(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 106899552 B
(45)授权公告日 2020.03.20

(21)申请号 201510961781.5

(22)申请日 2015.12.21

(65)同一申请的已公布的文献号
申请公布号 CN 106899552 A

(43)申请公布日 2017.06.27

(73)专利权人 中国电信股份有限公司
地址 100033 北京市西城区金融大街31号

(72)发明人 张湘东 张文安 黄泽龙 李庆艳 杨豫湘 李洪波 杨光

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 许蓓

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 105046488 A,2015.11.11,
CN 103095704 A,2013.05.08,
CN 101765108 A,2010.06.30,

审查员 李珍珍

权利要求书2页 说明书5页 附图3页

(54)发明名称

认证方法,认证终端以及系统

(57)摘要

本发明公开了一种认证方法,认证终端以及系统,涉及移动互联网技术领域。该方法包括:支付可信应用接收用户通过支付客户端发送的用户身份验证请求和交易信息;支付可信应用对用户身份进行验证,若验证成功,则对交易信息进行签名;支付可信应用将签名后的交易信息发送到支付客户端,支付客户端将交易信息及签名后的交易信息发送给的服务器进行验证。本发明中,在终端的可信执行环境中设置支付可信应用,通过终端的可信执行环境完成交易保护,利用这种软硬件结合的技术方案替代纯软件的安全方案,增强交易的安全性,并且服务器通过对交易签名的验证确保交易是由用户的终端发起,进一步提升了手机线下支付的安全性,满足交易的不可抵赖性要求。

CN 106899552 B

1.一种认证方法,其特征在于,包括:

对支付可信应用的签名进行验证,验证成功后将所述支付可信应用加载到可信执行环境中运行;

支付可信应用接收用户通过支付客户端发送的用户身份验证请求和交易信息;其中,支付客户端通过操作系统所提供的安全服务API发起对支付可信应用的访问;支付可信应用对支付客户端的签名进行验证,验证合法后,支付可信应用对用户身份进行验证,如果验证成功,则对所述交易信息进行签名;

支付可信应用将签名后的交易信息发送到支付客户端,以便支付客户端将交易信息及签名后的交易信息发送给的服务器进行验证。

2.根据权利要求1所述的方法,其特征在于,还包括:

生成公钥和私钥的密钥对,私钥存储在可信执行环境,用于对所述交易信息进行签名,公钥发送至服务器,用于服务器对交易信息及签名后的交易信息进行验证。

3.根据权利要求2所述的方法,其特征在于,其中,

所述支付可信应用使用私钥对交易信息进行签名;

所述服务器使用公钥对签名后的交易信息进行解密,并将解密结果与所述交易信息进行比对,如果一致则验证成功。

4.根据权利要求1所述的方法,其特征在于,所述支付可信应用对用户身份进行验证包括:

所述支付可信应用对用户输入的密码或指纹进行验证。

5.根据权利要求1-4任一项所述的方法,其特征在于,还包括:

通过二维码、声波、或者近场通信NFC方式将交易信息推送到所述支付客户端。

6.根据权利要求1-4任一项所述的方法,其特征在于,其中,所述交易信息包括交易关键数据。

7.一种认证终端,其特征在于,包括:

验证单元,用于对支付可信应用的签名进行验证,验证成功后将所述支付可信应用加载到可信执行环境中运行;

支付可信应用,用于接收用户通过支付客户端发送的用户身份验证请求和交易信息;对支付客户端的签名进行验证,验证合法后,对用户身份进行验证,如果验证成功,则对所述交易信息进行签名;将签名后的交易信息发送到支付客户端,以便支付客户端将交易信息及签名后的交易信息发送给的服务器进行验证;其中,支付客户端通过操作系统所提供的安全服务API发起对支付可信应用的访问。

8.根据权利要求7所述的认证终端,其特征在于,还包括:

密钥生成单元,用于生成公钥和私钥的密钥对,并将私钥存储在可信执行环境,用于对所述交易信息进行签名,公钥发送至服务器,用于服务器对交易信息及签名后的交易信息进行验证。

9.根据权利要求8所述的认证终端,其特征在于,

所述支付可信应用,用于使用私钥对交易信息进行签名。

10.根据权利要求7所述的认证终端,其特征在于,

所述支付可信应用,用于对用户输入的密码或指纹进行验证。

11.根据权利要求7-10任一项所述的认证终端，其特征在于，还包括：

交易信息推送单元，用于通过二维码、声波、或者近场通信NFC方式将交易信息推送到所述支付客户端。

12.根据权利要求7-10任一项所述的认证终端，其特征在于，其中，所述交易信息包括交易关键数据。

13.一种认证系统，其特征在于，包括：权利要求7-12任一项所述的认证终端，以及服务器；

所述服务器，用于接收支付客户端发送的交易信息及签名后的交易信息，使用公钥对签名后的交易信息进行解密，并将解密结果与所述交易信息进行比对，如果一致则验证成功。

认证方法,认证终端以及系统

技术领域

[0001] 本发明涉及移动互联网技术领域,特别涉及一种认证方法,认证终端以及系统。

背景技术

[0002] 随着移动互联网高速发展,使用手机通过各种不同的技术实现线下交易的应用越来越普遍。通过二维码扫描进行线下支付已经遍布各类商户;通过声波、蓝牙、Wifi等方式实现近场当面支付应用发展迅猛;通过手机终端的NFC(Near Field Communication,近场通信)技术替代传统POS(Point of Sale,销售终端)实现的手机POS应用也越来越普及。

[0003] 但现有的手机线下交易技术均存在一些安全问题:目前的各类技术方案基本都是通过软件方式实现安全防护,缺乏硬件的交易保护,尤其对于支付类的交易难以满足不可抵赖性的要求,交易过程存在安全隐患。

发明内容

[0004] 本发明实施例所要解决的一个技术问题是:提高终端线下交易的安全性。

[0005] 根据本发明实施例的一个方面,提供的一种认证方法,包括:支付可信应用接收用户通过支付客户端发送的用户身份验证请求和交易信息;支付可信应用对用户身份进行验证,如果验证成功,则对交易信息进行签名;支付可信应用将签名后的交易信息发送到支付客户端,以便支付客户端将交易信息及签名后的交易信息发送给的服务器进行验证。

[0006] 在一个实施例中,认证方法还包括:对支付可信应用的签名进行验证,验证成功后将支付可信应用加载到可信执行环境中运行。

[0007] 在一个实施例中,认证方法还包括:生成公钥和私钥的密钥对,私钥存储在可信执行环境,用于对交易信息进行签名,公钥发送至服务器,用于服务器对交易信息及签名后的交易信息进行验证。

[0008] 在一个实施例中,支付可信应用使用私钥对交易信息进行签名;服务器使用公钥对签名后的交易信息进行解密,并将解密结果与交易信息进行比对,如果一致则验证成功。

[0009] 在一个实施例中,支付可信应用对用户输入的密码或指纹进行验证。

[0010] 在一个实施例中,通过二维码、声波、或者近场通信NFC方式将交易信息推送到支付客户端。

[0011] 在一个实施例中,交易信息包括交易关键数据。

[0012] 根据本发明实施例的第二个方面,提供的一种认证终端,包括:支付可信应用,用于接收用户通过支付客户端发送的用户身份验证请求和交易信息;对用户身份进行验证,如果验证成功,则对交易信息进行签名;将签名后的交易信息发送到支付客户端,以便支付客户端将交易信息及签名后的交易信息发送给的服务器进行验证。

[0013] 在一个实施例中,认证终端还包括:验证单元,用于对支付可信应用的签名进行验证,验证成功后将支付可信应用加载到可信执行环境中运行。

[0014] 在一个实施例中,认证终端还包括:密钥生成单元,用于生成公钥和私钥的密钥

对，并将私钥存储在可信执行环境，用于对交易信息进行签名，公钥发送至服务器，用于服务器对交易信息及签名后的交易信息进行验证。

[0015] 在一个实施例中，支付可信应用，用于使用私钥对交易信息进行签名。

[0016] 在一个实施例中，支付可信应用，用于对用户输入的密码或指纹进行验证。

[0017] 在一个实施例中，认证终端还包括：交易信息推送单元，用于通过二维码、声波、或者近场通信NFC方式将交易信息推送到支付客户端。

[0018] 在一个实施例中，交易信息包括交易关键数据。

[0019] 根据本发明实施例的第三个方面，提供的一种认证系统，包括：前述任一个实施例中的认证终端，以及服务器；服务器，用于接收支付客户端发送的交易信息及签名后的交易信息，使用公钥对签名后的交易信息进行解密，并将解密结果与交易信息进行比对，如果一致则验证成功。

[0020] 本发明中，在终端的可信执行环境中设置支付可信应用，通过终端的可信执行环境完成交易保护，利用这种软硬件结合的技术方案替代纯软件的安全方案，增强交易的安全性，并且服务器通过对交易签名的验证确保交易是由用户的终端发起，进一步提升了手机线下支付的安全性，满足交易的不可抵赖性要求。

[0021] 通过以下参照附图对本发明的示例性实施例的详细描述，本发明的其它特征及其优点将会变得清楚。

附图说明

[0022] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，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。

[0023] 图1示出终端的安全区域体系架构示意图。

[0024] 图2示出本公开的示例性实施例的认证方法的流程示意图。

[0025] 图3示出本公开的另一种示例性实施例的认证方法的流程示意图。

[0026] 图4示出本公开的示例性实施例的认证终端的结构示意图。

[0027] 图5示出本公开的示例性实施例的认证系统的结构示意图。

具体实施方式

[0028] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。以下对至少一个示例性实施例的描述实际上仅仅是说明性的，决不作为对本发明及其应用或使用的任何限制。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0029] 针对现有技术中通过终端线下交易的过程中存在的安全问题以及交易难以满足不可抵赖性的要求，提出本方案。本方案中主要利用目前越来越多手机终端支持的Trust Zone(安全区域)技术，在终端的可信执行环境中进行交易安全数据的存储及运算，从而实现一种安全、体验良好的移动终端线下交易技术方案。下面结合图1对本方案中应用的可信

执行环境进行描述。如图1所示，可信执行环境(Trusted Execution Environment，TEE)是存在于移动设备内，与主处理器相隔离的安全区域。可信执行环境通过双域切换、内存与外设隔离、中断隔离等技术，实现了与普通手机终端应用相分离，确保各种敏感数据在一个可信环境中被存储、处理和受到保护，同时可信执行环境上装载着可信应用(Trusted Application，TA)，并为这些可信应用提供了一个安全的执行环境。应用方首先需要开发一个专门的可信应用(Trusted Application，TA)用于访问可信执行环境内的数据，用户通过普通应用调用操作系统所提供的安全服务API(Application Programming Interface，应用程序编程接口)发起对可信应用的访问，将调用请求转发到TEE Driver(可信执行环境驱动)，然后透过安全隔离，将请求转发到指定的可信应用执行。可信应用会对调用它的普通应用的身份(签名)进行验证，验证合法后才会执行普通应用发起的业务请求，并返回执行结果。下面具体描述认证过程。

[0030] 下面结合图2对本发明认证方法的一个实施例进行描述。

[0031] 图2为本发明认证方法一个实施例的流程图。如图2所示，该实施例的方法包括：

[0032] 步骤S202，支付客户端向支付可信应用发送用户身份验证请求和交易信息，相应的，支付可信应用接收支付客户端发送的用户身份验证请求和交易信息。

[0033] 其中，应用方首先需要开发一个专门的支付可信应用用于访问可信执行环境内的数据，并可以调用可信执行环境中所提供的用户信息验证驱动，进行用户身份的验证。支付可信应用并不提供用户界面，因此用户不能直接访问支付可信应用。用户使用支付客户端进行访问，在支付客户端需要对用户身份进行验证的时候，由支付客户端通过操作系统所提供的安全服务API发起对支付可信应用的访问。安全服务API由操作系统提供，在支付客户端对其进行调用时，会将调用请求转发到TEE Driver，然后透过安全隔离，将请求转发到支付可信应用执行。

[0034] 步骤S204，支付可信应用对用户身份进行验证，如果验证成功，则执行步骤S206。

[0035] 其中，用户的身份验证信息可以包括例如指纹等生物特征信息、或密码等可以用于识别用户身份的的信息，但不限于所举示例。可以将指纹、密码等表示用户身份的信息存储于可信执行环境中，避免外部的访问和篡改。

[0036] 步骤S206，支付可信应用对交易信息进行签名。

[0037] 其中，交易信息是由应用方自行定义的，是交易过程中客户端需要向服务器传送的交易关键数据，例如交易商品编号、数量、金额等，可以采用二进制数据块的形式进行发送。支付可信应用可以使用私钥对交易信息进行签名。

[0038] 步骤S208，支付可信应用将签名后的交易信息发送到支付客户端，以便支付客户端将交易信息及签名后的交易信息发送给的服务器进行验证。

[0039] 上述实施例的方法，在终端的可信执行环境中设置支付可信应用，通过终端的可信执行环境完成交易保护，利用这种软硬件结合的技术方案替代纯软件的安全方案，增强交易的安全性，并且服务器通过对交易签名的验证确保交易是由用户的终端发起，进一步提升了手机线下支付的安全性，满足交易的不可抵赖性要求。

[0040] 下面结合图3对本发明认证方法的一个具体的实施例进行描述。

[0041] 图3为本发明认证方法另一个实施例的流程图。如图3所示，该实施例的方法包括：

[0042] 步骤S302，对支付可信应用的签名进行验证，验证成功后将支付可信应用加载到

可信执行环境中运行。

[0043] 其中，支付可信应用需要由终端厂商进行签名，可信执行环境验证支付可信应用的签名通过后，才将支付可信应用加载到可信执行环境中运行。

[0044] 步骤S304，生成公钥和私钥的密钥对，私钥存储在可信执行环境，公钥发送至服务器。

[0045] 步骤S306，将交易信息推送到支付客户端。

[0046] 其中，可以通过二维码、声波、或者近场通信NFC方式等方式将交易信息推送到支付客户端，例如用户扫描二维码将交易信息通过支付客户端进行显示。

[0047] 步骤S308，用户在支付客户端输入身份验证信息，支付客户端向支付可信应用发送用户身份验证请求和交易信息。

[0048] 其中，支付客户端通过调用终端操作系统对外提供的安全服务API向支付可信应用发送用户身份验证请求和交易信息。

[0049] 步骤S310，支付可信应用对用户身份进行验证，如果验证成功，则执行步骤S312。

[0050] 步骤S312，支付可信应用使用私钥对交易信息进行签名，将签名后的交易信息发送到支付客户端。

[0051] 步骤S314，支付客户端向服务器发送交易信息和签名后的交易信息，相应的，服务器接收支付客户端发送的交易信息和签名后的交易信息。

[0052] 步骤S316，服务器使用公钥对签名后的交易信息进行解密，并将解密结果与交易信息进行比对，如果一致则验证成功。

[0053] 上述实施例的方法，在终端的可信执行环境中设置支付可信应用，通过终端的可信执行环境完成交易保护，交易过程不能被外部访问或篡改，利用这种软硬件结合的技术方案替代纯软件的安全方案，增强交易的安全性，并且对交易信息采用公私密钥对的非对称加密方式进行签名，服务器通过对交易签名的验证确保交易是由用户的终端发起，进一步提升了手机线下支付的安全性，满足交易的不可抵赖性要求。

[0054] 本发明还提供一种认证终端，下面结合图4对认证终端的一个实施例进行描述。

[0055] 图4为本发明认证终端一个实施例的结构图。如图4所示，认证终端40包括：支付客户端402，支付可信应用404。

[0056] 支付可信应用404，用于接收用户通过支付客户端402发送的用户身份验证请求和交易信息；对用户身份进行验证，如果验证成功，则对交易信息进行签名；将签名后的交易信息发送到支付客户端402，以便支付客户端402将交易信息及签名后的交易信息发送给的服务器进行验证。

[0057] 其中，支付可信应用404，用于对用户输入的密码或指纹进行验证。交易信息是由应用方自行定义的，是交易过程中客户端需要向服务器传送的交易关键数据，例如交易商品编号、数量、金额等，可以采用二进制数据块的形式进行发送。支付可信应用404是可以访问可信执行环境的软件功能模块。

[0058] 如图4所示，认证终端40还包括：验证单元406，用于对支付可信应用404的签名进行验证，验证成功后将支付可信应用404加载到可信执行环境中运行。

[0059] 密钥生成单元408，用于生成公钥和私钥的密钥对，并将私钥存储在可信执行环境，用于对交易信息进行签名，公钥发送至服务器，用于服务器对交易信息及签名后的交易

信息进行验证。其中，支付可信应用404，用于使用私钥对交易信息进行签名。

[0060] 交易信息推送单元410，用于通过二维码、声波、或者近场通信NFC方式将交易信息推送到支付客户端402。

[0061] 本发明还提供一种认证系统，下面结合图5进行描述。

[0062] 图5为本发明认证系统一个实施例的结构图。如图5所示，认证系统50包括：前述实施例中的认证终端40，以及服务器502。服务器502，用于接收支付客户端402发送的交易信息及签名后的交易信息，使用公钥对签名后的交易信息进行解密，并将解密结果与交易信息进行比对，如果一致则验证成功。

[0063] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0064] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

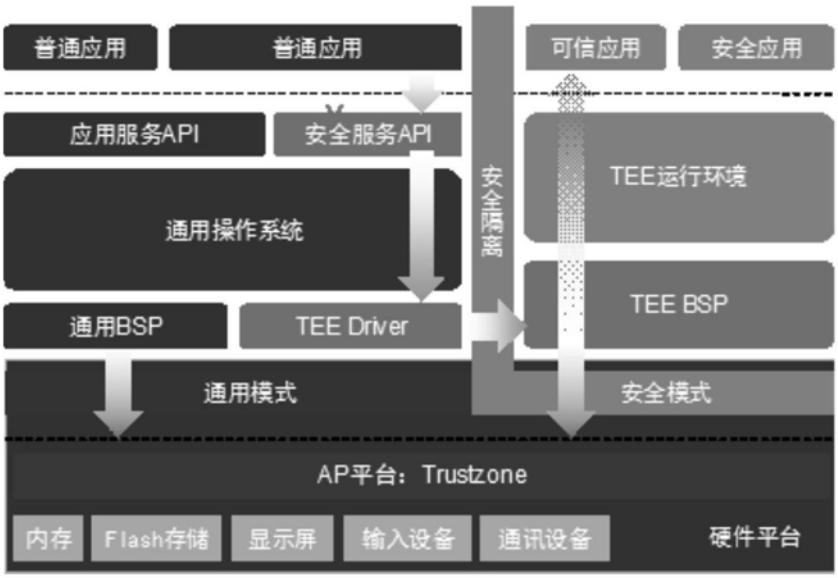
普通应用
普通应用
可信应用
安全应用
应用服务API
安全服务API
安全通路
TEE运行环境
通用操作系统
TEE BSP
通用BSP
TEE Driver
通用模式
安全模式
AP平台：Trustzone
内存
Flash存储
显示屏
输入设备
通讯设备
硬件平台

图1

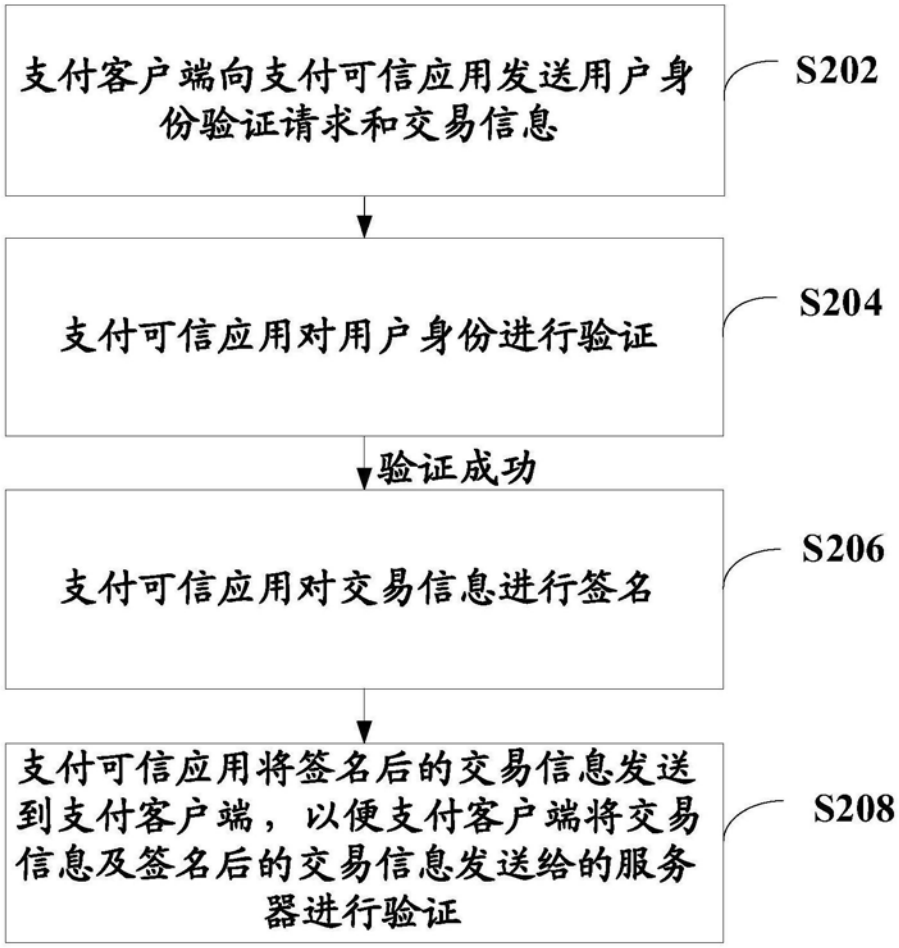
支付客户端向支付可信应用发送用户身份验证请求和交易信息
S202
支付可信应用对用户身份进行验证
S204
验证成功
支付可信应用对交易信息进行签名
S206
支付可信应用将签名后的交易信息发送到支付客户端，以便支付客户端将交易信息及签名后的交易信息发送给的服务器进行验证
S208

图2

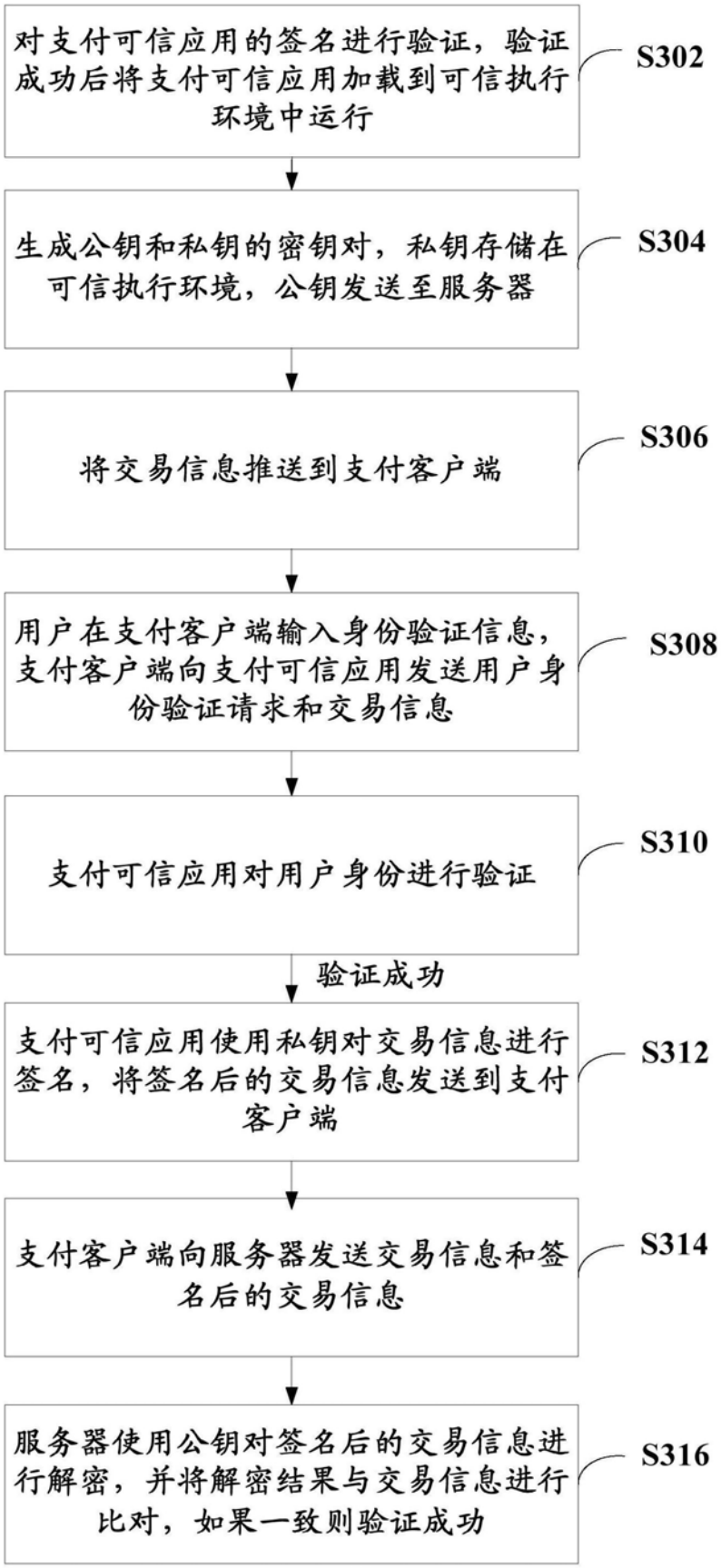
对支付可信应用的签名进行验证，验证成功后将支付可信应用加载到可信执行环境中运行
S302
生成公钥和私钥的密钥对，私钥存储在可信执行环境，公钥发送至服务器
S304
将交易信息推送到支付客户端
S306
用户在支付客户端输入身份验证信息，支付客户端向支付可信应用发送用户身份验证请求和交易信息
S308
支付可信应用对用户身份进行验证
S310
验证成功
支付可信应用使用私钥对交易信息进行签名，将签名后的交易信息发送到支付客户端
S312
支付客户端向服务器发送交易信息和签名后的交易信息
S314
服务器使用公钥对签名后的交易信息进行解密，并将解密结果与交易信息进行比对，如果一致则验证成功
S316

图3


40
密钥生成单元
408
交易信息推送单元
410
支付客户端
402
支付可信应用
404
验证单元
406

图4

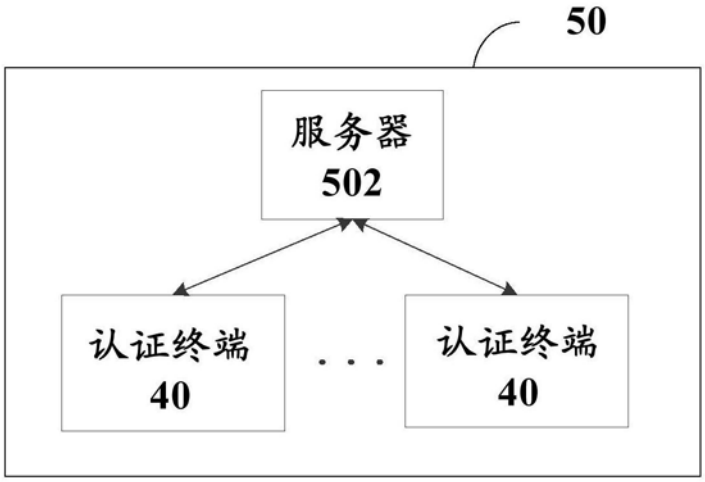
50
服务器
502
认证终端
40
. . .
认证终端
40

图5