

移动支付账户端用户凭证生成转换方法、系统及存储介质

技术领域

本发明涉及移动支付技术领域，具体涉及一种移动支付账户端用户凭证生成转换方法、系统及存储介质。

背景技术

目前，移动支付领域中的账户系统设计分为近场支付和远程支付两种：其中近场支付的账户设计以 NFC 为主的基于卡片的账户凭证系统；而在远程支付的账户系统设计中，NFC 并不合适，基于此，大多数支付机构和银行采用了数字通证（TOKEN）的方式在远程支付场景中。

在这种情况下，因为各家支付机构和银行采用了自定义的 TOKEN 体系和实现方法，给在互联网情况下的互联互通带来很多不便。为了能够让各种账户体系可以互联互通，本发明给出了一种简单易用的方法，来帮助不同的账户拥有方实现生产，交互，存储和转换。

发明内容

针对现有技术的不足，本发明公开了一种移动支付账户端用户凭证生成转换方法、系统及存储介质，用于解决目前的支付远程账户体系中，生成凭证的方法有很多而且非常分散和碎片化，短期内无法实现统一标准和规范来适应全球化支付系统和用户需求。

现有的用户凭证设计，大致采用了基于数字编码的方式，位数在 18-25 位阿拉伯数字之间，数字编码的设计是为了方便商户端的受理改造，但是在不同的账户凭证交互中会带来很多商户端的改造成本。

同时，用户凭证使用在金融交易中，对于安全性和隐私性有很高要求，因此对于用户凭证的转换和脱敏的技术方案有很高的要求问题。

本发明通过以下技术方案予以实现：

第一方面，本发明公开一种移动支付账户端用户凭证生成转换方法，所述方法包括以下步骤：

S1 获取账户 B 的设备信息,并对账户 B 的用户凭证进行分散运算;
S2 利用账户 A 和账户 B 之间约定的运算方法,将账户 B 的凭证在 S1 处理后进行序列化;
S3 对 S2 序列化之后的账户 B 的凭证通过约定的加密算法加密;
S4 通过用户的账户信息将加密算法加密后的结果进行分散处理;
S5 将分散处理后的数据进行序列化后形成数字串;
S6 将数字串和账户 A 的用户凭证标识符进行混淆,形成基于账户 A 的用户凭证。

更进一步的,所述账户 B 的用户凭证为指纹相关的凭证,通过新生成的账户 A 的用户凭证可反推溯源到用户 B 的初始用户凭证。

更进一步的,在账户 B 的用户凭证为和用户指纹无关的用户凭证时,使用随机匹配的算法,来随机匹配不同账户用户凭证,所述算法包括以下步骤:

T1 将服务器端账户 A 和账户 B 的用户凭证进行池化;
T2 在账户端开辟独立的存储空间,来和服务端对话建立池化数字凭证体系之间的关联;
T3 在不同的客户端和对端的用户凭证池里面的数字凭证进行服务器端的单向关联;
T4 在客户端将凭证池的数字序列化之后,在前端展示。

更进一步的,所述算法在不同账户体系的用户凭证之间的相互对应关系是一次行单向对应关系,在使用完成后无法进行复原或者逆向还原。

第二方面,本发明提供了一种移动支付账户端用户凭证生成转换系统,所述系统用于实现如第一方面所述的移动支付账户端用户凭证生成转换方法,所述系统包括凭证对应、序列化、临时存储、安全、持久化组,连接不同的账户体系和凭证生成方法。

更进一步的,所述系统支持以字符化 ID 为体系的账户凭证转换服务,字符化凭证包括电子邮件、电话、身份证号、银行卡号或其他账

户 ID。

更进一步的，所述系统可在不同的用户端设备上展示和进行金融交易，其中包括手机，平板电脑，电脑，带有屏幕的设备非联网能力和带有屏幕联网能力的设备，以不同形式运行在不同的设备上，通过提供应用系统接口和开发工具等方式来进行集成。

更进一步的，所述系统通过 APP 内嵌应用、web 应用、快易用或小程序的方式在账户 APP，网站上进行呈现，其呈现模式可在金融机构和账户系统拥有方系统之间进行部署和服务，用以连接不同的金融和非金融机构的账户系统，实现互联互通服务。

更进一步的，所述系统产生的序列化数字在前端使用多种方式进行展示，包括条码、二维码、蓝牙、近场 NFC、声波、磁力传输和光传输等传输方式进行传输。

更进一步的，所述系统产生的凭证可在不同的金融终端和场景使用，同时序列数字化后的凭证可以被多种前端读取设备读取该系统可以在多种形式的设备上部署，可容器化和序列化并在多种复杂的云环境和本地环境上进行部署和运行。

更进一步的，该系统生成的金融凭证在不同的终端上进行交易时，当用户端的多个账户凭证和商户终端支持的凭证进行对比和握手，则选择双方优选的匹配结果来进行金融交易。其生成的金融凭证在不同的终端上进行交易时，用户端上显示账户凭证代码，选择人工进行选择判断后进行金融交易。

更进一步的，所述系统向前端提供服务的方式是，通过多种方式，包括但不限于 SDK，API，小程序或者富文本，瘦客户端和富 web 的方式同现有的多种应用形式进行对接和植入实现。

更进一步的，所述系统利用用户端的 UI 设计方法，可简答快速的集成多个账户凭证体系，在一个 UI 上进行快速展示和切换，并可应用在不同的前端技术上。

第三方面，本发明提供一种存储介质，所述存储介质上存储有计

算机程序，并将不同的用户凭证进行存储，混淆，并在不同的账户系统间进行交换，所述计算机程序被处理器执行时，实现第一方面所述的移动支付账户端用户凭证生成转换方法。

本发明的有益效果为：

本发明在远程支付账户用户凭证的生成，转换和交互使用，从而做到账户系统的用户凭证可以简单快速地在不同的账户体系中互联互通，很好的解决了账户凭证间的安全转换问题。

附图说明

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。

图 1 是移动支付账户端用户凭证生成转换原理图；

图 2 是本发明实施例两个账户系统转换凭证图；

图 3 是本发明实施例基于账户指纹的用户凭证转换原理图；

图 4 是本发明实施例没有账户指纹的用户凭证转换原理图；

图 5 是本发明实施例基于应用程序接口的设计原理图；

图 6 是本发明实施例基于开发者工具的封装模式原理图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，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。

实施例 1

本实施例公开一种移动支付账户端用户凭证生成转换方法，所述方法包括以下步骤：

S1 获取账户 B 的设备信息，并对账户 B 的用户凭证进行分散运算；

S2 利用账户 A 和账户 B 之间约定的运算方法，将账户 B 的凭证在 S1 处理后进行序列化；

S3 对 S2 序列化之后的账户 B 的凭证通过约定的加密算法加密；

S4 通过用户的账户信息将加密算法加密后的结果进行分散处理；

S5 将分散处理后的数据进行序列化后形成数字串；

S6 将数字串和账户 A 的用户凭证标识符进行混淆，形成基于账户 A 的用户凭证。

账户 B 的用户凭证为指纹相关的凭证，通过新生成的账户 A 的用户凭证可反推溯源到用户 B 的初始用户凭证。

在账户 B 的用户凭证为和用户指纹无关的用户凭证时，使用随机匹配的算法，来随机匹配不同账户用户凭证。

所述算法包括以下步骤：

T1 将服务器端账户 A 和账户 B 的用户凭证进行池化；

T2 在账户端开辟独立的存储空间，来和服务器对话建立池化数字凭证体系之间的关联；

T3 在不同的客户端和对端的用户凭证池里面的数字凭证进行服务器端的单向关联；

T4 在客户端将凭证池的数字序列化之后，在前端展示。

算法在不同账户体系的用户凭证之间的相互对应关系是一次行单向对应关系，在使用完成后无法进行复原或者逆向还原。

实施例 2

本实施例公开一种简单的快速的基于不同账户凭证间的安全转换的方法，大致方法具体如图 1 所示，基于账户凭证间的转换可以简单理解为不同钱包之间可以显示不同的账户凭证来实现在不同账户网络

的受理。例如，在账户 A 中（基于移动端应用程序和网页应用程序）可以动态的显示账户 B 的用户凭证，在账户 B 的网络里互联互通。

在技术上，不同账户用户凭证之间的转化需要极高的安全性和通用行。因此在本发明中，对于不同账户系统的用户凭证的转换，采用了不同的安全策略和方法。

如图 2 所示假设在两个账户系统中，账户 B 需要使用到账户 A 的用户凭证，账户 B 会向账户 A 发起请求来请求一个符合账户凭证 A 的凭证。

实施例 3

本实施例公开如图 3 所示的基于账户指纹的用户凭证转换方法：

在这种方法下，在账户 B 转换获得账户 A 的用户凭证时，会生成一个基于 B 账户用户凭证指纹的 token，这个时候，两个账户凭证之间可以通过用户指纹进行关联和还原。

具体的转换和实现方法如下：

第一步：通过获取账户 B 的设备信息（硬件序列号，时间戳）来和账户 B 的用户凭证进行分散运算。

第二步：通过账户 A 和账户 B 之间约定的运算方法，将账户 B 的凭证在第一步处理后进行序列化。序列化之后通过约定的加密算法加密。

第三步：通过用户的账户信息（电子邮件，或者电话号码）将第二步的结果进行分散处理。

第四步：将第三步的数据进行序列化后形成数字串。

第五步：将数字串和账户 A 的用户凭证标识符进行混淆，形成基于账户 A 的用户凭证。

同时，该方法保证了上述步骤是可逆的，即通过新生成的账户 A 的用户凭证可以反推溯源到用户 B 的初始用户凭证。

实施例 4

上述实施例是基于账户指纹相关的凭证转化方法，除了用户指纹

相关的凭证转换方法外，本实施例公开一另一种和用户指纹无关的用户凭证转换方法。

如图 4 所示没有账户指纹的用户凭证转换方法：

在这种方法下，在账户 B 转换获得账户 A 的用户凭证时，账户 A 和账户 B 的用户凭证之间是随机匹配的，这个时候，两个账户凭证之间的关系无法进行关联和还原。

在这种方法下，本发明将使用一种随机匹配的算法，来随机匹配不同账户用户凭证，具体说明如下：

第一步：将服务器端账户 A 和账户 B 的用户凭证进行池化，即在不同的凭证体系中的数字进行缓存和池化。

第二步：在账户端开辟一个独立的存储空间，用来和服务器对话建立池化数字凭证体系之间的关联。

第三步：在不同的客户端和对端的用户凭证池里面的数字凭证进行服务器端的一次性单向关联，本发明可以实现一对一的单向关联，或者一对多的单向关联。

第四步：在客户端将凭证池的数字序列化之后，在前端展示。

在这种方法下，不同账户体系的用户凭证之间的相互对应关系是一次行单向对应关系，不会在使用完成后进行复原或者逆向还原。

实施例 5

本实施例公开一种移动支付账户端用户凭证生成转换系统，所述系统用于实现上述实施例所述的移动支付账户端用户凭证生成转换方法，所述系统包括凭证对应、序列化、临时存储、安全、持久化组，连接不同的账户体系和凭证生成方法。

系统支持以字符化 ID 为体系的账户凭证转换服务，字符化凭证包括电子邮件、电话、身份证号、银行卡号或其他账户 ID。系统可在不同的用户端设备上展示和进行金融交易，其中包括手机，平板电脑，电脑，带有屏幕的设备非联网能力和带有屏幕联网能力的设备，以不同形式运行在不同的设备上，通过提供应用系统接口和开发工具

等方式来进行集成。

系统通过 APP 内嵌应用、web 应用、快易用或小程序的方式在账户 APP，网站上进行呈现，其呈现模式可在金融机构和账户系统拥有方系统之间进行部署和服务，用以连接不同的金融和非金融机构的账户系统，实现互联互通服务。系统产生的序列化数字在前端使用多种方式进行展示，包括条码、二维码、蓝牙、近场 NFC、声波、磁力传输和光传输等传输方式进行传输。

系统产生的凭证可在不同的金融终端和场景使用，同时序列数字化后的凭证可以被多种前端读取设备读取该系统可以在多种形式的设备上部署，可容器化和序列化并在多种复杂的云环境和本地环境上进行部署和运行。该系统生成的金融凭证在不同的终端上进行交易时，当用户端的多个账户凭证和商户终端支持的凭证进行对比和握手，则选择双方优选的匹配结果来进行金融交易。其生成的金融凭证在不同的终端上进行交易时，用户端上显示账户凭证代码，选择人工进行选择判断后进行金融交易。

系统向前端提供服务的方式是，通过多种方式，包括但不限于 SDK，API，小程序或者富文本，瘦客户端和富 web 的方式同现有的多种应用形式进行对接和植入实现。系统利用用户端的 UI 设计方法，可简答快速的集成多个账户凭证体系，在一个 UI 上进行快速展示和切换，并可应用在不同的前端技术上。

实施例 6

对于实施例 5 中系统的技术实现，本实施例公开在系统实现中，采用不同的实现方式：如图 5 所示基于应用程序接口的设计，本方法下的凭证系统可以提供完整的应用程序接口给账户系统进行对接和使用。如图 6 所示的基于开发者工具的封装模式，除了应用程序接口以外，本方法下的凭证转化系统也可以提供基于各种设备，后台系统的开发者工具接口来实现凭证转换服务。在受理环境中，账户凭证子系统 and 商户端受理设备之间实现交互，已实现在不同多个账户凭证间进

行选择和激活，这里的连接方式包括蓝牙，wifi 或者进场通讯手段。

实施例 7

本实施例公开一种存储介质，所述存储介质上存储有计算机程序，并将不同的用户凭证进行存储，混淆，并在不同的账户系统间进行交换，所述计算机程序被处理器执行时，实现上述实施例所述的移动支付账户端用户凭证生成转换方法。

综上本发明在远程支付账户用户凭证的生成，转换和交互使用，从而做到账户系统的用户凭证可以简单快速的在不同的账户体系中互联互通。在目前的支付远程账户体系中，生成凭证的方法有很多而且非常分散和碎片化，短期内无法实现统一标准和规范来适应全球化支付系统和用户需求，因此，本发明中的方法可以简单快速的实施转换和互通。

现有的用户凭证设计，大致采用了基于数字编码的方式，位数在 18-25 位阿拉伯数字之间，数字编码的设计是为了方便商户端的受理改造，但是在不同的账户凭证交互中会带来很多商户端的改造成本，所以为了可以快速的实现交互和互通，使账户凭证转换简单和经济。

同时，用户凭证使用在金融交易中，对于安全性和隐私性有很高要求，因此对于用户凭证的转换和脱敏的技术方案有很高的要求。本发明很好的解决了账户凭证间的安全转换问题。

以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。