(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 104657860 A
(43)申请公布日 2015.05.27

(21)申请号 201510042986.3

(22)申请日 2015.01.28

(71)申请人 郑州大学
地址 450001 河南省郑州市高新区科学大道100号郑州大学新校区

(72)发明人 王国卿 刘涛涛 阮春阳 卢耀恩 王瑞民 庄雷 宋玉

(74)专利代理机构 北京科亿知识产权代理事务所(普通合伙) 11350
代理人 汤东凤

(51)Int.Cl.
G06Q 20/40(2012.01)
G06Q 20/36(2012.01)
G06Q 20/32(2012.01)

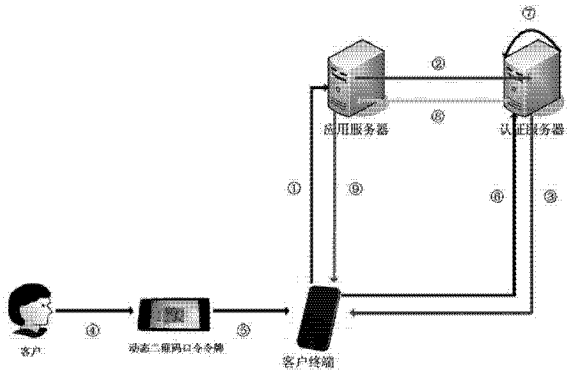
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种手机银行安全认证方法

(57)摘要

本发明公开了一种手机银行安全认证方法：A、客户使用客户终端请求接入应用服务器；B、应用服务器请求认证服务器对客户身份进行认证；C、认证服务器向客户终端索取认证信息；D、动态二维码口令令牌生成包含有自身账号和口令信息的动态二维码；E、扫描令牌屏幕上的动态二维码并通过网络传输给认证服务器；F、认证服务器调用相应的客户信息，产生与客户信息和事件相关的随机序列，并解析二维码口令进行比对以判别客户身份的合法性和真实性，将认证结果报告给应用服务器；G、应用服务器将认证结果反馈给客户终端，并决定可以提供服务或拒绝服务。本发明利用动态口令令牌和二维码相结合，提供双因素强身份认证，为手机银行的安全提供了保障。



CN 104657860 A

1.一种手机银行安全认证方法，其特征在于：所述方法包括以下步骤：

A、客户使用客户终端请求接入应用服务器；

B、应用服务器请求认证服务器对请求接入的客户的身份的合法性和真实性进行认证；

C、认证服务器向客户终端索取客户的身份认证信息；

D、客户激活动态二维码口令令牌，生成包含有自身账号和口令信息的动态二维码，呈现在令牌屏幕上等待扫描；

E、客户使用客户终端扫描动态二维码口令令牌屏幕上的动态二维码，并将该动态二维码通过网络传输给认证服务器；

F、认证服务器根据接收到的帐号信息调用相应的客户信息，产生与客户信息和事件相关的随机序列，并解析二维码口令进行比对，以判别客户身份的合法性和真实性，最后将认证结果报告给应用服务器；

G、应用服务器根据认证服务器提供的客户身份的合法性和真实性反馈给客户终端，并决定向客户提供服务或拒绝服务。

2.根据权利要求1所述的手机银行安全认证方法，其特征在于：所述的步骤D中，口令信息为动态密码，其位数为6位或多于6位的不定位数，包括数字、字母和符号的任两种或三种的组合。

3.根据权利要求1所述的手机银行安全认证方法，其特征在于：所述的步骤D中，口令信息为加入了全部或部分客户账号的随机口令。

4.根据权利要求1所述的手机银行安全认证方法，其特征在于：所述的客户终端为具有二维码扫描功能的智能手机。

一种手机银行安全认证方法

技术领域

[0001] 本发明涉及手机银行交易安全保障技术领域，尤其是一种基于动态二维码的手机银行安全认证方法。

背景技术

[0002] 随着智能手机及其应用软件的迅猛发展，手机银行作为一种全新的银行业务，受到广大客户的欢迎。由于其给客户带来极大的方便性和成本效益，越来越多的客户开始使用手机银行服务。因此，手机银行在提供方便性的同时，其安全性也引起了银行及客户的极大关注。由于手机银行建立在移动互联网络平台上，其安全性主要依赖于移动互联网络的安全。一般的手机银行都采用了多重安全保障机制，主要包括一些基本措施：1、手机号验证或短信认证；2、手机银行密码和银行卡密码的双重密码认证；3、图片附加码保护；4、预留信息验证；5、业务控制：如资讯、查询和理财类服务无需申请，转账、缴费类服务须申请开通方能使用；6、交易限额等。

[0003] 但是，虽然使用手机银行十分方便，但是相比传统的网上银行，手机银行支付的环节增加，而且支付环境更加开放和复杂，用户对手机银行安全的担忧较为突出，现有的几种基本保障机制并不能够完全的保障资金的安全。而随着网银安全性的逐步提高，一些诸如U盾、动态口令令牌等跟成熟有效的网银安全机制是否可以成功移植到手机银行的应用中，是值得人们思考的。

发明内容

[0004] 本发明要解决的技术问题是提供一种基于动态二维码的手机银行安全认证方法，利用动态口令令牌和二维码相结合，结合手机银行原有口令认证技术，提供双因素强身份认证，为手机银行的安全提供了保障。

[0005] 为解决上述技术问题，本发明所采取的技术方案如下：

一种手机银行安全认证方法，包括以下步骤：

A、客户使用客户终端请求接入应用服务器；

B、应用服务器请求认证服务器对请求接入的客户的身份的合法性和真实性进行认证；

C、认证服务器向客户终端索取客户的身份认证信息；

D、客户激活动态二维码口令令牌，生成包含有自身账号和口令信息的动态二维码，呈现在令牌屏幕上等待扫描；

E、客户使用客户终端扫描动态二维码口令令牌屏幕上的动态二维码，并将该动态二维码通过网络传输给认证服务器；

F、认证服务器根据接收到的帐号信息调用相应的客户信息，产生与客户信息和事件相关的随机序列，并解析二维码口令进行比对，以判别客户身份的合法性和真实性，最后将认证结果报告给应用服务器；

G、应用服务器根据认证服务器提供的客户身份的合法性和真实性反馈给客户终端，并决定向客户提供服务或拒绝服务。

[0006] 上述步骤 D 中，口令信息为动态密码，其位数为 6 位或多于 6 位的不定位数，包括数字、字母和符号的任两种或三种的组合。

[0007] 上述步骤 D 中，口令信息为加入了全部或部分客户账号的随机口令。

[0008] 上述客户终端为具有二维码扫描功能的智能手机。

[0009] 采用上述技术方案所产生的有益效果在于 ：

1、借助二维码技术特点，进一步完善动态口令的生成和验证方法

二维码具有高密度编码、信息容量大的特点，，这使得基于相关的加密算法生成的动态密码不再仅限定于 6 位数字，可以是多位甚至是位数不定的，也可以加入除数字外的其它字符，如字母（区分大小写）和标点符号等，目的是提高密码保密性。

[0010] 二维码可引入加密措施，因此其保密性、防伪性较好。本发明的动态二维码含有账号、动态密码等多种信息，对动态密码等部分的二维码编码方式进行特殊加密，避免普通的二维码识别软件轻易解读动态口令，而只能由手机银行客户端或者终端服务器完成解码工作。

[0011] 2、丰富动态口令的身份认证模式

网银动态密码的认证主要有三种模式 ：时间同步认证技术、事件同步认证技术和挑战 / 应答认证技术。而二维码中含有多种信息，大大拓展了动态密码的认证模式，如加入客户账号等其它因素来计算随机口令，这些信息是可以通过二维码一并发给认证服务器来计算的。

附图说明

[0012] 图 1 是本发明的实现原理图。

具体实施方式

[0013] 动态密码基本的思路是将共同密钥信息（作为计算动态密码的常量）和加密算法同时保存在认证服务器和动态密码令牌硬件内，再选择一个认证服务器和动态令牌都可以使用的变量（比如动态密码生成次数或者当前时间或者挑战码）用于计算动态密码。需要认证的时候，由动态密码令牌首先计算出动态密码，然后传输给认证服务器，认证服务器采用对应的信息计算出该动态密码，通过比较这两个密码是否相同来判断输入的动态密码是否正确。

[0014] 如图 1 所示，本发明的手机银行动态二维码口令令牌，实现了动态口令和二维码的有效结合，保障了客户使用手机银行时的账户安全，其使用方式与网银动态口令令牌类似，进一步借助二维码技术特点，使得动态口令的传递更加安全有效。在使用手机银行进行账户操作时，动态二维码口令令牌首先生成一个动态二维码口令，客户持手机扫描该动态二维码口令，并通过移动互联网络将动态二维码传递给银行认证服务器，由认证服务器产生与客户信息和事件相关的随机序列，并解析二维码口令进行比对，进而判别客户身份的合法性和真实性。

[0015] 本发明的具体实现步骤为 ：

1、客户使用智能手机等客户终端请求接入应用服务器；客户终端为具有二维码扫描功能的智能手机。

[0016] 2、应用服务器请求认证服务器对客户的身份的合法性和真实性进行认证；

3、客户终端需要扫描动态二维码口令，以进行身份认证；

4、客户激活动态二维码口令令牌，生成动态二维码，呈现在令牌屏幕上等待扫描；

5、客户持手机直接扫描动态二维码，动态二维码中包含有账号、口令等多种信息，可提供给认证服务器；其中口令信息为动态密码，其位数为 6 位或多于 6 位的不定位数，包括数字、字母和符号的任两种或三种的组合。进一步，口令信息为加入了全部或部分客户账号的随机口令。

[0017] 6、客户持手机将账号和口令通过网络传输给认证服务器；

7、认证服务器调用客户信息，产生与客户信息和事件相关的随机序列，并与客户输入的口令进行比对，判别客户身份的合法性和真实性；

8、认证服务器将认证结果报告给应用服务器；

9、应用服务器根据客户身份的合法性和真实性反馈给客户终端，并决定可以提供服务或拒绝服务。

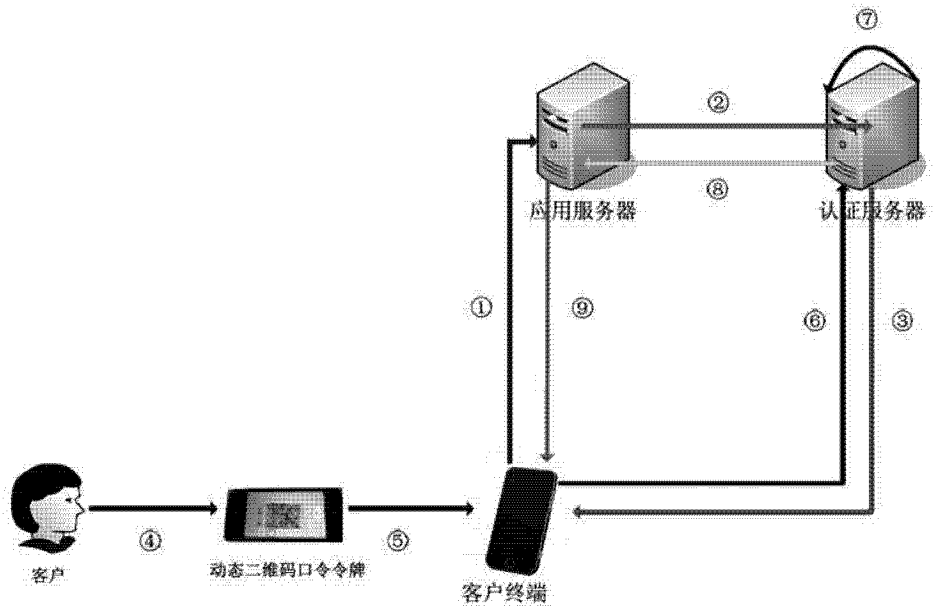


图 1