(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103164792 B
(45)授权公告日 2016.02.10

(21)申请号 201110418302.7
(22)申请日 2011.12.14
(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼岛资本大厦一座四层 847 号邮箱
(72)发明人 诸寅嘉 吕雪峰 印浩奇
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 郭润湘
(51)Int.Cl.
G06F 17/00(2006.01)
G06Q 20/32(2012.01)
(56)对比文件
CN 101576989 A,2009.11.11, 说明书第 4 页第 4 段至第 7 页第 7 段 .
US 2007/0027775 A1,2007.02.01, 全文 .
CN 1941009 A,2007.04.04, 全文 .
CN 101414375 A,2009.04.22, 全文 .
审查员 李腾

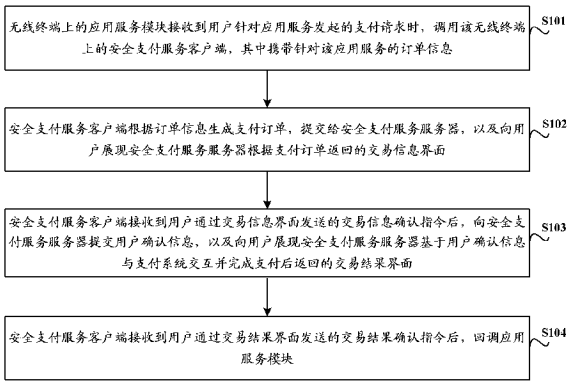
权利要求书2页 说明书9页 附图5页

(54)发明名称

无线终端上的支付服务提供方法及相关设备和系统

(57)摘要

本申请公开了一种无线终端上的支付服务提供方法及相关设备和系统，用以在无线终端上实现应用与支付的平滑切换。无线终端上的支付服务提供方法，包括：无线终端上的应用服务模块接收到支付请求时，调用安全支付服务客户端；安全支付服务客户端生成支付订单提交给安全支付服务服务器，以及向用户展现交易信息界面，接收到用户发送的交易信息确认指令后，向安全支付服务服务器提交用户确认信息，以及向用户展现交易结果界面；安全支付服务客户端接收到用户发送的交易结果确认指令后，回调应用服务模块。



CN 103164792 B

1. 一种无线终端上的支付服务提供方法，其特征在于，包括：

无线终端上的应用服务模块接收到用户针对应用服务发起的支付请求时，调用所述无线终端上的安全支付服务客户端，其中携带针对所述应用服务的订单信息；

所述安全支付服务客户端根据所述订单信息生成携带无线终端的授权码及硬件信息的支付订单，提交给安全支付服务服务器，以及向用户展现所述安全支付服务服务器根据支付订单返回的交易信息界面；所述交易信息界面为所述安全支付服务服务器根据保存的授权码与硬件信息的绑定关系，对支付订单中携带的无线终端的授权码以及硬件信息进行安全认证，并确认安全认证通过后返回给所述安全支付服务客户端的；

所述安全支付服务客户端接收到用户通过交易信息界面发送的交易信息确认指令后，向所述安全支付服务服务器提交用户确认信息，以及向用户展现所述安全支付服务服务器基于用户确认信息与支付系统交互并完成支付后返回的交易结果界面；

所述安全支付服务客户端接收到用户通过交易结果界面发送的交易结果确认指令后，回调所述应用服务模块。

2. 如权利要求 1 所述的方法，其特征在于，还包括：

所述安全支付服务客户端被首次调用时，在生成支付订单之前，向所述安全支付服务服务器获取短信发送信息；

根据获取到的短信发送信息，调用所述无线终端上的短信模块，通过运营商短信通道向所述安全支付服务服务器发送相应短信，并向所述安全支付服务服务器获取与所述短信的发送方号码绑定的账户信息展现给用户；

所述安全支付服务客户端接收到用户发送的账户信息确认指令后，向所述安全支付服务服务器提交账户确认信息，其中携带无线终端的硬件信息，以及接收并存储所述安全支付服务服务器为所述无线终端生成的授权码；

所述安全支付服务服务器保存所述账户信息、为所述无线终端生成的授权码、以及所述安全支付服务客户端上报的无线终端的硬件信息之间的绑定关系。

3. 如权利要求 1 所述的方法，其特征在于，所述安全支付服务服务器基于用户确认信息与支付系统交互并完成支付的流程，具体包括：

所述安全支付服务服务器接收到用户确认信息之后，将交易信息提交给支付系统；以及

接收所述支付系统确认本次交易并完成计费之后返回的交易结果，并通知所述应用服务模块对应的网络服务器本次交易结果。

4. 一种无线终端，其特征在于，包括应用服务模块和安全支付服务客户端，其中：

所述应用服务模块，用于接收到用户针对应用服务发起的支付请求时，调用所述安全支付服务客户端，其中携带针对所述应用服务的订单信息；

所述安全支付服务客户端，用于根据所述订单信息生成携带所述无线终端的授权码及硬件信息的支付订单，提交给安全支付服务服务器，以及向用户展现所述安全支付服务服务器根据支付订单返回的交易信息界面，所述交易信息界面为所述安全支付服务服务器根据保存的授权码与硬件信息的绑定关系，对支付订单中携带的无线终端的授权码以及硬件信息进行安全认证，并确认安全认证通过后返回给所述安全支付服务客户端的；接收到用户通过交易信息界面发送的交易信息确认指令后，向所述安全支付服务服务器提交用户确

认信息，以及向用户展现所述安全支付服务服务器基于用户确认信息与支付系统交互并完成支付后返回的交易结果界面；接收到用户通过交易结果界面发送的交易结果确认指令后，回调所述应用服务模块。

5. 如权利要求 4 所述的无线终端，其特征在于，

所述安全支付服务客户端，还用于被首次调用时，在生成支付订单之前，向所述安全支付服务服务器获取短信发送信息；根据获取到的短信发送信息，调用所述无线终端上的短信模块，通过运营商短信通道向所述安全支付服务服务器发送相应短信，并向所述安全支付服务服务器获取与所述短信的发送方号码绑定的账户信息展现给用户；接收到用户发送的账户信息确认指令后，向所述安全支付服务客户端提交账户确认信息，其中携带无线终端的硬件信息，以及接收并存储所述安全支付服务服务器为所述无线终端生成的授权码。

6. 如权利要求 4 所述的无线终端，其特征在于，所述应用服务模块为应用客户端或第三方浏览器。

7. 一种无线终端上的支付服务提供系统，其特征在于，包括无线终端、安全支付服务服务器和支付系统，所述无线终端包括应用服务模块和安全支付服务客户端，其中：

所述应用服务模块，用于接收到用户针对应用服务发起的支付请求时，调用所述安全支付服务客户端，其中携带针对所述应用服务的订单信息；

所述安全支付服务客户端，用于根据所述订单信息生成携带所述无线终端的授权码及硬件信息的支付订单，提交给所述安全支付服务服务器，以及向用户展现所述安全支付服务服务器返回的交易信息界面；接收到用户通过交易信息界面发送的交易信息确认指令后，向所述安全支付服务服务器提交用户确认信息，以及向用户展现所述安全支付服务服务器返回的交易结果界面；接收到用户通过交易结果界面发送的交易结果确认指令后，回调所述应用服务模块；

所述安全支付服务服务器，用于根据保存的授权码与硬件信息的绑定关系，对支付订单中携带的无线终端的授权码以及硬件信息进行安全认证，并确认安全认证通过后，向所述安全支付服务客户端返回所述交易信息界面，以及基于接收到的用户确认信息与所述支付系统交互并完成支付后向所述安全支付服务客户端返回所述交易结果界面。

8. 如权利要求 7 所述的系统，其特征在于，

所述安全支付服务客户端，还用于被首次调用时，在生成支付订单之前，向所述安全支付服务服务器获取短信发送信息；根据获取到的短信发送信息，调用所述无线终端上的短信模块，通过运营商短信通道向所述安全支付服务服务器发送相应短信，并向所述安全支付服务服务器获取与所述短信的发送方号码绑定的账户信息；接收到用户发送的账户信息确认指令后，向所述安全支付服务服务器提交账户确认信息，其中携带无线终端的硬件信息，以及接收并存储所述安全支付服务服务器为所述无线终端生成的授权码；

所述安全支付服务服务器，还用于在接收到所述安全支付服务客户端提交的账户确认信息之后，为所述无线终端生成授权码并发送给所述安全支付服务客户端，并保存所述账户信息、为所述无线终端生成的授权码、以及所述安全支付服务客户端上报的无线终端的硬件信息之间的绑定关系。

无线终端上的支付服务提供方法及相关设备和系统

技术领域

[0001] 本申请涉及无线通信技术领域，尤其涉及一种无线终端上的支付服务提供方法及相关设备和系统。

背景技术

[0002] 随着互联网技术的发展，各种应用服务例如电子图书订阅服务、在线翻译服务等被用户广泛接受并使用，用户一般通过应用使用提供商提供的应用服务。目前的支付领域，针对提供商为用户提供的应用服务，能够为用户提供运营商话费支付、银行支付、第三方WAP(Wireless Application Protocol，无线应用协议）支付等多种支付方式。运营商话费支付是指用户通过发送短信、或者进入运营商的WAP网站完成的支付，消耗用户的手机话费余额。银行支付是指用户通过进入银行的WAP网站填写银行卡相关信息完成的支付。第三方WAP支付是指用户通过进入第三方支付机构的WAP网站填写账户相关信息完成的支付。其中：

[0003] 运营商话费支付的缺点在于，仅提供短信、或WAP计费通道，交易信息只能由应用在应用内通过交互流程实现，无法避免提供商对显示的商品及金额信息进行篡改；同时，由于运营商话费的虚拟性，在费率、结算等环节需要消耗较多的服务器资源。

[0004] 银行支付的缺点在于，只能使用WAP浏览器进行付费，这就要求应用必须中断当前用户操作，调用WAP浏览器使用户与银行页面进行交互，在很多单进程手机上造成了用户无法返回应用继续支付流程的问题。

[0005] 第三方WAP支付同样存在着用户操作中断的弊端，同时也缺少快速、安全的支付机制。

[0006] 可见，现有支付领域为用户提供的支付方式，无法实现应用与支付的平滑切换，并且支付的安全性也无法得到保障。

发明内容

[0007] 本申请实施例提供一种无线终端上的支付服务提供方法及相关设备和系统，用以在无线终端上实现应用与支付的平滑切换。

[0008] 本申请实施例提供一种无线终端上的支付服务提供方法，包括：

[0009] 无线终端上的应用服务模块接收到用户针对应用服务发起的支付请求时，调用所述无线终端上的安全支付服务客户端，其中携带针对所述应用服务的订单信息；

[0010] 所述安全支付服务客户端根据所述订单信息生成支付订单，提交给安全支付服务服务器，以及向用户展现所述安全支付服务服务器根据支付订单返回的交易信息界面；

[0011] 所述安全支付服务客户端接收到用户通过交易信息界面发送的交易信息确认指令后，向所述安全支付服务服务器提交用户确认信息，以及向用户展现所述安全支付服务服务器基于用户确认信息与支付系统交互并完成支付后返回的交易结果界面；

[0012] 所述安全支付服务客户端接收到用户通过交易结果界面发送的交易结果确认指

令后，回调所述应用服务模块。

[0013] 本申请实施例提供一种无线终端，包括应用服务模块和安全支付服务客户端，其中：

[0014] 所述应用服务模块，用于接收到用户针对应用服务发起的支付请求时，调用所述安全支付服务客户端，其中携带针对所述应用服务的订单信息；

[0015] 所述安全支付服务客户端，用于根据所述订单信息生成支付订单，提交给安全支付服务服务器，以及向用户展现所述安全支付服务服务器根据支付订单返回的交易信息界面；接收到用户通过交易信息界面发送的交易信息确认指令后，向所述安全支付服务服务器提交用户确认信息，以及向用户展现所述安全支付服务服务器基于用户确认信息与支付系统交互并完成支付后返回的交易结果界面；接收到用户通过交易结果界面发送的交易结果确认指令后，回调所述应用服务模块。

[0016] 本申请实施例提供一种无线终端上的支付服务提供系统，包括无线终端、安全支付服务服务器和支付系统，所述无线终端包括应用服务模块和安全支付服务客户端，其中：

[0017] 所述应用服务模块，用于接收到用户针对应用服务发起的支付请求时，调用所述安全支付服务客户端，其中携带针对所述应用服务的订单信息；

[0018] 所述安全支付服务客户端，用于根据所述订单信息生成支付订单，提交给所述安全支付服务服务器，以及向用户展现所述安全支付服务服务器返回的交易信息界面；接收到用户通过交易信息界面发送的交易信息确认指令后，向所述安全支付服务服务器提交用户确认信息，以及向用户展现所述安全支付服务服务器返回的交易结果界面；接收到用户通过交易结果界面发送的交易结果确认指令后，回调所述应用服务模块；

[0019] 所述安全支付服务服务器，用于根据接收到的支付订单向所述安全支付服务客户端返回所述交易信息界面，以及基于接收到的用户确认信息与所述支付系统交互并完成支付后向所述安全支付服务客户端返回所述交易结果界面。

[0020] 本申请实施例提供的无线终端上的支付服务提供方法及相关设备和系统，为应用服务提供安全支付服务，在无线终端上设置应用服务模块和安全支付服务客户端，由支付请求触发安全支付服务客户端的调用，进入交易信息界面，支付完成之后安全支付服务客户端能够回调应用服务模块，继续应用流程，从而在无线终端上实现了应用与支付的平滑切换，无需跳出应用，不会中断应用既有的流程。

[0021] 本申请的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请而了解。本申请的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0022] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0023] 图 1 为本申请实施例中无线终端上的支付服务提供方法流程图；

[0024] 图 2 为本申请实施例中用户账户与无线终端的绑定流程流程图；

[0025] 图 3 为本申请实施例中用户通过应用使用提供商提供的应用服务时，无线终端上

的支付服务提供方法流程图；

[0026] 图 4 为本申请实施例中用户通过第三方浏览器访问提供商提供应用服务的网站时，无线终端上的支付服务提供方法流程图；

[0027] 图 5 为本申请实施例中无线终端上的支付服务提供系统框图。

具体实施方式

[0028] 本申请实施例提供一种无线终端上的支付服务提供方法及相关设备和设备，能够在无线终端上实现应用与支付的平滑切换；进一步，能够有效防止交易信息的篡改和用户账户的盗用，保障支付的安全性。

[0029] 以下结合说明书附图对本申请的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本申请，并不用于限定本申请，并且在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0030] 首先澄清一个基本概念。本申请实施例中，所述的无线终端是指区别于传统的 PC(Personal Computer，个人电脑）、LapTop（笔记本电脑）等，用户可以随身携带且能够通过 WLAN(Wireless Local Area Network，无线局域网）、GPRS(General Packet Radio Service，通用分组无线业务）、3G（第三代移动通信系统）等无线方式接入互联网的终端设备。本申请实施例中，所述的无线终端包括但不限于手机、Netbook（上网本）等，无线终端一般具有语音采集、语音和数据传输等功能。

[0031] 本申请实施例的应用场景为：针对提供商为用户提供的应用服务，在无线终端上提供相应的安全支付服务，安全支付服务涉及的网络实体包括无线终端上的安全支付服务客户端和网络侧的安全支付服务服务器。用户一般通过应用使用提供商提供的应用服务，具体实施中，用户可以通过应用客户端使用提供商提供的应用服务，用户也可以通过第三方浏览器访问提供商提供应用服务的网站。如果用户通过应用客户端使用提供商提供的应用服务，相应的无线终端上需要设置应用客户端，网络侧需要设置应用客户端对应的应用服务器；如果用户通过第三方浏览器访问提供商提供应用服务的网站，相应的无线终端上需要设置第三方浏览器，网络侧需要设置第三方浏览器访问的网站服务器。本申请实施例中，将无线终端上的应用客户端或第三方浏览器统称为应用服务模块，将应用客户端对应的应用服务器或第三方浏览器访问的网站服务器统称为网络服务器。

[0032] 如图 1 所示，本申请实施例提供一种无线终端上的支付服务提供方法，包括如下步骤：

[0033] S101、无线终端上的应用服务模块接收到用户针对应用服务发起的支付请求时，调用该无线终端上的安全支付服务客户端，其中携带针对该应用服务的订单信息；

[0034] S102、安全支付服务客户端根据订单信息生成支付订单，提交给安全支付服务服务器，以及向用户展现安全支付服务服务器根据支付订单返回的交易信息界面；

[0035] S103、安全支付服务客户端接收到用户通过交易信息界面发送的交易信息确认指令后，向安全支付服务服务器提交用户确认信息，以及向用户展现安全支付服务服务器基于用户确认信息与支付系统交互并完成支付后返回的交易结果界面；

[0036] S104、安全支付服务客户端接收到用户通过交易结果界面发送的交易结果确认指令后，回调应用服务模块。

[0037] 在S103的具体实施中，所述的安全支付服务服务器基于用户确认信息与支付系统交互并完成支付的流程，具体包括：

[0038] 安全支付服务服务器接收到用户确认信息之后，将交易信息提交给支付系统；以及

[0039] 接收支付系统确认本次交易并完成计费之后返回的交易结果，并通知网络服务器本次交易结果。

[0040] 具体实施中，为了保障安全支付服务的安全性，采用在用户首次使用安全支付服务时，将用户账户与无线终端绑定的安全机制，具体的：

[0041] 在用户首次使用安全支付服务时，通过短信通道和账户名/密码双重认证方式确定用户的账户信息；

[0042] 在首次确定用户的账户信息之后，为用户使用的无线终端分配授权码，并将用户的账户信息、为无线终端分配的授权码、以及无线终端的硬件信息绑定，以便后续用户使用时以授权码为依据校验硬件信息，确保对用户账户进行操作的为用户本人，防止用户账户被盗用而造成财产损失；需要说明的是，如果用户使用的无线终端发生硬件变化，则需要重新绑定。

[0043] 在S101的具体实施中，安全支付服务客户端被首次调用时，在生成支付订单之前，向安全支付服务服务器获取短信发送信息；根据获取到的短信发送信息，调用无线终端上的短信模块，通过运营商短信通道向安全支付服务服务器发送相应短信，并向安全支付服务服务器获取与该短信的发送方号码绑定的账户信息展现给用户；安全支付服务客户端接收到用户发送的账户信息确认指令后，向安全支付服务服务器提交账户确认信息，其中携带无线终端的硬件信息，以及接收并存储安全支付服务服务器为无线终端生成的授权码；相应的，

[0044] 安全支付服务服务器保存账户信息、为无线终端生成的授权码、以及安全支付服务客户端上报的无线终端的硬件信息之间的绑定关系。

[0045] 基于用户账户与无线终端绑定的安全机制，在S102的具体实施中，安全支付服务客户端在提交给安全支付服务服务器的支付订单中携带无线终端的授权码以及硬件信息；以及安全支付服务服务器根据支付订单返回交易信息界面之前，根据保存的授权码与硬件信息的绑定关系，对支付订单中携带的无线终端的授权码以及硬件信息进行安全认证，并确认安全认证通过。

[0046] 下面，对本申请实施例提供的无线终端上的支付服务提供方法进行详细说明。

[0047] 首先介绍用户账户与无线终端的绑定流程，该绑定流程在用户首次使用安全支付服务时执行。无线终端上的应用服务模块接收到用户针对应用服务发起的支付请求时，调用安全支付服务客户端，如果安全支付服务客户端被首次调用，则在生成支付订单之前，执行如下绑定流程，如图2所示，包括：

[0048] S201、安全支付服务客户端向安全支付服务服务器发送短信发送信息获取请求，请求安全支付服务服务器提供短信的接收方号码、以及需要发送的短信内容等；

[0049] S202、安全支付服务服务器向安全支付服务客户端返回短信发送信息，向安全支付服务客户端提供短信的接收方号码、以及需要发送的短信内容等；

[0050] S203、安全支付服务客户端根据获取到的短信发送信息，调用无线终端上的短信

模块，通过运营商短信通道向安全支付服务服务器发送相应短信，即该短信的接收方号码为短信发送信息指定的接收方号码，该短信的内容为短信发送信息指定的短信内容；

[0051] S204、安全支付服务服务器根据从运营商短信通道接收到的短信，能够提取到该短信的发送方号码，即无线终端的 MSISDN（移动台国际 ISDN 号码，俗称手机号）；如果用户已经申请了用于支付应用服务的账户，则直接根据 MSISDN 获取与该 MSISDN 绑定的账户信息，如果用户未申请用于支付应用服务的账户，则先创建与 MSISDN 绑定的账户，再获取账户信息；

[0052] 所述的账户信息包括账户名、与该账户绑定的 MSISDN、该账户对应的支付系统、是否需要用户名 / 密码认证等；

[0053] S205、安全支付服务客户端向安全支付服务服务器发送账户信息获取请求；

[0054] S206、安全支付服务服务器向安全支付服务客户端返回账户信息；

[0055] 需要说明的是，为了确保接收到安全支付服务服务器返回的账户信息，安全支付服务客户端通过运营商短信通道向安全支付服务服务器发送相应短信之后，在一定时间长度（例如 3 分钟之内）内会每隔设定时间段（例如 10 秒）向安全支付服务服务器发送账户信息获取请求，直至接收到安全支付服务服务器返回的账户信息；

[0056] S207 ～ S208、安全支付服务客户端会将账户信息展现给用户，以便用户确认，安全支付服务客户端接收到用户发送的账户信息确认指令后，向安全支付服务服务器提交账户确认信息，其中携带无线终端的硬件信息；

[0057] 用户会对安全支付服务客户端展现的账户信息进行核实，如果是用户希望用于支付应用服务的账户，则会向安全支付服务客户端发送账户信息确认指令；

[0058] 无线终端的硬件信息包括但不限于无线终端的 IMEI(International Mobile Equipment Identity，国际移动设备识别码）、IMSI(International Mobile Subscriber Identity，国际移动用户识别码）等。

[0059] S209、安全支付服务服务器接收到安全支付服务客户端提交的账户确认信息之后，指示安全支付服务客户端继续支付流程，即生成支付订单等后续流程；

[0060] 需要说明的是，如果该账户需要账户名 / 密码认证，则账户信息确认指令中会携带用户输入的密码，在这种情况下，安全支付服务客户端向安全支付服务服务器提交的账户确认信息中，同时携带用户输入的密码，安全支付服务服务器需要对账户名 / 密码认证通过后，指示安全支付服务客户端继续支付流程；

[0061] S210、安全支付服务服务器为用户使用的无线终端生成授权码，并保存账户信息、为无线终端生成的授权码、以及安全支付服务客户端上报的无线终端的硬件信息之间的绑定关系；授权码一般为安全支付服务服务器随机生成的字符串信息，无线终端的授权码具有唯一性。

[0062] S211、安全支付服务服务器将生成的授权码发送给安全支付服务客户端；

[0063] S212、安全支付服务客户端存储账户初始化信息，其中包括安全支付服务服务器为无线终端生成的授权码，以便后续使用。

[0064] 下面介绍用户通过应用客户端使用提供商提供的应用服务时，无线终端上的支付服务提供方法，涉及的网络实体包括应用客户端、安全支付服务客户端、安全支付服务服务器、支付系统和应用服务器。应用客户端和安全支付服务客户端设置在用户使用的无线终

端上。需要说明的是，此处介绍的无线终端上的支付服务提供流程，是用户非首次使用安全支付服务的一般流程，如图 3 所示，包括：

[0065] S301、用户针对提供商提供的应用服务，向应用客户端发起支付请求；

[0066] S302、应用客户端根据用户发起的支付请求，调用安全支付服务客户端，其中携带订单信息，订单信息一般包括订购商品的数量、及其他相关信息；

[0067] 具体实施中，是应用客户端根据用户发起的支付请求，通过安全支付服务对外公布的 API(API(Application Programming Interface，应用程序编程接口)，向安全支付服务客户端发送调用请求，调用请求中携带订单信息；

[0068] S303、安全支付服务客户端根据订单信息生成支付订单，提交给安全支付服务服务器，其中携带无线终端的授权码以及硬件信息，支付订单一般包括需要支付商品的单价、需要支付的总金额等；

[0069] S304、安全支付服务服务器根据保存的授权码与硬件信息的绑定关系，对支付订单中携带的无线终端的授权码以及硬件信息进行安全认证；

[0070] S305 ～ S306、如果安全认证通过，安全支付服务服务器将交易信息界面发送到安全支付服务客户端上进行展现，交易信息一般包括交易金额、用于支付的账户等；

[0071] 如果安全认证不通过，则该支付服务提供流程直接结束；

[0072] S307 ～ S308、如果安全支付服务客户端接收到用户通过交易信息界面发送的交易信息确认指令，向安全支付服务服务器提交用户确认信息；

[0073] S309、安全支付服务服务器接收到用户确认信息之后，将交易信息提交给支付系统，支付系统可以为银行系统、银联系统、财富通、支付宝等；

[0074] 需要说明的是，如果该账户需要账户名 / 密码认证，则交易信息确认指令中会携带用户输入的密码，在这种情况下，安全支付服务客户端向安全支付服务服务器提交的用户确认信息中，同时携带用户输入的密码，安全支付服务服务器需要对账户名 / 密码认证通过后，将交易信息提交给支付系统；

[0075] S310 ～ S311、支付系统确认本次交易并完成计费之后，向安全支付服务服务器返回交易结果；

[0076] S312 ～ S314、安全支付服务服务器通知应用服务器本次交易结果，并将交易结果界面发送到安全支付服务客户端上进行展现；

[0077] S315 ～ S316、如果安全支付服务客户端接收到用户通过交易结果界面发送的交易结果确认指令，回调应用客户端；

[0078] 具体实施中，是安全支付服务客户端通过 API 向应用客户端返回调用响应，实现对应用客户端的回调；

[0079] S317、应用客户端继续应用流程。

[0080] 下面介绍用户通过第三方浏览器访问提供商提供应用服务的网站时，无线终端上的支付服务提供方法，涉及的网络实体包括第三方浏览器、安全支付服务客户端、安全支付服务服务器、支付系统和网站服务器。第三方浏览器和安全支付服务客户端设置在用户使用的无线终端上。需要说明的是，此处介绍的无线终端上的支付服务提供流程，是用户非首次使用安全支付服务的一般流程，如图 4 所示，包括：

[0081] S401、用户针对提供商提供的应用服务，向第三方浏览器发起支付请求；

[0082] S402、第三方浏览器根据用户发起的支付请求，调用安全支付服务客户端，其中携带订单信息；

[0083] 具体实施中，是第三方浏览器根据用户发起的支付请求，通过安全支付服务对外公布的 API(API(Application Programming Interface，应用程序编程接口)，向安全支付服务客户端发送调用请求，调用请求中携带订单信息；

[0084] S403、安全支付服务客户端根据订单信息生成支付订单，提交给安全支付服务服务器，其中携带无线终端的授权码以及硬件信息；

[0085] S404、安全支付服务服务器根据保存的授权码与硬件信息的绑定关系，对支付订单中携带的无线终端的授权码以及硬件信息进行安全认证；

[0086] S405 ～ S406、如果安全认证通过，安全支付服务服务器将交易信息界面发送到安全支付服务客户端上进行展现；

[0087] S407 ～ S408、如果安全支付服务客户端接收到用户通过交易信息界面发送的交易信息确认指令，向安全支付服务服务器提交用户确认信息；

[0088] S409、安全支付服务服务器接收到用户确认信息之后，将交易信息提交给支付系统；

[0089] S410 ～ S411、支付系统确认本次交易并完成计费之后，向安全支付服务服务器返回交易结果；

[0090] S412 ～ S414、安全支付服务服务器通知网站服务器本次交易结果，并将交易结果界面发送到安全支付服务客户端上进行展现；

[0091] S415 ～ S416、如果安全支付服务客户端接收到用户通过交易结果界面发送的交易结果确认指令，回调第三方浏览器；

[0092] 具体实施中，是安全支付服务客户端通过 API 向第三方浏览器返回调用响应，实现对第三方浏览器的回调；

[0093] S417、第三方浏览器继续访问流程。

[0094] 本申请实施例提供的安全支付服务，在无线终端上可以以应用的形式存在，也可以以插件的形式存在，并且可以被无线终端上所有的应用（应用客户端或第三方浏览器）调用，所述的应用包括各种应用软件、游戏程序、多媒体程序等。

[0095] 基于同一技术构思，本申请实施例还提供了一种无线终端上的支付服务提供系统，由于该支付服务提供系统解决问题的原理与支付服务提供方法相似，因此该系统的实施可以参见方法的实施，重复之处不再赘述。

[0096] 如图 5 所示，无线终端上的支付服务提供系统包括无线终端 501、安全支付服务服务器 502 和支付系统 503，其中，无线终端 501 包括应用服务模块 511 和安全支付服务客户端 512，其中：

[0097] 应用服务模块 511，用于接收到用户针对应用服务发起的支付请求时，调用安全支付服务客户端 512，其中携带针对应用服务的订单信息；

[0098] 安全支付服务客户端 512，用于根据订单信息生成支付订单，提交给安全支付服务服务器 502，以及向用户展现安全支付服务服务器 502 返回的交易信息界面；接收到用户通过交易信息界面发送的交易信息确认指令后，向安全支付服务服务器 502 提交用户确认信息，以及向用户展现安全支付服务服务器 502 返回的交易结果界面；接收到用户通过交易

结果界面发送的交易结果确认指令后，回调应用服务模块 511 ；

[0099] 安全支付服务服务器 502，用于根据接收到的支付订单向安全支付服务客户端 512 返回交易信息界面，以及基于接收到的用户确认信息与支付系统 503 交互并完成支付后向安全支付服务客户端 512 返回所述交易结果界面。

[0100] 较佳的，为了保障安全支付服务的安全性，安全支付服务客户端 512，还用于被首次调用时，在生成支付订单之前，向安全支付服务服务器 502 获取短信发送信息 ；根据获取到的短信发送信息，调用无线终端 501 上的短信模块，通过运营商短信通道向安全支付服务服务器 502 发送相应短信，并向安全支付服务服务器 502 获取与短信的发送方号码绑定的账户信息 ；接收到用户发送的账户信息确认指令后，向安全支付服务服务器 502 提交账户确认信息，其中携带无线终端的硬件信息，以及接收并存储安全支付服务服务器 502 为无线终端生成的授权码 ；

[0101] 安全支付服务服务器 502，还用于在接收到安全支付服务客户端 512 提交的账户确认信息之后，为无线终端生成授权码并发送给安全支付服务客户端 512，并保存账户信息、为无线终端生成的授权码、以及安全支付服务客户端上报的无线终端的硬件信息之间的绑定关系。

[0102] 较佳的，安全支付服务客户端 512，还用于在提交给安全支付服务服务器 502 的支付订单中携带无线终端的授权码以及硬件信息 ；

[0103] 安全支付服务服务器 502，还用于根据支付订单返回交易信息界面之前，根据保存的授权码与硬件信息的绑定关系，对支付订单中携带的无线终端的授权码以及硬件信息进行安全认证，并确认安全认证通过。

[0104] 本申请实施例提供的无线终端上的支付服务提供方法及相关设备和系统，为应用服务提供安全支付服务，在无线终端上设置应用服务模块和安全支付服务客户端，由支付请求触发安全支付服务客户端的调用，进入交易信息界面，支付完成之后安全支付服务客户端能够回调应用服务模块，继续应用流程，从而在无线终端上实现了应用与支付的平滑切换，无需跳出应用，不会中断应用既有的流程。

[0105] 进一步，安全支付服务采用在用户首次使用时，将用户账户与无线终端绑定的安全机制保障支付的安全性。在用户首次使用安全支付服务时，通过短信通道和账户名 / 密码双重认证方式确定用户的账户信息 ；在首次确定用户的账户信息之后，为用户使用的无线终端分配授权码，并将用户的账户信息、为无线终端分配的授权码、以及无线终端的硬件信息绑定，以便后续用户使用时以授权码为依据校验硬件信息，确保对用户账户进行操作的为用户本人，防止用户账户被盗用而造成财产损失。并且，通过安全支付服务服务器与支付系统交互完成支付，防止提供商对交易信息的篡改，保证交易信息的透明度。

[0106] 本申请实施例提供的无线终端上的支付服务提供方法及相关设备和系统，不存在虚拟货币的费率、结算等环节的服务器资源消耗。

[0107] 本领域的技术人员应该明白，本申请的实施例可提供为方法、装置、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0108] 本申请是参照根据本申请实施例的方法、装置和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0109] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0110] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0111] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例、以及落入本申请范围的所有变更和修改。

[0112] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

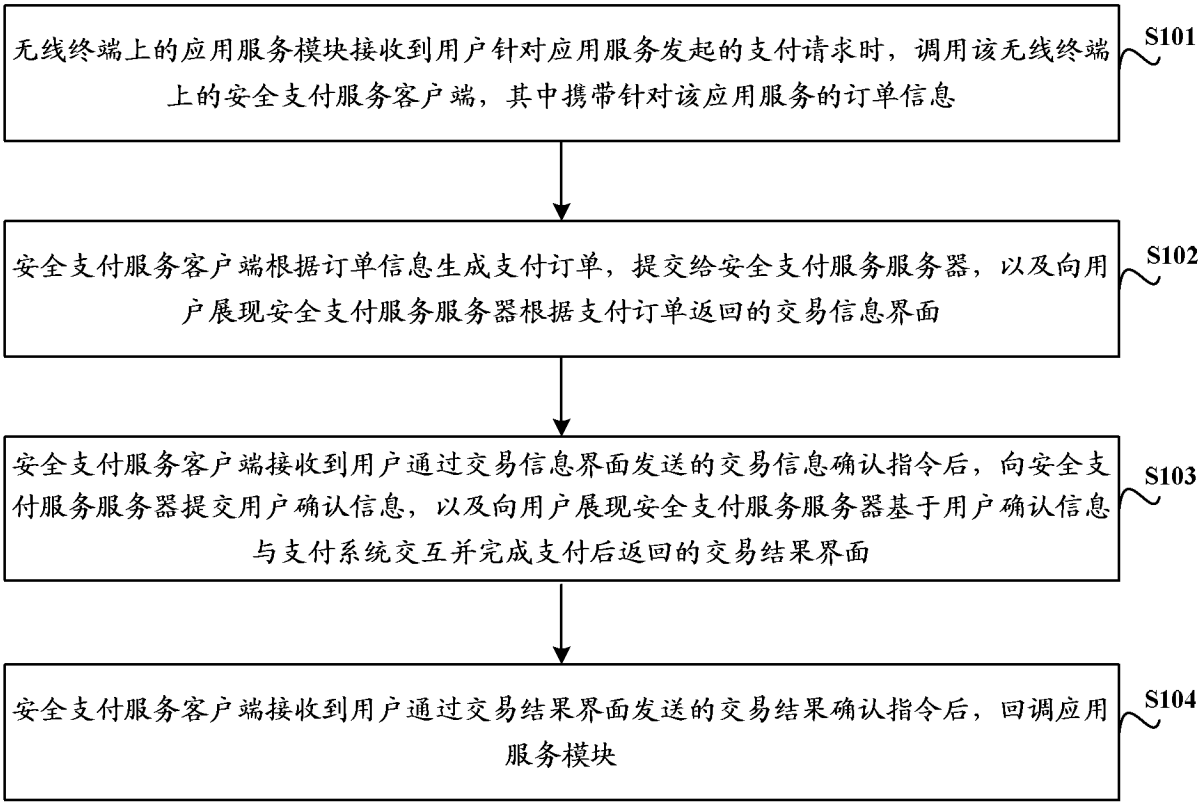

无线终端上的应用服务模块接收到用户针对应用服务发起的支付请求时，调用该无线终端上的安全支付服务客户端，其中携带针对该应用服务的订单信息
S101
安全支付服务客户端根据订单信息生成支付订单，提交给安全支付服务服务器，以及向用户展现安全支付服务服务器根据支付订单返回的交易信息界面
S102
安全支付服务客户端接收到用户通过交易信息界面发送的交易信息确认指令后，向安全支付服务服务器提交用户确认信息，以及向用户展现安全支付服务服务器基于用户确认信息与支付系统交互并完成支付后返回的交易结果界面
S103
安全支付服务客户端接收到用户通过交易结果界面发送的交易结果确认指令后，回调应用服务模块
S104

图 1

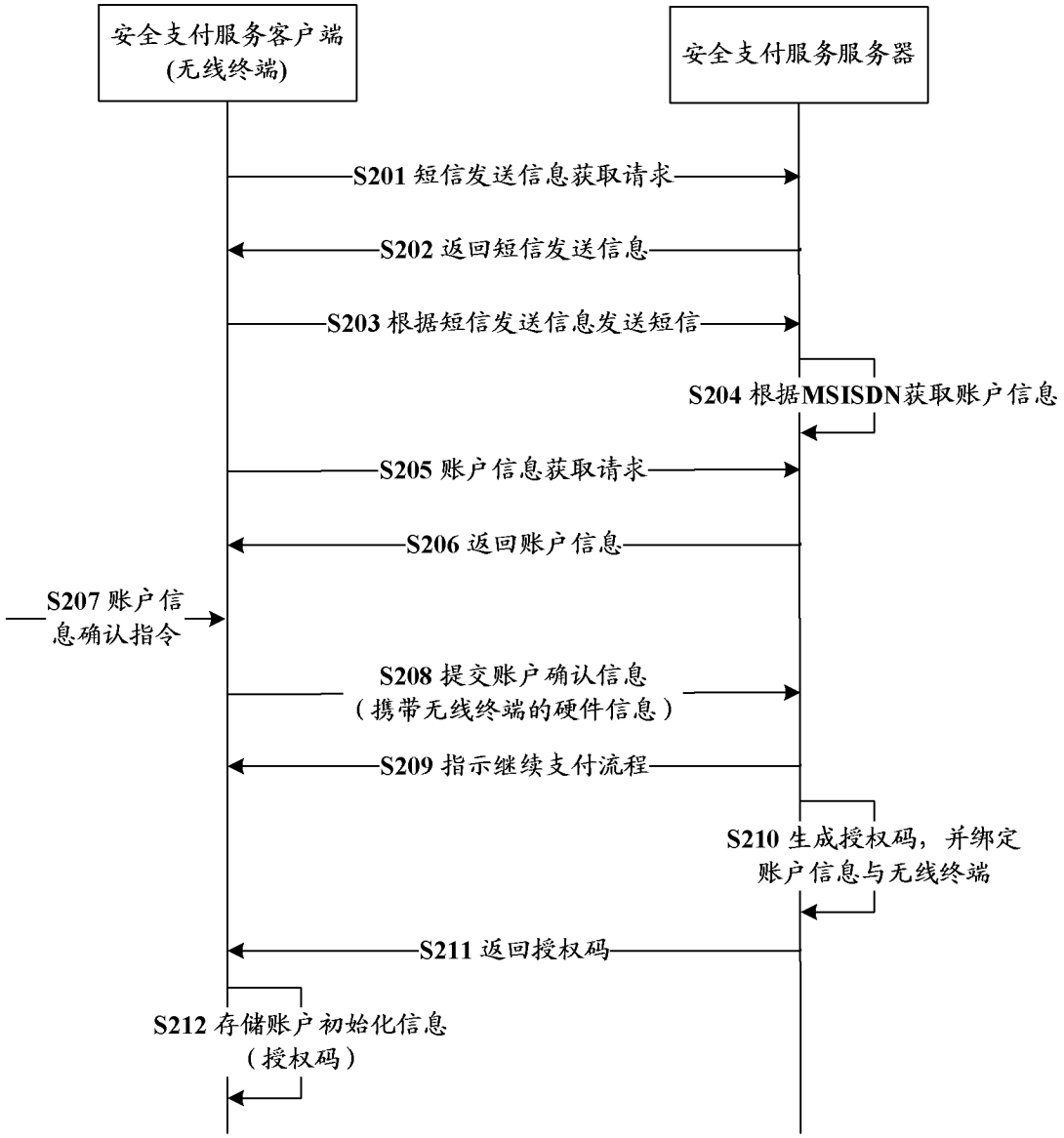

安全支付服务客户端
(无线终端)
安全支付服务服务器
S201 短信发送信息获取请求
S202 返回短信发送信息
S203 根据短信发送信息发送短信
S204 根据MSISDN获取账户信息
S205 账户信息获取请求
S206 返回账户信息
S207 账户信息确认指令
S208 提交账户确认信息
（携带无线终端的硬件信息）
S209 指示继续支付流程
S210 生成授权码，并绑定账户信息与无线终端
S211 返回授权码
S212 存储账户初始化信息
（授权码）

图 2

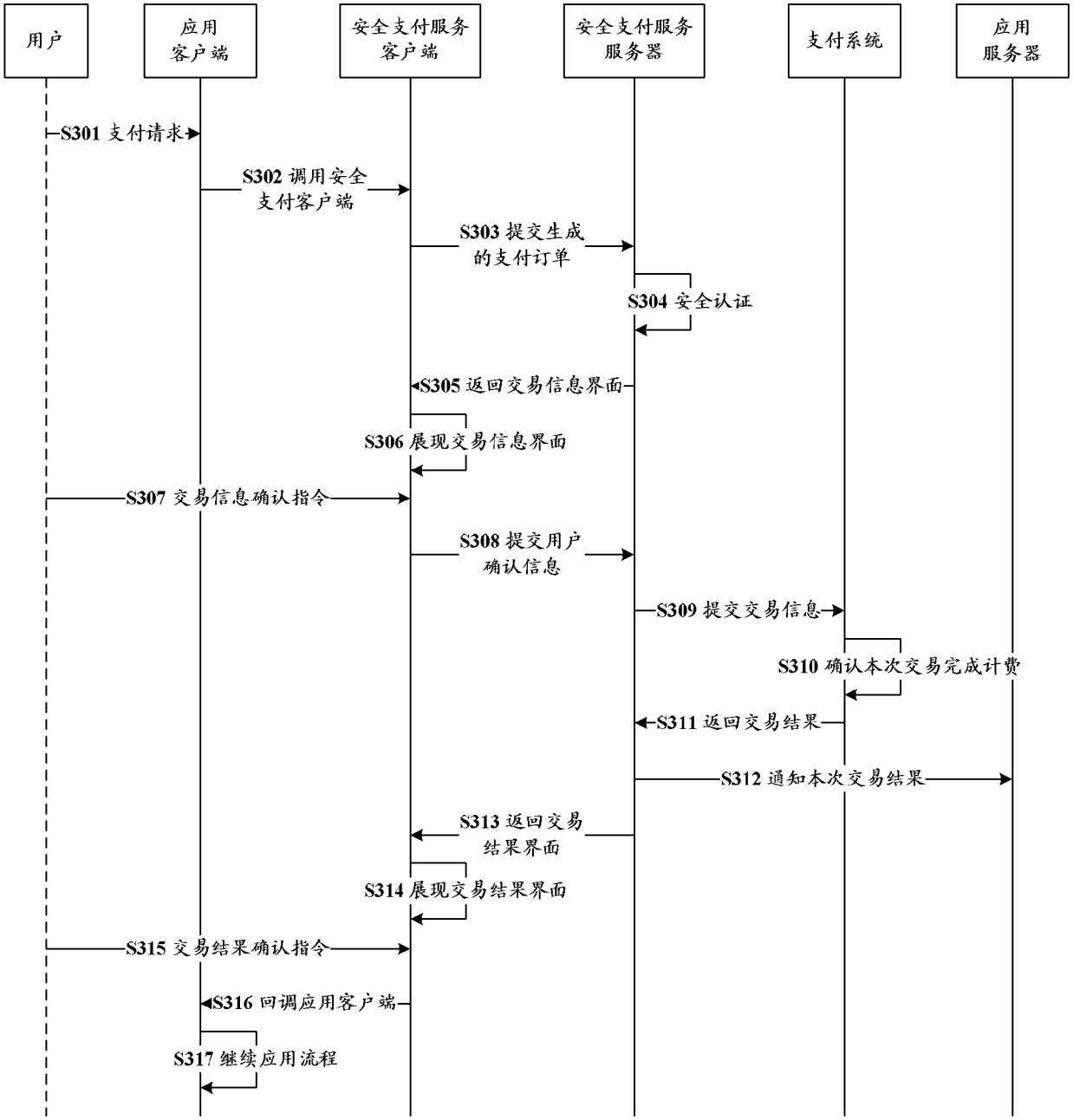

用户
应用客户端
安全支付服务客户端
安全支付服务服务器
支付系统
应用服务器
S301 支付请求
S302 调用安全支付客户端
S303 提交生成的支付订单
S304 安全认证
S305 返回交易信息界面
S306 展现交易信息界面
S307 交易信息确认指令
S308 提交用户确认信息
S309 提交交易信息
S310 确认本次交易完成计费
S311 返回交易结果
S312 通知本次交易结果
S313 返回交易结果界面
S314 展现交易结果界面
S315 交易结果确认指令
S316 回调应用客户端
S317 继续应用流程

图 3

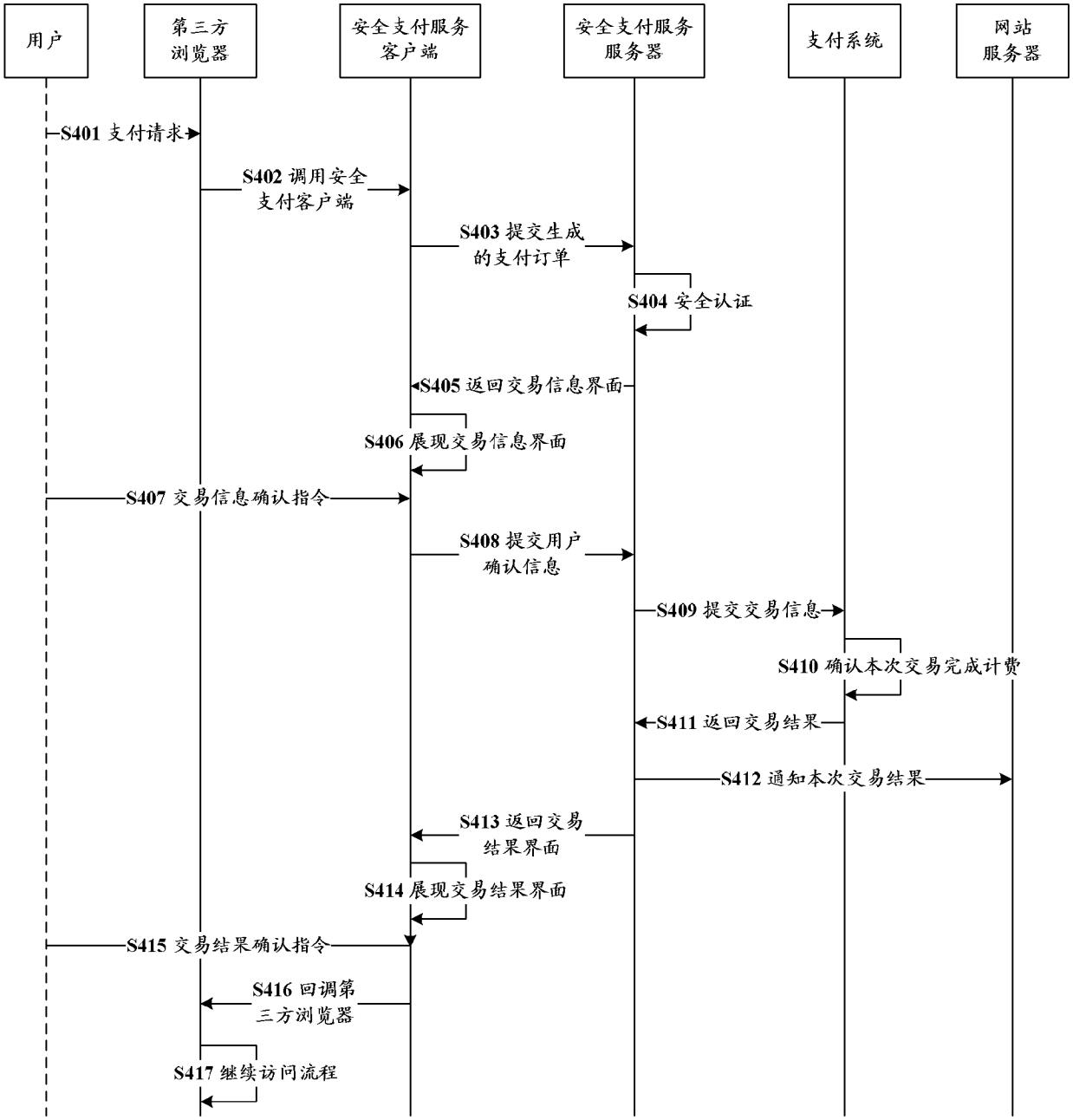

用户
第三方浏览器
安全支付服务客户端
安全支付服务服务器
支付系统
网站服务器
S401 支付请求
S402 调用安全支付客户端
S403 提交生成的支付订单
S404 安全认证
S405 返回交易信息界面
S406 展现交易信息界面
S407 交易信息确认指令
S408 提交用户确认信息
S409 提交交易信息
S410 确认本次交易完成计费
S411 返回交易结果
S412 通知本次交易结果
S413 返回交易结果界面
S414 展现交易结果界面
S415 交易结果确认指令
S416 回调第三方浏览器
S417 继续访问流程

图 4

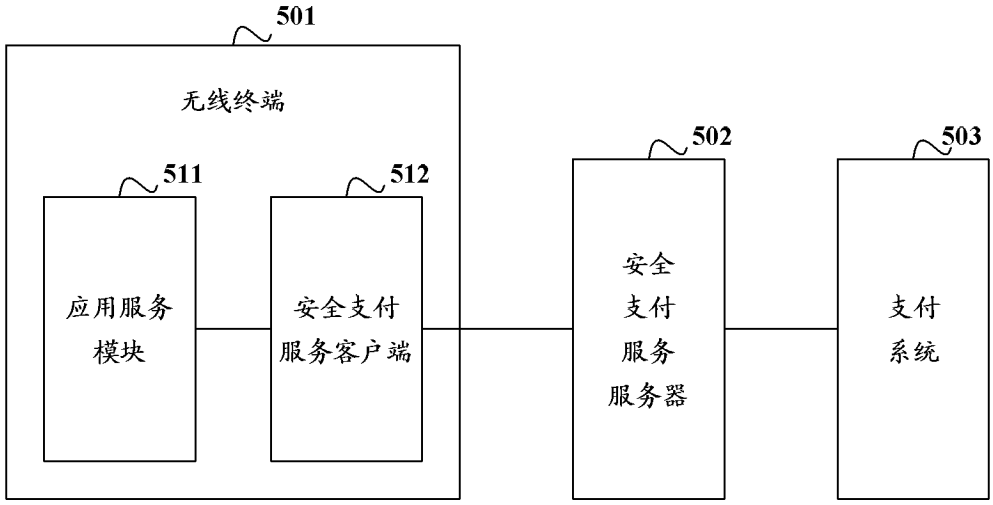


图 5