(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106230824 A
(43)申请公布日 2016.12.14

(21)申请号 201610622390.5

(22)申请日 2016.07.29

(71)申请人 浙商银行股份有限公司
地址 310006 浙江省杭州市庆春路288号

(72)发明人 陈嘉俊 臧铖

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 刘静 邱启旺

(51)Int.Cl.
H04L 29/06(2006.01)
G06Q 20/40(2012.01)
G06Q 20/38(2012.01)
G06Q 20/32(2012.01)

权利要求书2页 说明书4页 附图1页

(54)发明名称

一种移动设备可信认证系统及方法

(57)摘要

本发明公开了一种移动设备可信认证系统及方法;客户发起交易请求,交易访问装置受理客户请求,访问信息存储装置获取动态设备码,并通过数据交互装置与服务端进行通讯,服务端的身份认证装置完成设备可信认证。本发明避免了短信发送的费用,规避了运营商出现问题时动态验证码无法送达客户的问题,提升客户体验;本发明是对移动设备本身的绑定,同时解决了客户更换号码后原号码被他人获取并获取验证码的风险;加之目前手机普遍支持指纹解锁、密码解锁,等价于三重验证机制,安全程度更高;增加了后续优化业务流程的可能性,在基于移动设备实现可信认证的基础上,可利用移动设备这一可信介质,优化银行现有业务流程,为简化客户认证步骤提供了可能。

CN 106230824 A

1.一种移动设备可信认证系统，其特征在于，该系统在客户端设有交易访问装置、信息加密装置、信息存储装置和数据交互装置，在服务端设有身份认证装置；

所述交易访问装置受理客户登陆及交易请求，访问客户端的信息存储装置获取动态设备码，若无法获取到动态设备码，则访问信息加密装置获取当前动态设备码，并将获取的动态设备码发送到客户端的数据交互装置；

所述信息加密装置将设备的唯一ID信息通过时间戳签名得到动态设备码；

所述信息存储装置接收并存储交易访问装置上送的数据包，包括交易数据和动态设备码；

所述数据交互装置根据交易访问装置上送的数据，与服务端进行通讯，并接收服务端返回的处理结果；

所述身份认证装置将客户端上送的动态设备码与服务端登记的动态设备码进行比对，如果一致则通过验证，如果不一致，则判断身份认证装置设定的参数设置，如果参数设置为根据先进先出原则覆盖最早预留的动态设备码，则通过服务端发送短信或提示用户使用Ukey进行二次验证，验证通过后在服务端登记客户身份与客户端发送的动态设备码的关系，并通过验证；否则禁止客户操作。如果参数设置为先解除原设备绑定再进行预留操作，则需通过绑定设备管理功能进行自主设置。

2.根据权利要求1所述的一种移动设备可信认证系统，其特征在于，该系统还包括交易处理装置，所述交易处理装置接收客户端上送的数据及请求，根据具体业务类型提供相应业务处理服务。

3.根据权利要求1所述的一种移动设备可信认证系统，其特征在于，所述信息存储装置保存本设备动态设备码信息，通过智能芯片或本设备私有区域存储，并在认证过程中进行缓存。

4.根据权利要求1所述的一种移动设备可信认证系统，其特征在于，所述设备的唯一ID信息为移动设备国际识别码IMEI或物理硬件的MAC地址；所述物理硬件为网卡或蓝牙。

5.根据权利要求1所述的一种移动设备可信认证方法，其特征在于，所述客户端为应用软件或浏览器。

6.根据权利要求1所述的一种移动设备可信认证系统，其特征在于，所述客户端可根据客户意愿，自主新增可信认证或者删除可信认证，或由服务端统一设置，要求客户端强制新增可信认证。

7.根据权利要求1所述的一种移动设备可信认证系统，其特征在于，所述绑定设备管理功能包括通过原绑定设备进行解绑操作，或登录浏览器对已绑定设备进行解绑。

8.一种移动设备可信认证方法，其特征在于，该方法包括以下步骤：

(1)客户向客户端的交易访问装置发送登陆请求，登陆账号密码验证成功后，交易访问装置访问客户端的信息存储装置获取动态设备码，如果没有预留动态设备码，则执行步骤2；否则将动态设备码发送到客户端的数据交互装置，执行步骤3；

(2)客户端的信息加密装置将设备的唯一ID信息通过时间戳签名得到动态设备码；

(3)数据交互装置将接收的动态设备码发送到服务端的身份认证装置；

(4)身份认证装置将接收的动态设备码与服务端登记的动态设备码进行比对，如果一致则通过验证，如果不一致或未登记则执行步骤5；

(5)判断身份认证装置设定的参数设置,如果参数设置为根据先进先出原则覆盖最早预留的动态设备码,则通过服务端发送短信或提示用户使用Ukey进行二次验证,验证通过后在服务端登记客户身份与客户端发送的动态设备码的关系,并通过验证;否则禁止客户操作。如果参数设置为先解除原设备绑定再进行预留操作,则需通过绑定设备管理功能进行自主设置。

9.根据权利要求8所述的一种移动设备可信认证方法,其特征在于,所述绑定设备管理功能包括通过原绑定设备进行解绑操作,或登录浏览器对已绑定设备进行解绑。

10.根据权利要求8所述的一种移动设备可信认证方法,其特征在于,数据交互装置对交易数据签名加密。

一种移动设备可信认证系统及方法

技术领域

[0001] 本发明属于计算机系统领域，尤其涉及一种移动设备可信认证系统及方法。

背景技术

[0002] 商业银行根据监管要求，普遍采用了双因子认证的方式对客户身份进行验证，如手机银行转账汇款，除了传统的登陆密码验证之外，还提供了短信动态验证码、Ukey认证等多重安全机制防范盗刷等风险。目前短信动态验证码及Ukey认证存在以下不足：

[0003] 1、安全性不高。短信动态验证码在认证过程中采用明文传输与存储，易被不法分子获取，若通过复制卡片等技术手段盗取手机号码，短信动态验证码也就失去了二次认证的作用。

[0004] 2、交易链路较长。在涉及短信动态验证码的交易中，需通过移动运营商进行短信发送，交易依赖于移动运营商服务的可用性及处理效率，同时也可能增加系统处理的负荷，在业务处理高峰时，短信发送可能会成为整个流程中的瓶颈。

[0005] 3、客户体验不佳。对于短信动态码认证方式，客户需要记住短信验证码并录入，操作不便；对于Ukey认证方式，每家银行的Ukey互不兼容、无法共用，客户保管、使用Ukey不便，体验相对较差。

[0006] 针对现有认证方式在安全性、易用性、便携性等方面的不足，为了提升系统安全性，保障客户账户及资金安全，需要进一步采用移动设备可信认证技术，通过与移动设备硬件进行关联绑定，实现安全的客户身份可信认证。

发明内容

[0007] 本发明的目的在于针对现有技术的不足，提供一种移动设备可信认证系统及方法。

[0008] 本发明的目的是通过以下技术方案来实现的：一种移动设备可信认证系统，其特征在于，该系统在客户端设有交易访问装置、信息加密装置、信息存储装置和数据交互装置，在服务端设有身份认证装置；

[0009] 所述交易访问装置受理客户登陆及交易请求，访问客户端的信息存储装置获取动态设备码，若无法获取到动态设备码，则访问信息加密装置获取当前动态设备码，并将获取的动态设备码发送到客户端的数据交互装置；

[0010] 所述信息加密装置将设备的唯一ID信息通过时间戳签名得到动态设备码；

[0011] 所述信息存储装置接收并存储交易访问装置上送的数据包，包括交易数据和动态设备码；

[0012] 所述数据交互装置根据交易访问装置上送的数据，与服务端进行通讯，并接收服务端返回的处理结果；

[0013] 所述身份认证装置将客户端上送的动态设备码与服务端登记的动态设备码进行比对，如果一致则通过验证，如果不一致，则判断身份认证装置设定的参数设置，如果参数

设置为根据先进先出原则覆盖最早预留的动态设备码，则通过服务端发送短信或提示用户使用Ukey进行二次验证，验证通过后在服务端登记客户身份与客户端发送的动态设备码的关系，并通过验证；否则禁止客户操作。如果参数设置为先解除原设备绑定再进行预留操作，则需通过绑定设备管理功能进行自主设置。

[0014] 进一步地，该系统还包括交易处理装置，所述交易处理装置接收客户端上送的数据及请求，根据具体业务类型提供相应业务处理服务。

[0015] 进一步地，所述信息存储装置保存本设备动态设备码信息，通过智能芯片或本设备私有区域存储，并在认证过程中进行缓存。

[0016] 进一步地，所述设备的唯一ID信息为移动设备国际识别码IMEI或物理硬件的MAC地址；所述物理硬件为网卡或蓝牙。

[0017] 进一步地，所述客户端为应用软件或浏览器。

[0018] 进一步地，所述客户端可根据客户意愿，自主新增可信认证或者删除可信认证，或由服务端统一设置，要求客户端强制新增可信认证。

[0019] 进一步地，所述绑定设备管理功能包括通过原绑定设备进行解绑操作，或登录浏览器对已绑定设备进行解绑。

[0020] 一种移动设备可信认证方法，该方法包括以下步骤：

[0021] (1)客户向客户端的交易访问装置发送登陆请求，登陆账号密码验证成功后，交易访问装置访问客户端的信息存储装置获取动态设备码，如果没有预留动态设备码，则执行步骤2；否则将动态设备码发送到客户端的数据交互装置，执行步骤3；

[0022] (2)客户端的信息加密装置将设备的唯一ID信息通过时间戳签名得到动态设备码；

[0023] (3)数据交互装置将接收的动态设备码发送到服务端的身份认证装置；

[0024] (4)身份认证装置将接收的动态设备码与服务端登记的动态设备码进行比对，如果一致则通过验证，如果不一致或未登记则执行步骤5；

[0025] (5)判断身份认证装置设定的参数设置，如果参数设置为根据先进先出原则覆盖最早预留的动态设备码，则通过服务端发送短信或提示用户使用Ukey进行二次验证，验证通过后在服务端登记客户身份与客户端发送的动态设备码的关系，并通过验证；否则禁止客户操作。如果参数设置为先解除原设备绑定再进行预留操作，则需通过绑定设备管理功能进行自主设置。

[0026] 进一步地，所述绑定设备管理功能包括通过原绑定设备进行解绑操作，或登录浏览器对已绑定设备进行解绑。

[0027] 进一步地，数据交互装置对交易数据签名加密。

[0028] 本发明提供的移动设备可信认证系统及方法，减少了对短信动态认证码的依赖，并且提升了客户体验，加强了系统安全性，主要具有如下效果与优点：

[0029] 1.提升客户体验。本发明与短信动态验证码相比，既避免了短信发送的费用，又方便了客户使用，同时还规避了运营商出现问题时动态验证码无法送达客户的问题，具有较大优势。

[0030] 2.加强系统安全性。从安全性角度看，短信动态验证码事实上是对电话号码的绑定，而本发明技术方案是对移动设备本身的绑定，同时解决了客户更换号码后原号码被他

人获取并获取验证码的风险;加之目前手机普遍支持指纹解锁、密码解锁,事实上这等价于三重验证机制,安全程度更高。

[0031] 3.增加了后续优化业务流程的可能性。在基于移动设备实现可信认证的基础上,可利用移动设备这一可信介质,优化银行现有业务流程,为简化客户认证步骤提供了可能。

附图说明

[0032] 图1是本发明可信认证系统总体结构框图;

[0033] 图2是本发明可信认证方法的示意图。

具体实施方式

[0034] 下面结合附图和具体实施例对本发明作进一步详细说明。

[0035] 如图1所示,本发明提供的一种移动设备可信认证系统,该系统在客户端设有交易访问装置、信息加密装置、信息存储装置和数据交互装置,在服务端设有身份认证装置;

[0036] 所述交易访问装置受理客户从手机银行、网上银行、微信银行等渠道发起的登陆及交易请求,访问客户端的信息存储装置获取动态设备码,若无法获取到动态设备码,则访问信息加密装置获取当前动态设备码,并将获取的动态设备码发送到客户端的数据交互装置;

[0037] 所述信息加密装置将设备的唯一ID信息通过时间戳签名得到动态设备码;

[0038] 所述信息存储装置接收并存储交易访问装置上送的数据包,包括交易数据和动态设备码;

[0039] 所述数据交互装置根据交易访问装置上送的数据,与服务端进行通讯,并接收服务端返回的处理结果;

[0040] 所述身份认证装置将客户端上送的动态设备码与服务端登记的动态设备码进行比对,如果一致则通过验证,如果不一致,则判断身份认证装置设定的参数设置,如果参数设置为根据先进先出原则覆盖最早预留的动态设备码,则通过服务端发送短信或提示用户使用Ukey进行二次验证,验证通过后在服务端登记客户身份与客户端发送的动态设备码的关系,并通过验证;否则禁止客户操作。如果参数设置为先解除原设备绑定再进行预留操作,则需通过绑定设备管理功能进行自主设置。

[0041] 进一步地,该系统还包括交易处理装置,所述交易处理装置接收客户端上送的数据及请求,根据具体业务类型提供相应业务处理服务。

[0042] 进一步地,所述信息存储装置保存本设备动态设备码信息,通过智能芯片或本设备私有区域存储,并在认证过程中进行缓存,减少访问次数,提升处理效率。

[0043] 进一步地,所述设备的唯一ID信息为移动设备国际识别码IMEI或物理硬件的MAC地址;所述物理硬件为网卡或蓝牙。

[0044] 进一步地,所述客户端为应用软件或浏览器。

[0045] 进一步地,所述客户端可根据客户意愿,自主新增可信认证或者删除可信认证,或由服务端统一设置,要求客户端强制新增可信认证。

[0046] 如图2所示,本发明提供的一种移动设备可信认证方法,该方法包括以下步骤:

[0047] (1)客户向客户端的交易访问装置发送登陆请求,登陆账号密码验证成功后,交易

访问装置访问客户端的信息存储装置获取动态设备码，如果没有预留动态设备码，则执行步骤2；否则将动态设备码发送到客户端的数据交互装置，执行步骤3；

[0048] (2)客户端的信息加密装置将设备的唯一ID信息通过时间戳签名得到动态设备码；

[0049] (3)数据交互装置将接收的动态设备码发送到服务端的身份认证装置；

[0050] (4)身份认证装置将接收的动态设备码与服务端登记的动态设备码进行比对，如果一致则通过验证，如果不一致或未登记则执行步骤5；

[0051] (5)判断身份认证装置设定的参数设置，如果参数设置为根据先进先出原则覆盖最早预留的动态设备码，则通过服务端发送短信或提示用户使用Ukey进行二次验证，验证通过后在服务端登记客户身份与客户端发送的动态设备码的关系，并通过验证；否则禁止客户操作。如果参数设置为先解除原设备绑定再进行预留操作，则需通过绑定设备管理功能进行自主设置。

[0052] 进一步地，所述绑定设备管理功能包括通过原绑定设备进行解绑操作，或登录浏览器对已绑定设备进行解绑(例如登录个人网上银行等)。

[0053] 进一步地，数据交互装置对交易数据签名加密，确保信息完整性。

[0054] 以银行领域为例，在需要远程对客户身份进行认证时，通过本发明提供的系统和方法，客户在首次登陆手机银行后，通过手机动态验证码绑定操作设备(手机)，绑定之后，后续登陆操作只需验证该手机是否为绑定过的设备，而无需再通过短信动态验证码的方式来进行交叉验证。本发明提供的系统和方法替代了短信动态验证码的二次认证功能，在优化业务流程的同时，提升了客户体验及系统安全性。

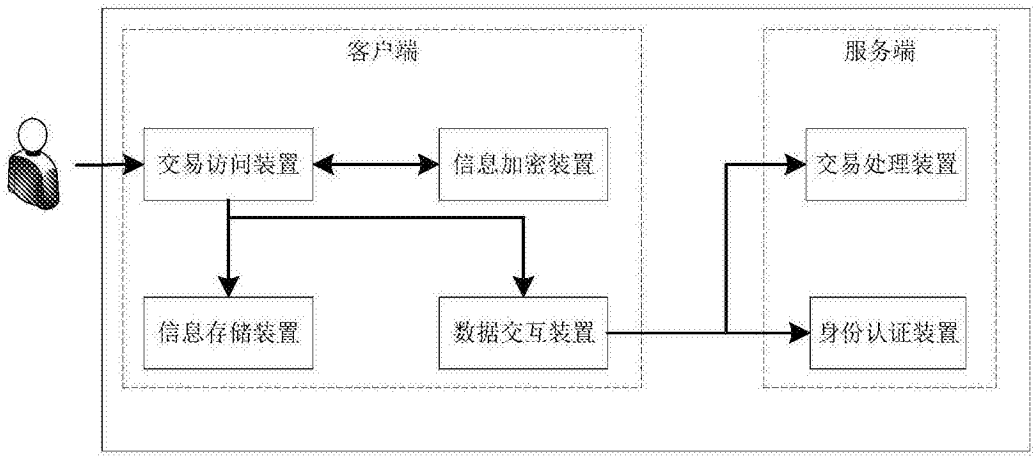
客户端
服务端
交易访问装置
信息加密装置
交易处理装置
信息存储装置
数据交互装置
身份认证装置

图1

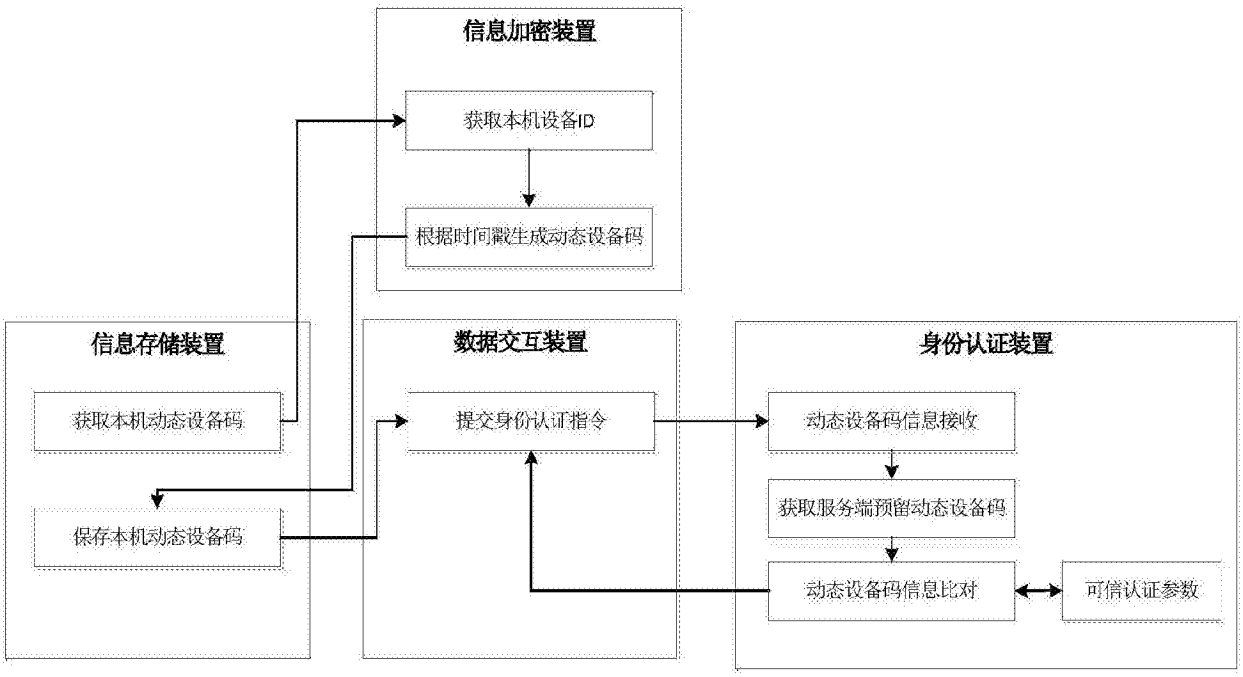
信息加密装置
获取本机设备ID
根据时间戳生成动态设备码
信息存储装置
获取本机动态设备码
保存本机动态设备码
数据交互装置
提交身份认证指令
身份认证装置
动态设备码信息接收
获取服务端预留动态设备码
动态设备码信息比对
可信认证参数

图2