第一应用模块的调用指令后，展示已绑定的支付账户，以供用户从已绑定的支付账户中选择一个支付账户，其中，所述调用指令携带所述第一应用模块的商户信息。

商户信息例如是商户号或者令牌请求者编号。商户信息是第一应用模块在服务器的唯一标识。

步骤 S102、向服务器发送绑定令牌授权请求，以供所述第一应用模块根据请求到的绑定令牌授权码向所述服务器申请支付令牌，其中，所述绑定令牌授权请求携带所述第一应用模块的商户信息、以及用户所选取的支付账户。

例如第二应用模块展示其已经绑定的支付账户，可以是展示已经绑定的银行卡的部分卡号、已经绑定的银行卡的单日单日交易限额、单日单日交易次数等交易控制参数。用户在第二应用模块上选择一个支付账户作为第一应用模块申请绑定的支付账户。

第二应用模块所申请的绑定令牌授权码是一串编码，作为第一应用模块于服务器之间通信的一个凭证，绑定令牌授权码的编码本身并无特定含义。

服务器可以将绑定令牌授权码直接发送至第一应用模块，也可以是首先发送至第二应用模块，随后所述第二应用模块将接收到的绑定令牌授权码转发至所述第一应用模块。随后，第一应用模块可以凭借这个绑定令牌授权码向服务器申请最终的支付令牌。

用户只需要在第二应用模块上绑定支付账户，第一应用模块通过第二应用模块从服务器获得绑定令牌授权码，然后依靠绑定令牌授权码从服务

器获得支付令牌。如需在第一应用模块上绑定支付账户，第一应用模块在绑卡的全程中都不会接触所要绑定的支付账户，减少了支付账户暴露的机会，增加安全性。

基于图 1 的支付令牌申请方法，本申请的一些实施例还提供了该支付令牌申请方法的一些具体实施方案，以及扩展方案，下面进行说明。

可选地，所述绑定令牌授权请求还携带交易控制参数。所述交易控制参数例如包括：所述支付令牌的有效期、所述支付令牌的单日交易限额和所述支付令牌的单日交易次数中的至少一项。

交易控制参数可以是默认采用第二应用模块中所选支付账户的交易控制参数。也可以是在所述终端设备，所述第二应用模块还提供设置界面，以供用户设置所述交易控制参数。

可选地，将接收到的绑定令牌授权码转发至所述第一应用模块的同时，还将所述支付账号的提示信息和/或用户的身份信息的提示信息发送给所述第一应用模块。

如此，在所述终端设备，所述第一应用模块能够展示所述支付账号的提示信息和/或用户的身份信息的提示信息，以供用户进行确认。

基于相同的发明构思，参考图 2，本申请实施例所提供的支付令牌申请方法，应用于终端设备的第一应用模块。从软件角度看，执行主体是需要绑定支付账户的软件（本文称为第一应用模块），例如是云闪付[®]应用、或者云闪付[®]HTML5 页面；从硬件角度看，执行主体可以是运行这些软件的终端设备或者为终端设备提供 HTML5 页面服务的服务器。该方法包括以下步骤。

步骤 S201、调用第二应用模块，并向所述第二应用模块传递第一应用模块的商户信息，以供所述第二应用模块向服务器发送绑定令牌授权请求，所述绑定令牌授权请求携带所述第一应用模块的商户信息、以及用户在所述第二应用模块选取的支付账户，其中，所述第一应用模块为调用所述第二应用模块的软件，用户在所述第二应用模块能够选取的支付账户为用户在所述第二应用模块已经绑定的支付账户。

步骤 S202、接收绑定令牌授权码，所述绑定令牌授权码为所述服务器根据所述绑定令牌授权请求而生成的。可以从服务器接收，也可能是经第二应用模块中转而接收。

步骤 S203、向所述服务器发送支付令牌请求，所述支付令牌请求携带所述绑定令牌授权码；

步骤 S204、从所述服务器接收支付令牌。

第一应用模块通过第二应用模块向服务器申请绑定令牌授权码，然后凭借绑定令牌授权码向服务器申请支付令牌，第一应用模块全程不接触诸如支付账户的敏感信息，提高了安全性。

基于图 2 的支付令牌申请方法，本申请的一些实施例还提供了该支付令牌申请方法的一些具体实施方案，以及扩展方案，下面进行说明。

可选地，所述绑定令牌授权码是所述服务器经所述第二应用模块转发至所述第一应用模块的；从所述第二应用模块接收绑定令牌授权码的同时，还从所述第二应用模块接收所述支付账户的提示信息 and/或用户的身份信息的提示信息；所述方法还包括：展示所述支付账户的提示信息和/或用户的身份信息的提示信息，以供用户确认所述提示信息是否正确；在用户确认所述提示信息正确的情况下，执行所述向所述服务器发送支付令

牌请求的步骤。

支付账号的提示信息例如是银行卡后 4 位卡号、银行卡类型、银行名称等。用户的身份信息的提示信息例如是用户的隐去部分位后的身份证号、用户为该银行卡注册的手机号等。为用户提供更多的提示信息，供用户确认。

如此，用户可以在第一应用模块对即将绑定的支付账户以及个人信息进行确认。

可选地，还包括选取第二应用模块的步骤，包括：向所述服务器发送查询请求，以查询所述服务器所支持的应用；展示查询到的应用列表，以供用户从中选取一个应用作为所述第二应用模块。

也就是用户可以选择具体通过那个软件作为中转为第一应用模块申请绑定令牌授权码。

除此之外，第一应用模块还可以提供展示界面，展示已经绑定的支付账户的相关信息（例如是发卡银行、账户类型、对应的支付账户的尾号、支付令牌的有效期、交易限额等）。

第一应用模块（此时已经完成绑卡）还可以提供解除绑定的功能。根据用户的解绑操作，第一应用模块向服务器发送标记状态变更的信息即可。

如第二应用模块对第一应用模块所绑定的支付账户进行了操作，第一应用模块也会从服务器接收到相应的通知。第一应用模块可以从该通知中获知支付令牌的最新状态信息。

可选地，在调用所述第二应用模块的情况下，还将加密判别码和所述第一应用模块的商户信息发送至服务器，所述加密判别码为所述第一应用

模块在所述服务器进行注册时获取的其商户信息的密文。

第一应用模块在服务器进行注册时会获得加密判别码，加密判别码是第一应用模块的商户信息经加密后的密文。第一应用模块在发送绑定令牌授权请求的同时还发送加密判别码以及自身的商户信息。服务器可据此对绑定令牌授权请求进行验证。

这样做可以防止某些钓鱼类欺诈 APP 假冒第一应用模块的相关商户信息，导致用户将银行卡绑定至钓鱼 APP 中，避免用户财产损失。

可选地，还包括：从服务器接收第一加密数据、第二秘钥和时钟信息，所述第一加密数据为所述绑定令牌授权码经第一秘钥加密得到的密文；根据接收到的时钟信息同步时钟，采用所述第二秘钥以及同步后的时钟信息对自身的商户信息加密得到第二加密数据；在调用所述第二应用模块的情况下，还将所述第二加密数据以及所述第一加密数据发送至所述服务器。

时钟信息的加入，可以实现服务器一定时期无响应时，拒绝第一应用模块的支付令牌的申请，避免用户长时间等待。

基于相同的发明构思，参考图 3，本申请的实施例还提供一种支付令牌申请方法，应用于服务器。从软件角度来讲，执行主体为服务器所运行的软件，从硬件角度来讲，执行主体是服务器。该方法包括以下步骤。

步骤 S301、从第二应用模块接收绑定令牌授权请求，所述绑定令牌授权请求携带第一应用模块的商户信息、以及用户在所述第二应用模块的已绑定支付账户中所选取的支付账户。

步骤 S302、在所述绑定令牌授权请求验证通过的情况下，生成绑定

令牌授权码，并将所述绑定令牌授权码发送至所述第一应用模块。

步骤 S303、从所述第一应用模块接收支付令牌请求，所述支付令牌请求携带所述绑定令牌授权码。

步骤 S304、在所述支付令牌请求验证通过的情况下，生成支付令牌，并将所述支付令牌发送至所述第一应用模块。

服务器基于与第二应用模块的交互为第一应用模块生成绑定令牌授权码，随后第一应用模块凭借绑定令牌授权码向服务器申请支付令牌。第一应用模块全程不接触支付账户等敏感信息，提高安全性。

基于图 3 的支付令牌申请方法，本申请的一些实施例还提供了该支付令牌申请方法的一些具体实施方案，以及扩展方案，下面进行说明。

可选地，所述支付令牌请求还携带所述第一应用模块的商户信息；在所述绑定令牌授权码携带的商户信息为已注册的商户信息的情况下，所述绑定令牌授权请求验证通过。

可选地，还包括：对所述第一应用模块提供注册服务；对所述第一应用模块的商户信息进行加密得到加密判别码；将所述加密判别码发送至所述第一应用模块；从所述第一应用模块接收加密判别码和商户信息；对所述加密判别码进行解密，并将解密得到的明文与接收到的商户信息进行比较，如二者一致则所述绑定令牌授权请求验证通过。

也就是第一应用模块在服务器进行注册时，服务器将第一应用模块的商户信息进行加密，并将密文（即上述加密判别码）发送至第一应用模块。第一应用模块需要提供正确的加密判别码和正确的商户信息，才能获得绑定令牌授权码。

这样做可以防止某些钓鱼类欺诈 APP 假冒商户应用的相关商户信息，

导致用户将银行卡绑定至钓鱼应用中，避免用户财产损失。

对支付令牌请求进行验证的一种方式如下。可选地，所述支付令牌请求还携带所述第一应用模块的商户信息；对所述支付令牌请求进行验证的步骤包括以下三种验证方式中的至少一种：如所述绑定令牌授权码存在，则验证通过；如所述商户信息与所述绑定令牌授权码申请时的商户信息一致，则验证通过；如所述绑定令牌授权码在有效期内，则验证通过。

例如：判断所述支付令牌请求中携带的绑定令牌授权码是否在所述服务器存在，如是，则判断所述支付令牌请求中携带的商户信息是否与所述绑定令牌授权码所对应的绑定令牌授权请求中携带的商户信息一致，如是，则判断当前时间是否在所述绑定令牌授权码的有效期内，如是，则所述支付令牌请求验证通过。

也就是服务器只有判断接收到的支付令牌请求中携带的绑定令牌授权码和商户信息都是正确的并且未超过有效期，支付令牌请求即验证通过。

可选地，生成所述绑定令牌授权码的同时，还向所述第一应用模块发送第一加密数据、第二密钥和时钟信息，所述第一加密数据为所述绑定令牌授权码经第一密钥加密得到的密文；所述方法还包括：从所述第一应用模块接收第二加密数据以及第一加密数据；所述方法还包括：采用自身的第二密钥和自身的时钟信息对自身保留的所述第一应用模块的商户信息加密，得到第三密文，判断所述第三密文与从所述第一应用模块接收的第二密文是否一致，并且判断接收到的第一加密数据经所述第一密钥解密后得到的绑定令牌授权码与自身保留的绑定令牌授权码是否一致，如均一致，则所述支付令牌请求验证通过。

详细的过程如下：

首先，服务器在生成绑定令牌授权码时，还会生成第一秘钥、第二秘钥，并采用第一秘钥对绑定令牌授权码加密，得到第一加密数据，并将第一加密数据、第二秘钥和时钟信息发送给第一应用模块（可以是直接发送至第一应用模块，也可以是经第二应用模块转发）。

随后，第一应用模块根据接收到的时钟信息进行时钟同步，用第二秘钥和同步后的时钟信息对商户信息加密，形成第二加密数据。第一应用模块向服务器发送第二加密数据、其接受到的第一加密数据。

最后，标记附图提供设备使用自身保存的第二秘钥、自身的时钟信息对自身保存的商户信息加密得到第三加密数据，判断第二加密数据和第三加密数据是否一致，同时用自身保留的第一秘药对第一加密数据进行解密，将解密得到的绑定令牌授权码与自身保存的绑定令牌授权码进行比对，判断是否一致，如果两次判断的结果都是一致的，那么支付令牌请求合法。

由于是在信息的加入，可以实现服务器在一定时期无响应时，拒绝支付令牌请求，避免用户长时间等待。

例如第一应用模块调用第二应用模块，并向服务器发送上述信息。服务器接收到上述信息后并没有及时从第二应用模块接收到绑定令牌授权请求，如此便可以向第一应用模块发送拒绝信息。

可选地，将所述支付令牌发送至所述第一应用模块，包括：经所述第二应用模块转发而将所述绑定令牌授权码发送至所述第一应用模块。

服务器完成支付令牌的分发后，用户在使用第一应用模块时，即可根据该支付令牌进行支付。支付请求会发送至服务器。服务器将支付请求中

的支付令牌替换成支付账户（例如银行卡号），随后再讲支付请求发送至对应的发卡机构。

发卡机构对于支付令牌发起的支付交易，服务器在转换卡号后的支付请求中增加标记支付标识，发卡机构承兑带标记支付标识但无验证要素的卡号交易。

基于相同的发明构思，参考图 4 并结合图 5，本申请的实施例还提供一种支付令牌申请方法。该方法展示了终端设备上运行的第一应用模块、第二应用模块以及服务器三者之间完整的交互过程。所述支付令牌申请方法包括以下步骤。

步骤 S401、在终端设备，第一应用模块调用第二应用模块，并向所述第二应用模块传递所述第一应用模块的商户信息。

步骤 S402、在所述终端设备，所述第二应用模块接收第一应用模块的调用指令后，展示在所述第二应用模块已绑定的支付账户，以供用户从已绑定的支付账户中选择一个支付账户，向服务器发送绑定令牌授权请求，其中，所述绑定令牌授权请求携带所述第一应用模块的商户信息、以及用户所选取的支付账户。

步骤 S403、在所述服务器，在所述绑定令牌授权请求验证通过的情况下，生成绑定令牌授权码，并将所述绑定令牌授权码发送至所述第一应用模块；

步骤 S404、在所述终端设备，所述第一应用模块向所述服务器发送支付令牌请求，所述支付令牌请求携带所述绑定令牌授权码。

步骤 S405、在所述服务器，在所述支付令牌请求验证通过的情况

下，生成支付令牌，并将所述支付令牌发送至所述第一应用模块。

各个步骤的实现细节以及变式均可参考前述的实施例，对此不作赘述。

参考图 5，在一个具体的例子中，第一步，第一应用模块调用第二应用模块，以在第二应用模块选择需要绑定的银行卡。第二步，第二应用模块向服务器发送绑定令牌授权请求，第一应用模块的商户信息、交易控制参数以及第一应用模块的商户号。第三步，服务器验证绑定令牌授权请求，生成绑定令牌授权码。第四步，服务器将绑定令牌授权码发送至第二应用模块。第五步，第二应用模块将绑定令牌授权码和提示信息发送给第一应用模块。第六步，第一应用模块展示提示信息，供用户确认提示信息是否正确。第七步，第一应用模块向服务器发送支付令牌请求，携带商户信息和绑定令牌授权码。第八步，服务器验证支付令牌请求，验证通过则生成支付令牌并发送至第一应用模块。

参考图 6，基于相同的发明构思，本申请的实施例还提供一种终端设备 1 具有第一存储器 11 和第一处理器 12，第一存储器 11 存储第一指令和/或第二指令，第一指令在第一处理器 12 运行时用于执行前述应用于第一应用模块的支付令牌申请方法，第二指令在第一处理器 12 运行而执行前述应用于第二应用模块的支付令牌申请方法。

相应地，本申请的实施例还提供一种服务器 2，服务器 2 包括第二存储器 21 和第二处理器 22，第二存储器 21 存储支付令牌管理程序，第二处理器 22 运行支付令牌管理程序以执行前述应用在服务器的支付令牌申请方法。

相应地，本申请的实施例提供一种支付令牌申请系统，包括上述的终

端设备和上述的服务器。

本申请中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。

本申请的保护范围不限于上述的实施例，显然，本领域的技术人员可以对本申请进行各种改动和变形而不脱离本申请的范围和精神。倘若这些改动和变形属于本申请权利要求及其等同技术的范围，则本申请的意图也包含这些改动和变形在内。