支付方法、终端设备、服务器、系统及介质

相关申请的交叉引用

本申请要求享有于 2022 年 03 月 10 日提交的名称为“支付方法、终端设备、服务器、系统及介质”的中国专利申请 202210238575.1 的优先权，该申请的全部内容通过引用并入本文中。

技术领域

本申请属于数据处理领域，尤其涉及一种支付方法、终端设备、服务器、系统及介质。

背景技术

随着支付技术的发展，电子支付的应用越来越广泛。用户可通过终端设备实现支付。终端设备中安装有应用程序和软件开发工具包（Software Development Kit，SDK），SDK 可集成在应用程序中，共同实现支付。

支付过程在终端设备中涉及应用程序和 SDK 两个主体，支付过程涉及的主体增多，支付存在的安全风险也随之增大。因此，亟需一种能够提高安全性的支付方法。

发明内容

本申请实施例提供一种支付方法、终端设备、服务器、系统及介质，能够提高支付的安全性。

第一方面，本申请实施例提供一种支付方法，应用于软件开发工具包 SDK 服务器，方法包括：响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息，安全验证请求消息包括安全验证信息，用于指示安全控制系统根据安全验证信息对支付请求消息对应的支付进行安全验证；接收安全控制系统发送的安全验证结果信息；在安全验证结果信息表征安

全验证通过的情况下，向终端设备中的 SDK 发送第一通知消息，终端设备具有 SDK 和宿主程序，第一通知消息用于指示 SDK 通知宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息，第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息；在用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

第二方面，本申请实施例提供一种支付方法，应用于终端设备，终端设备具有软件开发工具包 SDK 和宿主程序，方法包括：通过 SDK 获取 SDK 服务器发送的第一通知消息，第一通知消息是 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的，安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应的支付进行安全验证得到的，安全验证请求消息由 SDK 服务器响应于接收的支付请求消息发送；响应于第一通知消息，通过 SDK 通知宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息；通过宿主程序向宿主程序服务器反馈第一用户验证输入信息，第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息；通过 SDK 向 SDK 服务器发送通过宿主程序从宿主程序服务器获取的用户验证结果信息，使 SDK 服务器在用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

第三方面，本申请实施例提供一种支付方法，应用于宿主程序服务器，方法包括：接收终端设备通过宿主程序反馈的第一用户验证输入信息，终端设备具有软件开发工具包 SDK 和宿主程序，第一用户验证输入信息在 SDK 响应于第一通知消息通知宿主程序展示用户验证页面后得到，第一通知消息是 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的，安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应支付进行安全验证得到的，安全验证请求消息由 SDK 服务器响应于接收的支付请求消息发送；根据第一用户验证输入信息进行用户验证，得到用户验证结果信息；向终端设备中的宿主程序发送用户验证结果信息，通过宿主程序将用户验证结果信息传输给

SDK，以使 SDK 向 SDK 服务器发送用户验证结果信息，在用户验证结果信息表征用户验证通过的情况下，使 SDK 服务器发起付款请求，以完成支付。

第四方面，本申请实施例提供一种 SDK 服务器，包括：发送模块，用于响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息，安全验证请求消息包括安全验证信息，用于指示安全控制系统根据安全验证信息对支付请求消息对应的支付进行安全验证；接收模块，用于接收安全控制系统发送的安全验证结果信息；发送模块还用于在安全验证结果信息表征安全验证通过的情况下，向终端设备中的 SDK 发送第一通知消息，终端设备具有 SDK 和宿主程序，第一通知消息用于指示 SDK 通知宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息，第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息；发送模块还用于在用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

第五方面，本申请实施例提供一种终端设备，终端设备具有软件开发工具包 SDK 和宿主程序，终端设备包括：接收模块，用于通过 SDK 获取 SDK 服务器发送的第一通知消息，第一通知消息是 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的，安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应的支付进行安全验证得到的，安全验证请求消息由 SDK 服务器响应于接收的支付请求消息发送；显示模块，用于响应于第一通知消息，通过 SDK 通知宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息；发送模块，用于通过宿主程序向宿主程序服务器反馈第一用户验证输入信息，第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息；发送模块还用于通过 SDK 向 SDK 服务器发送通过宿主程序从宿主程序服务器获取的用户验证结果信息，使 SDK 服务器在用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

第六方面，本申请实施例提供一种宿主程序服务器，包括：接收模块，用于接收终端设备通过宿主程序反馈的第一用户验证输入信息，终端

设备具有软件开发工具包 SDK 和宿主程序，第一用户验证输入信息在 SDK 响应于第一通知消息通知宿主程序展示用户验证页面后得到，第一通知消息是 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的，安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应支付进行安全验证得到的，安全验证请求消息由 SDK 服务器响应于接收的支付请求消息发送；验证模块，用于根据第一用户验证输入信息进行用户验证，得到用户验证结果信息；发送模块，用于向终端设备中的宿主程序发送用户验证结果信息，通过宿主程序将用户验证结果信息传输给 SDK，以使 SDK 向 SDK 服务器发送用户验证结果信息，在用户验证结果信息表征用户验证通过的情况下，使 SDK 服务器发起付款请求，以完成支付。

第七方面，本申请实施例提供一种 SDK 服务器，包括：处理器以及存储有计算机程序指令的存储器；处理器执行计算机程序指令时实现第一方面的支付方法。

第八方面，本申请实施例提供一种终端设备，包括：处理器以及存储有计算机程序指令的存储器；处理器执行计算机程序指令时实现第二方面的支付方法。

第九方面，本申请实施例提供一种宿主程序服务器，包括：处理器以及存储有计算机程序指令的存储器；处理器执行计算机程序指令时实现第三方面的支付方法。

第十方面，本申请实施例提供一种支付系统，包括第七方面的 SDK 服务器、第八方面的终端设备和第九方面的宿主程序服务器。

第十一方面，本申请实施例提供一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序指令，计算机程序指令被处理器执行时实现第一方面的支付方法、第二方面的支付方法或第三方面的支付方法。

申请实施例提供一种支付方法、终端设备、服务器、系统及介质，SDK 服务器响应于支付请求消息，向安全控制系统发送安全验证请求消息，以请求安全控制系统对本次支付进行安全验证，以完成 SDK 所属方所需的安全性方面的验证。在安全验证通过的情况下，SDK 服务器向终端

设备的 SDK 发送用于指示 SDK 通知宿主程序展示用户验证页面的消息，以使 SDK 能够触发宿主程序主动发起用户验证，以完成宿主程序所属方所需的用户身份安全性方面的验证。在支付过程中实现了 SDK 所属方和宿主程序所属方两个主体的双向验证，提高了支付的安全性。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单的介绍，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请实施例提供的支付方法的应用场景的一示例的示意图；

图 2 为本申请第一方面提供的支付方法的一实施例的流程图；

图 3 为本申请第一方面提供的支付方法的另一实施例的流程图；

图 4 为本申请第一方面提供的支付方法的又一实施例的流程图；

图 5 为本申请第一方面提供的支付方法的又另一实施例的流程图；

图 6 为本申请第一方面提供的支付方法的再一实施例的流程图；

图 7 为本申请第二方面提供的支付方法的一实施例的流程图；

图 8 为本申请第二方面提供的支付方法的另一实施例的流程图；

图 9 为本申请第二方面提供的支付方法的又一实施例的流程图；

图 10 为本申请第二方面提供的支付方法的又另一实施例的流程图；

图 11 为本申请第二方面提供的支付方法的再一实施例的流程图；

图 12 为本申请第三方面提供的支付方法的一实施例的流程图；

图 13 为本申请第三方面提供的支付方法的另一实施例的流程图；

图 14 为本申请实施例提供的支付流程的一示例的流程图；

图 15 为本申请实施例提供的支付流程的另一示例的流程图；

图 16 为本申请实施例提供的支付流程的又一示例的流程图；

图 17 为本申请第四方面提供的 SDK 服务器的一实施例的结构示意图；

图 18 为第五方面提供的终端设备的一实施例的结构示意图；

图 19 为第六方面提供的宿主程序服务器的一实施例的结构示意图；

图 20 为本申请第七方面提供的 SDK 服务器的一实施例的结构示意图。

具体实施方式

下面将详细描述本申请的各个方面的特征和示例性实施例，为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及具体实施例，对本申请进行进一步详细描述。应理解，此处所描述的具体实施例仅意在解释本申请，而不是限定本申请。对于本领域技术人员来说，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本申请的示例来提供对本申请更好的理解。

随着支付技术的发展，电子支付的应用越来越广泛。用户可通过终端设备实现支付。终端设备中安装有用于支付的应用程序，但应用程序的功能有限，为了使得支付功能更加完善，终端设备中还可设置 SDK，SDK 可集成在应用程序中，和应用程序共同实现支付。在这种情况下，支付过程在终端设备中会涉及应用程序和 SDK 两个主体，支付过程涉及的主体增多，支付存在的安全风险也随之增大。因此，亟需一种能够提高安全性的支付方法。

本申请实施例提供一种支付方法、终端设备、服务器、系统及介质，能够分别以 SDK 和宿主程序为主体，进行双重验证，在 SDK 为主体的验证和宿主程序为主体的验证均通过的情况下，完成支付。通过 SDK 和宿主程序两方面的验证来保证 SDK 相关交互和宿主程序相关交互的安全性，从而提高整个支付过程的安全性。

本申请提供的支付方法应用于支付场景中，主要可涉及终端设备、SDK 后台系统、宿主程序后台系统和安全控制系统。图 1 为本申请实施例提供的支付方法的应用场景的一示例的示意图。如图 1 所示，终端设备 11 可分别与 SDK 后台系统 12、宿主程序后台系统 13 进行通信交互，SDK 后台系统 12 还可分别与宿主程序后台系统 13、安全控制系统 14 进行通信交互。

终端设备 11 具有宿主程序和 SDK。终端设备 11 的支付功能需要宿主

程序调用 SDK 共同实现。终端设备 11 中的 SDK 与宿主程序之间可交互。终端设备 11 中的 SDK 可与 SDK 后台系统 12 通信交互，终端设备 11 中的宿主程序可与宿主程序后台系统 13 通信交互。终端设备 11 为用户用于进行支付的设备，具体可包括手机、平板电脑、电子计算机、只能穿戴设备等，在此并不限定。

SDK 后台系统 12 为 SDK 的后台系统，可包括一台以上的 SDK 服务器，在此并不限定 SDK 后台系统 12 中 SDK 服务器的种类和数量。终端设备 11 在支付过程中，会通过 SDK 将支付相关的信息发送给 SDK 后台系统 12。SDK 后台系统 12 也可预先存储支付的用户的账户信息及个人信息等。

在一些实施例中，SDK 后台系统 12 可包括 SDK 后台子系统和支付码子系统，SDK 后台子系统与支付码子系统之间可通信交互，SDK 后台子系统还可与终端设备 11 中的 SDK 通信交互，支付码子系统可与宿主程序后台系统通信交互。支付码子系统存储有支付码的相关信息，可对支付码进行管理和验证。支付码可包括收款码、付款码等，支付码具体可为二维码或其他形式的图形码，在此并不限定。

宿主程序后台系统 13 为宿主程序的后台系统，可包括一台以上的宿主程序服务器，在此并不限定宿主程序后台系统 13 中宿主程序服务器的种类和数量。终端设备 11 在支付过程中，会通过宿主程序与宿主程序后台系统 13 交互。宿主程序后台系统 13 还可与 SDK 后台系统 12 通信交互。

安全控制系统 14 可用于对支付进行安全验证，可包括一台以上的电子设备，在此并不限定安全控制系统 14 中电子设备的种类和数量。安全控制系统 14 可与 SDK 后台系统 12 通信交互。在 SDK 后台系统 12 包括 SDK 后台子系统和支付码子系统的情况下，安全控制系统 14 可与其中的 SDK 后台子系统通信交互。

在一些实施例中，终端设备 11 中 SDK 和宿主程序之间的信息传输为加密传输，即终端设备 11 中 SDK 和宿主程序之间交互的信息为加密信息。SDK 和宿主程序中各自存储有加、解密所需的加、解密算法，SDK

和宿主程序中的加、解密算法可根据应用环境、需求等设定，例如，SDK 和宿主程序中的加、解密算法可包括 SM2 算法、SM4 算法、数据加密标准（Data Encryption Standard，DES）、RSA 算法等，在此并不限定。SDK 中加、解密算法所需的密钥可由 SDK 后台系统 12 存储和管理，即 SDK 中加、解密的密钥可存储于 SDK 后台系统 12 中的 SDK 服务器，SDK 可通过与 SDK 后台系统 12 进行交互以实现加、解密。宿主程序中加、解密算法所需的密钥可由宿主程序后台系统 13 存储和管理，即宿主程序中加、解密的密钥存储于宿主程序后台系统 13 中的宿主程序服务器，宿主程序可通过与宿主程序后台系统 13 进行交互以实现加、解密。通过 SDK 与宿主程序之间的密文传输，SDK 与宿主程序之间传输的信息不容易被窃取，可保证 SDK 与宿主程序之间的通信安全。

在一些实施例中，终端设备 11 中 SDK 可具有安全域，SDK 中的信息可存储于安全域。安全域可为加密的数据存储空间，具体可通过硬件和/或软件实现，如通过安全元件（Secure Element，SE）和/或可信执行环境（TrustedExecutionEnvironment，TEE）等实现。SDK 可对安全域的权限进行管理，如划分不可开放读取的数据和仅有宿主程序有权限读取的数据等。

下面对本申请中的支付方法、终端设备、服务器、系统及介质依次进行说明。

本申请第一方面提供一种支付方法，该支付方法应用于 SDK 服务器，即该支付方法可由 SDK 服务器执行。图 2 为本申请第一方面提供的支付方法的一实施例的流程图。如图 2 所示，该支付方法可包括步骤 S201 至步骤 S204。

在步骤 S201 中，响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息。

支付请求消息用于发起支付。支付请求消息可由终端设备中的 SDK 向 SDK 服务器发送，或者，支付请求消息可由支付受理设备向 SDK 服务器发送。在 SDK 后台系统包括 SDK 后台子系统和支付码子系统的情况下，可由支付受理设备向支付码子系统中的 SDK 服务器发起支付，支付

码子系统中的 SDK 服务器再向 SDK 后台子系统中的 SDK 服务器发送支付请求消息。支付请求消息可包括订单信息、终端设备信息、支付信息等。订单信息可包括订单标识、订单发起方、订单明细、订单金额、订单时间等与订单关联的信息，在此并不限定。终端设备信息可包括对进行本次支付的终端设备的地理位置、设备标识等与终端设备关联的信息，在此并不限定。支付信息可包括支付付款方信息、支付收款方信息、支付金额、支付时间等与支付相关的信息，在此并不限定。支付收款方信息可包括商户名称、商户账户等信息，支付付款方信息可包括支付方账户、支付方支付卡信息、支付方标识等信息，在此并不限定。

安全验证请求消息包括安全验证信息。安全验证请求消息用于指示安全控制系统根据安全验证信息对支付请求消息对应的支付进行安全验证。安全验证信息可包括终端设备中 SDK 向 SDK 服务器发送的至少部分信息，安全验证信息还可包括 SDK 服务器中预存的与支付请求消息指示的支付付款方信息等，在此并不限定。例如，安全验证信息可包括支付卡卡号、支付方登录账号、支付方登录账号关联的手机号、支付卡关联的手机号、终端设备标识、终端设备的地理位置、支付金额、支付时间、支付卡的历史支付信息等信息中的一项或两项以上，安全验证信息还可包括其他能够进行安全性方面验证的信息，在此并不限定。

在一些示例中，在安全验证请求消息包括支付卡卡号的情况下，该支付卡卡号可以为终端设备中 SDK 提供的默认支付卡卡号，若用户在终端设备切换默认支付卡即默认支付卡卡号发生变化的情况下，SDK 会向 SDK 服务器发送包括新的默认支付卡卡号的消息，SDK 服务器会被触发向安全控制系统再次发送包括新的默认支付卡卡号的安全验证请求消息。也就是说，若用户在终端设备显示的付款详情页切换默认支付卡，对应地，SDK 服务器会重新向安全控制系统发送包括切换后的默认支付卡卡号的安全验证请求消息。

安全控制系统接收到安全验证请求消息，根据安全验证请求消息中的安全验证信息进行安全验证。安全验证可对支付的合法性以及支付的终端设备的登录状态的安全性进行验证，具体可通过安全验证信息是否满足预

定的安全判定条件，来确定安全验证是否通过。安全判定条件可根据具体场景、需求等设定，在此并不限定。例如，安全验证信息包括本次支付的终端设备标识和支付卡的历史支付信息，支付卡的历史支付信息包括支付卡的历史支付中的终端设备标识，若本次支付的终端设备标识和支付卡的历史支付中的终端设备标识一致，则安全验证通过；反之，安全验证未通过。又例如，安全验证信息包括本次支付的终端设备的地理位置、支付时间和支付卡的历史支付信息，支付卡的历史支付信息包括支付卡最近一次支付的终端设备的地理位置和支付时间，若支付卡最近一吃支付的支付时间与本次支付的支付时间之间的时长小于预设时长，且支付卡最近一次支付的终端设备的地理位置与本次支付的终端设备的地理位置之间的距离大于预设距离，则安全验证未通过；反之，安全验证通过。还例如，安全验证信息包括支付方登录账号关联的手机号和支付卡关联的手机号，若支付方登录账号关联的手机号与支付卡关联的手机号一致，则安全验证通过；反之，则安全验证未通过。

在一些示例中，在安全风险度非常高的情况下，如账户余额不足、支付为非法支付等情况，才判定安全验证未通过。在安全风险度中、低，能够通过后续的用户验证来判断支付的安全的情况下，可判定安全验证通过。例如，安全验证信息包括本次支付的终端设备标识和支付卡的历史支付信息，支付卡的历史支付信息包括支付卡的历史支付中的终端设备标识，由于用户存在更换终端设备的可能性，若本次支付的终端设备标识和支付卡的历史支付中的终端设备标识不一致，也可视为安全验证通过，在后续过程中可通过用户验证判断是否为用户本人使用更换的终端设备进行支付。又例如，安全验证信息包括本次支付的支付金额和支付方账户余额，若本次支付的支付金额小于等于支付方账户余额，则安全验证通过；反之，安全验证未通过。

在一些示例中，SDK 在接收到支付请求消息的情况下，若检测到当前登录的用户账号并未关联支付卡，可发出绑卡提示信息，以提示用户进入绑卡流程以绑定支付卡。在绑定支付卡后，SDK 再向安全控制系统发送安全验证请求消息。

在步骤 S202 中，接收安全控制系统发送的安全验证结果信息。

安全控制系统根据安全验证信息进行安全验证，可得到对于本次支付即支付请求消息指示的支付的安全验证结果信息。安全验证结果信息用于表征安全验证是否通过。若安全验证结果信息表征安全验证未通过，SDK 服务器可向终端设备中的 SDK 发送指示消息，以使 SDK 发出中止支付的弹窗信息。

在一些示例中，在 SDK 服务器接收到表征安全验证通过的安全验证结果信息后，终端设备中的 SDK 可调用预设的查询接口，将本次支付的如付款方信息等支付信息、订单号等订单信息等传输至 SDK 服务器，SDK 服务器可进一步补充本次支付的如商户号等其他订单信息以及与付款相关的其他支付信息等，将支付信息、订单信息同步至宿主程序服务器，以实现 SDK 服务器与宿主程序服务器关于本次支付的信息的同步。

在一些示例中，在 SDK 后台系统包括 SDK 后台子系统和支付码子系统的情况下，在 SDK 后台子系统中的 SDK 服务器接收到表征安全验证通过的安全验证结果信息后，SDK 后台子系统中的 SDK 服务器可可调用预设的查询接口，将本次支付的如付款方信息等支付信息、订单号等订单信息等传输至支付码子系统的 SDK 服务器，支付码子系统的 SDK 服务器可进一步补充本次支付的如商户号等其他订单信息以及与付款相关的其他支付信息等，将支付信息、订单信息同步至宿主程序服务器，以实现 SDK 后台系统中的 SDK 服务器与宿主程序服务器关于本次支付的信息的同步。

在步骤 S203 中，在安全验证结果信息表征安全验证通过的情况下，向终端设备中的 SDK 发送第一通知消息。

安全验证结果信息表征安全验证通过，则可再进行宿主程序的所属方的用户验证流程。第一通知消息用于指示 SDK 通知宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息。第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息。

终端设备中的 SDK 响应于第一通知消息，可向宿主程序发送用于指示宿主程序展示用户验证页面的消息。响应于该消息，宿主程序使终端设

备显示用户验证页面。用户验证页面可包括密码填写区、验证码填写区、生物特征采集区等，在此并不限定用户验证的方式。用户向用户验证页面输入的信息即为第一用户验证输入信息。宿主程序可向宿主程序服务器发送第一用户验证输入信息。宿主程序服务器可根据接收到的第一用户验证输入信息进行用户验证，并得到用户验证结果信息。用户验证用于验证用户的身份。用户验证通过表示进行支付操作的用户是合法的用户本人。例如，第一用户验证输入信息为密码，宿主程序服务器验证第一用户验证输入信息与宿主程序服务器中用户注册的密码是否一致，若一致，则用户验证通过；反之，则用户验证未通过。又例如，第一用户验证输入信息为人脸图像，宿主程序服务器验证第一用户验证输入信息与宿主程序服务器中用户预留的人脸图像是否属于同一用户，若属于同一用户，则用户验证通过；反之，则用户验证未通过。

用户验证结果信息用于表征用户验证是否通过。宿主程序服务器可将用户验证结果信息分别向宿主程序和 SDK 服务器反馈，宿主程序还会将用户验证结果传输给 SDK，以使 SDK 的所属方和宿主程序的所属方均可得知用户验证是否通过。

在一些示例中，在宿主程序展示用户验证页面时，SDK 可添加与展示用户验证页面这一动作关联的埋点信息，以便后续对宿主程序展示用户验证页面这一过程的执行情况的分析和排查。

在步骤 S204 中，在用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

用户验证结果信息表征用户验证通过，表示用户身份安全性较高，可向支付方账户管理系统发起付款请求，正常进行支付。用户验证结果信息表征用户验证未通过，可中止该支付。

在一些实施例中，由于用户验证结果信息在传输过程中可能被窃取或篡改，为了进一步保证支付安全，可通过一致性验证条件来对用户验证结果信息在传输过程中的安全性进行验证。在用户验证结果信息满足一致性验证条件的情况下，发起所述付款请求。一致性验证条件用于判断用户验证结果信息在传输过程中是否安全、有效。用户验证结果信息满足一致性

验证条件，表示用户验证结果信息在传输过程中是安全、有效的，可向支付方账户管理系统发起付款请求，正常进行支付，或者，由 SDK 服务器通过宿主程序服务器向支付方账户管理系统发起付款请求，正常进行支付；用户验证结果信息不满足一致性验证条件，表示用户验证结果信息在传输过程中并不安全、有效，可中止该支付。

在一些示例中，一致性验证条件可包括第一用户验证结果信息和第二用户验证结果信息一致。其中，第一用户验证结果信息为由宿主程序服务器通过宿主程序传输给 SDK 的用户验证结果信息。第二用户验证结果信息为从宿主程序服务器获取的用户验证结果信息。第一用户验证结果信息和第二用户验证结果信息一致，表示用户验证结果信息在传输过程中是安全、有效的；第一用户验证结果信息和第二用户验证结果信息不一致，表示用户验证结果信息在传输过程中并不安全、有效。

支付成功后，SDK 服务器可获取付款结果信息，付款结果信息表征付款是否成功。SDK 服务器可将付款结果信息传输给 SDK、商户系统等，以将付款是否成功的结果展示给用户、商户等。

在上述支付过程中，用户验证通过后，由于用户验证结果信息的传输、付款、以及付款结果信息的传输都需要一定时间，终端设备不会立即显示支付完成页面，在这种情况下，SDK 可控制终端设备显示付款中标识，如包含“loading”字样的图像，在终端设备显示支付完成页面时，停止显示付款中标识。

在本申请实施例中，SDK 服务器响应于支付请求消息，向安全控制系统发送安全验证请求消息，以请求安全控制系统对本次支付进行安全验证，以完成 SDK 所属方所需的安全性方面的验证。在安全验证通过的情况下，SDK 服务器向终端设备的 SDK 发送用于指示 SDK 通知宿主程序展示用户验证页面的消息，以使 SDK 能够触发宿主程序主动发起用户验证，以完成宿主程序所属方所需的用户身份安全性方面的验证。在支付过程中实现了 SDK 所属方和宿主程序所属方两个主体的双向验证，提高了支付的安全性，也满足了 SDK 所属方和宿主程序所属方两个主体对安全性管控的需求。

在一些示例中，在 SDK 服务器通过宿主程序服务器向支付方账户管理系统发起付款请求的情况下，SDK 服务器可提供 SDK 所属方的第一支付策略信息，第一支付策略信息可包括 SDK 所属方的优惠信息、支付活动信息等，可用于参与支付请求消息指示的支付的金额计算。宿主程序服务器可提供宿主程序所属方的第二支付策略信息，第二支付策略信息可包括宿主程序所属方的优惠信息、支付活动信息等，可用于参与支付请求消息指示的支付的金额计算。

在一些实施例中，SDK 服务器也可在接收支付请求消息后，直接向宿主程序服务器或通过支付策略系统向宿主程序服务器查询优惠信息、支付活动信息等支付策略信息。

在上述实施例中，SDK 与宿主程序之间交互的信息为加密信息，SDK 需要对信息进行加、解密。对应地，SDK 服务器存储有用于对 SDK 与宿主程序之间交互的信息进行加、解密的密钥。

在一些实施例中，SDK 服务器可向宿主程序服务器请求用户验证方式，并将宿主程序服务器的反馈传输给 SDK，以使 SDK 做出对应的操作。图 3 为本申请第一方面提供的支付方法的另一实施例的流程图。图 3 与图 2 的不同之处在于，图 3 所示的支付方法还可包括步骤 S205 至步骤 S208，图 2 中的步骤 S203 可具体细化为图 3 中的步骤 S2031。

在步骤 S205 中，在安全验证结果信息表征安全验证通过的情况下，向宿主程序服务器发送用户验证方式请求消息。

用户验证方式请求消息用于向宿主程序服务器请求用户验证方式，可包括支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上。订单信息、终端设备信息和支付信息的具体内容可参见上述实施中的相关说明，在此不再赘述。

宿主程序服务器可根据用户验证方式请求消息中的信息，确定验证操作信息，验证操作信息用于指示是否进行用户验证以及用户验证的方式。宿主程序服务器可存储有用于确定是否进行用户验证以及用户验证的方式的判断条件，可通过用户验证方式请求消息中的信息是否满足参考条件来判断是否进行用户验证以及用户验证的方式。判断条件可根据支付场景、

需求等设置，在此并不限定。例如，用户验证方式请求消息可包括支付信息，支付信息包括支付金额，判断条件可包括支付金额范围与是否进行用户验证以及用户验证的方式的对应关系，如判断条件包括：支付金额小于 100 元，不需进行用户验证；支付金额在 100 元至 500 元的范围内，需进行用户验证，且用户验证的方式为密码验证；支付金额在 500 元至 1000 元的范围内，需进行用户验证，且用户验证的方式为验证码验证；支付金额大于 1000 元，需进行用户验证，且用户验证的方式为生物特征验证。又例如，用户验证方式请求消息可包括订单信息和支付信息，订单信息包括订单标识和下订单用户账号，支付信息包括付款方登录账号，判断条件可包括：下订单用户账号与付款方登录账号不一致，需进行用户验证，且用户验证方式为生物特征验证；下订单用户账号与付款方登录账号一致，需进行用户验证，且用户验证方式为密码验证。

宿主程序服务器确定验证操作信息后，可向 SDK 服务器发送用户验证方式反馈消息。用户验证方式反馈消息包括验证操作信息。

在步骤 S206 中，接收宿主程序服务器发送的用户验证方式反馈消息。

在步骤 S207 中，在验证操作信息包括拒绝支付标识的情况下，向 SDK 发送第二通知消息。

拒绝支付标识表示不需进行用户验证且停止支付。响应于用户验证方式反馈信息，SDK 服务器向终端设备中 SDK 发送第二通知信息。第二通知消息用于指示 SDK 发出拒绝支付提示信息。SDK 响应于第二通知消息，可发出提示信息，以提示用户存在支付风险。例如，提示信息使终端设备显示“宿主程序风险受限”等文字。在一些示例中，用户验证方式反馈消息还可包括拒绝支付原因，对应地，第二通知信息也可包括该拒绝支付原因，SDK 响应于第二通知信息发出的提示信息可包括该拒绝支付原因，终端设备可显示该决绝支付原因，以告知用户。拒绝支付原因可包括 SDK 异常、宿主程序服务器异常等导致用户验证方式标识失败的原因。

在步骤 S208 中，在验证操作信息包括免密支付标识的情况下，向 SDK 发送第三通知消息。

免密支付标识表示不需进行用户验证且可继续支付流程。响应于用户验证方式反馈信息，SDK 服务器向终端设备中 SDK 发送第三通知信息。第三通知消息用于指示 SDK 发出免密支付提示信息。免密支付提示信息可提示用户该支付为免密方式的支付。

在步骤 S2031 中，在验证操作信息包括用户验证方式标识且安全验证结果信息表征安全验证通过的情况下，向 SDK 发送第一通知消息。

第一通知消息包括用户验证方式标识。用户验证方式标识用于指示用户验证的方式。第一通知消息用于指示 SDK 通知宿主程序展示与用户验证方式标识匹配的用户验证页面，以提示用户输入与用户验证方式标识匹配的第一用户验证输入信息。即 SDK 响应于第一通知消息，可向宿主程序发送包括用户验证方式标识的指示消息，宿主程序根据用户验证方式标识，展现与用户验证方式标识指示的用户验证的方式对应的用户验证页面，对应地，用户输入的第一用户验证输入信息也与用户验证方式标识指示的用户验证的方式对应。

例如，用户验证方式标识为 01，用户验证的方式为密码验证，宿主程序展示的用户验证页面为密码验证页面，用户需输入的第一用户验证输入信息为密码；用户验证方式标识为 10，用户验证的方式为验证码验证，宿主程序展示的用户验证页面为验证码验证页面，用户需输入的第一用户验证输入信息为验证码；用户验证方式标识为 11，用户验证的方式为生物特征验证，宿主程序展示的用户验证页面为生物特征验证页面，用户需输入的第一用户验证输入信息为生物特征。

在一些实施例中，支付请求消息、安全验证请求消息和安全验证结果信息可包括目标宿主程序标识。目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识，即目标宿主程序标识可表征支付请求消息对应的支付关联的宿主程序。

SDK 服务器预设有第一对应关系。第一对应关系包括宿主程序标识与用户验证调起方的关系。宿主程序标识用于标识宿主程序。用户验证调起方用于指示展示用户验证页面的主体，用户验证调起方包括终端设备中的 SDK 或宿主程序。在接收安全验证结果信息后，SDK 服务器可根据目标

宿主程序标识和第一对应关系，确定与目标宿主程序标识对应的目标用户验证调起方。目标用户验证调起方为在第一对应关系中与目标宿主程序标识对应的用户验证调起方。

在目标用户验证调起方为宿主程序的情况下，SDK 服务器向 SDK 发送第一通知消息。在目标用户验证调起方为 SDK 的情况下，SDK 服务器向 SDK 发送第四通知消息。第四通知消息用于指示 SDK 展示用户验证页面，以提示用户输入第二用户验证输入信息。第二用户验证输入信息用于 SDK 服务器进行用户验证以得到用户验证结果信息。终端设备中的 SDK 响应于第四通知消息，可由 SDK 直接展示用户验证页面，对应地，用户验证由 SDK 服务器执行。终端设备中的 SDK 可向 SDK 服务器发送第二用户验证输入信息。SDK 服务器根据第二用户验证输入信息进行用户验证，得到用户验证结果信息，用户验证的具体内容可参见上述实施例中宿主程序服务器进行的用户验证的相关说明，在此不再赘述。

通过第一对应关系的设置，可使终端设备中用户验证的主体设置更加灵活，具有更多选择性。

在一些实施例中，支付由商户系统或通过终端设备中安装的商户程序发起，在 SDK 服务器接收到支付请求消息前，商户系统与 SDK 之间、SDK 与 SDK 服务器之间还需就订单的相关信息进行交互。图 4 为本申请第一方面提供的支付方法的又一实施例的流程图。图 4 与图 2 的不同之处在于，图 4 所示的支付方法还可包括步骤 S209 至步骤 S211。

在步骤 S209 中，响应于商户系统发送的订单请求消息，生成订单标识。

在用户下单生成订单后，商户系统可向 SDK 服务器发送订单请求消息，以向 SDK 服务器请求能够标识该笔订单的标识即订单标识。SDK 服务器生成的订单标识具体可为订单流水号。

在步骤 S210 中，向商户系统发送订单反馈消息，以使商户系统向 SDK 发送 SDK 调用请求消息。

SDK 服务器可生成订单反馈消息，订单反馈消息包括订单标识。SDK 服务器向商户系统发送该订单反馈消息，订单反馈消息包括订单标识。商

户系统接收到订单反馈消息后，可向终端设备的 SDK 发送 SDK 调用请求消息，SDK 调用请求包括订单标识。SDK 调用请求消息用于请求调用终端设备中的 SDK。终端设备中的 SDK 在初始化的过程中，可采集终端设备的地理位置、终端设备标识等信息。

在步骤 S211 中，响应于 SDK 发送的第一订单查询消息，向 SDK 发送第一查询反馈消息。

SDK 可向 SDK 服务器发送第一订单查询消息，以在 SDK 服务器通过订单标识查询订单标识对应的订单信息。第一订单查询消息包括订单标识。SDK 服务器查找到与订单标识对应的订单消息后，通过第一查询反馈消息将与订单标识对应的订单消息反馈给 SDK。第一查询反馈消息包括与订单标识对应的订单信息。SDK 接收到第一查询反馈消息后，可向 SDK 服务器发送支付请求消息。

在一些实施例中，商户可指定特定的付款方付款，订单请求消息包括指定付款方身份信息，即通过订单请求消息制定特定的付款方。SDK 向 SDK 服务器发送的支付请求消息包括如用户登录账号等支付的付款方身份信息，SDK 服务器可在指定付款方身份信息与支付请求消息指示的支付的付款方身份信息不一致的情况下，向 SDK 发送支付中止通知消息，以使 SDK 发出支付提示信息。支付提示信息可提示用户切换用户登录账号重新支付，支付提示信息也可提示用户支付中止的原因，如支付提示信息为终端设备显示的“登录账号信息与商户指定信息不符，暂无法支付”等字样。

在一些实施例中，支付可为用户利用终端设备扫描他人的收款码发起的支付。在 SDK 服务器接收到支付请求消息前，SDK 与 SDK 服务器之间还需就订单的相关信息进行交互。图 5 为本申请第一方面提供的支付方法的又另一实施例的流程图。图 5 与图 2 的不同之处在于，图 5 所示的支付方法还可包括步骤 S212 和步骤 S213。

在步骤 S212 中，接收终端设备的 SDK 发送的第二订单查询消息。

终端设备扫描收款码，可得到第一码信息。第一码信息为从收款码中读取得到的码信息。终端设备的 SDK 可向 SDK 服务器发送第二订单查询

消息。第二订单查询消息用于向 SDK 服务器请求查询与第一码信息对应的订单消息。第二订单查询消息包括终端设备扫描收款码得到的第一码信息。

在步骤 S213 中，向 SDK 发送第二查询反馈消息。

SDK 服务器根据第一码信息，查找与第一码信息对应的订单信息。在查找到与第一码信息对应的订单信息后，SDK 服务器可生产第二查询反馈消息，并向 SDK 发送第二查询反馈消息。第二查询反馈消息包括与第一码信息对应的订单信息。

SDK 接收到第二查询反馈消息后，可根据用户的输入确定支付金额，生成支付请求消息，向 SDK 服务器发送支付请求消息。SDK 服务器在接收到支付请求消息后，可判断支付请求消息指示的支付的付款卡是否可用，在付款卡可用的情况下，向安全控制系统发送安全验证请求消息。

在一些实施例中，支付可为用户利用终端设备显示付款码，由他人利用支付受理终端扫描付款码发起的支付。在 SDK 服务器接收到支付请求消息前，SDK 可向 SDK 服务器申请付款码。图 6 为本申请第一方面提供的支付方法的再一实施例的流程图。图 6 与图 2 的不同之处在于，图 6 所示的支付方法还可包括步骤 S214。

在步骤 S214 中，响应于接收的付款码申请消息，向 SDK 发送付款码反馈消息。

付款码申请消息由 SDK 发送。即终端设备中的 SDK 可向 SDK 服务器发送付款码申请消息，付款码申请消息用于向 SDK 服务器申请付款码。SDK 服务器为付款码申请消息分配付款码，并通过付款码反馈消息将付款码反馈给 SDK。付款码反馈消息包括付款码。

在一些示例中，SDK 后台系统包括 SDK 后台子系统和支付码子系统。SDK 可向 SDK 后台子系统中的 SDK 服务器发送付款码申请消息，SDK 后台子系统中的 SDK 服务器向支付码子系统中的 SDK 服务器转发付款码申请消息，支付码子系统中的 SDK 服务器为付款码申请消息分配付款码，并向 SDK 后台子系统中的 SDK 服务器发送付款码反馈消息，SDK 后台子系统中的 SDK 服务器向 SDK 转发付款码反馈消息。

支付请求消息由支付受理设备基于扫描的付款码生成。SDK 收到付款码反馈消息后，可在支付时显示付款码。支付受理设备扫描付款码，得到第二码信息，第二码信息为从付款码中读取得到的码信息。支付受理设备可基于第二码信息生成支付请求消息，并向 SDK 服务器发送支付请求消息。

本申请第二方面提供一种支付方法，该支付方法应用于终端设备，即该支付方法可由终端设备执行。终端设备具有 SDK 和宿主程序。图 7 为本申请第二方面提供的支付方法的一实施例的流程图。如图 7 所示，该支付方法可包括步骤 S301 至步骤 S304。

在步骤 S301 中，通过 SDK 获取 SDK 服务器发送的第一通知消息。

第一通知消息是 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的。安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应的支付进行安全验证得到的。安全验证请求消息由 SDK 服务器响应于接收的支付请求消息发送。

在步骤 S302 中，响应于第一通知消息，通过 SDK 通知宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息。

在步骤 S303 中，通过宿主程序向宿主程序服务器反馈第一用户验证输入信息。

第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息。

在步骤 S304 中，通过 SDK 向 SDK 服务器发送通过宿主程序从宿主程序服务器获取的用户验证结果信息，使 SDK 服务器在用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

在一些实施例中，用户验证结果信息还用于使 SDK 服务器在用户验证结果信息满足一致性验证条件的情况下，发起付款请求。

在一些示例中，一致性验证条件包括：第一用户验证结果信息和第二用户验证结果信息一致，第一用户验证结果信息为由宿主程序服务器通过宿主程序传输给 SDK 的用户验证结果信息，第二用户验证结果信息为从宿主程序服务器获取的用户验证结果信息。

上述步骤 S301 至步骤 S304 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在本申请实施例中，SDK 服务器响应于支付请求消息，向安全控制系统发送安全验证请求消息，以请求安全控制系统对本次支付进行安全验证，以完成 SDK 所属方所需的安全性方面的验证。在安全验证通过的情况下，终端设备中的 SDK 接收到 SDK 服务器发送的用于指示 SDK 通知宿主程序展示用户验证页面的消息，SDK 响应于该消息，触发宿主程序主动发起用户验证，以完成宿主程序所属方所需的用户身份安全性方面的验证。在支付过程中实现了 SDK 所属方和宿主程序所属方两个主体的双向验证，提高了支付的安全性，也满足了 SDK 所属方和宿主程序所属方两个主体对安全性管控的需求。

在一些实施例中，SDK 服务器可向宿主程序服务器请求用户验证方式，SDK 可通过 SDK 服务器获取宿主程序服务器的反馈，并做出对应的操作。图 8 为本申请第二方面提供的支付方法的另一实施例的流程图。图 8 与图 7 的不同之处在于，图 8 所示的支付方法还可包括步骤 S305 和步骤 S306。

在步骤 S305 中，响应于 SDK 接收的第二通知消息，通过 SDK 发出拒绝提示信息。

第二通知消息由 SDK 服务器在验证操作信息包括拒绝支付标识的情况下发送。

在步骤 S306 中，响应于 SDK 接收的第三通知消息，通过 SDK 发出免密支付提示信息。

第三通知消息由 SDK 服务器在验证操作信息包括免密支付标识的情况下发送。

用户验证方式反馈消息包括验证操作信息。用户验证方式反馈消息由宿主服务器响应于用户验证方式请求消息发送。用户验证方式请求消息由 SDK 服务器在安全验证结果信息表征安全验证通过的情况下向宿主程序服务器发送。用户验证方式请求消息包括支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上。

在一些实施例中，第一通知消息由 SDK 服务器在验证操作信息包括用户验证方式标识的情况下发送。第一通知消息包括用户验证方式标识，用于指示 SDK 通知宿主程序展示与用户验证方式标识匹配的用户验证页面，以提示用户输入与用户验证方式标识匹配的第一用户验证输入信息。

上述步骤 S305 和步骤 S306 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在一些实施例中，安全验证结果信息包括目标宿主程序标识。目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识。第一通知消息由 SDK 服务器在目标用户验证调起方为宿主程序的情况下发送。目标用户验证调起方为第一对应关系中与目标宿主程序标识匹配的用户验证调起方，目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识。第一对应关系包括宿主程序标识与用户验证调起方的关系。

在一些实施例中，在目标用户验证调起方为 SDK 的情况下，终端设备通过 SDK 获取 SDK 服务器发送的第四通知消息。第四通知消息由 SDK 服务器在目标用户验证调起方为 SDK 的情况下发送。终端设备响应于第四通知消息，调用 SDK 展示用户验证页面，以提示用户输入第二用户验证输入信息。终端设备通过 SDK 向 SDK 服务器反馈第二用户验证输入信息。第二用户验证输入信息用于 SDK 服务器进行用户验证以得到用户验证结果信息。

在一些实施例中，支付由商户系统或通过终端设备中安装的商户程序发起，在 SDK 服务器接收到支付请求消息前，商户系统与 SDK 之间、SDK 与 SDK 服务器之间还需就订单的相关信息进行交互。图 9 为本申请第二方面提供的支付方法的又一实施例的流程图。图 9 与图 7 的不同之处在于，图 9 所示的支付方法还可包括步骤 S307 至步骤 S309。

在步骤 S307 中，通过 SDK 接收 SDK 调用请求消息，SDK 调用请求消息由商户系统响应于订单反馈消息生成。

订单反馈消息和 SDK 调用请求消息包括订单标识。订单标识由 SDK 服务器响应于商户系统发送的订单请求消息生成。

在步骤 S308 中，响应于 SDK 调用请求消息，通过 SDK 向 SDK 服务

器发送第一订单查询消息。

在步骤 S309 中，通过 SDK 接收 SDK 服务器响应于第一订单查询消息发送的第一查询反馈消息。

第一查询反馈消息包括与订单标识对应的订单信息。

在一些实施例中，订单请求消息包括指定付款方身份信息。响应于通过 SDK 接收的支付中止通知消息，终端设备可通过 SDK 发出支付提示信息。支付中止通知消息由 SDK 服务器在指定付款方身份信息与支付请求消息指示的支付的付款方身份信息不一致的情况下发送。

上述步骤 S307 至步骤 S309 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在一些实施例中，支付可为用户利用终端设备扫描他人的收款码发起的支付。在 SDK 服务器接收到支付请求消息前，SDK 与 SDK 服务器之间还需就订单的相关信息进行交互。图 10 为本申请第二方面提供的支付方法的又另一实施例的流程图。图 10 与图 7 的不同之处在于，图 10 所示的支付方法还可包括步骤 S310 至步骤 S312。

在步骤 310 中，扫描付款码，得到第一码信息。

在步骤 311 中，通过 SDK 向 SDK 服务器发送第二订单查询消息。

第二订单查询消息包括第一码信息。

在步骤 312 中，通过 SDK 接收 SDK 服务器发送的第二查询反馈消息。

第二查询反馈消息包括与第一码信息对应的订单信息。

上述步骤 S310 至步骤 S312 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在一些实施例中，支付可为用户利用终端设备显示付款码，由他人利用支付受理终端扫描付款码发起的支付。在 SDK 服务器接收到支付请求消息前，SDK 可向 SDK 服务器申请付款码。图 11 为本申请第二方面提供的支付方法的再一实施例的流程图。图 11 与图 7 的不同之处在于，图 11 所示的支付方法还可包括步骤 S313 至步骤 S315。

在步骤 S313 中，通过 SDK 向 SDK 服务器发送付款码申请消息。

在步骤 S314 中，通过 SDK 接收 SDK 服务器发送的付款码反馈消息。

付款码反馈消息包括付款码。

在步骤 S315 中，显示付款码。

付款码用于被支付受理设备扫描以生成支付请求消息。

上述步骤 S313 至步骤 S315 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

本申请第三方面提供一种支付方法，应用于宿主程序服务器，即该支付方法可由宿主程序服务器执行。图 12 为本申请第三方面提供的支付方法的一实施例的流程图。如图 12 所示，该支付方法可包括步骤 S401 至步骤 S403。

在步骤 S401 中，接收终端设备通过宿主程序反馈的第一用户验证输入信息。

第一用户验证输入信息在 SDK 响应于第一通知消息通知宿主程序展示用户验证页面后得到。第一通知消息是 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的。安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应支付进行安全验证得到的。安全验证请求消息由 SDK 服务器响应于接收的支付请求消息发送。

在步骤 S402 中，根据第一用户验证输入信息进行用户验证，得到用户验证结果信息。

在步骤 S403 中，向终端设备中的宿主程序发送用户验证结果信息，通过宿主程序将用户验证结果信息传输给 SDK，以使 SDK 向 SDK 服务器发送用户验证结果信息，在用户验证结果信息表征用户验证通过的情况下，使 SDK 服务器发起付款请求，以完成支付。

在一些实施例中，在执行步骤 S403 之后，宿主程序服务器还可向 SDK 服务器发送用户验证结果信息，以使 SDK 服务器在用户验证结果信息表征用户验证通过且用户验证结果信息满足一致性验证条件的情况下，发起付款请求，以完成支付。

在一些示例中，一致性验证条件包括第一用户验证结果信息和第二用户验证结果信息一致。第一用户验证结果信息为由宿主程序服务器通过宿主程序传输给 SDK 的用户验证结果信息，第二用户验证结果信息为从宿主程序服务器获取的用户验证结果信息。

上述步骤 S401 至步骤 S403 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在本申请实施例中，SDK 服务器响应于支付请求消息，向安全控制系统发送安全验证请求消息，以请求安全控制系统对本次支付进行安全验证，以完成 SDK 所属方所需的安全性方面的验证。在安全验证通过的情况下，SDK 服务器向终端设备的 SDK 发送用于指示 SDK 通知宿主程序展示用户验证页面的消息，以使 SDK 能够触发宿主程序主动发起用户验证。终端设备可接收用户输入的第一用户验证输入信息，并将第一用户验证输入信息向宿主程序服务器发送，宿主程序服务器可完成宿主程序所属方所需的用户身份安全性方面的验证。在支付过程中实现了 SDK 所属方和宿主程序所属方两个主体的双向验证，提高了支付的安全性，也满足了 SDK 所属方和宿主程序所属方两个主体对安全性管控的需求。

在上述实施例中，宿主程序服务器存储有用于对宿主程序与 SDK 之间交互的信息进行加、解密的密钥，具体内容可参见上述实施例中的现关说明，在此不再赘述。

在一些实施例中，宿主程序服务器可接受 SDK 服务器的请求，向 SDK 服务器提供用户验证方式，SDK 可通过 SDK 服务器获取宿主程序服务器的反馈，并做出对应的操作。图 13 为本申请第三方面提供的支付方法的另一实施例的流程图。图 13 与图 12 的不同之处在于，图 13 所示的支付方法还可包括步骤 S404 和步骤 S405。

在步骤 S404 中，接收 SDK 服务器在安全验证结果信息表征安全验证通过的情况下发送的用户验证方式请求消息。

用户验证方式请求消息包括支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上。

在步骤 S405 中，根据用户验证方式请求消息，向 SDK 服务器发送用

户验证方式反馈消息。

用户验证方式反馈消息包括验证操作信息。

在验证操作信息包括拒绝支付标识的情况下，SDK 服务器向 SDK 发送第二通知消息，第二通知消息用于指示 SDK 发出拒绝支付提示信息。在验证操作信息包括免密支付标识的情况下，SDK 服务器向 SDK 发送第三通知消息，第三通知消息用于指示 SDK 发出免密支付提示信息。

在一些实施例中，第一通知消息由 SDK 服务器在验证操作信息包括用户验证方式标识的情况下发送。第一通知消息包括用户验证方式标识，用于指示 SDK 通知宿主程序展示与用户验证方式标识匹配的用户验证页面，以提示用户输入与用户验证方式标识匹配的第一用户验证输入信息。

上述步骤 S404 和步骤 S405 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在一些示例中，安全验证结果信息包括目标宿主程序标识。目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识。第一通知消息由 SDK 服务器在目标用户验证调起方为宿主程序的情况下发送。目标用户验证调起方为第一对应关系中与目标宿主程序标识匹配的用户验证调起方。目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识。第一对应关系包括宿主程序标识与用户验证调起方的关系。

为了便于说明，下面分别以支付由商户系统或通过终端设备中安装的商户程序发起、支付由终端设备扫描他人的收款码发起、支付由支付受理终端扫描付款码发起三种场景为例，对终端设备、系统、服务器之间的支付流程的交互进行说明。

在该示例中，支付由商户系统或通过终端设备中安装的商户程序发起。图 14 为本申请实施例提供的支付流程的一示例的流程图。终端设备包括 SDK 和宿主程序。如图 14 所示，该支付流程包括步骤 S501 至步骤 S522。

在步骤 S501 中，用户下单后，商户系统向 SDK 服务器发送订单请求消息。

在步骤 S502 中，SDK 服务器响应于订单请求消息，向商户系统发送

订单反馈消息。订单反馈消息可包括 SDK 服务器生成的订单标识。

在步骤 S503 中，商户系统向终端设备中 SDK 发送 SDK 调用请求消息。

在步骤 S504 中，SDK 采集终端设备信息。

在步骤 S505 中，SDK 向 SDK 服务器发送第一订单查询消息。

在步骤 S506 中，SDK 服务器向 SDK 反馈第一查询反馈消息。

在步骤 S507 中，SDK 向 SDK 服务器发送支付请求消息。

在步骤 S508 中，SDK 服务器向安全控制系统发送安全验证请求消息。

在步骤 S509 中，安全控制系统对支付请求消息指示的支付进行安全验证。

在步骤 S510 中，安全控制系统向 SDK 服务器反馈安全验证结果信息。

在步骤 S511 中，在安全验证结果信息表征安全验证通过的情况下，SDK 服务器向宿主程序服务器发送用户验证方式请求消息。

在步骤 S512 中，宿主程序服务器响应于用户验证方式请求消息，向 SDK 服务器发送用户验证方式反馈消息。用户验证方式反馈消息包括用户验证方式标识。

在步骤 S513 中，SDK 服务器向 SDK 发送第一通知消息。第一通知消息包括用户验证方式标识。

在步骤 S514 中，SDK 向宿主程序传输用户验证方式标识。

在步骤 S515 中，宿主程序被触发，展示与用户验证方式标识匹配的用户验证页面。

在步骤 S516 中，宿主程序接收用户输入的第一用户验证输入信息，向宿主程序服务器发送第一用户验证输入信息。

在步骤 S517 中，宿主程序服务器根据第一用户验证输入信息进行用户验证，得到用户验证结果信息。

在步骤 S518 中，SDK 服务器从宿主程序服务器获取用户验证结果信息。为了便于说明，将 SDK 服务器直接从宿主服务器获取到的用户验证

结果信息称为第二用户验证结果信息。

在步骤 S519 中，宿主程序服务器向宿主程序发送用户验证结果信息。

在步骤 S520 中，宿主程序将用户验证结果信息反馈给 SDK。

在步骤 S521 中，SDK 将用户验证结果信息反馈给 SDK 服务器。为了便于说明，将 SDK 服务器从 SDK 获取到的用户验证结果信息称为第一用户验证结果信息。

在步骤 S522 中，在第一用户验证结果信息和第二用户验证结果信息一致的情况下，SDK 服务器发起付款请求，以完成支付。

上述步骤 S501 至步骤 S522 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在该示例中，支付由终端设备扫描他人的收款码发起。图 15 为本申请实施例提供的支付流程的另一示例的流程图。终端设备包括 SDK 和宿主程序。如图 15 所示，该支付流程可包括步骤 S601 至步骤 S621。

在步骤 S601 中，终端设备扫描收款码，得到第一码信息，SDK 向 SDK 服务器发送第二订单查询消息。第二订单查询消息包括第一码信息。

在步骤 S602 中，SDK 服务器向 SDK 发送第二查询反馈消息。

在步骤 S603 中，SDK 接收用户输入，确定支付金额。

在步骤 S604 中，SDK 向 SDK 服务器发送支付请求消息。

在步骤 S605 中，SDK 服务器判断是否有可用的付款卡。

在步骤 S606 中，在存在可用的付款卡的情况下，SDK 服务器向安全控制系统发送安全验证请求消息。

在步骤 S607 中，安全控制系统对支付请求消息指示的支付进行安全验证。

在步骤 S608 中，安全控制系统向 SDK 服务器反馈安全验证结果信息。

在步骤 S609 中，在安全验证结果信息表征安全验证通过的情况下，SDK 服务器向宿主程序服务器发送用户验证方式请求消息。

在步骤 S610 中，宿主程序服务器响应于用户验证方式请求消息，向

SDK 服务器发送用户验证方式反馈消息。用户验证方式反馈消息包括用户验证方式标识。

在步骤 S611 中，SDK 服务器向 SDK 发送第一通知消息。第一通知消息包括用户验证方式标识。

在步骤 S612 中，SDK 向宿主程序传输用户验证方式标识。

在步骤 S613 中，宿主程序被触发，展示与用户验证方式标识匹配的用户验证页面。

在步骤 S614 中，宿主程序接收用户输入的第一用户验证输入信息，向宿主程序服务器发送第一用户验证输入信息。

在步骤 S615 中，宿主程序服务器根据第一用户验证输入信息进行用户验证，得到用户验证结果信息。

在步骤 S616 中，SDK 服务器从宿主程序服务器获取用户验证结果信息。为了便于说明，将 SDK 服务器直接从宿主服务器获取到的用户验证结果信息称为第二用户验证结果信息。

在步骤 S617 中，宿主程序服务器向宿主程序发送用户验证结果信息。

在步骤 S618 中，宿主程序将用户验证结果信息反馈给 SDK。

在步骤 S619 中，SDK 将用户验证结果信息反馈给 SDK 服务器。为了便于说明，将 SDK 服务器从 SDK 获取到的用户验证结果信息称为第一用户验证结果信息。

在步骤 S620 中，在第一用户验证结果信息和第二用户验证结果信息一致的情况下，SDK 服务器向宿主程序服务器发起付款请求。

在步骤 S621 中，宿主程序服务器向付款方账户管理系统发起付款请求，以完成支付。

上述步骤 S601 至步骤 S621 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在该示例中，支付由支付受理终端扫描终端设备显示的付款码发起。终端设备包括 SDK 和宿主程序。这里以 SDK 后台系统包括 SDK 后台子系统和支付码子系统为例进行说明，为了便于说明，将 SDK 后台子系统中

的 SDK 服务器称为第一 SDK 服务器，将支付码子系统中的 SDK 服务器称为第二 SDK 服务器。图 16 为本申请实施例提供的支付流程的又一示例的流程图。如图 16 所示，该支付流程可包括步骤 S701 至步骤 S723。

在步骤 S701 中，终端设备中 SDK 通过第一 SDK 服务器向第二 SDK 服务器发送付款码申请消息。

在步骤 S702 中，第二 SDK 服务器分配付款码，并通过第一 SDK 服务器向 SDK 发送付款码反馈消息。付款码反馈消息包括付款码。

在步骤 S703 中，支付受理终端扫描终端设备显示的付款码，得到第二码信息，向第二 SDK 服务器发送支付请求消息。

在步骤 S704 中，第二 SDK 服务器可通过支付策略系统向宿主程序服务器发送支付策略查询消息。

在步骤 S705 中，宿主程序服务器通过支付策略系统向第二 SDK 服务器反馈支付策略信息。

在步骤 S706 中，第二 SDK 服务器向第一 SDK 服务器发送附加处理请求消息。附加处理请求消息包括支付策略信息。

在步骤 S707 中，第一 SDK 服务器向安全控制系统发送安全验证请求消息。

在步骤 S708 中，安全控制系统对支付请求消息指示的支付进行安全验证。

在步骤 S709 中，安全控制系统向第一 SDK 服务器反馈安全验证结果信息。

在步骤 S710 中，第一 SDK 服务器通过第二 SDK 服务器将支付信息、订单信息等信息同步至宿主程序服务器。

在步骤 S711 中，第一 SDK 服务器通过第二 SDK 服务器向宿主程序服务器发送用户验证方式请求消息。

在步骤 S712 中，宿主程序服务器通过第二 SDK 服务器向第一 SDK 服务器发送用户验证方式反馈消息。用户验证方式反馈消息包括用户验证方式标识。

在步骤 S713 中，第一 SDK 服务器向 SDK 发送第一通知消息。第一

通知消息包括用户验证方式标识。

在步骤 S714 中，SDK 向宿主程序传输用户验证方式标识。

在步骤 S715 中，宿主程序被触发，展示与用户验证方式标识匹配的用户验证页面。

在步骤 S716 中，宿主程序接收用户输入的第一用户验证输入信息，向宿主程序服务器发送第一用户验证输入信息。

在步骤 S717 中，宿主程序服务器根据第一用户验证输入信息进行用户验证，得到用户验证结果信息。

在步骤 S718 中，第一 SDK 服务器通过第二 SDK 服务器从宿主程序服务器获取用户验证结果信息。为了便于说明，将 SDK 服务器通过第二 SDK 服务器从宿主服务器获取到的用户验证结果信息称为第二用户验证结果信息。

在步骤 S719 中，宿主程序服务器向宿主程序发送用户验证结果信息。

在步骤 S720 中，宿主程序将用户验证结果信息反馈给 SDK。

在步骤 S721 中，SDK 将用户验证结果反馈给第一 SDK 服务器。为了便于说明，将第一 SDK 服务器从 SDK 获取到的用户验证结果信息称为第一用户验证结果信息。若宿主程序的所属方与付款卡所属方相同，跳转步骤 S724；若宿主程序的所属方与付款卡所属方不同，跳转步骤 S725

在步骤 S722 中，在第一用户验证结果信息和第二用户验证结果信息一致的情况下，第一 SDK 服务器通过第二 SDK 服务器和宿主程序服务器向付款方账户管理系统发起付款请求，以完成支付。

在步骤 S723 中，在第一用户验证结果信息和第二用户验证结果信息一致的情况下，第一 SDK 服务器通过第二 SDK 服务器向付款方账户管理系统发起付款请求，以完成支付。

在上述步骤 S722 和步骤 S723 之前，若支付使用了支付策略信息，第二 SDK 服务器还可与支付策略系统交互以承兑支付策略信息。

上述步骤 S701 至步骤 S723 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

本申请第四方面提供一种 SDK 服务器。图 17 为本申请第四方面提供的 SDK 服务器的一实施例的结构示意图。如图 17 所示，该 SDK 服务器 800 可包括发送模块 801 和接收模块 802。

发送模块 801 可用于响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息。

安全验证请求消息包括安全验证信息，用于指示安全控制系统根据安全验证信息对支付请求消息对应的支付进行安全验证。

接收模块 802 可用于接收安全控制系统发送的安全验证结果信息。

发送模块 801 还可用于在安全验证结果信息表征安全验证通过的情况下，向终端设备中的 SDK 发送第一通知消息。

终端设备具有 SDK 和宿主程序。第一通知消息用于指示 SDK 通知宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息。第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息。

发送模块 801 还可用于在用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

在一些实施例中，发送模块 801 可用于在用户验证结果信息满足一致性验证条件的情况下，发起所述付款请求。

在一些示例中，一致性验证条件包括：第一用户验证结果信息和第二用户验证结果信息一致。

第一用户验证结果信息为由宿主程序服务器通过宿主程序传输给 SDK 的用户验证结果信息。第二用户验证结果信息为从宿主程序服务器获取的用户验证结果信息。

在本申请实施例中，SDK 服务器响应于支付请求消息，向安全控制系统发送安全验证请求消息，以请求安全控制系统对本次支付进行安全验证，以完成 SDK 所属方所需的安全性方面的验证。在安全验证通过的情况下，SDK 服务器向终端设备的 SDK 发送用于指示 SDK 通知宿主程序展示用户验证页面的消息，以使 SDK 能够触发宿主程序主动发起用户验证，以完成宿主程序所属方所需的用户身份安全性方面的验证。在支付过

程中实现了 SDK 所属方和宿主程序所属方两个主体的双向验证，提高了支付的安全性，也满足了 SDK 所属方和宿主程序所属方两个主体对安全性管控的需求。

在一些示例中，SDK 服务器存储有用于对 SDK 与宿主程序之间交互的信息进行加、解密的密钥。

在一些实施例中，发送模块 801 还可用于在安全验证结果信息表征安全验证通过的情况下，向宿主程序服务器发送用户验证方式请求消息。

用户验证方式请求消息包括支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上。

接收模块 802 还可用于接收宿主程序服务器发送的用户验证方式反馈消息。

用户验证方式反馈消息包括验证操作信息。

发送模块 801 还可用于在验证操作信息包括拒绝支付标识的情况下，向 SDK 发送第二通知消息。

第二通知消息用于指示 SDK 发出拒绝支付提示信息。

接收模块 802 还可用于在验证操作信息包括免密支付标识的情况下，向 SDK 发送第三通知消息。

第三通知消息用于指示 SDK 发出免密支付提示信息。

在一些实施例中，发送模块 801 可用于：在验证操作信息包括用户验证方式标识的情况下，向 SDK 发送第一通知消息。

第一通知消息包括用户验证方式标识，用于指示 SDK 通知宿主程序展示与用户验证方式标识匹配的用户验证页面，以提示用户输入与用户验证方式标识匹配的第一用户验证输入信息。

在一些实施例中，SDK 服务器还可包括查询模块。

查询模块可用于根据目标宿主程序标识和预设的第一对应关系，确定与目标宿主程序标识对应的目标用户验证调起方。

第一对应关系包括宿主程序标识与用户验证调起方的关系。

发送模块 801 可用于在目标用户验证调起方为宿主程序的情况下，向 SDK 发送第一通知消息。

在一些实施例中，发送模块 801 还可用于在目标用户验证调起方为 SDK 的情况下，向 SDK 发送第四通知消息。

第四通知消息用于指示 SDK 展示用户验证页面，以提示用户输入第二用户验证输入信息。第二用户验证输入信息用于 SDK 服务器进行用户验证以得到用户验证结果信息。

在一些实施例中，SDK 服务器 800 还可包括订单标识生成模块。

订单标识生成模块可用于响应于商户系统发送的订单请求消息，生成订单标识。

发送模块 801 还可用于向商户系统发送订单反馈消息，以使商户系统向 SDK 发送 SDK 调用请求消息。

订单反馈消息和 SDK 调用请求消息包括订单标识。

发送模块 801 还可用于响应于 SDK 发送的第一订单查询消息，向 SDK 发送第一查询反馈消息。

第一查询反馈消息包括与订单标识对应的订单信息。

在一些实施例中，订单请求消息包括指定付款方身份信息。

发送模块 801 还可用于在指定付款方身份信息与支付请求消息指示的支付的付款方身份信息不一致的情况下，向 SDK 发送支付中止通知消息，以使 SDK 发出支付提示信息。

在一些实施例中，接收模块 802 还可用于接收终端设备的 SDK 发送的第二订单查询消息。

第二订单查询消息包括终端设备扫描收款码得到的第一码信息。

发送模块 801 还可用于向 SDK 发送第二查询反馈消息。

第二查询反馈消息包括与第一码信息对应的订单信息。

在一些实施例中，发送模块 801 还可用于响应于接收的付款码申请消息，向 SDK 发送付款码反馈消息。

付款码申请消息由 SDK 发送。付款码反馈消息包括付款码。对应地，支付请求消息由支付受理设备基于扫描的付款码生成。

本申请第五方面提供一种终端设备。终端设备具有 SDK 和宿主程序。图 18 为第五方面提供的终端设备的一实施例的结构示意图。如图 18

所示，该终端设备 900 可包括接收模块 901、显示模块 902 和发送模块 903。

接收模块 901 可用于通过 SDK 获取 SDK 服务器发送的第一通知消息。

第一通知消息是 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的。安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应的支付进行安全验证得到的。安全验证请求消息由 SDK 服务器响应于接收的支付请求消息发送。

显示模块 902 可用于响应于第一通知消息，通过 SDK 通知宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息。

发送模块 903 可用于通过宿主程序向宿主程序服务器反馈第一用户验证输入信息。

第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息。

发送模块 903 还可用于通过 SDK 向 SDK 服务器发送通过宿主程序从宿主程序服务器获取的用户验证结果信息，使 SDK 服务器在用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

在一些实施例中，所述用户验证结果信息还用于使所述 SDK 服务器在所述用户验证结果信息满足一致性验证条件的情况下，发起所述付款请求。

在一些示例中，一致性验证条件包括：第一用户验证结果信息和第二用户验证结果信息一致。第一用户验证结果信息为由宿主程序服务器通过宿主程序传输给 SDK 的用户验证结果信息，第二用户验证结果信息为从宿主程序服务器获取的用户验证结果信息。

在本申请实施例中，SDK 服务器响应于支付请求消息，向安全控制系统发送安全验证请求消息，以请求安全控制系统对本次支付进行安全验证，以完成 SDK 所属方所需的安全性方面的验证。在安全验证通过的情况下，终端设备中的 SDK 接收到 SDK 服务器发送的用于指示 SDK 通知宿主程序展示用户验证页面的消息，SDK 响应于该消息，触发宿主程序主动

发起用户验证，以完成宿主程序所属方所需的用户身份安全性方面的验证。在支付过程中实现了 SDK 所属方和宿主程序所属方两个主体的双向验证，提高了支付的安全性，也满足了 SDK 所属方和宿主程序所属方两个主体对安全性管控的需求。

在一些示例中，SDK 具有安全域，SDK 中的信息存储于安全域。

SDK 与宿主程序之间交互的信息为加密信息。SDK 中加、解密的密钥存储于 SDK 服务器。宿主程序中加、解密的密钥存储于宿主程序服务器。

在一些实施例中，显示模块 902 还可用于响应于 SDK 接收的第二通知消息，通过 SDK 发出拒绝提示信息。

第二通知消息由 SDK 服务器在验证操作信息包括拒绝支付标识的情况下发送。

显示模块 902 还可用于响应于 SDK 接收的第三通知消息，通过 SDK 发出免密支付提示信息。

第三通知消息由 SDK 服务器在验证操作信息包括免密支付标识的情况下发送。

其中，用户验证方式反馈消息包括验证操作信息。用户验证方式反馈消息由宿主服务器响应于用户验证方式请求消息发送。用户验证方式请求消息由 SDK 服务器在安全验证结果信息表征安全验证通过的情况下向宿主程序服务器发送。用户验证方式请求消息包括支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上。

在一些实施例中，第一通知消息由 SDK 服务器在验证操作信息包括用户验证方式标识的情况下发送。第一通知消息包括用户验证方式标识，用于指示 SDK 通知宿主程序展示与用户验证方式标识匹配的用户验证页面，以提示用户输入与用户验证方式标识匹配的第一用户验证输入信息。

在一些实施例中，安全验证结果信息包括目标宿主程序标识。目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识。第一通知消息由 SDK 服务器在目标用户验证调起方为宿主程序的情况下发送，目标用户验证调起方为第一对应关系中与目标宿主程序标识匹配的用户验证调起

方，目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识，第一对应关系包括宿主程序标识与用户验证调起方的关系。

在一些实施例中，接收模块 901 还可用于通过 SDK 获取 SDK 服务器发送的第四通知消息。第四通知消息由 SDK 服务器在目标用户验证调起方为 SDK 的情况下发送。

显示模块 902 还可用于响应于第四通知消息，调用 SDK 展示用户验证页面，以提示用户输入第二用户验证输入信息。

发送模块 903 还可用于通过 SDK 向 SDK 服务器反馈第二用户验证输入信息。

第二用户验证输入信息用于 SDK 服务器进行用户验证以得到用户验证结果信息。

在一些实施例中，接收模块 901 还可用于通过 SDK 接收 SDK 调用请求消息。

SDK 调用请求消息由商户系统响应于订单反馈消息生成。订单反馈消息和 SDK 调用请求消息包括订单标识。订单标识由 SDK 服务器响应于商户系统发送的订单请求消息生成。

发送模块 903 还可用于响应于 SDK 调用请求消息，通过 SDK 向 SDK 服务器发送第一订单查询消息。

接收模块 901 还可用于通过 SDK 接收 SDK 服务器响应于第一订单查询消息发送的第一查询反馈消息。

第一查询反馈消息包括与订单标识对应的订单信息。

在一些实施例中，订单请求消息包括指定付款方身份信息。

显示模块 902 还可用于响应于通过 SDK 接收的支付中止通知消息，通过 SDK 发出支付提示信息。

支付中止通知消息由 SDK 服务器在指定付款方身份信息与支付请求消息指示的支付的付款方身份信息不一致的情况下发送。

在一些实施例中，终端设备 900 还可包括扫描模块。

扫描模块可用于扫描付款码，得到第一码信息；

发送模块 903 还可用于通过 SDK 向 SDK 服务器发送第二订单查询消

息。

第二订单查询消息包括第一码信息。

接收模块 901 还可用于通过 SDK 接收 SDK 服务器发送的第二查询反馈消息。

第二查询反馈消息包括与第一码信息对应的订单信息。

在一些实施例中，发送模块 903 还可用于通过 SDK 向 SDK 服务器发送付款码申请消息。

接收模块 901 还可用于通过 SDK 接收 SDK 服务器发送的付款码反馈消息，付款码反馈消息包括付款码。

显示模块 902 还可用于显示付款码。

付款码用于被支付受理设备扫描以生成支付请求消息。

本申请第六方面提供一种宿主程序服务器。图 19 为第六方面提供的宿主程序服务器的一实施例的结构示意图。如图 19 所示，宿主程序服务器 1000 可包括接收模块 1001、验证模块 1002 和发送模块 1003。

接收模块 1001 可用于接收终端设备通过宿主程序反馈的第一用户验证输入信息。

终端设备具有软件开发工具包 SDK 和宿主程序。第一用户验证输入信息在 SDK 响应于第一通知消息通知宿主程序展示用户验证页面后得到。第一通知消息是 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的。安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应支付进行安全验证得到的。安全验证请求消息由 SDK 服务器响应于接收的支付请求消息发送。

验证模块 1002 可用于根据第一用户验证输入信息进行用户验证，得到用户验证结果信息。

发送模块 1003 可用于向终端设备中的宿主程序发送用户验证结果信息，通过宿主程序将用户验证结果信息传输给 SDK，以使 SDK 向 SDK 服务器发送用户验证结果信息，在用户验证结果信息表征用户验证通过的情况下，使 SDK 服务器发起付款请求，以完成支付。

在一些实施例中，发送模块 1003 还可用于向 SDK 服务器发送用户验

证结果信息，以使 SDK 服务器在用户验证结果信息表征用户验证通过且用户验证结果信息满足一致性验证条件的情况下，发起付款请求，以完成支付。

在一些示例中，一致性验证条件包括第一用户验证结果信息和第二用户验证结果信息一致。

第一用户验证结果信息为由宿主程序服务器通过宿主程序传输给 SDK 的用户验证结果信息。第二用户验证结果信息为从宿主程序服务器获取的用户验证结果信息。

在本申请实施例中，SDK 服务器响应于支付请求消息，向安全控制系统发送安全验证请求消息，以请求安全控制系统对本次支付进行安全验证，以完成 SDK 所属方所需的安全性方面的验证。在安全验证通过的情况下，SDK 服务器向终端设备的 SDK 发送用于指示 SDK 通知宿主程序展示用户验证页面的消息，以使 SDK 能够触发宿主程序主动发起用户验证。终端设备可接收用户输入的第一用户验证输入信息，并将第一用户验证输入信息向宿主程序服务器发送，宿主程序服务器可完成宿主程序所属方所需的用户身份安全性方面的验证。在支付过程中实现了 SDK 所属方和宿主程序所属方两个主体的双向验证，提高了支付的安全性，也满足了 SDK 所属方和宿主程序所属方两个主体对安全性管控的需求。

在一些示例中，宿主程序服务器存储有用于对宿主程序与 SDK 之间交互的信息进行加、解密的密钥。

在一些实施例中，接收模块 1001 还可用于接收 SDK 服务器在安全验证结果信息表征安全验证通过的情况下发送的用户验证方式请求消息。

用户验证方式请求消息包括支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上。

发送模块 1003 还可用于根据用户验证方式请求消息，向 SDK 服务器发送用户验证方式反馈消息。

用户验证方式反馈消息包括验证操作信息。

其中，在验证操作信息包括拒绝支付标识的情况下，SDK 服务器向 SDK 发送第二通知消息，第二通知消息用于指示 SDK 发出拒绝支付提示

信息。在验证操作信息包括免密支付标识的情况下，SDK 服务器向 SDK 发送第三通知消息，第三通知消息用于指示 SDK 发出免密支付提示信息。

在一些实施例中，第一通知消息由 SDK 服务器在验证操作信息包括用户验证方式标识的情况下发送。第一通知消息包括用户验证方式标识，用于指示 SDK 通知宿主程序展示与用户验证方式标识匹配的用户验证页面，以提示用户输入与用户验证方式标识匹配的第一用户验证输入信息。

在一些实施例中，安全验证结果信息包括目标宿主程序标识。目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识。

第一通知消息由 SDK 服务器在目标用户验证调起方为宿主程序的情况下发送。目标用户验证调起方为第一对应关系中与目标宿主程序标识匹配的用户验证调起方。目标宿主程序标识包括支付请求消息对应的支付的宿主程序标识。第一对应关系包括宿主程序标识与用户验证调起方的关系。

本申请第七方面提供了一种 SDK 服务器。图 20 为本申请第七方面提供的 SDK 服务器的一实施例的结构示意图。如图 20 所示，SDK 服务器 1100 包括存储器 1101、处理器 1102 及存储在存储器 1101 上并可在处理器 1102 上运行的计算机程序。

在一些示例中，上述处理器 1102 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit，ASIC），或者可以被配置成实施本申请实施例的一个或多个集成电路。

存储器 1101 可包括只读存储器（Read-Only Memory，ROM），随机存取存储器（Random Access Memory，RAM），磁盘存储介质设备，光存储介质设备，闪存设备，电气、光学或其他物理/有形的存储器存储设备。因此，通常，存储器包括一个或多个编码有包括计算机可执行指令的软件的有形（非暂态）计算机可读存储介质（例如，存储器设备），并且当该软件被执行（例如，由一个或多个处理器）时，其可操作来执行参考根据本申请第一方面实施例中的支付方法所描述的操作。

处理器 1102 通过读取存储器 1101 中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述第一方面的实施例中的支付方法。

在一些示例中，SDK 服务器 1100 还可包括通信接口 1103 和总线 1104。其中，如图 20 所示，存储器 1101、处理器 1102、通信接口 1103 通过总线 1104 连接并完成相互间的通信。

通信接口 1103，主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口 1103 接入输入设备和/或输出设备。

总线 1104 包括硬件、软件或两者，将 SDK 服务器 1100 的部件彼此耦接在一起。举例来说而非限制，总线 1104 可包括加速图形端口（Accelerated Graphics Port，AGP）或其他图形总线、增强工业标准架构（Enhanced Industry Standard Architecture，EISA）总线、前端总线（Front Side Bus，FSB）、超传输（HyperTransport，HT）互连、工业标准架构（Industry Standard Architecture，ISA）总线、无限带宽互连、低引脚数（Low pin count，LPC）总线、存储器总线、微信道架构（MicroChannel Architecture，MCA）总线、外围组件互连（Peripheral Component Interconnect，PCI）总线、PCI-Express（PCI-E）总线、串行高级技术附件（Serial Advanced Technology Attachment，SATA）总线、视频电子标准协会局部（Video Electronics Standards Association Local Bus，VLB）总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线 1104 可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线，但本申请考虑任何合适的总线或互连。

本申请第八方面提供了一种终端设备，终端设备可包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序。存储器和处理器的种类及关系可参见上述 SDK 服务器中存储器和处理器的相关说明。与上述 SDK 服务器的不同之处包括，当存储器中的软件被执行时，其可操作来执行参考根据本申请第二方面实施例中的支付方法所描述的操作；以及，处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序

代码对应的计算机程序，以用于实现上述第二方面的实施例中的支付方法。在一些示例中，终端设备还可包括通信接口和总线。存储器、处理器、通信接口可通过总线连接并完成相互间的通信，存储器、处理器、通信接口和总线之间的通信连接可参见图 20 所示的 SDK 服务器中的存储器、处理器、通信接口和总线之间的通信连接，在此不再赘述。

本申请第九方面提供了一种宿主程序服务器，宿主程序服务器可包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序。存储器和处理器的种类及关系可参见上述 SDK 服务器中存储器和处理器的相关说明。与上述 SDK 服务器的不同之处包括，当存储器中的软件被执行时，其可操作来执行参考根据本申请第三方面实施例中的支付方法所描述的操作；以及，处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述第三方面的实施例中的支付方法。在一些示例中，宿主程序服务器还可包括通信接口和总线。存储器、处理器、通信接口可通过总线连接并完成相互间的通信，存储器、处理器、通信接口和总线之间的通信连接可参见图 20 所示的 SDK 服务器中的存储器、处理器、通信接口和总线之间的通信连接，在此不再赘述。

本申请第十方面提供一种支付系统，该支付系统可包括上述实施例中的 SDK 服务器、终端设备和宿主程序服务器，SDK 服务器、终端设备和宿主程序服务器的具体内容可参见上述实施例中的相关说明，在此不再赘述。

本申请第十一方面还提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序指令，该计算机程序指令被处理器执行时可实现上述实施例中第一方面的支付方法、第二方面的支付方法和/或第三方面的支付方法，且能达到相同的技术效果，为避免重复，这里不再赘述。其中，上述计算机可读存储介质可包括非暂态计算机可读存储介质，如只读存储器（Read-Only Memory，简称 ROM）、随机存取存储器（Random Access Memory，简称 RAM）、磁碟或者光盘等，在此并不限定。

本申请实施例还可提供一种计算机程序产品，该计算机程序产品中的

指令可由 SDK 服务器、终端设备、宿主程序服务器的处理器执行时，使得 SDK 服务器、终端设备、宿主程序服务器执行上述第一方面的实施例中的支付方法、第二方面的实施例中的支付方法或第三方面的实施例中的支付方法。

需要明确的是，本说明书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或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。对于 SDK 服务器实施例、终端设备实施例、宿主程序服务器实施例、系统实施例、计算机可读存储介质实施例和计算机程序产品实施例而言，相关之处可以参见方法实施例的说明部分。本申请并不局限于上文所描述并在图中示出的特定步骤和结构。本领域的技术人员可以在领会本申请的精神之后，作出各种改变、修改和添加，或者改变步骤之间的顺序。并且，为了简明起见，这里省略对已知方法技术的详细描述。

上面参考根据本申请的实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本申请的各方面。应当理解，流程图和/或框图中的每个方框以及流程图和/或框图中各方框的组合可以由计算机程序指令实现。这些计算机程序指令可被提供给通用计算机、专用计算机、或其它可编程数据处理装置的处理器，以产生一种机器，使得经由计算机或其它可编程数据处理装置的处理器执行的这些指令使能对流程图和/或框图的一个或多个方框中指定的功能/动作的实现。这种处理器可以是但不限于是通用处理器、专用处理器、特殊应用处理器或者现场可编程逻辑电路。还可理解，框图和/或流程图中的每个方框以及框图和/或流程图中的方框的组合，也可以由执行指定的功能或动作的专用硬件来实现，或可由专用硬件和计算机指令的组合来实现。

本领域技术人员应能理解，上述实施例均是示例性而非限制性的。在不同实施例中出现的不同技术特征可以进行组合，以取得有益效果。本领域技术人员在研究附图、说明书及权利要求书的基础上，应能理解并实现所揭示的实施例的其他变化的实施例。在权利要求书中，术语“包括”并不排除其他装置或步骤；数量词“一个”不排除多个；术语“第一”、

“第二”用于标示名称而非用于表示任何特定的顺序。权利要求中的任何附图标记均不应被理解为对保护范围的限制。权利要求中出现的多个部分的功能可以由一个单独的硬件或软件模块来实现。某些技术特征出现在不同的从属权利要求中并不意味着不能将这些技术特征进行组合以取得有益效果。

权 利 要 求 书

1．一种支付方法，应用于软件开发工具包 SDK 服务器，所述方法包括：

响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息，所述安全验证请求消息包括安全验证信息，用于指示所述安全控制系统根据所述安全验证信息对所述支付请求消息对应的支付进行安全验证；

接收所述安全控制系统发送的安全验证结果信息；

在所述安全验证结果信息表征安全验证通过的情况下，向终端设备中的 SDK 发送第一通知消息，所述终端设备具有 SDK 和宿主程序，所述第一通知消息用于指示所述 SDK 通知所述宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息，所述第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息；

在所述用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

2．根据权利要求 1 所述的方法，在所述接收所述安全控制系统发送的安全验证结果信息之后，还包括：

在所述安全验证结果信息表征安全验证通过的情况下，向所述宿主程序服务器发送用户验证方式请求消息，所述用户验证方式请求消息包括所述支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上；

接收所述宿主程序服务器发送的用户验证方式反馈消息，所述用户验证方式反馈消息包括验证操作信息；

在所述验证操作信息包括拒绝支付标识的情况下，向所述 SDK 发送第二通知消息，所述第二通知消息用于指示所述 SDK 发出拒绝支付提示信息；

在所述验证操作信息包括免密支付标识的情况下，向所述 SDK 发送第三通知消息，所述第三通知消息用于指示所述 SDK 发出免密支付提示信息。

3．根据权利要求 2 所述的方法，其中，所述向终端设备中的 SDK 发送第一通知消息，包括：

在所述验证操作信息包括所述用户验证方式标识的情况下，向所述 SDK 发送所述第一通知消息，所述第一通知消息包括所述用户验证方式标识，用于指示所述 SDK 通知所述宿主程序展示与所述用户验证方式标识匹配的用户验证页面，以提示用户输入与所述用户验证方式标识匹配的所述第一用户验证输入信息。

4．根据权利要求 1 至 3 中任意一项所述的方法，其中，所述安全验证结果信息包括目标宿主程序标识，所述目标宿主程序标识包括所述支付请求消息对应的支付的宿主程序标识，

在所述向终端设备中的 SDK 发送第一通知消息之前，还包括：

根据所述目标宿主程序标识和预设的第一对应关系，确定与所述目标宿主程序标识对应的目标用户验证调起方，所述第一对应关系包括宿主程序标识与用户验证调起方的关系；

所述向终端设备中的 SDK 发送第一通知消息，包括：

在所述目标用户验证调起方为所述宿主程序的情况下，向所述 SDK 发送所述第一通知消息。

5．根据权利要求 4 所述的方法，在所述根据所述目标宿主程序标识和预设的第一对应关系，确定与所述目标宿主程序标识对应的目标用户验证调起方之后，还包括：

在所述目标用户验证调起方为所述 SDK 的情况下，向所述 SDK 发送第四通知消息，所述第四通知消息用于指示所述 SDK 展示用户验证页面，以提示用户输入第二用户验证输入信息，所述第二用户验证输入信息用于所述 SDK 服务器进行用户验证以得到用户验证结果信息。

6．根据权利要求 1 所述的方法，其中，所述发起付款请求，包括：

在所述用户验证结果信息满足一致性验证条件的情况下，发起所述付款请求。

7．根据权利要求 1 所述的方法，其中，所述一致性验证条件包括：

第一用户验证结果信息和第二用户验证结果信息一致，所述第一用户

验证结果信息为由所述宿主程序服务器通过所述宿主程序传输给所述 SDK 的所述用户验证结果信息，所述第二用户验证结果信息为从宿主程序服务器获取的所述用户验证结果信息。

8．根据权利要求 1 所述的方法，其中，所述 SDK 服务器存储有用于对所述 SDK 与所述宿主程序之间交互的信息进行加、解密的密钥。

9．根据权利要求 1 所述的方法，在所述响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息之前，还包括：

响应于商户系统发送的订单请求消息，生成订单标识；

向所述商户系统发送订单反馈消息，以使所述商户系统向所述 SDK 发送 SDK 调用请求消息，所述订单反馈消息和所述 SDK 调用请求消息包括所述订单标识；

响应于所述 SDK 发送的第一订单查询消息，向所述 SDK 发送第一查询反馈消息，所述第一查询反馈消息包括与所述订单标识对应的订单信息。

10．根据权利要求 9 所述的方法，其中，所述订单请求消息包括指定付款方身份信息，

所述方法还包括：

在所述指定付款方身份信息与所述支付请求消息指示的支付的付款方身份信息不一致的情况下，向所述 SDK 发送支付中止通知消息，以使所述 SDK 发出支付提示信息。

11．根据权利要求 1 所述的方法，在所述响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息之前，还包括：

接收所述终端设备的所述 SDK 发送的第二订单查询消息，所述第二订单查询消息包括所述终端设备扫描收款码得到的第一码信息；

向所述 SDK 发送第二查询反馈消息，所述第二查询反馈消息包括与所述第一码信息对应的订单信息。

12．根据权利要求 1 所述的方法，在所述响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息之前，还包括：

响应于接收的付款码申请消息，向所述 SDK 发送付款码反馈消息，

所述付款码申请消息由所述 SDK 发送，所述付款码反馈消息包括付款码；

所述支付请求消息由支付受理设备基于扫描的所述付款码生成。

13．一种支付方法，应用于终端设备，所述终端设备具有软件开发工具包 SDK 和宿主程序，所述方法包括：

通过所述 SDK 获取 SDK 服务器发送的第一通知消息，所述第一通知消息是所述 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的，所述安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应的支付进行安全验证得到的，所述安全验证请求消息由所述 SDK 服务器响应于接收的所述支付请求消息发送；

响应于所述第一通知消息，通过所述 SDK 通知所述宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息；

通过所述宿主程序向宿主程序服务器反馈第一用户验证输入信息，所述第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息；

通过所述 SDK 向所述 SDK 服务器发送通过宿主程序从所述宿主程序服务器获取的所述用户验证结果信息，使所述 SDK 服务器在所述用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

14．根据权利要求 13 所述的方法，还包括：

响应于所述 SDK 接收的第二通知消息，通过所述 SDK 发出拒绝提示信息，所述第二通知消息由所述 SDK 服务器在所述验证操作信息包括拒绝支付标识的情况下发送；

或者，

响应于所述 SDK 接收的第三通知消息，通过所述 SDK 发出免密支付提示信息，所述第三通知消息由所述 SDK 服务器在所述验证操作信息包括免密支付标识的情况下发送；

其中，用户验证方式反馈消息包括所述验证操作信息，所述用户验证方式反馈消息由所述宿主服务器响应于用户验证方式请求消息发送，所述用户验证方式请求消息由 SDK 服务器在所述安全验证结果信息表征安全

验证通过的情况下向所述宿主程序服务器发送，所述用户验证方式请求消息包括所述支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上。

15．根据权利要求 14 所述的方法，其中，所述第一通知消息由所述 SDK 服务器在所述验证操作信息包括所述用户验证方式标识的情况下发送，所述第一通知消息包括所述用户验证方式标识，用于指示所述 SDK 通知所述宿主程序展示与所述用户验证方式标识匹配的用户验证页面，以提示用户输入与所述用户验证方式标识匹配的所述第一用户验证输入信息。

16．根据权利要求 13 至 15 中任意一项所述的方法，其中，

所述安全验证结果信息包括目标宿主程序标识，所述目标宿主程序标识包括所述支付请求消息对应的支付的宿主程序标识，

所述第一通知消息由所述 SDK 服务器在目标用户验证调起方为所述宿主程序的情况下发送，所述目标用户验证调起方为第一对应关系中与目标宿主程序标识匹配的用户验证调起方，所述目标宿主程序标识包括所述支付请求消息对应的支付的宿主程序标识，所述第一对应关系包括宿主程序标识与用户验证调起方的关系。

17．根据权利要求 16 所述的方法，还包括：

通过所述 SDK 获取 SDK 服务器发送的第四通知消息，所述第四通知消息由所述 SDK 服务器在所述目标用户验证调起方为所述 SDK 的情况下发送；

响应于所述第四通知消息，调用所述 SDK 展示用户验证页面，以提示用户输入第二用户验证输入信息；

通过所述 SDK 向所述 SDK 服务器反馈所述第二用户验证输入信息，所述第二用户验证输入信息用于所述 SDK 服务器进行用户验证以得到用户验证结果信息。

18．根据权利要求 13 所述的方法，其中，所述用户验证结果信息还用于使所述 SDK 服务器在所述用户验证结果信息满足一致性验证条件的情况下，发起所述付款请求。

19．根据权利要求 18 所述的方法，其中，所述一致性验证条件包括：

所述第一用户验证结果信息和第二用户验证结果信息一致，所述第一用户验证结果信息为由所述宿主程序服务器通过所述宿主程序传输给所述 SDK 的所述用户验证结果信息，所述第二用户验证结果信息为从宿主程序服务器获取的所述用户验证结果信息。

20．根据权利要求 13 所述的方法，其中，所述 SDK 具有安全域，所述 SDK 中的信息存储于所述安全域；

所述 SDK 与所述宿主程序之间交互的信息为加密信息，所述 SDK 中加、解密的密钥存储于所述 SDK 服务器，所述宿主程序中加、解密的密钥存储于所述宿主程序服务器。

21．根据权利要求 13 所述的方法，在所述通过所述 SDK 获取 SDK 服务器发送的第一通知消息之前，还包括：

通过所述 SDK 接收 SDK 调用请求消息，所述 SDK 调用请求消息由商户系统响应于订单反馈消息生成，所述订单反馈消息和所述 SDK 调用请求消息包括订单标识，所述订单标识由所述 SDK 服务器响应于所述商户系统发送的订单请求消息生成；

响应于所述 SDK 调用请求消息，通过所述 SDK 向所述 SDK 服务器发送第一订单查询消息；

通过所述 SDK 接收所述 SDK 服务器响应于所述第一订单查询消息发送的第一查询反馈消息，所述第一查询反馈消息包括与所述订单标识对应的订单信息。

22．根据权利要求 21 所述的方法，其中，所述订单请求消息包括指定付款方身份信息，

所述方法还包括：

响应于通过所述 SDK 接收的支付中止通知消息，通过所述 SDK 发出支付提示信息，所述支付中止通知消息由所述 SDK 服务器在所述指定付款方身份信息与所述支付请求消息指示的支付的付款方身份信息不一致的情况下发送。

23．根据权利要求 13 所述的方法，在所述通过所述 SDK 获取 SDK 服务器发送的第一通知消息之前，还包括：

扫描付款码，得到第一码信息；

通过所述 SDK 向所述 SDK 服务器发送第二订单查询消息，所述第二订单查询消息包括所述第一码信息。

通过所述 SDK 接收所述 SDK 服务器发送的第二查询反馈消息，所述第二查询反馈消息包括与所述第一码信息对应的订单信息。

24．根据权利要求 13 所述的方法，在所述通过所述 SDK 获取 SDK 服务器发送的第一通知消息之前，还包括：

通过所述 SDK 向所述 SDK 服务器发送付款码申请消息；

通过所述 SDK 接收所述 SDK 服务器发送的付款码反馈消息，所述付款码反馈消息包括付款码；

显示所述付款码，所述付款码用于被支付受理设备扫描以生成所述支付请求消息。

25．一种支付方法，应用于宿主程序服务器，所述方法包括：

接收终端设备通过宿主程序反馈的第一用户验证输入信息，所述终端设备具有软件开发工具包 SDK 和所述宿主程序，所述第一用户验证输入信息在所述 SDK 响应于第一通知消息通知所述宿主程序展示用户验证页面后得到，所述第一通知消息是所述 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的，所述安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应支付进行安全验证得到的，所述安全验证请求消息由所述 SDK 服务器响应于接收的所述支付请求消息发送；

根据所述第一用户验证输入信息进行用户验证，得到用户验证结果信息；

向所述终端设备中的所述宿主程序发送所述用户验证结果信息，通过所述宿主程序将所述用户验证结果信息传输给所述 SDK，以使所述 SDK 向所述 SDK 服务器发送所述用户验证结果信息，在所述用户验证结果信息表征用户验证通过的情况下，使 SDK 服务器发起付款请求，以完成支

付。

26．根据权利要求 25 所述的方法，在所述接收终端设备通过宿主程序反馈的第一用户验证输入信息之前，还包括：

接收所述 SDK 服务器在所述安全验证结果信息表征安全验证通过的情况下发送的用户验证方式请求消息，所述用户验证方式请求消息包括所述支付请求消息指示的支付对应的订单信息、终端设备信息、支付信息中的一项或两项以上；

根据所述用户验证方式请求消息，向所述 SDK 服务器发送用户验证方式反馈消息，所述用户验证方式反馈消息包括验证操作信息；

其中，在所述验证操作信息包括拒绝支付标识的情况下，所述 SDK 服务器向所述 SDK 发送第二通知消息，所述第二通知消息用于指示所述 SDK 发出拒绝支付提示信息；在所述验证操作信息包括免密支付标识的情况下，所述 SDK 服务器向所述 SDK 发送第三通知消息，所述第三通知消息用于指示所述 SDK 发出免密支付提示信息。

27．根据权利要求 26 所述的方法，其中，所述第一通知消息由所述 SDK 服务器在所述验证操作信息包括所述用户验证方式标识的情况下发送，所述第一通知消息包括所述用户验证方式标识，用于指示所述 SDK 通知所述宿主程序展示与所述用户验证方式标识匹配的用户验证页面，以提示用户输入与所述用户验证方式标识匹配的所述第一用户验证输入信息。

28．根据权利要求 25 至 27 中任意一项所述的方法，其中，

所述安全验证结果信息包括目标宿主程序标识，所述目标宿主程序标识包括所述支付请求消息对应的支付的宿主程序标识，

所述第一通知消息由所述 SDK 服务器在目标用户验证调起方为所述宿主程序的情况下发送，所述目标用户验证调起方为第一对应关系中与目标宿主程序标识匹配的用户验证调起方，所述目标宿主程序标识包括所述支付请求消息对应的支付的宿主程序标识，所述第一对应关系包括宿主程序标识与用户验证调起方的关系。

29．根据权利要求 25 所述的方法，还包括：

向所述 SDK 服务器发送所述用户验证结果信息，以使所述 SDK 服务器在所述用户验证结果信息表征用户验证通过且所述用户验证结果信息满足一致性验证条件的情况下，发起付款请求，以完成支付。

30．根据权利要求 29 所述的方法，其中，所述一致性验证条件包括：

第一用户验证结果信息和第二用户验证结果信息一致，所述第一用户验证结果信息为由所述宿主程序服务器通过所述宿主程序传输给所述 SDK 的所述用户验证结果信息，所述第二用户验证结果信息为从宿主程序服务器获取的所述用户验证结果信息。

31．根据权利要求 25 所述的方法，其中，所述宿主程序服务器存储有用于对所述宿主程序与所述 SDK 之间交互的信息进行加、解密的密钥。

32．一种软件开发工具包 SDK 服务器，包括：

发送模块，用于响应于接收的支付请求消息，向安全控制系统发送安全验证请求消息，所述安全验证请求消息包括安全验证信息，用于指示所述安全控制系统根据所述安全验证信息对所述支付请求消息对应的支付进行安全验证；

接收模块，用于接收所述安全控制系统发送的安全验证结果信息；

所述发送模块还用于在所述安全验证结果信息表征安全验证通过的情况下，向终端设备中的 SDK 发送第一通知消息，所述终端设备具有 SDK 和宿主程序，所述第一通知消息用于指示所述 SDK 通知所述宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息，所述第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息；

所述发送模块还用于在所述用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

33．一种终端设备，所述终端设备具有软件开发工具包 SDK 和宿主程序，所述终端设备包括：

接收模块，用于通过所述 SDK 获取 SDK 服务器发送的第一通知消

息，所述第一通知消息是所述 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的，所述安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应的支付进行安全验证得到的，所述安全验证请求消息由所述 SDK 服务器响应于接收的所述支付请求消息发送；

显示模块，用于响应于所述第一通知消息，通过所述 SDK 通知所述宿主程序展示用户验证页面，以提示用户输入第一用户验证输入信息；

发送模块，用于通过所述宿主程序向宿主程序服务器反馈第一用户验证输入信息，所述第一用户验证输入信息用于宿主程序服务器进行用户验证以得到用户验证结果信息；

所述发送模块还用于通过所述 SDK 向所述 SDK 服务器发送通过宿主程序从所述宿主程序服务器获取的所述用户验证结果信息，使所述 SDK 服务器在所述用户验证结果信息表征用户验证通过的情况下，发起付款请求，以完成支付。

34．一种宿主程序服务器，包括：

接收模块，用于接收终端设备通过宿主程序反馈的第一用户验证输入信息，所述终端设备具有软件开发工具包 SDK 和所述宿主程序，所述第一用户验证输入信息在所述 SDK 响应于第一通知消息通知所述宿主程序展示用户验证页面后得到，所述第一通知消息是所述 SDK 服务器基于表征安全验证通过的安全验证结果信息发送的，所述安全验证结果信息是安全控制系统基于安全验证请求消息中的安全验证信息对支付请求消息对应支付进行安全验证得到的，所述安全验证请求消息由所述 SDK 服务器响应于接收的所述支付请求消息发送；

验证模块，用于根据所述第一用户验证输入信息进行用户验证，得到用户验证结果信息；

发送模块，用于向所述终端设备中的所述宿主程序发送所述用户验证结果信息，通过所述宿主程序将所述用户验证结果信息传输给所述 SDK，以使所述 SDK 向所述 SDK 服务器发送所述用户验证结果信息，在所述用户验证结果信息表征用户验证通过的情况下，使 SDK 服务器发起付款请

求，以完成支付。

35．一种软件开发工具包 SDK 服务器，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 1 至 12 中任意一项所述的支付方法。

36．一种终端设备，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 13 至 24 中任意一项所述的支付方法。

37．一种宿主程序服务器，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 25 至 31 中任意一项所述的支付方法。

38．一种支付系统，包括如权利要求 35 所述的软件开发工具包 SDK 服务器、如权利要求 36 所述的终端设备和如权利要求 37 所述的宿主程序服务器。

39．一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现如权利要求 1 至 31 中任意一项所述的支付方法。