

用于电子资源转移的安全性信息交互方法

技术领域

本发明涉及信息交互方法，更具体地，涉及用于电子资源转移的安全性信息交互方法。

背景技术

目前，随着网络应用（尤其是移动网络）的日益广泛以及不同领域的业务种类的日益丰富，进行与电子资源的转移相关的安全性信息（即对安全性要求较高的信息）的交互变得越来越重要。

现有的与电子资源的转移相关的安全性信息交互方法通常仅应用于现场脱机形式的安全性信息交互（例如借助于金融机具以脱机方式应用电子现金），而无法实现安全性信息交互终端（例如移动终端）之间的直接的电子资源的转移。

因此，存在如下需求：提供能够进行安全性信息交互终端之间的直接的电子资源的转移并具有高的安全性和可靠性的安全性信息交互方法。

发明内容

为了解决上述现有技术方案所存在的问题，本发明提出了能够进行安全性信息交互终端之间的直接的电子资源的转移并具有高的安全性和可靠性的安全性信息交互方法。

本发明的目的是通过以下技术方案实现的：

一种安全性信息交互方法，所述安全性信息交互方法包括下列步骤：

（A1）第一安全性信息交互终端基于资源移出方的安全性信息交互指令构造安全性信息交互请求，并将所述安全性信息交互请求经由第一通信信道传送到第二安全性信息交互终端，其中，所述安全性信息交互请求包含下列信息：待转移的电子资源的数量、以及资源移出方电子资源标识符；

（A2）所述第二安全性信息交互终端处理接收到的所述安全性信息交互请求并基于处理结果返回安全性信息交互应答，其中所述安全性信息交互应答包

含资源移入方电子资源标识符;

(A3) 所述第一安全性信息交互终端基于所述安全性信息交互应答并经由第二通信信道与第一安全载体进行数据通信以构造安全性信息交互报文, 并将所述安全性信息交互报文传送到数据处理服务器, 以完成后续的安全性信息交互过程而实现电子资源的转移, 其中, 所述安全性信息交互报文包含执行后续的安全性信息交互过程所需的信息。

在上面所公开的方案中, 优选地, 所述第一通信信道是基于近场通信协议的通信信道。

在上面所公开的方案中, 优选地, 所述第一安全性信息交互终端经由所述第二通信信道从所述第一安全载体获取所述执行后续的安全性信息交互过程所需的信息。

在上面所公开的方案中, 优选地, 所述第一安全性信息交互终端和所述第二安全性信息交互终端均是移动终端。

在上面所公开的方案中, 优选地, 所述步骤(A3)进一步包括: 所述数据处理服务器解析接收到的安全性信息交互报文, 并执行脱机验证和判决操作; 如果所述脱机验证和判决操作的结果是“批准待进行的电子资源的转移”, 则向所述第一安全性信息交互终端传送回批准应答, 否则向所述第一安全性信息交互终端传送回拒绝应答。

在上面所公开的方案中, 优选地, 所述步骤(A3)进一步包括: 如果接收到批准应答, 则所述第一安全性信息交互终端经由所述第二通信信道与所述第一安全载体进行数据通信以便脱机地执行与电子资源的移出相关的操作并获取相应的安全性信息交互凭证, 而如果接收到拒绝应答, 则所述第一安全性信息交互终端终止安全性信息交互过程并提示用户安全性信息交互失败。

在上面所公开的方案中, 优选地, 所述步骤(A3)进一步包括: 在所述与电子资源的移出相关的操作被执行之后, 所述第一安全性信息交互终端向所述数据处理服务器传送移出操作成功应答, 其中, 所述移出操作成功应答包含所述安全性信息交互凭证以及所述资源移入方电子资源标识符。

在上面所公开的方案中, 优选地, 所述步骤(A3)进一步包括: 在接收到所述移出操作成功应答后, 所述数据处理服务器记录与当前的安全性信息交互

相关联的信息并将该记录的状态设置为“未完成”，以及向第一服务提供方服务器发送安全性信息交互应答，其中，所述安全性信息交互应答包含与当前的安全性信息交互相关联的信息；所述数据处理服务器随后向所述第二安全性信息交互终端发送资源转入通知。

- 5 在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：在接收到所述资源转入通知后，所述第二安全性信息交互终端向所述数据处理服务器发送安全性信息交互记录查询/同步请求以获取状态为“未完成”的安全性信息交互记录。

10 在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：在获取状态为“未完成”的安全性信息交互记录后，所述第二安全性信息交互终端针对状态为“未完成”的安全性信息交互记录向所述数据处理服务器发送安全载体电子资源同步请求，其中，所述安全载体电子资源同步请求至少包含资源移入方电子资源标识符。

15 在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：在接收到所述安全载体电子资源同步请求后，所述数据处理服务器向所述第二安全性信息交互终端发送安全载体电子资源同步应答，其中，所述安全载体电子资源同步应答包含带有防篡改保护的待转入电子资源数量值。

20 在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：在接收到所述安全载体电子资源同步应答后，所述第二安全性信息交互终端经由第三通信信道与第二安全载体进行数据通信以获取与电子资源的移入相关的信息，并随后将所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值传送到所述数据处理服务器。

25 在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：在接收到所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值后，所述数据处理服务器基于所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值构造电子资源转入请求报文，并将所述电子资源转入请求报文发送到第二服务提供方服务器。

 在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：在接收到所述电子资源转入请求报文后，所述第二服务提供方服务器基于所述电子资源

转入请求报文执行判决操作，并且如果判决操作的结果是“批准待进行的电子资源的转移”，则从所述与电子资源的移入相关的信息中提取出电子资源余量值，并根据所述电子资源余量值和所述待转入电子资源数量值计算新的电子资源余量值，并基于所述新的电子资源余量值生成电子资源余量值更新脚本，以及将所述电子资源余量值更新脚本发送到所述数据处理服务器。

在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：在接收到所述电子资源余量值更新脚本后，所述数据处理服务器将其转发给所述第二安全性信息交互终端；在接收到所述电子资源余量值更新脚本后，所述第二安全性信息交互终端将其转发给所述第二安全载体；在接收到所述电子资源余量值更新脚本后，所述第二安全载体执行所述电子资源余量值更新脚本以更新电子资源余量值并将脚本执行结果传送回所述第二安全性信息交互终端。

在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：在接收到脚本执行结果后，所述第二安全性信息交互终端将其转发给所述数据处理服务器；在接收到脚本执行结果后，所述数据处理服务器将其转发给所述第二服务提供方服务器，并且向所述第一安全性信息交互终端发送电子资源转移成功通知。

在上面所公开的方案中，优选地，所述数据处理服务器针对待转移的电子资源的数量计算鉴别码，并将所述鉴别码和待转移的电子资源的数量的明文结合在一起构成所述带有防篡改保护的待转入电子资源数量值。

本发明所公开的安全性信息交互方法具有如下优点：（1）能够进行安全性信息交互终端（尤其是移动终端）之间的直接的电子资源的转移操作；（2）具有高的安全性和可靠性。

附图说明

结合附图，本发明的技术特征以及优点将会被本领域技术人员更好地理解，其中：

图1是根据本发明的实施例的安全性信息交互方法的流程图。

具体实施方式

图1是根据本发明的实施例的安全性信息交互方法的流程图。如图1所示，本发明所公开的安全性信息交互方法包括下列步骤：(A1) 第一安全性信息交互终端基于资源移出方（例如支付交易中的付款方）的安全性信息交互指令构造安全性信息交互请求，并将所述安全性信息交互请求经由第一通信信道传送到第二安全性信息交互终端，其中，所述安全性信息交互请求包含下列信息：待转移的电子资源的数量（例如交易金额）、以及资源移出方电子资源标识符（例如付款方电子现金账号）；(A2) 所述第二安全性信息交互终端处理接收到的所述安全性信息交互请求并基于处理结果返回安全性信息交互应答，其中所述安全性信息交互应答包含资源移入方电子资源标识符（例如收款方电子现金账号）；(A3) 所述第一安全性信息交互终端基于所述安全性信息交互应答并经由第二通信信道与第一安全载体（即可以在其上存储并运行用于执行安全性信息交互过程的安全应用的载体，例如SIM卡、智能SD卡等）进行数据通信以构造安全性信息交互报文，并将所述安全性信息交互报文传送到数据处理服务器（例如金融领域中的支付平台），以完成后续的安全性信息交互过程而实现电子资源的转移，其中，所述安全性信息交互报文包含执行后续的安全性信息交互过程所需的信息（例如第一安全载体中的电子现金应用数据）。

优选地，在本发明所公开的安全性信息交互方法中，所述第一通信信道是基于近场通信协议（例如NFC协议）的通信信道。

优选地，在本发明所公开的安全性信息交互方法中，所述第一安全性信息交互终端经由所述第二通信信道从所述第一安全载体（即资源转出方安全载体）获取所述执行后续的安全性信息交互过程所需的信息（例如第一安全载体中的电子现金应用数据）。

示例性地，在本发明所公开的安全性信息交互方法中，所述第一安全性信息交互终端和所述第二安全性信息交互终端均是移动终端（例如手机）。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤(A3)进一步包括：所述数据处理服务器解析接收到的安全性信息交互报文，并执行脱机验证和判决操作；如果所述脱机验证和判决操作的结果是“批准待进行的电子资源的转移”，则向所述第一安全性信息交互终端传送回批准应答，否则向所述第一安全性信息交互终端传送回拒绝应答。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A3）进一步包括：如果接收到批准应答，则所述第一安全性信息交互终端经由所述第二通信信道与所述第一安全载体进行数据通信以便脱机地执行与电子资源的移出相关的操作（例如脱机扣款）并获取相应的安全性信息交互凭证，而如果接收
5 收到拒绝应答，则所述第一安全性信息交互终端终止安全性信息交互过程并提示用户安全性信息交互失败。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A3）进一步包括：在所述与电子资源的移出相关的操作被执行之后，所述第一安全性信息交互终端向所述数据处理服务器传送移出操作成功应答，其中，所述移出操
10 作成功应答包含所述安全性信息交互凭证以及所述资源移入方电子资源标识符（例如收款方电子现金账号）。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A3）进一步包括：在接收到所述移出操作成功应答后，所述数据处理服务器记录与当前的安全性信息交互相关联的信息（例如当前交易信息）并将该记录的状态设置
15 为“未完成”，以及向第一服务提供方服务器（例如付款方发卡机构）发送安全性信息交互应答，其中，所述安全性信息交互应答包含与当前的安全性信息交互相关联的信息（例如当前交易信息）；所述数据处理服务器随后向所述第二安全性信息交互终端发送资源转入通知（例如通过短信的形式发送账户转入通知）。

20 优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A3）进一步包括：在接收到所述资源转入通知后，所述第二安全性信息交互终端向所述数据处理服务器发送安全性信息交互记录查询/同步请求以获取状态为“未完成”的安全性信息交互记录。

优选地，在本发明所公开的安全性信息交互方法中，所述步骤（A3）进一步
25 步包括：在获取状态为“未完成”的安全性信息交互记录后，所述第二安全性信息交互终端针对状态为“未完成”的安全性信息交互记录向所述数据处理服务器发送安全载体电子资源同步请求（例如智能卡电子现金余额同步交易请求），其中，所述安全载体电子资源同步请求至少包含资源移入方电子资源标识符。

优选地,在本发明所公开的安全性信息交互方法中,所述步骤(A3)进一步包括:在接收到所述安全载体电子资源同步请求后,所述数据处理服务器向所述第二安全性信息交互终端发送安全载体电子资源同步应答,其中,所述安全载体电子资源同步应答包含带有防篡改保护的待转入电子资源数量值(例如
5 转入金额信息)。

优选地,在本发明所公开的安全性信息交互方法中,所述步骤(A3)进一步包括:在接收到所述安全载体电子资源同步应答后,所述第二安全性信息交互终端经由第三通信信道与第二安全载体(即资源转入方安全载体)进行数据通信以获取与电子资源的移入相关的信息(例如第二安全载体中的电子现金应用数据和余额),并随后将所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值传送到所述数据处理服务器。
10

优选地,在本发明所公开的安全性信息交互方法中,所述步骤(A3)进一步包括:在接收到所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值后,所述数据处理服务器基于所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值构造电子资源转入请求报文,并将所述电子资源转入请求报文发送到第二服务提供方服务器(例如收款方发卡机构)。
15

优选地,在本发明所公开的安全性信息交互方法中,所述步骤(A3)进一步包括:在接收到所述电子资源转入请求报文后,所述第二服务提供方服务器基于所述电子资源转入请求报文执行判决操作,并且如果判决操作的结果是“批准待进行的电子资源的转移”,则从所述与电子资源的移入相关的信息中提取出电子资源余量值(例如电子现金余额),并根据所述电子资源余量值和所述待转入电子资源数量值计算新的电子资源余量值(其是电子资源余量值与待转入电子资源数量值之和,例如新的电子现金余额),并基于所述新的电子资源余量值生成电子资源余量值更新脚本,以及将所述电子资源余量值更新脚本发送到所述数据处理服务器。
20
25

优选地,在本发明所公开的安全性信息交互方法中,所述步骤(A3)进一步包括:在接收到所述电子资源余量值更新脚本后,所述数据处理服务器将其转发给所述第二安全性信息交互终端;在接收到所述电子资源余量值更新脚本

后,所述第二安全性信息交互终端将其转发给所述第二安全载体;在接收到所述电子资源余量值更新脚本后,所述第二安全载体执行所述电子资源余量值更新脚本以更新电子资源余量值(即将所述新的电子资源余量值作为当前生效的电子资源余量值)并将脚本执行结果传送回所述第二安全性信息交互终端。

5 优选地,在本发明所公开的安全性信息交互方法中,所述步骤(A3)进一步包括:在接收到脚本执行结果后,所述第二安全性信息交互终端将其转发给所述数据处理服务器;在接收到脚本执行结果后,所述数据处理服务器将其转发给所述第二服务提供方服务器,并且向所述第一安全性信息交互终端发送电子资源转移成功通知(例如以短信的形式发送交易成功结果通知)。

10 优选地,在本发明所公开的安全性信息交互方法中,所述数据处理服务器针对待转移的电子资源的数量计算鉴别码,并将所述鉴别码和待转移的电子资源的数量的明文结合在一起构成所述带有防篡改保护的待转入电子资源数量值。

由上可见,本发明所公开的安全性信息交互方法具有下列优点:(1)能够
15 进行安全性信息交互终端(尤其是移动终端)之间的直接的电子资源的转移操作;(2)具有高的安全性和可靠性。

尽管本发明是通过上述的优选实施方式进行描述的,但是其实现形式并不局限于上述的实施方式。应该认识到:在不脱离本发明主旨和范围的情况下,本领域技术人员可以对本发明做出不同的变化和修改。

20

25

权利要求

1. 一种安全性信息交互方法, 所述安全性信息交互方法包括下列步骤:

(A1) 第一安全性信息交互终端基于资源移出方的安全性信息交互指令构造安全性信息交互请求, 并将所述安全性信息交互请求经由第一通信信道传送到第二安全性信息交互终端, 其中, 所述安全性信息交互请求包含下列信息: 待转移的电子资源的数量、以及资源移出方电子资源标识符;

(A2) 所述第二安全性信息交互终端处理接收到的所述安全性信息交互请求并基于处理结果返回安全性信息交互应答, 其中所述安全性信息交互应答包含资源移入方电子资源标识符;

(A3) 所述第一安全性信息交互终端基于所述安全性信息交互应答并经由第二通信信道与第一安全载体进行数据通信以构造安全性信息交互报文, 并将所述安全性信息交互报文传送到数据处理服务器, 以完成后续的安全性信息交互过程而实现电子资源的转移, 其中, 所述安全性信息交互报文包含执行后续的安全性信息交互过程所需的信息。

2. 根据权利要求1所述的安全性信息交互方法, 其特征在于, 所述第一通信信道是基于近场通信协议的通信信道。

3. 根据权利要求2所述的安全性信息交互方法, 其特征在于, 所述第一安全性信息交互终端经由所述第二通信信道从所述第一安全载体获取所述执行后续的安全性信息交互过程所需的信息。

4. 根据权利要求3所述的安全性信息交互方法, 其特征在于, 所述第一安全性信息交互终端和所述第二安全性信息交互终端均是移动终端。

5. 根据权利要求4所述的安全性信息交互方法, 其特征在于, 所述步骤(A3)进一步包括: 所述数据处理服务器解析接收到的安全性信息交互报文, 并执行脱机验证和判决操作; 如果所述脱机验证和判决操作的结果是“批准待进行的电子资源的转移”, 则向所述第一安全性信息交互终端传送回批准应答, 否则向所述第一安全性信息交互终端传送回拒绝应答。

6. 根据权利要求5所述的安全性信息交互方法, 其特征在于, 所述步骤(A3)进一步包括: 如果接收到批准应答, 则所述第一安全性信息交互终端经由所述

第二通信信道与所述第一安全载体进行数据通信以便脱机地执行与电子资源的移出相关的操作并获取相应的安全性信息交互凭证，而如果接收到拒绝应答，则所述第一安全性信息交互终端终止安全性信息交互过程并提示用户安全性信息交互失败。

5 7. 根据权利要求6所述的安全性信息交互方法，其特征在于，所述步骤(A3)进一步包括：在所述与电子资源的移出相关的操作被执行之后，所述第一安全性信息交互终端向所述数据处理服务器传送移出操作成功应答，其中，所述移出操作成功应答包含所述安全性信息交互凭证以及所述资源移入方电子资源标识符。

10 8. 根据权利要求7所述的安全性信息交互方法，其特征在于，所述步骤(A3)进一步包括：在接收到所述移出操作成功应答后，所述数据处理服务器记录与当前的安全性信息交互相关联的信息并将该记录的状态设置为“未完成”，以及向第一服务提供方服务器发送安全性信息交互应答，其中，所述安全性信息交互应答包含与当前的安全性信息交互相关联的信息；所述数据处理服务器随
15 后向所述第二安全性信息交互终端发送资源转入通知。

9. 根据权利要求8所述的安全性信息交互方法，其特征在于，所述步骤(A3)进一步包括：在接收到所述资源转入通知后，所述第二安全性信息交互终端向所述数据处理服务器发送安全性信息交互记录查询/同步请求以获取状态为“未完成”的安全性信息交互记录。

20 10. 根据权利要求9所述的安全性信息交互方法，其特征在于，所述步骤(A3)进一步包括：在获取状态为“未完成”的安全性信息交互记录后，所述第二安全性信息交互终端针对状态为“未完成”的安全性信息交互记录向所述数据处理服务器发送安全载体电子资源同步请求，其中，所述安全载体电子资源同步请求至少包含资源移入方电子资源标识符。

25 11. 根据权利要求10所述的安全性信息交互方法，其特征在于，所述步骤(A3)进一步包括：在接收到所述安全载体电子资源同步请求后，所述数据处理服务器向所述第二安全性信息交互终端发送安全载体电子资源同步应答，其中，所述安全载体电子资源同步应答包含带有防篡改保护的待转入电子资源数量值。

12. 根据权利要求11所述的安全性信息交互方法,其特征在于,所述步骤(A3)进一步包括:在接收到所述安全载体电子资源同步应答后,所述第二安全性信息交互终端经由第三通信信道与第二安全载体进行数据通信以获取与电子资源的移入相关的信息,并随后将所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值传送到所述数据处理服务器。

13. 根据权利要求12所述的安全性信息交互方法,其特征在于,所述步骤(A3)进一步包括:在接收到所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值后,所述数据处理服务器基于所述与电子资源的移入相关的信息和所述带有防篡改保护的待转入电子资源数量值构造电子资源转入请求报文,并将所述电子资源转入请求报文发送到第二服务提供方服务器。

14. 根据权利要求13所述的安全性信息交互方法,其特征在于,所述步骤(A3)进一步包括:在接收到所述电子资源转入请求报文后,所述第二服务提供方服务器基于所述电子资源转入请求报文执行判决操作,并且如果判决操作的结果是“批准待进行的电子资源的转移”,则从所述与电子资源的移入相关的信息中提取出电子资源余量值,并根据所述电子资源余量值和所述待转入电子资源数量值计算新的电子资源余量值,并基于所述新的电子资源余量值生成电子资源余量值更新脚本,以及将所述电子资源余量值更新脚本发送到所述数据处理服务器。

15. 根据权利要求14所述的安全性信息交互方法,其特征在于,所述步骤(A3)进一步包括:在接收到所述电子资源余量值更新脚本后,所述数据处理服务器将其转发给所述第二安全性信息交互终端;在接收到所述电子资源余量值更新脚本后,所述第二安全性信息交互终端将其转发给所述第二安全载体;在接收到所述电子资源余量值更新脚本后,所述第二安全载体执行所述电子资源余量值更新脚本以更新电子资源余量值并将脚本执行结果传送回所述第二安全性信息交互终端。

16. 根据权利要求15所述的安全性信息交互方法,其特征在于,所述步骤(A3)进一步包括:在接收到脚本执行结果后,所述第二安全性信息交互终端将其转发给所述数据处理服务器;在接收到脚本执行结果后,所述数据处理服

务器将其转发给所述第二服务提供方服务器,并且向所述第一安全性信息交互终端发送电子资源转移成功通知。

17. 根据权利要求16所述的安全性信息交互方法,其特征在于,所述数据处理服务器针对待转移的电子资源的数量计算鉴别码,并将所述鉴别码和待转移的电子资源的数量的明文结合在一起构成所述带有防篡改保护的待转入电子资源数量值。

10

15

20

25