(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 103761802 A
(43)申请公布日 2014.04.30

(21)申请号 201410032790.1

(22)申请日 2014.01.24

(71)申请人 黄杰
地址 100077 北京市丰台区洋桥北里小区18-2-807

(72)发明人 黄杰 马文扬

(51)Int.Cl.
G07F 7/10(2006.01)

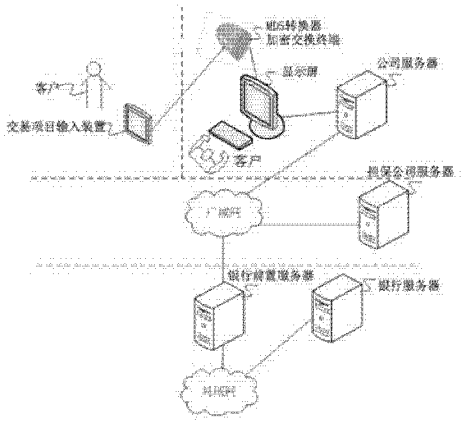
权利要求书1页 说明书9页 附图2页

(54)发明名称

一种移动存储支付认证系统

(57)摘要

本发明是一种移动存储支付认证系统，该系统包括：加密交换终端、公司服务器、银行服务器；公司服务器通过加密交换终端与银行服务器连接，读取移动存储中包含的介质号、认证口令、服务代码等用户信息，并将移动存储信息发送至公司服务器；公司服务器包括：移动存储IN接口、验证信息OUT接口及数据存储器；银行服务器包括：验证信息IN接口，接收缴费额、移动存储信息和对应的交易终端MAC地址；产品信息存储器，存储移动存储对应银行交易账户信息；认证结果OUT接口，将移动存储支付信息认证结果输出给公司服务器；公司服务器将该认证结果输出。本发明能够实现移动存储虚拟支付信息快速、准确、及时的认证操作。可广泛应用于移动办公、电子商务、电子政务、网络银行、云计算等领域。



CN 103761802 A

1. 一种移动存储支付认证系统，其特征在于系统包括：加密交换终端、公司服务器、银行服务器；用户终端通过公司内部网络与所述的公司服务器连接，所述的公司服务器通过所述的加密交换终端将广域网与所述的银行服务器连接，其中，

所述的读取移动存储中的信息包含介质号、认证口令、服务代码等用户信息，并将所述的移动存储信息通过公司内部网络发送到所述的公司服务器；

所述的公司服务器包括：移动存储 IN 接口，通过公司内部网络与所述的用户终端相连接，用于接收所述的移动存储信息；验证信息 OUT 接口，与所述的广域网相连接，用于输出缴费额、移动存储信息和对应的用户终端 MAC 地址；数据存储器，与所述的广域网连接，用于存储所述的交易信息；

所述的银行服务器包括：验证信息 IN 接口，与所述的广域网相连接，用于接收缴费额、移动存储信息和对应的交易终端 MAC 地址；产品信息存储器，与所述的广域网相连接，存储移动存储对应银行交易账户信息；认证结果 OUT 接口，用于将根据所述的交易信息、缴费额及用户银行账户信息生成的移动存储支付信息认证结果输出给公司服务器；

所述的公司服务器将所述的移动存储支付信息认证结果输出。

2. 如权利要求 1 所述的系统，其特征在于，所述的系统还包括：

交易担保公司服务器，通过广域网连接所述的银行服务器，所述的交易担保公司服务器包括：数据存储器，与所述的广域网相连接，用于存储担保交易数据；担保交易 OUT 接口，与所述的广域网相连接，用于将所述数据存储器存储的担保交易数据输出给所述的银行服务器。

3. 如权利要求 2 所述的系统，其特征在于，所述的系统还包括：

银行前置服务器，通过广域网分别与所述的公司服务器及交易担保公司服务器相连接，并通过局域网连接所述的银行服务器，所述银行前置服务器包括：数据 IN 接口，与所述的广域网相连接，用于接收从所述公司服务器及交易担保公司服务器发来的数据；格式转换封装单元，用于对接收的数据进行格式转换及封装；数据 OUT 接口，与所述的局域网相连接，用于将格式转换及封装后的数据输出给所述的银行服务器。

4. 如权利要求 1 所述的系统，其特征在于系统还包括：

MD5 转换器：与所述的用户终端相连接，用于输入移动存储的认证密钥；交易项目输入装置，与所述的用户终端相连接，用于输入银行名称及虚拟产品交易服务；交易项目服务器，与所述的用户终端相连接，用于根据所述银行名称及虚拟产品交易服务产生服务代码信息。

一种移动存储支付认证系统

技术领域

[0001] 本发明是关于移动存储技术，特别是一种移动存储支付信息认证系统。

背景技术

[0002] 普通移动存储设备具有容量大、低成本等优点，但是它存储的数据很容易被他人读出，无法满足大量数据安全存储应用的需求。随着电子商务 B2B 的逐渐完善，移动存储得到了普及的同时，数据安全日益受到人们的重视。目前本企业用户只需要使用公司配置的移动存储设备就可以到公司网站进行虚拟产品交易。移动存储设备的普及给客户的虚拟产品交易带来了很大的方便，但是现有技术中还存在如下问题：

首先，移动存储设备本身只是存储了用户的基本信息，不能够直接进行认证交易缴费，还需要进行网银绑定交易，有一定的局限性。其次，由于用户流动资金可能不足，此时无法做大额交易，往往错失商机；如果公司为其垫资又存在较大风险，需要处理大量数据，流程繁琐；而另一方面，担保公司很难在第一时间介入，出现商业断层。

发明内容

[0003] 本发明提供一种移动存储支付信息认证系统，以实现 B2B 模式下的虚拟产品交易信息认证。

[0004] 为了实现上述目的，本发明提供一种移动存储支付信息认证系统，该系统包括：加密交换终端、公司服务器、银行服务器，用户终端通过公司内部网络与所述的公司服务器连接，所述的公司服务器通过所述的加密交换终端将广域网与所述的银行服务器连接，所述的读取移动存储中的信息包含介质号、认证口令、服务代码等用户信息，并将所述的移动存储信息通过公司内部网络发送到所述的公司服务器；所述的公司服务器包括：移动存储 IN 接口，通过公司内部网络与所述的用户终端相连接，用于接收所述的移动存储信息；验证信息 OUT 接口，与所述的广域网相连接，用于输出缴费额、移动存储信息和对应的用户终端 MAC 地址；数据存储器，与所述的广域网连接，用于存储所述的交易信息；所述的银行服务器包括：验证信息 IN 接口，与所述的广域网相连接，用于接收缴费额、移动存储信息和对应的交易终端 MAC 地址；产品信息存储器，与所述的广域网相连接，存储移动存储对应银行交易账户信息；认证结果 OUT 接口，用于将根据所述的交易信息、缴费额及用户银行账户信息生成的移动存储支付信息认证结果输出给公司服务器；所述的公司服务器将所述的移动存储支付信息认证结果输出。

[0005] 进一步地，所述的系统还包括：交易担保公司服务器，通过广域网连接所述的银行服务器，所述的交易担保公司服务器包括：数据存储器，与所述的广域网相连接，用于存储担保交易数据；担保交易 OUT 接口，与所述的广域网相连接，用于将所述数据存储器存储的担保交易数据输出给所述的银行服务器。

[0006] 进一步地，所述的系统还包括：银行前置服务器，通过广域网分别与所述的医院服务器及保险公司服务器相连接，并通过局域网连接所述的银行服务器，所述银行前置服务

器包括 :数据接收接口,所述的广域网相连接,用于接收从所述医院服务器及保险公司服务器发来的数据 ;格式转换模块,用于对接收的数据进行格式转换 ;数据输出接口,与所述的局域网相连接,用于将格式转换后的数据输出给所述的银行服务器。

[0007] 进一步地,所述的系统还包括 :MD5 转换器 :与所述的用户终端相连接,用于输入移动存储的认证密钥 ;交易项目输入装置,与所述的用户终端相连接,用于输入银行名称及虚拟产品交易服务 ;交易项目服务器,与所述的用户终端相连接,用于根据所述银行名称及虚拟产品交易服务产生服务代码信息。

[0008] 本发明的有益效果在于,本发明的移动存储支付信息认证方法及系统能够快速的对公司、银行、但保公司保存的数据进行处理,实现移动存储交易支付信息快速、准确、及时的认证操作。

附图说明

[0009] 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。在附图中 :

图 1 为本实施例移动存储支付信息认证系统结构图 ;

图 2 为本实施例银行服务器 - 公司服务器的结构框图 ;

图 3 为本实施例银行前端服务器 - 提保公司服务器的结构框图。

具体实施方式

[0010] 为使本发明实施例的目的、技术方案和优点更加清楚明白,下面结合附图对本发明实施例做进一步详细说明。在此,本发明的示意性实施例及其说明用于解释本发明,但并不作为对本发明的限定。

[0011] 本实施例提供一种移动存储支付信息认证系统,该移动存储支付信息认证系统包括 :加密交换终端、公司服务器及银行服务器,所述的加密交换终端通过公司内部网络与所述的公司服务器连接,所述的公司服务器通过广域网与所述的银行服务器连接。

[0012] 所述的加密交换终端用于读取移动存储中的包含介质号、认证口令、服务代码等用户信息,并将所述的移动存储信息通过公司内部网络发送到所述的公司服务器。如图 1 所示,所述的持移动存储支付信息认证系统还包括 MD5 转换器,加密交换终端通过 MD5 转换器将所述的移动存储信息发送到公司服务器。

[0013] 所述移动存储支付信息认证系统还包括输入设备,输入设备包括 PIN 码扫描笔及交易项目输入装置。客户通过 PIN 码扫描笔扫描认证码,通过交易项目输入装置和 MD5 转换器输入银行名称及交易项目,此时,MD5 转换器根据所述银行名称及交易项目生成服务代码信息。交易项目输入装置包括一个显示屏,以显示交易项目供用户选择,该显示屏可以为触摸屏,交易客户通过该显示屏可以直接选择输入银行名称及交易项目。显示屏显示的服务项目包括金融机构及可交易虚拟产品项目,金融机构即持移动存储用户交易虚拟金融产品项目的银行,用户如果想要通过信用额度缴费,需要选择可用服务中的“XX 担保公司担保额度”。另外输入设备也可以只包括交易项目输入装置,通过交易项目输入装置的键盘(图

中未示）可用选择输入认证密令。

[0014] 所述的公司服务器根据所述的移动存储信息生成缴费额，并将缴费额、移动存储信息和对应的用户终端地址通过广域网发送到所述的银行服务器。

[0015] 如图 2 所示，所述的公司服务器包括：移动存储 IN 接口，验证信息 OUT 接口及数据存储器。

[0016] 移动存储 IN 接口通过公司内部网络与所述的用户终端相连接，用于接收所述的移动存储信息。验证信息 OUT 接口与所述的广域网相连接，用于输出缴费额、移动存储信息和对应的用户终端 MAC 地址。数据存储器与所述的广域网连接，用于存储所述的交易信息。

[0017] 不同用户支付可能会选用不同的银行，上述的银行服务器为与上述移动存储信息对应的支付银行。交易代码、认证密码、所述移动存储的终端 MAC 地址（交易终端 MAC 地址）及缴费额如表 1 所示。

[0018] 表 1

移动存储序列号	128 位加密密码	终端 MAC 地址	金额	交易代码	请求时间
5128800201871	F12XRU-H1 QADWQ!WD *$F3ER*+BE	EA89KYUP	25000	BOB1279075	20110705145268930

在表 1 中，128 位加密密码是根据用户输入的认证密码生成的，以在后续操作中与银行存储的服务认证密码进行验证。

[0019] 所述的银行服务器对接收的移动存储信息中的存储序列号、认证密码及交易代码进行验证，如果验证通过，则获取预存储的移动存储对应银行账户信息，根据所述的交易信息、缴费额及银行账户信息生成移动存储支付信息认证结果，并将所述的移动存储支付信息认证结果通过广域网发送到所述的公司服务器所述的公司服务器输出所述的移动存储支付信息认证结果。

[0020] 如图 2 所示，所述的银行服务器包括：验证信息 IN 接口，产品信息存储器及认证结果 OUT 接口。

[0021] 验证信息 IN 接口与与所述的广域网相连接，用于接收缴费额、移动存储信息和对应的交易终端 MAC 地址。产品信息存储器与所述的广域网相连接，存储移动存储对应银行交易账户信息。认证结果 OUT 接口用于将根据所述的交易信息、缴费额及用户银行账户信息生成的移动存储支付信息认证结果输出给公司服务器。所述的公司服务器将所述的移动存储支付信息认证结果输出。

[0022] 银行服务器对接收的移动存储信息中的序列号、认证码及交易代码进行验证，根据表 1 中移动存储序列号及交易代码查找是否存在对应的虚拟账号密码，并进行认证密码验证。如表 2 所示。

[0023] 表 2

移动存储序列号	交易代码	虚拟账户	服务认证密码
5128800201871	BOB1279075	9109782	F12XRU-H1 QADWQ!WD *$F3ER*+BE
5128800201871	BOB8627942	7429015	T#5YCC-K90BV?=!RXT#^Lo8!koP-
120401401450 21	BOB1279075	3714620	SDTY$DSSD*7ghh#E*9@DbT^FF$T
4308277030034	BOB1279075	4901274	@FSFG$V SW#$%C0FVQ@f4^FD!!23
3401087908262	BOB8627942	3714677	WDSF%^GD8%9u0SWSW@w2IoP[

表 1 中的移动存储序列号为 5128800201871，交易代码为 BOB1279075，身份认证装置查找表 2 中是否存在对应的移动存储序列号 5128800201871 及交易代码 BOB1279075，(其中的冗余可保证交易的完整性)由表 2 可以看出，存在对应的移动存储序列号 5128800201871 及交易代码 BOB1279075，并且该移动存储序列号及交易代码能够映射到虚拟账户 9109782。映射到虚拟账户 9109782 之后，可以进行密码认证，即查找表 2 中是否存在与表 1 中的 128 位加密密码对应的交易认证码，经过查找，可以看出，表 2 中的交易认证码与表 1 中的 128 位加密密码一致，均为 F12XRU-H1QADWQ!WD*$F3ER*+BE，此时，完成了对持移动存储序号用户的身份验证。

[0024] 银行服务器从所述交易信息中提取客户交易清单，将所述客户交易清单与预存储的交易项目列表进行比对，生成比对结果。公司的服务器中存储了该公司所有客户的交易信息，例如该持移动存储客户的 SNOMED PR1 的客户交易清单如下：

xxx IMPLIES

DrugTherapy

AND ∃rg.(

∃hasMethod.injectionAction

AND ∃hasDirectSubstance.warfarin

)

担保公司服务器中存储的允许担保的部分客户列表如下：

$$AnticoagulantTherapy \quad IMPLIES$$
$$DrugTherapy$$
$$AND\exists rg.($$
$$\exists hasMethod.administrationAction$$
$$AND\exists hasDirectSubstance.anticoagulant$$
$$)$$

由公司的客户交易清单及担保公司的担保客户列表可以看出，银行规定可以允许支付的交易有资金交易类，而持移动存储客户的交易清单中显示的为进行的虚拟金融产品交易，资金类为金融票据买卖，使用产品为 warfaring，通过 SNOMED PR1 电子交易的推理，发现 injectionAction 是一种 administrationAction，并且 warfarin 是一种 cogulant，因此可以得出该推荐产品是一种保值低风险类金融交易的结论，比对结果一致，从而通过支付费用的认证。利用 SNOMED PR1 电子交易进行支付信息认证操作的准确性较高，简单的关键词匹配则无法完成这种认证功能。

[0025] 客户交易账户信息包括资金账户近期收入、支出及余额如表 3 所示。

[0026] 表 3

移动存储序列号	交易账户号	收入	支出	交易日期	余额
5128800201871	9228800800477899275	758000	-	2014-1-1	3584000
5128800201871	9228800800477899275	758000	-	2014-2-1	3845000
12040140145021	9228800800477899275	758000	-	2014-3-1	4603000
4308277030034	9228800800477899275	758000	-	2014-4-1	5361000
3401087908262	9228800800477899275	-	3764000	2014-4-9	1597000
5128800201670	9228800800477899275	758000	-	2014-5-1	2355000
5128800201871	9228800800477899275	758000	3113000	2014-6-1	3113000
12040140145021	9228800800477899275	758000	-	2014-7-1	758000
1204012355021	9228800800477899275	758000	-	2014-8-1	1516000

表 3 中记录了存储序列号对应的收入、支出及余额情况，银行服务器可以从公司数据服务器中调取交易账户号对应的收入、支出及余额情况表，根据持移动存储客户的存储序列号查找对应的交易账户号的收入、支出及余额情况。银行服务器可以通过分析连续 3 个月交易账户收入为 0、支出超过某一数额（假设 2000000）、余额小于某一数额（500000）时拒绝支付认证。由表 3 可以看出，存储序列号为 5128800201871 的用户通过了支付认证。

[0027] 上述比对结果一致，并且交易账户信息的收入、支出及余额通过支付认证，银行服务器可以根据所述比对结果、缴费金额和银行交易账户信息的收入、支出及余额信息生成移动存储支付信息认证结果。

[0028] 移动存储支付信息认证结果可以包括认证是否通过信息，如果认证失败，银行服务器将通过公司服务器输出支付信息认证失败信息给持移动存储客户。

[0029] 如果认证成功，移动存储支付信息认证结果还包括包含支付金额、贷款利率及期限的认证信息，银行服务器将根据持移动存储客户的协议基准利率、担保风险附加生成的包含支付金额、担保款项利率及期限的认证成功信息。

[0030] 所述的银行服务器将所述的持移动存储支付信息认证结果通过广域网发送到所述的公司服务器，所述的公司服务器输出所述的持移动存储支付信息认证结果给所述的交易终端。

[0031] 银行服务器还可以包括：MAC 地址映射装置，用于在身份验证完成后，根据所述虚拟账户查找允许公司交易代码，然后根据查找所述公司交易代码对应的终端 MAC 地址中是否存在持移动存储客户终端 MAC 地址，如表 4 及表 5 所示。

[0032] 表 4

虚拟账户	允许公司交易代码
9109782	9785
9109782	2134
9109782	1234

表 5

公司交易代码	终端设备
2134	UI0092RS
2134	K9823TV3
2134	EA89KYUP
2134	L98HBM01
2134	K98J782Q

由表 4 可以根据虚拟账户查找到允许的公司交易代码，表 4 中的代码 2134 代表持移动存储客户公司交易代码，根据该代码可以在表 5 中查找是否终端 MAC 地址与表 1 中的 EA89KYUP 相同，经查找可知，表 1 与表 5 中的终端 MAC 地址相同。

[0033] 较佳地， 移动存储支付信息认证系统还可以包括：银行前置服务器及担保公司服务器。银行前置服务器通过广域网分别与所述的公司服务器及担保公司服务器相连接，并通过局域网连接所述的银行服务器。担保公司服务器通过广域网与所述的银行服务器相连接，用于向所述的银行服务器发送所述移动存储客户对应的担保金额数据。

[0034] 银行前置服务器，所述的公司服务器将交易金额、移动存储信息和对应的终端 MAC 地址通过广域网发送到所述的银行前置服务器，所述的银行前置服务器对交易金额、移动存储信息和对应的交易终端 MAC 地址进行格式转换后通过局域网发送给所述的银行服务器 205。

[0035] 如图 3 所示，所述银行前置服务器可以包括：数据 IN 接口，格式转换模块及数据 OUT 接口。

[0036] 数据 IN 接口与所述的广域网相连接，用于接收从所述公司服务器及担保公司服务器发来的数据。格式转换模块，连接数据 IN 接口及数据 OUT 接口，用于对接收的数据进行格式转换。数据 OUT 接口与所述的局域网相连接，用于将格式转换后的数据输出给所述的银行服务器。

[0037] 如图 3 所示，担保公司服务器可以包括：数据存储器，与所述的广域网相连接，用于存储保证金额数据；保证金额数据输出接口，与所述的广域网相连接，用于将所述数据存储器存储的保证金额数据输出给所述的银行服务器。

[0038] 所述的银行服务器根据所述的交易信息、交易金额、银行账户信息及保证金额数据生成移动存储支付信息认证结果。所述的银行系统服务器可以根据所述的虚拟账户判断持移动存储用户是否存在保证金，如果存在，根据保证金额及应缴交易费金额生成担保附加利率，以计算担保利率。

[0039] 银行服务器可以通过与担保公司服务器的接口，查询保证金额数据，分析持移动存储用户是否存在担保合同，判断担保合同能否涵盖该笔交易支出。

[0040] 银行服务器将包含支付金额、担保利率及期限的认证信息并发送给所述的移动存储用户读取终端。移动存储用户读取终端打印出包含支付金额，担保利率和期限回单供用户签字，完成担保缴费。

[0041] 本发明提供一种移动存储支付信息认证方法，该方法包括如下步骤：

步骤 1：读取移动存储中的包含移动存储序列号、认证码、交易代码及交易信息的移动存储信息，并将所述的移动存储信息通过公司内部网络发送到公司服务器。

[0042] 步骤 2：所述的公司服务器根据所述的移动存储信息生成交易金额，并将交易金额、移动存储信息和对应的终端 MAC 地址通过广域网发送到银行服务器。

[0043] 步骤 3：所述的银行服务器对接收的移动存储信息中的移动存储序列号、认证码、交易代码进行验证，如果验证通过，则获取预存储的移动存储对应银行账户信息，并根据所述的交易信息、交易金额及银行账户信息生成移动存储支付信息认证结果。

[0044] 根据表 1 中移动存储序列号及交易代码查找是否存在对应的虚拟账号密码。如果存在对应的虚拟账号密码，就可以进行验证认证密码。表 1 中的移动存储序列号为 5128800201871，交易代码为 BOB1279075，查找表 2 中是否存在对应的移动存储序列号 5128800201871 及交易代码 BOB1279075，由表 2 可以看出，存在对应的移动存储序列号 5128800201871 及交易代码 BOB1279075，并且该移动存储序列号及交易代码能够映射到虚拟账户 9109782。映射到虚拟账户 9109782 之后，可以进行密码认证，即查找表 2 中是否存在与表 1 中的 128 位加密密码对应的服务认证密码，经过查找，可以看出，表 2 中的服务认证密码与表 1 中的 128 位加密密码一致，均为 F12XRU-H1QADWQ!WD*$F3ER*+BE，此时，完成了对移动存储用户的身份认证。

[0045] 移动存储支付信息认证结果可以包括：是否允许交易支付，根据移动存储用户的协议基准利率、担保风险附加生成的包含支付金额、担保利率及期限的认证信息。移动存储用户满足担保支付的条件后，所述的银行服务器根据移动存储用户的协议基准利率、担保附加生成包含支付金额、担保利率及期限的认证信息。

[0046] 步骤 4：银行服务器将所述的移动存储支付信息认证结果通过广域网发送到所述的公司服务器。

[0047] 步骤 5：所述的公司服务器输出所述的移动存储支付信息认证结果。

[0048] 不管移动存储用户是否通过支付认证，所述的银行服务器都需要将所述的移动存储支付信息认证结果通过广域网发送到所述的公司服务器，所述的公司服务器输出所述的移动存储支付信息认证结果给用户终端。

[0049] 获取交易代码信息时，需要接收移动存储用户输入的银行名称及交易项目，根据所述银行名称及交易项目生成交易代码信息。移动存储用户通过 PIN 输入认证密码，通过交易项目输入装置银行名称及交易项目服务，用户终端根据所述银行名称及交易项目生成交易代码信息。交易项目输入装置包括一个显示屏，以显示交易项目供用户选择。另外输入设备也可以只包括交易项目输入装置，通过交易项目输入装置的键盘可用选择输入认证密码。

[0050] 在验证认证密码之后，所述的方法还包括：根据所述虚拟账户查找允许公司交易

代码，然后根据查找所述公司交易代码对应的终端MAC地址中是否存在所述终端MAC地址。由表4可以根据虚拟账户查找到允许的公司交易代码，表4中的代码2134代表交易代码，根据该代码可以在表5中查找是否终端MAC地址与表1中的EA89KYUP相同，经查找可知，表1与表5中的终端MAC地址相同。

[0051] 在所述的银行服务器根据用户的协议基准利率、担保风险附加生成包含支付金额、担保利率及期限的认证信息之前，所述的方法还包括：根据所述的虚拟账户判断用户是否存在担保合同；如果存在，根据担保金额及缴费金额生成担保附加利率，以计算担保利率。

[0052] 银行服务器将包含支付金额、担保利率及期限的认证信息并发送给所述的移动存储终端。读取终端打印出包含支付金额，担保利率和期限回单供持卡用户签字，完成了移动存储担保金额。

[0053] 本发明实施例的有益效果在于，本发明的有益效果在于，本发明的移动存储支付信息认证方法及系统能够快速的对公司、银行、担保保存的数据进行处理，实移动存储虚拟交易信息快速、准确、及时的认证操作。

[0054] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

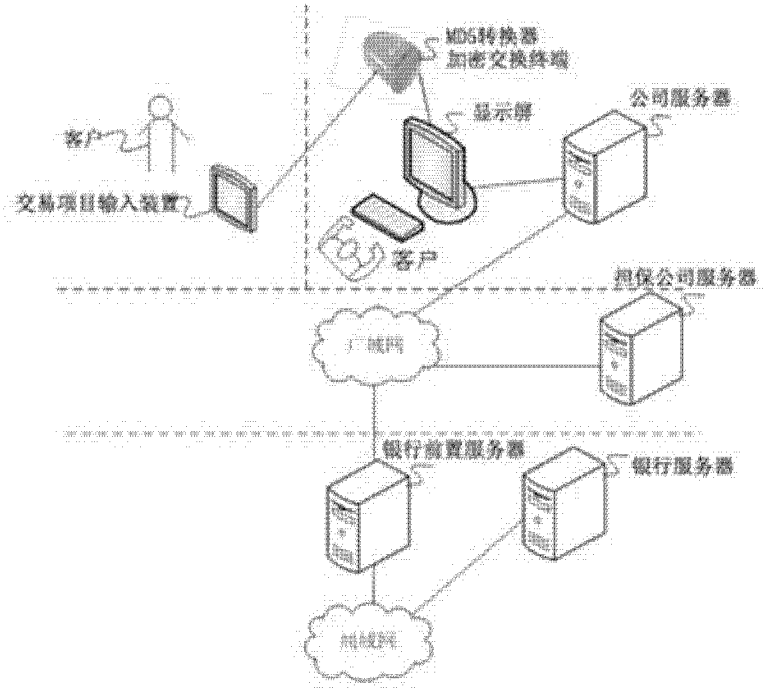

MD5转换器
加密交换终端
显示屏
公司服务器
客户
交易项目输入装置
客户
担保公司服务器
广域网
银行前置服务器
银行服务器
局域网

图 1

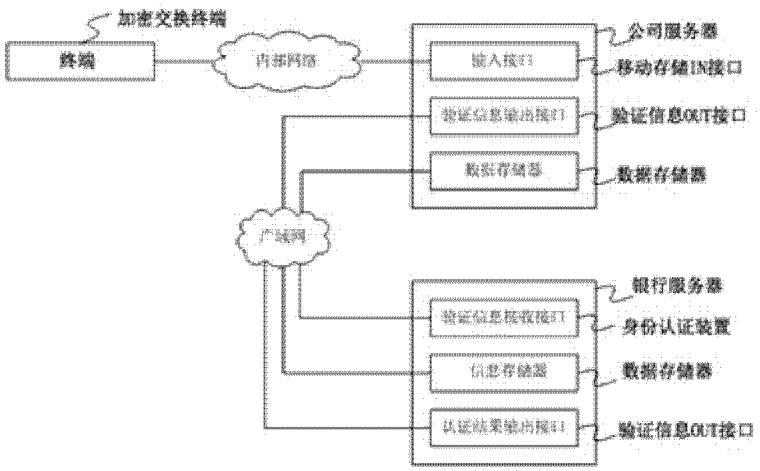

加密交换终端
终端
内部网络
输入接口
公司服务器
移动存储IN接口
验证信息输出接口
验证信息OUT接口
数据存储器
数据存储器
广域网
银行服务器
验证信息接收接口
身份认证装置
信息存储器
数据存储器
认证结果输出接口
验证信息OUT接口

图 2

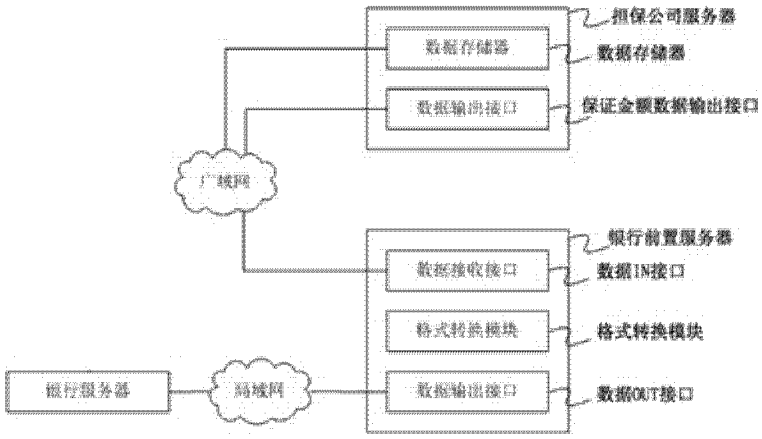

担保公司服务器
数据存储器
数据存储器
数据输出接口
保证金额数据输出接口
广域网
银行前置服务器
数据接收接口
数据IN接口
格式转换模块
格式转换模块
银行服务器
局域网
数据输出接口
数据OUT接口

图 3