



(12) 发明专利申请

(10) 申请公布号 CN 104574080 A

(43) 申请公布日 2015. 04. 29

(21) 申请号 201310513256. 8

(22) 申请日 2013. 10. 25

(71) 申请人 腾讯科技(深圳)有限公司

地址 518000 广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室

(72) 发明人 李建立

(74) 专利代理机构 广州三环专利代理有限公司

44202

代理人 郝传鑫 熊永强

(51) Int. Cl.

G06Q 20/40(2012. 01)

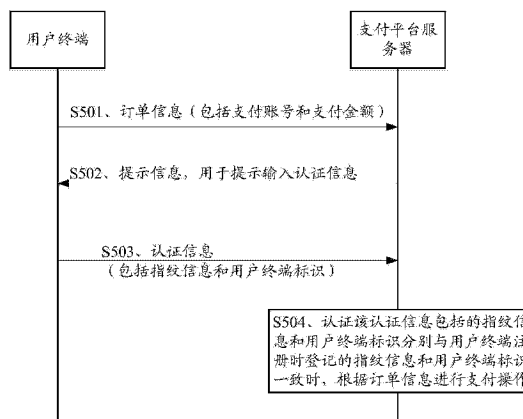
权利要求书6页 说明书14页 附图9页

(54) 发明名称

一种安全支付方法及相关设备、系统

(57) 摘要

本发明公开一种安全支付方法及相关设备、系统,该方法包括:用户终端发送订单信息至支付平台服务器,订单信息包括支付账号和支付金额;支付平台服务器接收用户终端发送的订单信息,并发送提示信息至用户终端,提示信息用于提示输入认证信息;用户终端接收支付平台服务器发送的提示信息,并将认证信息发送至支付平台服务器,认证信息包括用户终端标识和用户响应提示信息输入的指纹信息;支付平台服务器接收用户终端发送的认证信息,并认证该认证信息包括的指纹信息和用户终端标识是否分别与用户终端注册时登记的指纹信息和用户终端标识一致,若一致,根据订单信息进行支付操作。能够简化支付操作,提高在线支付效率,以及提高支付安全性。



1. 一种安全支付方法,其特征在于,包括:

用户终端发送订单信息至支付平台服务器,所述订单信息包括支付账号和支付金额;
所述支付平台服务器接收所述用户终端发送的所述订单信息,并发送提示信息至所述用户终端,所述提示信息用于提示输入认证信息;

所述用户终端接收所述支付平台服务器发送的所述提示信息,并将认证信息发送给所述支付平台服务器;其中,所述认证信息包括用户终端标识和用户响应所述提示信息输入的指纹信息;

所述支付平台服务器接收所述用户终端发送的所述认证信息,并认证所述认证信息包括的指纹信息和用户终端标识是否分别与所述用户终端注册时登记的指纹信息和用户终端标识一致,若一致,根据所述订单信息进行支付操作。

2. 根据权利要求1所述的方法,其特征在于,所述用户终端发送订单信息至支付平台服务器之前,所述方法还包括:

用户终端发送注册请求至支付平台服务器,所述注册请求包括用户终端标识;

所述支付平台服务器响应所述注册请求,发送通知消息至所述用户终端,所述通知消息用于提示输入指纹信息;

所述用户终端接收所述支付平台服务器发送的所述通知消息,并将用户响应所述通知消息输入的指纹信息发送给所述支付平台服务器;

所述支付平台服务器存储所述用户终端发送的所述指纹信息以及所述注册请求包括的用户终端标识;

所述支付平台服务器发送注册完成响应至所述用户终端;

所述用户终端接收所述支付平台服务器发送的所述注册完成响应。

3. 根据权利要求1或2所述的方法,其特征在于,所述支付平台服务器认证所述认证信息包括的指纹信息和用户终端标识分别与所述用户终端注册时登记的指纹信息和用户终端标识一致之后,以及所述根据所述订单信息进行支付操作之前,所述方法还包括:

所述支付平台服务器发送订单信息确认请求给所述用户终端,所述订单信息确认请求包括所述支付账号和支付金额;

所述用户终端接收所述支付平台服务器发送的所述订单信息确认请求,并将用户输入的针对所述订单信息确认请求的确认响应发送给所述支付平台服务器;

所述支付平台服务器接收到所述用户终端发送的针对所述订单信息确认请求的确认响应后,执行所述的根据所述订单信息进行支付操作的步骤。

4. 根据权利要求3所述的方法,其特征在于,所述用户终端发送订单信息至支付平台服务器包括:

所述用户终端发送订单信息至交易平台服务器;

所述交易平台服务器将所述订单信息发送至支付平台服务器;

所述交易平台服务器将所述订单信息发送至支付平台服务器之后,所述方法还包括:

所述交易平台服务器获取所述用户终端的历史支付金额;

所述交易平台服务器识别所述历史支付金额所属的金额范围,并识别所述历史支付金额所属的金额范围对应的折扣率;

所述交易平台服务器将所述折扣率发送至所述支付平台服务器;

所述支付平台服务器接收到所述用户终端发送的针对所述订单信息确认请求的确认响应后,根据所述订单信息和所述折扣率进行支付折扣操作。

5. 根据权利要求4所述的方法,其特征在于,所述交易平台服务器将所述折扣率发送至所述支付平台服务器之后,所述方法还包括:

所述交易平台服务器根据所述订单信息包括的所述支付金额更新所述历史支付金额。

6. 一种安全支付方法,其特征在于,包括:

用户终端发送订单信息至支付平台服务器,所述订单信息包括支付账号和支付金额;

所述用户终端接收所述支付平台服务器发送的提示信息,所述提示信息用于提示输入认证信息;

所述用户终端将认证信息发送给所述支付平台服务器,以使所述支付平台服务器认证所述认证信息包括的用户终端标识和用户响应所述提示信息输入的指纹信息分别与所述用户终端注册时登记的用户终端标识和指纹信息一致时,由所述支付平台服务器根据所述订单信息进行支付操作。

7. 根据权利要求6所述的方法,其特征在于,所述用户终端发送订单信息至支付平台服务器之前,所述方法还包括:

用户终端发送注册请求至支付平台服务器,所述注册请求包括用户终端标识;

所述用户终端接收所述支付平台服务器发送的通知消息,所述通知消息用于提示输入指纹信息;

所述用户终端将用户响应所述通知消息输入的指纹信息发送给所述支付平台服务器;

所述用户终端接收所述支付平台服务器发送的注册完成响应。

8. 根据权利要求6或7所述的方法,其特征在于,所述用户终端将认证信息发送给所述支付平台服务器之后,所述方法还包括:

所述用户终端接收所述支付平台服务器发送的订单信息确认请求,所述订单信息确认请求包括所述支付账号和支付金额;

所述用户终端将用户输入的针对所述订单信息确认请求的确认响应发送给所述支付平台服务器。

9. 根据权利要求8所述的方法,其特征在于,所述用户终端发送订单信息至支付平台服务器包括:

所述用户终端发送订单信息至交易平台服务器,由所述交易平台服务器将所述订单信息发送至支付平台服务器。

10. 一种安全支付方法,其特征在于,包括:

支付平台服务器接收用户终端发送的订单信息,所述订单信息包括支付账号和支付金额;

所述支付平台服务器发送提示信息至所述用户终端,所述提示信息用于提示输入认证信息;

所述支付平台服务器接收所述用户终端发送的认证信息,所述认证信息包括用户终端标识和用户响应所述提示信息输入的指纹信息;

所述支付平台服务器认证所述认证信息包括的指纹信息和用户终端标识是否分别与

所述用户终端注册时登记的指纹信息和用户终端标识一致,若一致,根据所述订单信息进行支付操作。

11. 根据权利要求 10 所述的方法,其特征在于,所述支付平台服务器接收用户终端发送的订单信息之前,所述方法还包括:

支付平台服务器接收用户终端发送的注册请求,所述注册请求包括用户终端标识;

所述支付平台服务器响应所述注册请求,发送通知消息至所述用户终端,所述通知消息用于提示输入指纹信息;

所述支付平台服务器接收所述用户终端发送的指纹信息,并存储所述用户终端发送的指纹信息以及所述注册请求包括的用户终端标识;

所述支付平台服务器发送注册完成响应至所述用户终端。

12. 根据权利要求 10 或 11 所述的方法,其特征在于,所述支付平台服务器认证所述认证信息包括的指纹信息和用户终端标识分别与所述用户终端注册时登记的指纹信息和用户终端标识一致之后,以及所述根据所述订单信息进行支付操作之前,所述方法还包括:

所述支付平台服务器发送订单信息确认请求给所述用户终端,所述订单信息确认请求包括所述支付账号和支付金额;

所述支付平台服务器接收到所述用户终端发送的针对所述订单信息确认请求的确认响应后,执行所述的根据所述订单信息进行支付操作的步骤。

13. 根据权利要求 12 所述的方法,其特征在于,所述支付平台服务器接收用户终端发送的订单信息包括:

支付平台服务器接收用户终端通过交易平台服务器发送的订单信息;

所述方法还包括:

所述支付平台服务器接收所述交易平台服务器发送的所述用户终端的历史支付金额所属的金额范围对应的折扣率;

所述支付平台服务器根据所述订单信息和所述折扣率进行支付折扣操作。

14. 一种计算机存储介质,其特征在于,所述计算机存储介质存储有程序,所述程序执行时包括权利要求 6 ~ 9 任一项所述的步骤。

15. 一种计算机存储介质,其特征在于,所述计算机存储介质存储有程序,所述程序执行时包括权利要求 10 ~ 13 任一项所述的步骤。

16. 一种用户终端,其特征在于,包括:

发送单元,用于发送订单信息至支付平台服务器,所述订单信息包括支付账号和支付金额;

接收单元,用于接收所述支付平台服务器发送的提示信息,所述提示信息用于提示输入认证信息;

所述发送单元,还用于将认证信息发送给所述支付平台服务器,以使所述支付平台服务器认证所述认证信息包括的用户终端标识和用户响应所述提示信息输入的指纹信息分别与所述用户终端注册时登记的用户终端标识和指纹信息一致时,由所述支付平台服务器根据所述订单信息进行支付操作。

17. 根据权利要求 16 所述的用户终端,其特征在于,

所述发送单元,还用于在发送订单信息至支付平台服务器之前,发送注册请求至支付

平台服务器,所述注册请求包括用户终端标识;

所述接收单元,还用于接收所述支付平台服务器发送的通知消息,所述通知消息用于提示输入指纹信息;

所述发送单元,还用于将用户响应所述通知消息输入的指纹信息发送给所述支付平台服务器;

所述接收单元,还用于接收所述支付平台服务器发送的注册完成响应。

18. 根据权利要求 16 或 17 所述的用户终端,其特征在于,

所述接收单元,还用于在所述发送单元将认证信息发送给所述支付平台服务器之后,接收所述支付平台服务器发送的订单信息确认请求,所述订单信息确认请求包括所述支付账号和支付金额;

所述发送单元,还用于将用户输入的针对所述订单信息确认请求的确认响应发送给所述支付平台服务器。

19. 一种支付平台服务器,其特征在于,包括:

接收单元,用于接收用户终端发送的订单信息,所述订单信息包括支付账号和支付金额;

发送单元,用于发送提示信息至所述用户终端,所述提示信息用于提示输入认证信息;

所述接收单元,还用于接收所述用户终端发送的认证信息,所述认证信息包括用户终端标识和用户响应所述提示信息输入的指纹信息;

认证单元,用于认证所述认证信息包括的指纹信息和用户终端标识是否分别与所述用户终端注册时登记的指纹信息和用户终端标识一致;

操作单元,用于在所述认证单元的认证结果为一致时,根据所述订单信息进行支付操作。

20. 根据权利要求 19 所述的支付平台服务器,其特征在于,

所述接收单元,还用于在接收用户终端发送的订单信息之前,接收用户终端发送的注册请求,所述注册请求包括用户终端标识;

所述发送单元,还用于响应所述注册请求,发送通知消息至所述用户终端,所述通知消息用于提示输入指纹信息;

所述接收单元,还用于接收所述用户终端发送的指纹信息;

所述支付平台服务器还包括:

存储单元,用于存储所述用户终端发送的指纹信息以及所述注册请求包括的用户终端标识;

所述发送单元,还用于发送注册完成响应至所述用户终端。

21. 根据权利要求 19 或 20 所述的支付平台服务器,其特征在于,

所述发送单元,还用于在所述认证单元认证所述认证信息包括的指纹信息和用户终端标识分别与所述用户终端注册时登记的指纹信息和用户终端标识一致之后,发送订单信息确认请求给所述用户终端,所述订单信息确认请求包括所述支付账号和支付金额;

所述接收单元,还用于接收到所述用户终端发送的针对所述订单信息确认请求的确认响应后,触发所述操作单元执行所述的根据所述订单信息进行支付操作的步骤。

22. 根据权利要求 21 所述的支付平台服务器,其特征在于,所述接收单元接收用户终端发送的订单信息的方式具体为:

接收单元,用于接收用户终端通过交易平台服务器发送的订单信息;

所述接收单元,还用于接收到所述交易平台服务器发送的所述用户终端的历史支付金额所属的金额范围对应的折扣率;

所述操作单元,还用于根据所述订单信息和所述折扣率进行支付折扣操作。

23. 一种安全支付系统,其特征在于,包括用户终端和支付平台服务器,其中:

所述用户终端,用于发送订单信息至支付平台服务器,所述订单信息包括支付账号和支付金额;

所述支付平台服务器,用于接收所述用户终端发送的所述订单信息,并发送提示信息至所述用户终端,所述提示信息用于提示输入认证信息;

所述用户终端,还用于接收所述支付平台服务器发送的所述提示信息,并将认证信息发送给所述支付平台服务器;其中,所述认证信息包括用户终端标识和用户响应所述提示信息输入的指纹信息;

所述支付平台服务器,还用于接收所述用户终端发送的所述认证信息,并认证所述认证信息包括的指纹信息和用户终端标识是否分别与所述用户终端注册时登记的指纹信息和用户终端标识一致,若一致,根据所述订单信息进行支付操作。

24. 根据权利要求 23 所述的系统,其特征在于,

所述用户终端,还用于在发送订单信息至支付平台服务器之前,发送注册请求至支付平台服务器,所述注册请求包括用户终端标识;

所述支付平台服务器,还用于响应所述注册请求,发送通知消息至所述用户终端,所述通知消息用于提示输入指纹信息;

所述用户终端,还用于接收所述支付平台服务器发送的所述通知消息,并将用户响应所述通知消息输入的指纹信息发送给所述支付平台服务器;

所述支付平台服务器,还用于存储所述用户终端发送的所述指纹信息以及所述注册请求包括的用户终端标识;

所述支付平台服务器,还用于发送注册完成响应至所述用户终端;

所述用户终端,还用于接收所述支付平台服务器发送的所述注册完成响应。

25. 根据权利要求 23 或 24 所述的系统,其特征在于,

所述支付平台服务器,还用于在认证所述认证信息包括的指纹信息和用户终端标识分别与所述用户终端注册时登记的指纹信息和用户终端标识一致之后,以及所述根据所述订单信息进行支付操作之前,发送订单信息确认请求给所述用户终端,所述订单信息确认请求包括所述支付账号和支付金额;

所述用户终端,还用于接收所述支付平台服务器发送的所述订单信息确认请求,并将用户输入的针对所述订单信息确认请求的确认响应发送给所述支付平台服务器;

所述支付平台服务器,还用于在接收到所述用户终端发送的针对所述订单信息确认请求的确认响应后,执行所述的根据所述订单信息进行支付操作的步骤。

26. 根据权利要求 25 所述的系统,其特征在于,所述系统还包括交易平台服务器:

所述用户终端,用于发送订单信息至所述交易平台服务器;

所述交易平台服务器,用于将所述订单信息发送至所述支付平台服务器;

所述交易平台服务器,还用于在将所述订单信息发送至支付平台服务器之后,获取所述用户终端的历史支付金额,识别所述历史支付金额所属的金额范围,并识别所述历史支付金额所属的金额范围对应的折扣率,以及将所述折扣率发送至所述支付平台服务器;

所述支付平台服务器,还用于在接收到所述用户终端发送的针对所述订单信息确认请求的确认响应后,根据所述订单信息和所述折扣率进行支付折扣操作。

27. 根据权利要求 26 所述的系统,其特征在于,

所述交易平台服务器,还用于在将所述折扣率发送至所述支付平台服务器之后,根据所述订单信息包括的所述支付金额更新所述历史支付金额。

一种安全支付方法及相关设备、系统

技术领域

[0001] 本发明涉及互联网技术领域,具体涉及一种安全支付方法及相关设备、系统。

背景技术

[0002] 随着互联网技术的快速发展,利用智能手机(如 Android 手机、iOS 手机等)、平板电脑、掌上电脑以及移动互联网设备(Mobile Internet Devices, MID)、PAD 等用户终端进行在线支付已成为一种便捷、流行的支付方式。而在实际应用中,用户利用用户终端进行在线支付时,用户通常需要在用户终端上手动输入支付密码,以完成在线支付。在实践中发现,这种支付方式需要用户手动输入支付密码,使得支付操作比较繁琐,从而降低了在线支付效率;而且,手动输入支付密码容易导致支付密码泄露,降低支付安全性。

发明内容

[0003] 本发明实施例公开了一种安全支付方法及相关设备、系统,能够简化支付操作,提高在线支付效率,以及提高支付安全性。

[0004] 本发明实施例第一方面公开了一种安全支付方法,包括:

[0005] 用户终端发送订单信息至支付平台服务器,所述订单信息包括支付账号和支付金额;

[0006] 所述支付平台服务器接收所述用户终端发送的所述订单信息,并发送提示信息至所述用户终端,所述提示信息用于提示输入认证信息;

[0007] 所述用户终端接收所述支付平台服务器发送的所述提示信息,并将认证信息发送给所述支付平台服务器;其中,所述认证信息包括用户终端标识和用户响应所述提示信息输入的指纹信息;

[0008] 所述支付平台服务器接收所述用户终端发送的所述认证信息,并认证所述认证信息包括的指纹信息和用户终端标识是否分别与所述用户终端注册时登记的指纹信息和用户终端标识一致,若一致,根据所述订单信息进行支付操作。

[0009] 本发明实施例第二方面公开了一种安全支付方法,包括:

[0010] 用户终端发送订单信息至支付平台服务器,所述订单信息包括支付账号和支付金额;

[0011] 所述用户终端接收所述支付平台服务器发送的提示信息,所述提示信息用于提示输入认证信息;

[0012] 所述用户终端将认证信息发送给所述支付平台服务器,以使所述支付平台服务器认证所述认证信息包括的用户终端标识和用户响应所述提示信息输入的指纹信息分别与所述用户终端注册时登记的用户终端标识和指纹信息一致时,由所述支付平台服务器根据所述订单信息进行支付操作。

[0013] 本发明实施例第三方面公开了一种安全支付方法,包括:

[0014] 支付平台服务器接收用户终端发送的订单信息,所述订单信息包括支付账号和支

付金额；

[0015] 所述支付平台服务器发送提示信息至所述用户终端，所述提示信息用于提示输入认证信息；

[0016] 所述支付平台服务器接收所述用户终端发送的认证信息，所述认证信息包括用户终端标识和用户响应所述提示信息输入的指纹信息；

[0017] 所述支付平台服务器认证所述认证信息包括的指纹信息和用户终端标识是否分别与所述用户终端注册时登记的指纹信息和用户终端标识一致，若一致，根据所述订单信息进行支付操作。

[0018] 本发明实施例第四方面公开了一种计算机存储介质，所述计算机存储介质存储有程序，所述程序执行时包括本发明实施例第二方面公开的安全支付方法的全部步骤。

[0019] 本发明实施例第五方面公开了一种计算机存储介质，所述计算机存储介质存储有程序，所述程序执行时包括本发明实施例第三方面公开的安全支付方法的全部步骤。

[0020] 本发明实施例第六方面公开一种用户终端，包括：

[0021] 发送单元，用于发送订单信息至支付平台服务器，所述订单信息包括支付账号和支付金额；

[0022] 接收单元，用于接收所述支付平台服务器发送的提示信息，所述提示信息用于提示输入认证信息；

[0023] 所述发送单元，还用于将认证信息发送给所述支付平台服务器，以使所述支付平台服务器认证所述认证信息包括的用户终端标识和用户响应所述提示信息输入的指纹信息分别与所述用户终端注册时登记的用户终端标识和指纹信息一致时，由所述支付平台服务器根据所述订单信息进行支付操作。

[0024] 本发明实施例第七方面公开一种支付平台服务器，包括：

[0025] 接收单元，用于接收用户终端发送的订单信息，所述订单信息包括支付账号和支付金额；

[0026] 发送单元，用于发送提示信息至所述用户终端，所述提示信息用于提示输入认证信息；

[0027] 所述接收单元，还用于接收所述用户终端发送的认证信息，所述认证信息包括用户终端标识和用户响应所述提示信息输入的指纹信息；

[0028] 认证单元，用于认证所述认证信息包括的指纹信息和用户终端标识是否分别与所述用户终端注册时登记的指纹信息和用户终端标识一致；

[0029] 操作单元，用于在所述认证单元的认证结果为一致时，根据所述订单信息进行支付操作。

[0030] 本发明实施例第八方面公开一种安全支付系统，包括用户终端和支付平台服务器，其中：

[0031] 所述用户终端，用于发送订单信息至支付平台服务器，所述订单信息包括支付账号和支付金额；

[0032] 所述支付平台服务器，用于接收所述用户终端发送的所述订单信息，并发送提示信息至所述用户终端，所述提示信息用于提示输入认证信息；

[0033] 所述用户终端，还用于接收所述支付平台服务器发送的所述提示信息，并将认证

信息发送给所述支付平台服务器；其中，所述认证信息包括用户终端标识和用户响应所述提示信息输入的指纹信息；

[0034] 所述支付平台服务器，还用于接收所述用户终端发送的所述认证信息，并认证所述认证信息包括的指纹信息和用户终端标识是否分别与所述用户终端注册时登记的指纹信息和用户终端标识一致，若一致，根据所述订单信息进行支付操作。

[0035] 本发明实施例中，支付平台服务器接收到用户终端发送的订单信息后，可以发送用于提示输入认证信息的提示信息至用户终端，这样用户终端可以将认证信息发送至支付平台服务器，而该认证信息包括用户终端标识和用户响应该提示信息输入的指纹信息，使得支付平台服务器认证该认证信息包括的指纹信息和用户终端标识分别与用户终端注册时登记的指纹信息和用户终端标识一致时，可以根据订单信息进行支付操作。可见，本发明实施例可以根据指纹信息和用户终端标识进行双重安全认证，从而可以提高支付安全性；另外，本发明实施例省去了用户手动输入支付密码带来的繁琐操作，从而可以简化支付操作，提高在线支付效率。

附图说明

[0036] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例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。

[0037] 图 1 是本发明实施例公开的一种安全支付方法的流程图；

[0038] 图 2 是本发明实施例公开的一种用户终端提示用户在指纹输入区域内输入指纹信息的界面示意图；

[0039] 图 3 是本发明实施例公开的一种用户终端的订单信息确认请求的显示界面示意图；

[0040] 图 4 是本发明实施例公开的另一种安全支付方法的流程图；

[0041] 图 5 是本发明实施例公开的另一种安全支付方法的流程图；

[0042] 图 6 是本发明实施例公开的另一种安全支付方法的流程图；

[0043] 图 7 是本发明实施例公开的另一种安全支付方法的流程图；

[0044] 图 8 是本发明实施例公开的一种用户终端的结构图；

[0045] 图 9 是本发明实施例公开的另一种用户终端的结构图；

[0046] 图 10 是本发明实施例公开的一种支付平台服务器的结构图；

[0047] 图 11 是本发明实施例公开的另一种支付平台服务器的结构图；

[0048] 图 12 是本发明实施例公开的一种安全支付系统的结构图。

具体实施方式

[0049] 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，所描述的实施例仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做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。

[0050] 本发明实施例公开了一种安全支付方法及相关设备、系统,能够简化支付操作,提高在线支付效率,以及提高支付安全性。以下分别进行详细说明。

[0051] 请参阅图 1,图 1 是本发明实施例公开的一种安全支付方法的流程图。其中,图 1 所描述的安全支付方法主要是从用户终端一侧来进行描述的。如图 1 所示,该安全支付方法可以包括以下步骤。

[0052] S101、用户终端发送订单信息至支付平台服务器,其中,该订单信息包括支付账号和支付金额。

[0053] 本发明实施例中,支付账号是指付款账号。其中,订单信息中还可以包括订单号。

[0054] 本发明实施例中,用户终端包括智能手机(如 Android 手机、iOS 手机等)、平板电脑、掌上电脑以及移动互联网设备(MID)、PAD 等用户终端。

[0055] S102、用户终端接收支付平台服务器发送的提示信息,该提示信息用于提示输入认证信息。

[0056] 本发明实施例中,用户终端接收支付平台服务器发送的提示信息后,可以通过显示屏提示用户输入指纹信息。在一个实施例中,如图 2 所示,用户终端可以提示用户在指纹输入区域内输入指纹信息。

[0057] S103、用户终端将认证信息发送至支付平台服务器,以使支付平台服务器认证该认证信息包括的用户终端标识和用户响应该提示信息输入的指纹信息分别与用户终端注册时登记的用户终端标识和指纹信息一致时,由支付平台服务器根据订单信息进行支付操作。

[0058] 作为一种可选的实施方式,在图 1 所示的方法中,用户终端执行步骤 S101 之前,可以先执行以下步骤:

[0059] 11)、用户终端发送注册请求至支付平台服务器,该注册请求包括用户终端标识。

[0060] 本发明实施例中,用户终端标识可以包括用户终端的国际移动设备识别码(International Mobile Equipment Identification Number,IMEI),或者包括用户终端的其他能够表征身份信息的系统信息。

[0061] 12)、用户终端接收支付平台服务器发送的通知消息,该通知消息用于提示输入指纹信息。

[0062] 本发明实施例中,用户终端接收支付平台服务器发送的通知消息后,可以如图 2 所示提示用户在指纹输入区域内输入指纹信息。

[0063] 13)、用户终端将用户响应通知消息输入的指纹信息发送至支付平台服务器。

[0064] 14)、用户终端接收支付平台服务器发送的注册完成响应。

[0065] 其中,通过步骤 11)~步骤 14)可以完成用户终端在支付平台服务器上的注册,并且在注册过程中实现在支付平台服务器中登记指纹信息和用户终端标识,以便后续进行双重安全认证。

[0066] 作为一种可选的实施方式,在图 1 所示的方法中,用户终端将认证信息发送至支付平台服务器之后,还可以执行以下步骤:

[0067] 21)、用户终端接收支付平台服务器发送的订单信息确认请求,该订单信息确认请求包括支付账号和支付金额。

[0068] 22)、用户终端将用户输入的针对订单信息确认请求的确认响应发送至支付平台

服务器。

[0069] 其中,通过步骤 21)~步骤 22)可以提高支付的安全性。

[0070] 本发明实施例中,如 3 所示,用户终端可以输出支付平台服务器发送的订单信息确认请求,该订单信息确认请求可以包括支付金额“XXXX”以及支付账号“1234567899876543210”。相应地,用户可以点击如图 3 所示界面中的“确定”选项,从而可以输入针对订单信息确认请求的确认响应给用户终端,相应地用户终端可以发送针对订单信息确认请求的确认响应给交易平台服务器。

[0071] 作为一种可选的实施方式,在图 1 所示的方法中,用户终端发送订单信息至支付平台服务器的方式具体可以为:

[0072] 用户终端发送订单信息至交易平台服务器,由交易平台服务器将订单信息发送至支付平台服务器。其中,这种方式允许用户在下单过程中进行安全支付。

[0073] 当然,本发明实施例中,用户终端也可以直接发送订单信息至支付平台服务器,这种方式允许点对点支付(如刷手机支付)过程中进行安全支付。

[0074] 可见,图 1 所描述的方法可以根据指纹信息和用户终端标识进行双重安全认证,并且在双重安全认证之后再允许进行支付操作,从而可以提高支付安全性;另外,图 1 所描述的方法还省去了用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0075] 请参阅图 4,图 4 是本发明实施例公开的另一种安全支付方法的流程图。其中,图 4 所描述的安全支付方法主要是从支付平台服务器一侧来进行描述的。如图 4 所示,该安全支付方法可以包括以下步骤。

[0076] S401、支付平台服务器接收用户终端发送的订单信息,该订单信息包括支付账号和支付金额。

[0077] S402、支付平台服务器发送提示信息至用户终端,该提示信息用于提示输入认证信息。

[0078] S403、支付平台服务器接收用户终端发送的认证信息,该认证信息包括用户终端标识和用户响应该提示信息输入的指纹信息。

[0079] S404、支付平台服务器认证该认证信息包括的指纹信息和用户终端标识是否分别与用户终端注册时登记的指纹信息和用户终端标识一致,若一致,根据订单信息进行支付操作。

[0080] 本发明实施例中,支付平台服务器根据订单信息进行支付操作具体可以为:支付平台服务器可以从订单信息包括的支付账号中扣除订单信息包括的支付金额,并将该支付金额支付到相应的收款账号。

[0081] 作为一种可选的实施方式,在图 4 所描述的方法中,支付平台服务器执行步骤 S401 之前,还可以执行以下步骤:

[0082] 31)、支付平台服务器接收用户终端发送的注册请求,该注册请求包括用户终端标识。

[0083] 32)、支付平台服务器响应该注册请求,发送通知消息至用户终端,该通知消息用于提示输入指纹信息。

[0084] 33)、支付平台服务器接收用户终端发送的指纹信息,并存储用户终端发送的指纹

信息以及注册请求包括的用户终端标识。

[0085] 34)、支付平台服务器发送注册完成响应至用户终端。

[0086] 其中,通过步骤 31)~步骤 34)可以完成用户终端在支付平台服务器上的注册,并且在注册过程中实现在支付平台服务器中登记指纹信息和用户终端标识,以便后续进行双重安全认证。

[0087] 作为一种可选的实施方式,在图 4 所描述的方法中,支付平台服务器认证该认证信息包括的指纹信息和用户终端标识分别与用户终端注册时登记的指纹信息和用户终端标识一致之后,以及根据订单信息进行支付操作之前,法还可以执行以下步骤:

[0088] 41)、支付平台服务器发送订单信息确认请求给用户终端,该订单信息确认请求包括该支付账号和支付金额。

[0089] 42)、支付平台服务器接收到用户终端发送的针对该订单信息确认请求的确认响应后,执行根据订单信息进行支付操作的步骤。

[0090] 其中,通过步骤 41)~步骤 42)可以提高支付的安全性。

[0091] 作为一种可选的实施方式,在图 4 所描述的方法中,支付平台服务器接收用户终端发送的订单信息的方式具体可以为:

[0092] 支付平台服务器接收用户终端通过交易平台服务器发送的订单信息;

[0093] 进一步地,图 4 所描述的方法还可以包括以下步骤:

[0094] 51)、支付平台服务器接收交易平台服务器发送的该用户终端的历史支付金额所属的金额范围对应的折扣率。

[0095] 52)、支付平台服务器根据该订单信息和该折扣率进行支付折扣操作。

[0096] 其中,通过步骤 51)~步骤 52)可以实现支付折扣操作,从而可以有利于刺激交易消费。

[0097] 可见,图 2 所描述的方法可以根据指纹信息和用户终端标识进行双重安全认证,并且在双重安全认证之后再允许进行支付操作,从而提高支付安全性;另外,图 2 所描述的方法还省去了用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0098] 请参阅图 5,图 5 是本发明实施例公开的另一种安全支付方法的流程图。其中,图 5 所描述的安全支付方法主要是从用户终端和支付平台服务器两侧来进行描述的。如图 5 所示,该安全支付方法可以包括以下步骤。

[0099] S501、用户终端发送订单信息至支付平台服务器,该订单信息包括支付账号和支付金额。

[0100] S502、支付平台服务器接收用户终端发送的订单信息,并发送提示信息至用户终端,该提示信息用于提示输入认证信息。

[0101] S503、用户终端接收支付平台服务器发送的提示信息,并将认证信息发送至支付平台服务器;其中,认证信息包括用户终端标识以及用户响应该提示信息输入的指纹信息。

[0102] S504、支付平台服务器接收用户终端发送的认证信息,并认证该认证信息包括的指纹信息和用户终端标识是否分别与用户终端注册时登记的指纹信息和用户终端标识一致,若一致,根据订单信息进行支付操作。

[0103] 可见,图 5 所描述的方法可以根据指纹信息和用户终端标识进行双重安全认证,

并且在双重安全认证之后再允许进行支付操作,从而可以提高支付安全性;另外,图 2 所描述的方法还省去了用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0104] 请参阅图 6,图 6 是本发明实施例公开的另一种安全支付方法的流程图。其中,图 6 所描述的安全支付方法主要是从用户终端和支付平台服务器两侧来进行描述的。如图 6 所示,该安全支付方法可以包括以下步骤。

[0105] S601、用户终端发送注册请求至支付平台服务器,该注册请求包括用户终端标识。

[0106] S602、支付平台服务器响应该注册请求,发送通知消息至用户终端,该通知消息用于提示输入指纹信息。

[0107] S603、用户终端接收支付平台服务器发送的该通知消息,并将用户响应通知消息输入的指纹信息发送至支付平台服务器。

[0108] S604、支付平台服务器存储用户终端发送的指纹信息以及注册请求包括的用户终端标识。

[0109] S605、支付平台服务器发送注册完成响应至用户终端。

[0110] S606、用户终端发送订单信息至支付平台服务器,该订单信息包括支付账号和支付金额。

[0111] S607、支付平台服务器接收用户终端发送的订单信息,并发送提示信息至用户终端,该提示信息用于提示输入认证信息。

[0112] S608、用户终端接收支付平台服务器发送的提示信息,并将认证信息发送至支付平台服务器;其中,认证信息包括用户终端标识和用户响应该提示信息输入的指纹信息。

[0113] S609、支付平台服务器接收用户终端发送的认证信息,并认证该认证信息包括的指纹信息和用户终端标识是否分别与用户终端注册时登记的指纹信息和用户终端标识一致,若一致,发送订单信息确认请求给用户终端,该订单信息确认请求包括所述支付账号和支付金额。

[0114] S610、用户终端接收支付平台服务器发送的订单信息确认请求,并将用户输入的针对该订单信息确认请求的确认响应发送至支付平台服务器。

[0115] S611、支付平台服务器接收到用户终端发送的针对该订单信息确认请求的确认响应后,根据订单信息进行支付操作。

[0116] S612、支付平台服务器发送支付操作结果至用户终端。

[0117] 可见,图 6 所描述的方法可以根据指纹信息和用户终端标识进行双重安全认证,并且在双重安全认证之后再允许进行支付操作,从而可以提高支付安全性;另外,图 6 所描述的方法还省去了用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0118] 请参阅图 7,图 7 是本发明实施例公开的另一种安全支付方法的流程图。其中,图 7 所描述的安全支付方法主要是从用户终端、交易平台服务器以及支付平台服务器两侧来进行描述的。如图 7 所示,该安全支付方法可以包括以下步骤。

[0119] S701、用户终端发送注册请求至支付平台服务器,该注册请求包括用户终端标识。

[0120] S702、支付平台服务器响应该注册请求,发送通知消息至用户终端,该通知消息用于提示输入指纹信息。

[0121] S703、用户终端接收支付平台服务器发送的该通知消息，并将用户响应通知消息输入的指纹信息发送至支付平台服务器。

[0122] S704、支付平台服务器存储用户终端发送的指纹信息以及注册请求包括的用户终端标识。

[0123] S705、支付平台服务器发送注册完成响应至用户终端。

[0124] S706、用户终端发送订单信息至交易平台服务器，该订单信息包括支付账号和支付金额。

[0125] S707、交易平台服务器将该订单信息发送至支付平台服务器。

[0126] S708、支付平台服务器接收支付平台服务器发送的订单信息，并发送提示信息至用户终端，该提示信息用于提示输入认证信息。

[0127] S709、交易平台服务器获取用户终端的历史支付金额。

[0128] S710、交易平台服务器识别历史支付金额所属的金额范围，并识别历史支付金额所属的金额范围对应的折扣率。

[0129] S711、交易平台服务器将折扣率发送至支付平台服务器。

[0130] S712、交易平台服务器根据订单信息包括的支付金额更新历史支付金额。

[0131] 本发明实施例中，交易平台服务器可以将订单信息包括的支付金额与历史支付金额进行累加，累计值作为新的历史支付金额。

[0132] S713、用户终端接收支付平台服务器发送的提示信息，并将认证信息发送给支付平台服务器；其中，认证信息包括用户终端标识和用户响应该提示信息输入的指纹信息。

[0133] S714、支付平台服务器接收用户终端发送的认证信息，并认证该认证信息包括的指纹信息和用户终端标识是否分别与用户终端注册时登记的指纹信息和用户终端标识一致，若一致，发送订单信息确认请求给用户终端，该订单信息确认请求包括所述支付账号和支付金额。

[0134] S715、用户终端接收支付平台服务器发送的订单信息确认请求，并将用户输入的针对该订单信息确认请求的确认响应发送给支付平台服务器。

[0135] S716、支付平台服务器接收到用户终端发送的针对该订单信息确认请求的确认响应后，根据订单信息和折扣率进行支付折扣操作。

[0136] S717、支付平台服务器发送支付折扣操作结果至用户终端。

[0137] 本发明实施例中，上述步骤 S709～步骤 S712 只要位于步骤 S707 之后以及位于步骤 S716 之前即可，本发明实施例不作限定。

[0138] 可见，图 7 所描述的方法可以根据指纹信息和用户终端标识进行双重安全认证，并且在双重安全认证之后再允许进行支付操作，从而可以提高支付安全性；另外，图 7 所描述的方法还省去了用户手动输入支付密码带来的繁琐操作，从而可以简化支付操作，提高在线支付效率。

[0139] 请参阅图 8，图 8 是本发明实施例公开的一种用户终端的结构图。其中，如图 8 所示，该用户终端 800 可以包括：

[0140] 发送单元 801，用于发送订单信息至支付平台服务器，该订单信息包括支付账号和支付金额；

[0141] 接收单元 802，用于接收支付平台服务器发送的提示信息，该提示信息用于提示输

入认证信息；

[0142] 发送单元 801,还用于将认证信息发送给支付平台服务器,以使支付平台服务器认证该认证信息包括的用户终端标识和用户响应该提示信息输入的指纹信息分别与用户终端注册时登记的用户终端标识和指纹信息一致时,由支付平台服务器根据订单信息进行支付操作。

[0143] 在一个实施例中,发送单元 801 还用于在发送订单信息至支付平台服务器之前,发送注册请求至支付平台服务器,该注册请求包括用户终端标识；

[0144] 相应地,接收单元 802 还用于接收支付平台服务器发送的通知消息,该通知消息用于提示输入指纹信息；

[0145] 相应地,发送单元 801 还用于将用户响应通知消息输入的指纹信息发送给支付平台服务器；

[0146] 相应地,接收单元 802 还用于接收支付平台服务器发送的注册完成响应。

[0147] 本发明实施例中,接收单元 802 还用于在发送单元 801 将认证信息发送至支付平台服务器之后,接收支付平台服务器发送的订单信息确认请求,该订单信息确认请求包括该支付账号和支付金额；

[0148] 相应地,发送单元 801 还用于将用户输入的针对订单信息确认请求的确认响应发送至支付平台服务器。

[0149] 可见,通过实施例图 8 所描述的用户终端,可以实现根据指纹信息和用户终端标识进行双重安全认证,并且在双重安全认证之后再允许进行支付操作,从而可以提高支付安全性；另外,图 8 所描述的用户终端还省去了用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0150] 请参阅图 9,图 9 是本发明实施例公开的另一种用户终端的结构图。其中,如图 9 所示,该用户终端 900 可以包括：至少一个处理器 9001,例如 CPU,至少一个网络接口 9004,用户接口 9003,存储器 9005,至少一个通信总线 9002 以及显示屏 9006。其中,通信总线 9002 用于实现这些组件之间的连接通信。其中,用户接口 9003 可以包括显示屏(Display)、键盘(Keyboard),可选用户接口 9003 还可以包括标准的有线接口、无线接口。网络接口 9004 可选的可以包括标准的有线接口、无线接口(如 WI-FI 接口)。存储器 9005 可以是高速 RAM 存储器,也可以是非不稳定的存储器(non-volatile memory),例如至少一个磁盘存储器。存储器 9005 可选的还可以是至少一个位于远离前述处理器 9001 的存储装置。如图 9 所示,作为一种计算机存储介质的存储器 9005 中可以包括操作系统、网络通信模块、用户接口模块以及安全支付应用程序。

[0151] 在图 9 所示的用户终端 9000 中,网络接口 9004 主要用于连接交易平台服务器、支付平台服务器,与交易平台服务器、支付平台服务器进行数据通信；而处理器 9001 可以用于调用存储器 9005 中存储的安全支付应用程序,并执行以下操作：

[0152] 通过网络接口 9004 发送订单信息至支付平台服务器,该订单信息包括支付账号和支付金额；

[0153] 通过网络接口 9004 接收支付平台服务器发送的提示信息,该提示信息用于提示输入认证信息；

[0154] 通过网络接口 9004 将认证信息发送至支付平台服务器,以使支付平台服务器认

证该认证信息包括的用户终端标识和用户响应该提示信息输入(如通过显示屏 9006 输入)的指纹信息分别与用户终端注册时登记的用户终端标识和指纹信息一致时,由支付平台服务器根据该订单信息进行支付操作。

[0155] 在一个实施例中,处理器 9001 调用存储器 9005 中存储的安全支付应用程序还可以执行以下操作:

[0156] 通过网络接口 9004 发送订单信息至支付平台服务器之前,通过网络接口 9004 发送注册请求至支付平台服务器,注册请求包括用户终端标识;

[0157] 通过网络接口 9004 接收支付平台服务器发送的通知消息,通知消息用于提示输入指纹信息;

[0158] 通过网络接口 9004 将用户响应通知消息输入的指纹信息发送至支付平台服务器;

[0159] 通过网络接口 9004 接收支付平台服务器发送的注册完成响应。

[0160] 在一个实施例中,处理器 9001 调用存储器 9005 中存储的安全支付应用程序还可以执行以下操作:

[0161] 通过网络接口 9004 将认证信息发送至支付平台服务器之后,通过网络接口 9004 接收支付平台服务器发送的订单信息确认请求,订单信息确认请求包括支付账号和支付金额;

[0162] 以及,通过网络接口 9004 将用户输入的针对订单信息确认请求的确认响应发送至支付平台服务器。

[0163] 本发明实施例中,处理器 9001 通过网络接口 9004 发送订单信息至支付平台服务器包括:

[0164] 处理器 9001 通过网络接口 9004 发送订单信息至交易平台服务器,由交易平台服务器将订单信息发送至支付平台服务器。

[0165] 可见,通过实施例图 9 所描述的用户终端,可以实现根据指纹信息和用户终端标识进行双重安全认证,并且在双重安全认证之后再允许进行支付操作,从而提高支付安全性;另外,图 9 所描述的用户终端还省去了用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0166] 请参阅图 10,图 10 是本发明实施例公开的一种支付平台服务器的结构图。如图 10 所示,该支付平台服务器 1000 包括:

[0167] 接收单元 1001,用于接收用户终端发送的订单信息,该订单信息包括支付账号和支付金额;

[0168] 发送单元 1002,用于发送提示信息至用户终端,该提示信息用于提示输入认证信息;

[0169] 接收单元 1001,还用于接收用户终端发送的认证信息,该认证信息包括用户终端标识和用户响应该提示信息输入的指纹信息;

[0170] 认证单元 1003,用于认证该认证信息包括的指纹信息和用户终端标识是否分别与用户终端注册时登记的指纹信息和用户终端标识一致;

[0171] 操作单元 1004,用于在认证单元 1003 的认证结果为一致时,根据订单信息进行支付操作。

[0172] 在一个实施例中,接收单元 1001 还用于在接收用户终端发送的订单信息之前,接收用户终端发送的注册请求,该注册请求包括用户终端标识;

[0173] 相应地,发送单元 1002 还用于响应接收单元 1001 接收到的注册请求,发送通知消息至用户终端,该通知消息用于提示输入指纹信息;

[0174] 相应地,接收单元 1001 还用于接收用户终端发送的指纹信息;

[0175] 相应地,支付平台服务器 1000 还包括;

[0176] 存储单元 1005,用于存储用户终端发送的指纹信息以及该注册请求包括的用户终端标识;

[0177] 相应地,发送单元 1002 还用于发送注册完成响应至用户终端。

[0178] 本发明实施例中,认证单元 1003 具体用于认证该认证信息包括的指纹信息和用户终端标识是否分别与存储单元 1005 存储的用户终端注册时登记的指纹信息和用户终端标识一致。

[0179] 在一个实施例中,发送单元 1002 还用于在认证单元 1003 认证该认证信息包括的指纹信息和用户终端标识分别与用户终端注册时登记的指纹信息和用户终端标识一致之后,发送订单信息确认请求给用户终端,该订单信息确认请求包括支付账号和支付金额;

[0180] 相应地,接收单元 1001 还用于接收到用户终端发送的针对订单信息确认请求的确认响应后,触发操作单元 1004 执行根据订单信息进行支付操作的步骤。

[0181] 在一个实施例中,接收单元 1001 接收用户终端发送的订单信息的方式具体为:

[0182] 接收单元 1001,用于接收用户终端通过交易平台服务器发送的订单信息;

[0183] 进一步地,接收单元 1001 还用于接收到交易平台服务器发送的用户终端的历史支付金额所属的金额范围对应的折扣率;

[0184] 相应地,操作单元 1004 还用于根据该订单信息和该折扣率进行支付折扣操作。

[0185] 可见,通过实施例图 10 所描述的支付平台服务器,可以实现根据指纹信息和用户终端标识进行双重安全认证,并且在双重安全认证之后再允许进行支付操作,从而可以提高支付安全性;另外,利用图 10 所描述的支付平台服务器还使得用户终端可以省去用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0186] 请参阅图 11,图 11 是本发明实施例公开的另一种支付平台服务器的结构图。如图 11 所示,该支付平台服务器 1100 包括:至少一个处理器 1101,例如 CPU,至少一个网络接口 1104,用户接口 1103,存储器 1105,至少一个通信总线 1102。其中,通信总线 1102 用于实现这些组件之间的连接通信。其中,用户接口 1103 可以包括显示屏(Display)、键盘(Keyboard),可选用户接口 1103 还可以包括标准的有线接口、无线接口。网络接口 1104 可选的可以包括标准的有线接口、无线接口(如 WI-FI 接口)。存储器 1105 可以是高速 RAM 存储器,也可以是非不稳定的存储器(non-volatile memory),例如至少一个磁盘存储器。存储器 1105 可选的还可以是至少一个位于远离前述处理器 1101 的存储装置。如图 11 所示,作为一种计算机存储介质的存储器 1105 中可以包括操作系统、网络通信模块、用户接口模块以及在线支付应用程序。

[0187] 在图 11 所示的支付平台服务器 1100 中,网络接口 1104 主要用于连接用户终端,与用户终端进行数据通信;而处理器 1101 可以用于调用存储器 1105 中存储的安全支付应用程序,并执行以下操作:

[0188] 通过网络接口 1104 接收用户终端发送的订单信息,该订单信息包括支付账号和支付金额;

[0189] 通过网络接口 1104 发送提示信息至用户终端,提示信息用于提示输入认证信息;

[0190] 通过网络接口 1104 接收用户终端发送的认证信息,该认证信息包括用户终端标识和用户响应该提示信息输入的指纹信息;

[0191] 以及,认证该认证信息包括的指纹信息和用户终端标识是否分别与用户终端注册时登记的指纹信息和用户终端标识一致,若一致,根据订单信息进行支付操作。

[0192] 在一个实施例中,处理器 1101 调用存储器 1105 中存储的安全支付应用程序还可以执行以下操作:

[0193] 通过网络接口 1104 接收用户终端发送的订单信息之前,通过网络接口 1104 接收用户终端发送的注册请求,该注册请求包括用户终端标识;

[0194] 响应注册请求,通过网络接口 1104 发送通知消息至用户终端,通知消息用于提示输入指纹信息;

[0195] 通过网络接口 1104 接收用户终端发送的指纹信息,并存储(如存储至存储器 1105)用户终端发送的指纹信息以及注册请求包括的用户终端标识;

[0196] 通过网络接口 1104 发送注册完成响应至用户终端。

[0197] 在一个实施例中,处理器 1101 调用存储器 1105 中存储的安全支付应用程序还可以执行以下操作:

[0198] 认证该认证信息包括的指纹信息和用户终端标识分别与用户终端注册时登记的指纹信息和用户终端标识一致之后,以及根据订单信息进行支付操作之前,通过网络接口 1104 发送订单信息确认请求给用户终端,订单信息确认请求包括支付账号和支付金额;

[0199] 以及,通过网络接口 1104 接收到用户终端发送的针对订单信息确认请求的确认响应后,执行根据订单信息进行支付操作的步骤。

[0200] 在一个实施例中,处理器 1101 通过网络接口 1104 接收用户终端发送的订单信息包括:

[0201] 处理器 1101 通过网络接口 1104 接收用户终端通过交易平台服务器发送的订单信息;

[0202] 进一步地,处理器 1101 调用存储器 1105 中存储的安全支付应用程序还可以执行以下操作:

[0203] 通过网络接口 1104 接收交易平台服务器发送的用户终端的历史支付金额所属的金额范围对应的折扣率;

[0204] 根据订单信息和折扣率进行支付折扣操作。

[0205] 可见,通过实施例图 11 所描述的支付平台服务器,可以实现根据指纹信息和用户终端标识进行双重安全认证,并且在双重安全认证之后再允许进行支付操作,从而提高支付安全性;另外,利用图 10 所描述的支付平台服务器还使得用户终端可以省去用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0206] 请参阅图 12,图 12 是本发明实施例公开的一种安全支付系统的结构图。如图 12 所示,该安全支付系统可以包括用户终端 1201 和支付平台服务器 1202,其中,用户终端 1201 可以通过网络连接支付平台服务器 1202,其中:

[0207] 用户终端 1201, 用于发送订单信息至支付平台服务器 1202, 该订单信息包括支付账号和支付金额;

[0208] 支付平台服务器 1202, 用于接收用户终端 1201 发送的订单信息, 并发送提示信息至用户终端 1201, 该提示信息用于提示输入认证信息;

[0209] 用户终端 1201, 还用于接收支付平台服务器 1202 发送的提示信息, 并将认证信息发送至支付平台服务器 1202; 其中, 认证信息包括用户终端标识和用户响应提示信息输入的指纹信息;

[0210] 支付平台服务器 1202, 还用于接收用户终端 1201 发送的认证信息, 并认证该认证信息包括的指纹信息和用户终端标识是否分别与用户终端 1201 注册时登记的指纹信息和用户终端标识一致, 若一致, 根据订单信息进行支付操作。

[0211] 在一个实施例中, 用户终端 1201 还用于在发送订单信息至支付平台服务器 1202 之前, 发送注册请求至支付平台服务器 1202, 该注册请求包括用户终端标识;

[0212] 相应地, 支付平台服务器 1202 还用于响应该注册请求, 发送通知消息至用户终端 1201, 通知消息用于提示输入指纹信息;

[0213] 相应地, 用户终端 1201 还用于接收支付平台服务器 1202 发送的通知消息, 并将用户响应该通知消息输入的指纹信息发送至支付平台服务器 1202;

[0214] 相应地, 支付平台服务器 1202 还用于存储用户终端 1201 发送的指纹信息以及注册请求包括的用户终端标识;

[0215] 相应地, 支付平台服务器 1202 还用于发送注册完成响应至用户终端 1201;

[0216] 相应地, 用户终端 1201 还用于接收支付平台服务器 1202 发送的注册完成响应。

[0217] 在一个实施例中, 支付平台服务器 1202 还用于在认证该认证信息包括的指纹信息和用户终端标识分别与用户终端 1201 注册时登记的指纹信息和用户终端标识一致之后, 以及根据订单信息进行支付操作之前, 发送订单信息确认请求给用户终端 1201, 订单信息确认请求包括支付账号和支付金额;

[0218] 相应地, 用户终端 1201 还用于接收支付平台服务器 1202 发送的订单信息确认请求, 并将用户输入的针对该订单信息确认请求的确认响应发送至支付平台服务器 1202;

[0219] 相应地, 支付平台服务器 1202 还用于在接收到用户终端 1201 发送的针对该订单信息确认请求的确认响应后, 执行根据订单信息进行支付操作的步骤。

[0220] 在一个实施例中, 图 12 所示的安全支付系统还包括交易平台服务器 1203, 其中:

[0221] 用户终端 1201, 用于发送订单信息至交易平台服务器 1203;

[0222] 交易平台服务器 1203, 用于将该订单信息发送至支付平台服务器 1202;

[0223] 交易平台服务器 1203, 还用于获取用户终端 1201 的历史支付金额, 识别历史支付金额所属的金额范围, 并识别历史支付金额所属的金额范围对应的折扣率, 以及将折扣率发送至支付平台服务器 1202;

[0224] 相应地, 支付平台服务器 1202 还用于在接收到用户终端 1201 发送的针对订单信息确认请求的确认响应后, 根据订单信息和折扣率进行支付折扣操作。

[0225] 本发明实施例中, 交易平台服务器 1203 还用于在将折扣率发送至支付平台服务器 1202 之后, 根据订单信息包括的支付金额更新历史支付金额。

[0226] 可见, 通过实施例图 12 所描述的安全支付系统, 可以实现根据指纹信息和用户终

端标识进行双重安全认证,并且在双重安全认证之后再允许进行支付操作,从而可以提高支付安全性;另外,利用图 12 所描述的安全支付系统还使得用户终端可以省去用户手动输入支付密码带来的繁琐操作,从而可以简化支付操作,提高在线支付效率。

[0227] 本领域普通技术人员可以理解图 1 所示方法中的全部或部分步骤是可以通过程序来指令用户终端相关的硬件来完成,该程序可以存储于用户终端的一计算机可读存储介质中,存储介质可以包括:闪存盘、只读存储器(Read-Only Memory, ROM)、随机存取器(Random Access Memory, RAM)、磁盘或光盘等。

[0228] 本领域普通技术人员可以理解图 4 所示方法中的全部或部分步骤是可以通过程序来指令支付平台服务器相关的硬件来完成,该程序可以存储于支付平台服务器的一计算机可读存储介质中,存储介质可以包括:闪存盘、只读存储器(Read-Only Memory, ROM)、随机存取器(Random Access Memory, RAM)、磁盘或光盘等。

[0229] 以上对本发明实施例公开的一种安全支付方法及相关设备、系统进行了详细介绍,本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

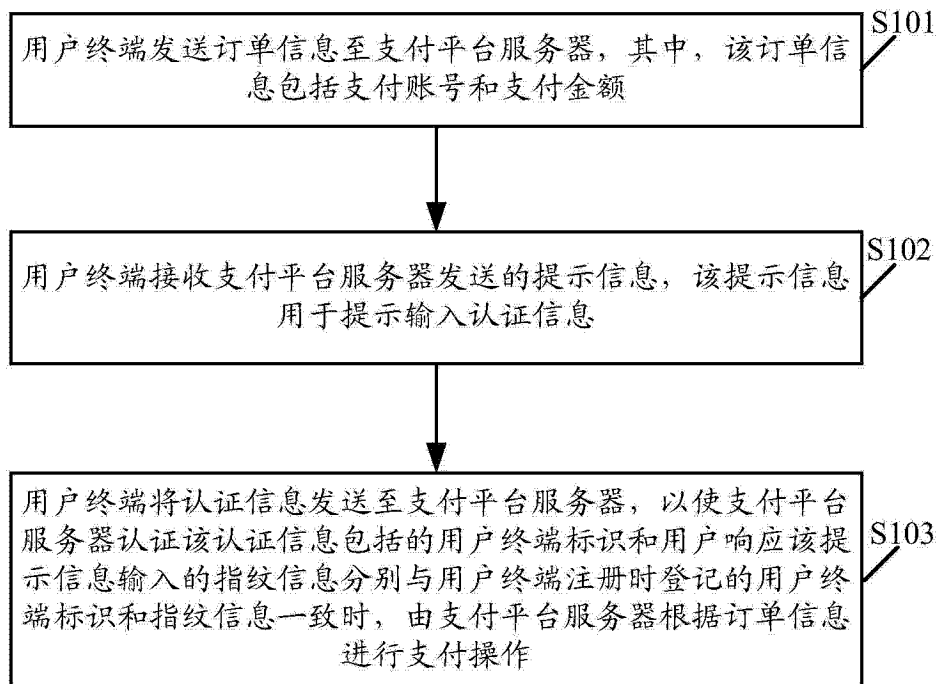


图 1

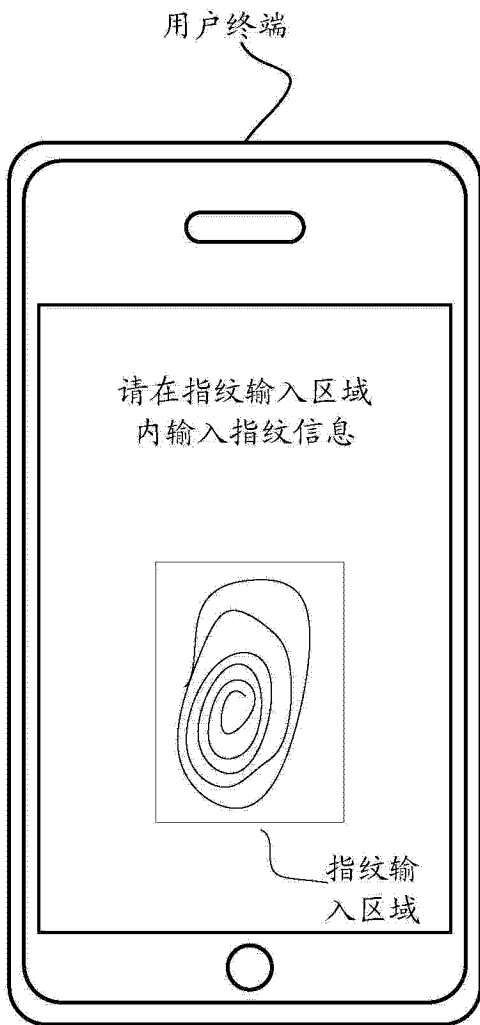


图 2



图 3

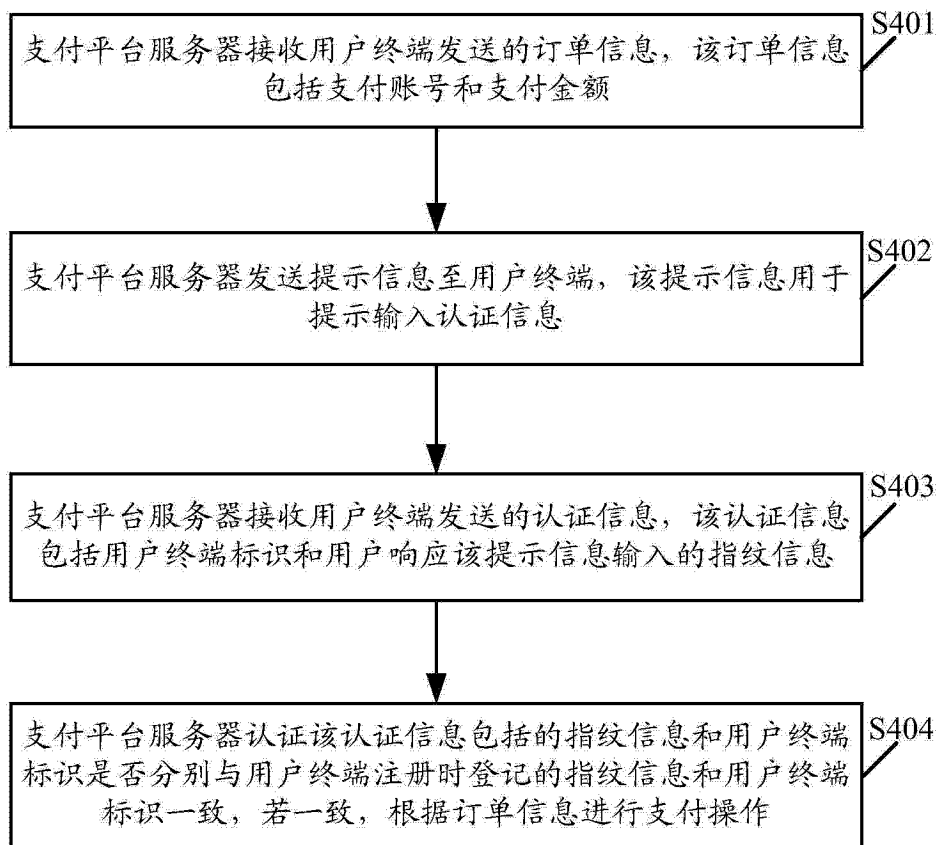


图 4

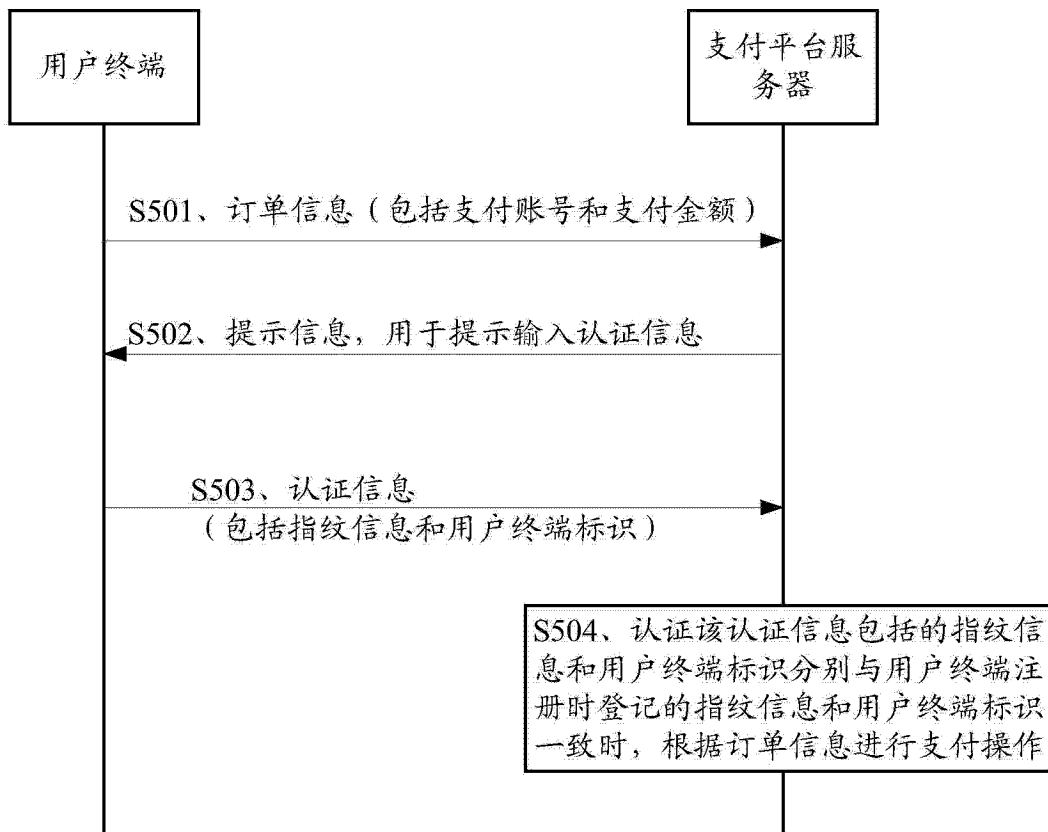


图 5

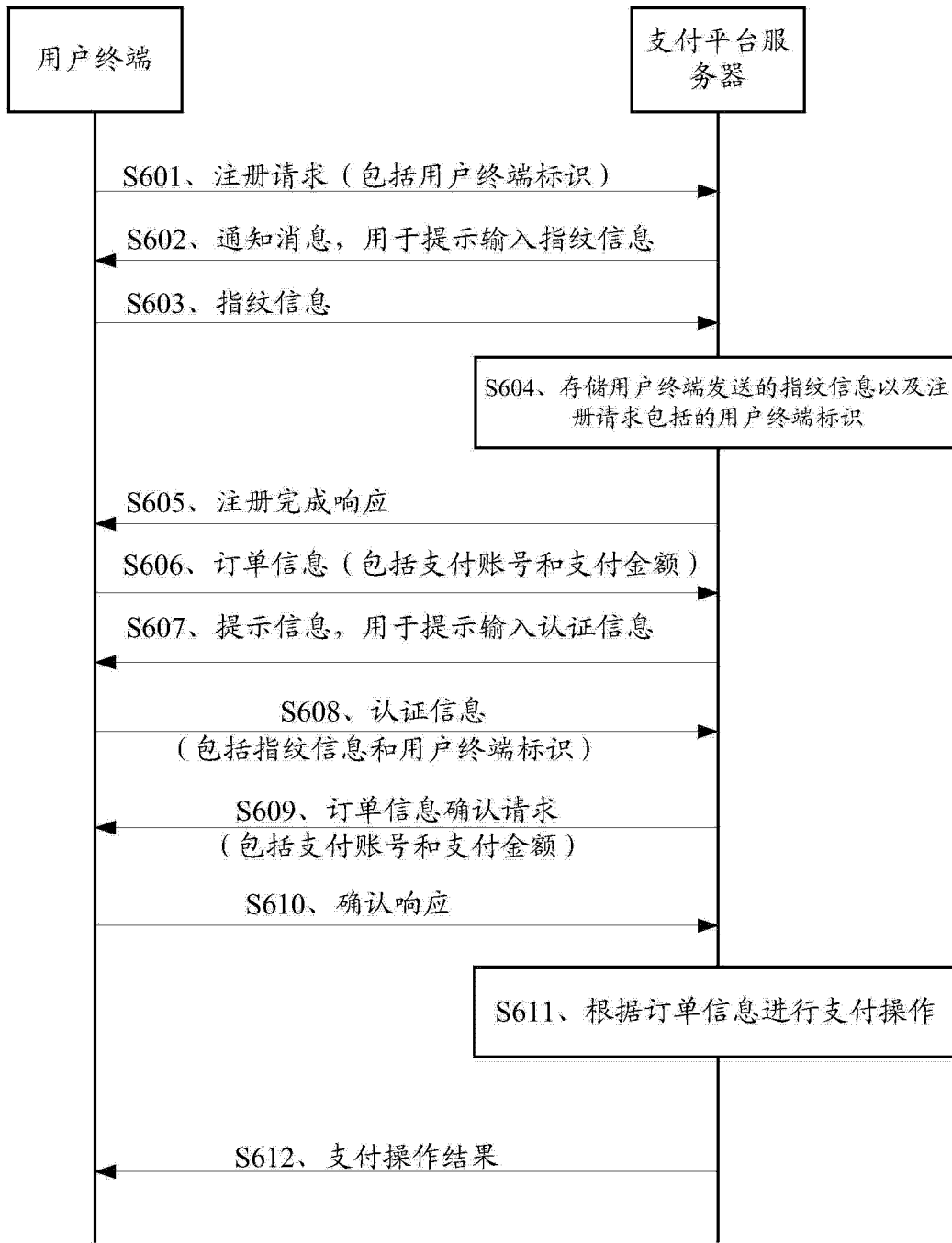


图 6

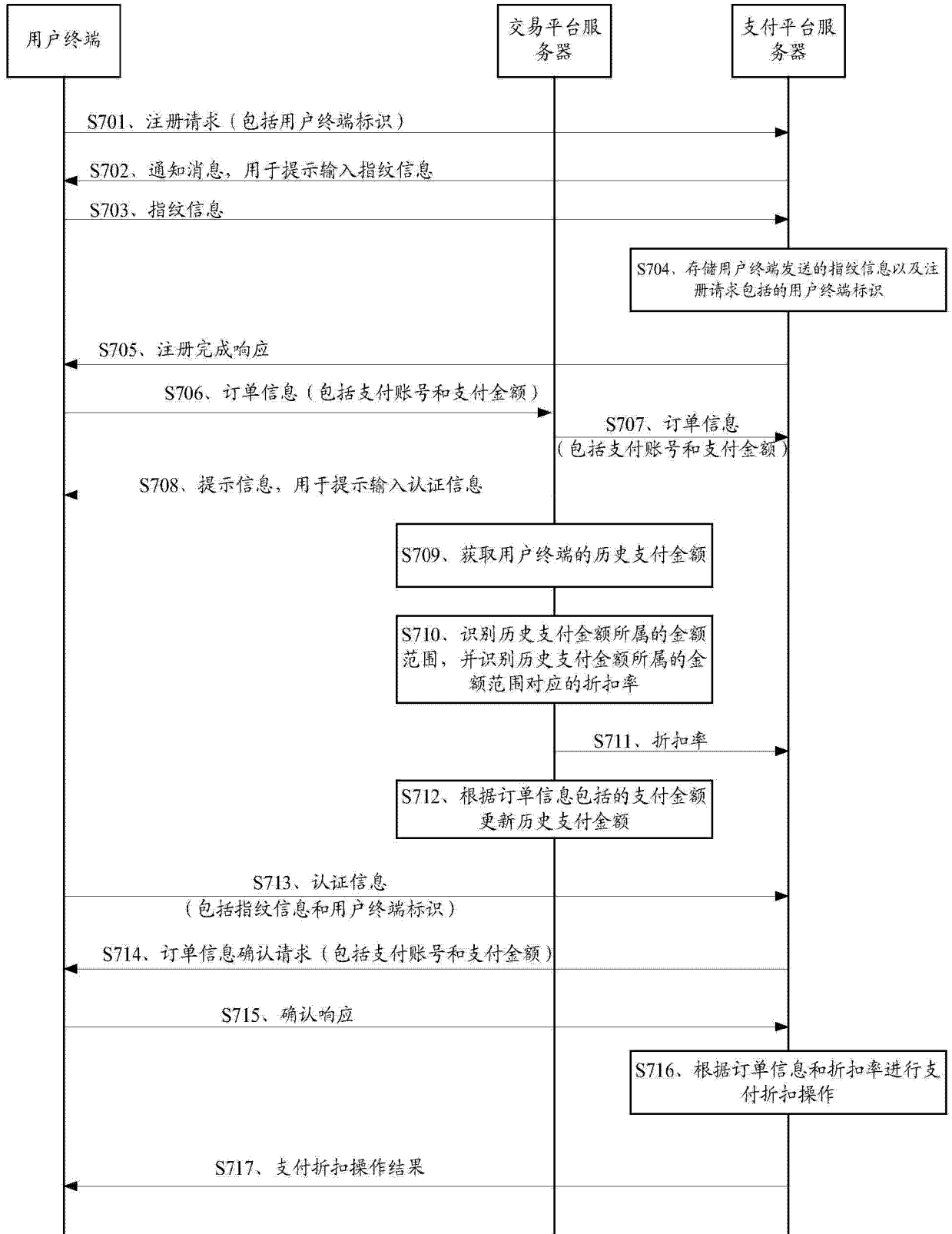


图 7

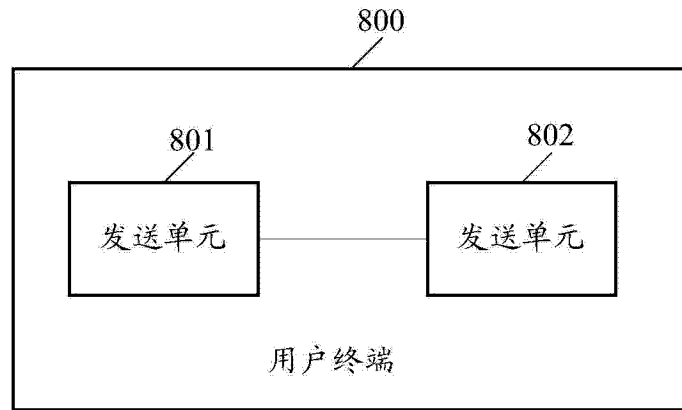


图 8

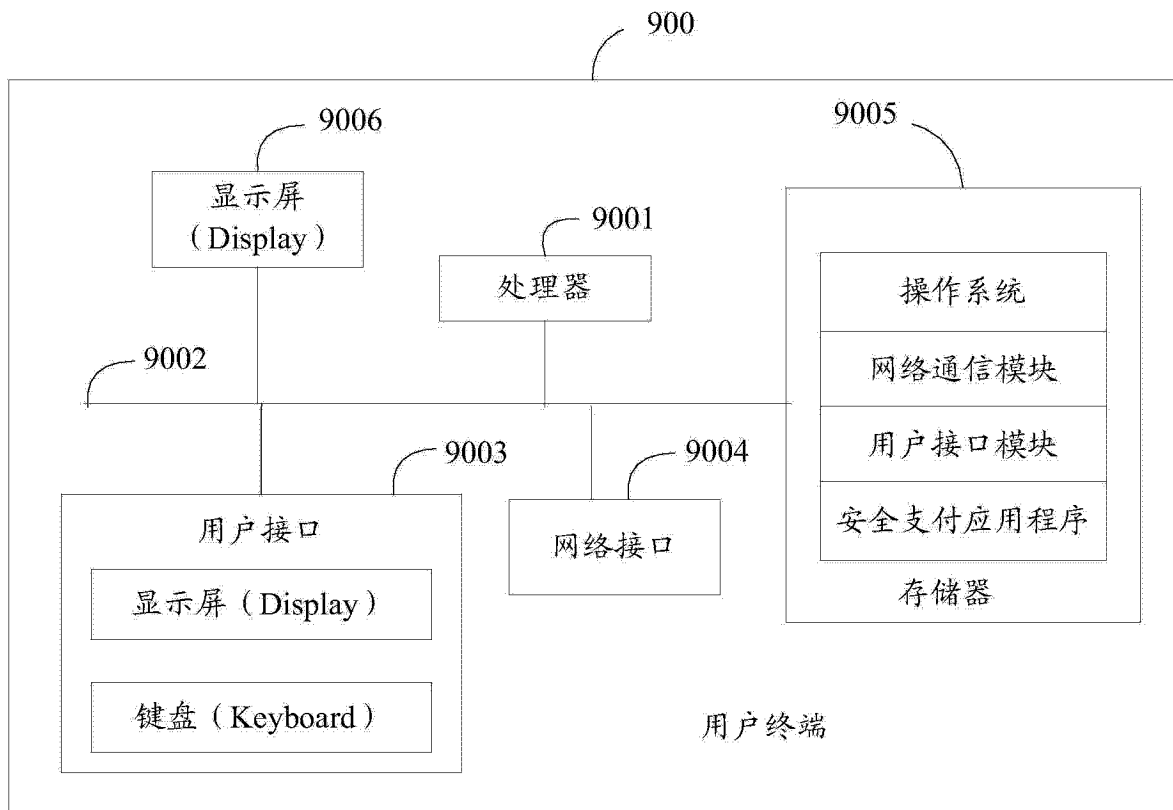


图 9

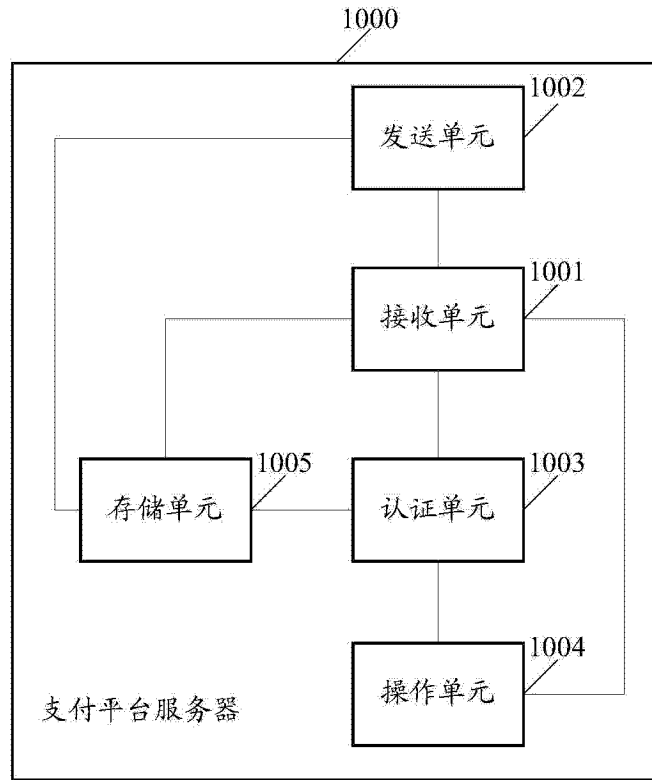


图 10

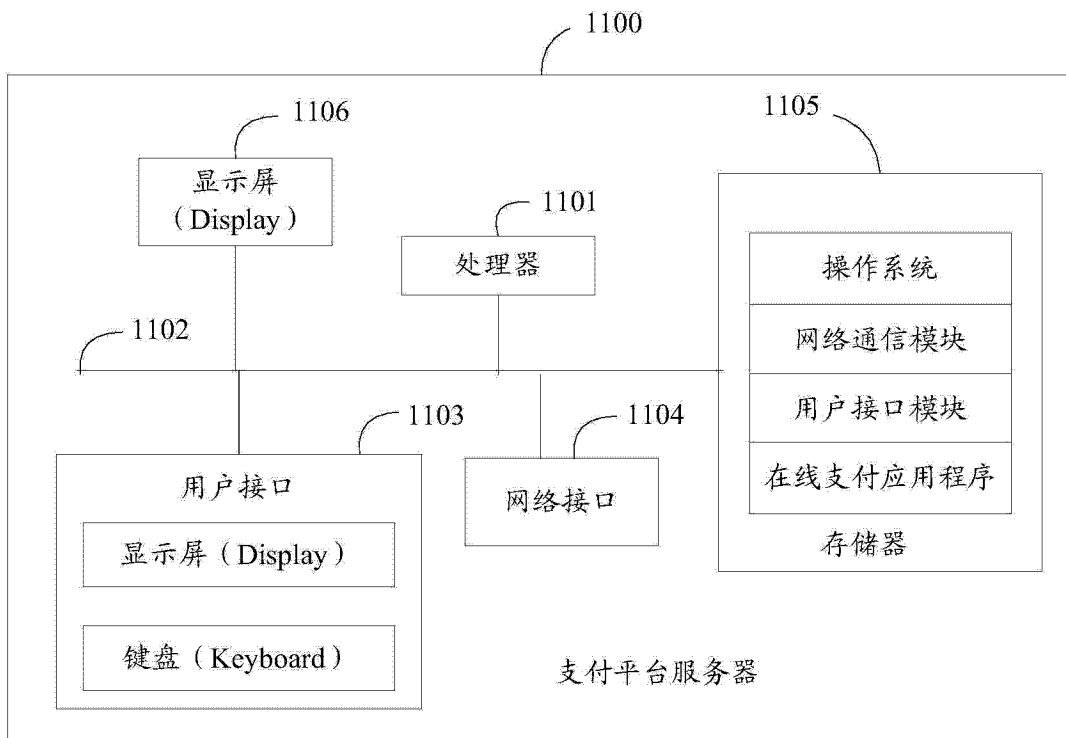


图 11

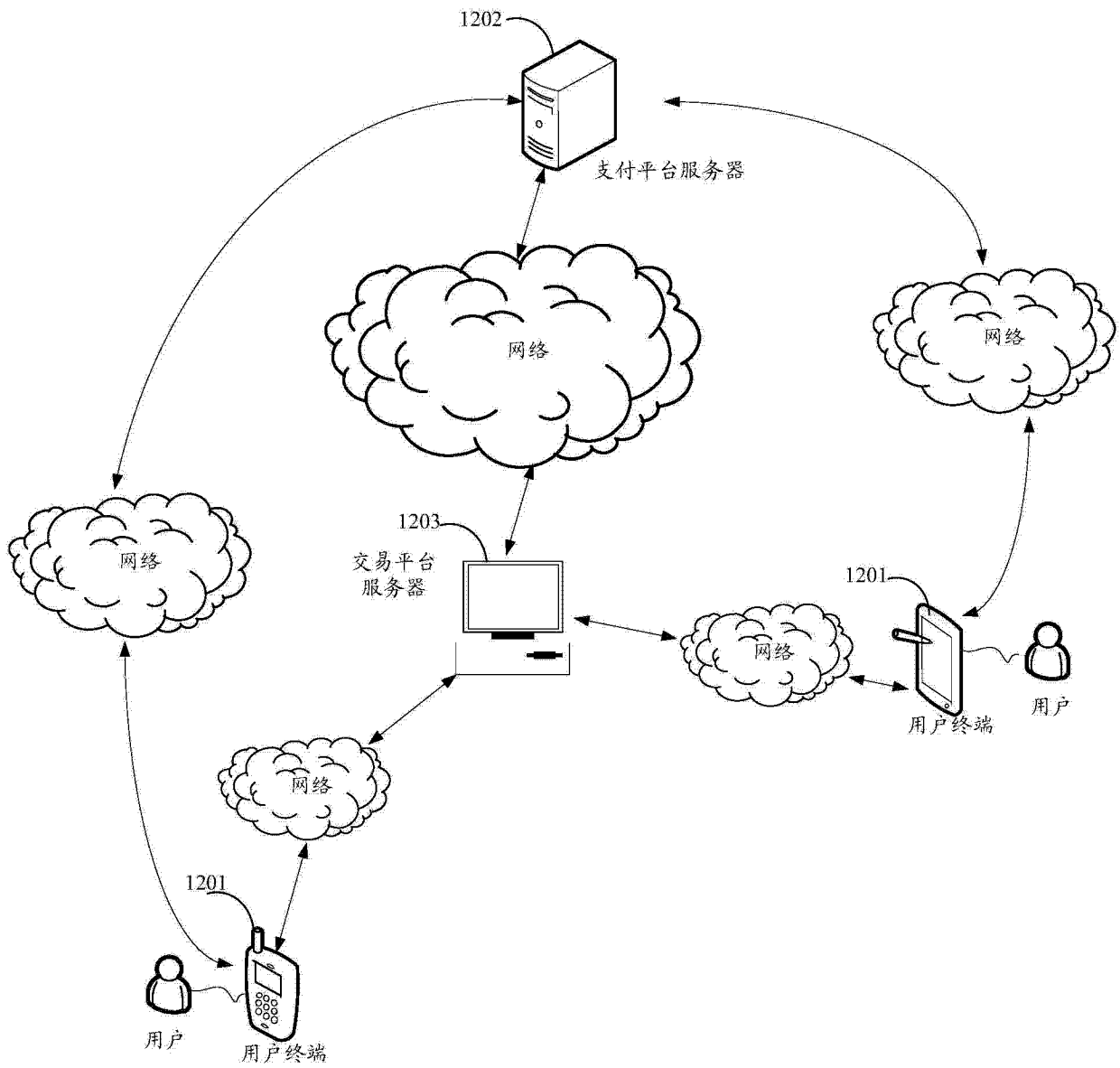


图 12