(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 103078742 A
(43)申请公布日 2013.05.01

(21)申请号 201310009380.0

(22)申请日 2013.01.10

(71)申请人 天地融科技股份有限公司
地址 100083 北京市海淀区学清路38号B座1810室

(72)发明人 李东声

(74)专利代理机构 北京清亦华知识产权代理事务所（普通合伙） 11201
代理人 张大威

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

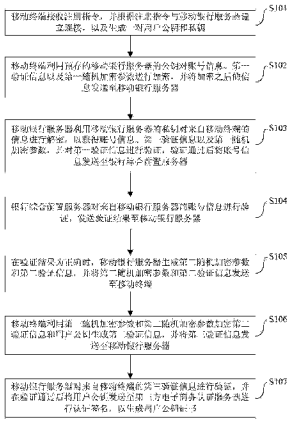
权利要求书4页 说明书8页 附图3页

(54)发明名称

数字证书的生成方法和系统

(57)摘要

本发明提出一种数字证书的生成方法和系统，该方法包括：移动终端与移动银行服务器建立连接，生成一对用户公钥和私钥，对账号信息、第一验证信息及第一随机加密参数加密并发送至移动银行服务器；移动银行服务器进行解密，并在验证通过后将账号信息发送至银行综合前置服务器；银行综合前置服务器验证账号信息；在验证结果为正确时，移动银行服务器将第二随机加密参数和第二验证信息发送至移动终端；移动终端生成第三验证信息，并将第三验证信息发送至移动银行服务器；以及移动银行服务器验证第三验证信息，并在验证通过后对用户公钥进行认证签名，以生成用户公钥证书。根据本发明可增加攻击的难度，提高安全性。



CN 103078742 A

1. 一种数字证书的生成方法，其特征在于，该方法包括：

a、移动终端接收注册指令，并根据所述注册指令与移动银行服务器建立连接，以及生成一对用户公钥和私钥；

b、移动终端利用预存的所述移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至所述移动银行服务器；

c、所述移动银行服务器利用所述移动银行服务器的私钥对来自所述移动终端的信息进行解密，以获得所述账号信息、所述第一验证信息以及第一随机加密参数，并对所述第一验证信息进行验证，验证通过后将所述账号信息发送至银行综合前置服务器；

d、所述银行综合前置服务器对来自所述移动银行服务器的所述账号信息进行验证，发送验证结果至所述移动银行服务器；

e、在所述验证结果为正确时，所述移动银行服务器生成第二随机加密参数和第二验证信息，并将所述第二随机加密参数和所述第二验证信息发送至所述移动终端；

f、所述移动终端利用所述第一随机加密参数和第二随机加密参数加密所述第二验证信息和所述用户公钥生成第三验证信息，并将第三验证信息发送至所述移动银行服务器；以及

g、所述移动银行服务器对来自所述移动终端的所述第三验证信息进行验证，并在验证通过后将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书。

2. 根据权利要求 1 所述的方法，其特征在于，所述步骤 a 中的移动终端接收注册指令，并根据所述注册指令与移动银行服务器建立连接的步骤包括：

所述移动终端从所加载的软件中获取移动银行服务器的公钥和银行综合前置服务器的公钥，对所述移动银行服务器的公钥和所述银行综合前置服务器的公钥进行验证，以及在验证通过之后根据所述注册指令与所述移动银行服务器建立连接。

3. 根据权利要求 1 所述的方法，其特征在于，所述步骤 b 还包括：

所述移动终端利用预存的所述移动银行服务器的公钥对所述移动终端的硬件特征信息进行加密，其中，所述硬件特征信息包括设备序列号和 / 或网卡的 MAC 地址；

或

所述移动终端利用预存的所述移动银行服务器的公钥对所述移动终端的硬件特征信息的哈希值进行加密，其中，所述硬件特征信息包括设备序列号和 / 或网卡的 MAC 地址。

4. 根据权利要求 3 所述的方法，其特征在于，所述账号信息包括手机号码、银行卡号和登录密码，所述步骤 b 包括：

所述移动终端接收所述移动银行服务器生成的所述第一验证信息，其中所述第一验证信息为图形验证码；以及

所述移动终端根据所述移动银行服务器的公钥对所述手机号码、银行卡号、登录密码、硬件特征信息、第一随机加密参数和第一验证信息进行加密，并将加密之后的信息发送至所述移动银行服务器，其中所述第一随机加密参数由所述移动终端生成；

或者

所述移动终端根据所述移动银行服务器的公钥对接收的所述手机号码、接收的所述银行卡号、计算得到的所述登录密码的哈希值、计算得到的所述硬件特征信息的哈希值、生成

的所述第一随机加密参数和接收的所述第一验证信息进行加密，并将加密之后的信息发送至所述移动银行服务器。

5. 根据权利要求 1 所述的方法，其特征在于，所述步骤 e 中将所述第二随机加密参数和所述第二验证信息发送至所述移动终端的步骤包括：

所述移动银行服务器根据所述第一随机加密参数对所述第二随机加密参数进行加密，并将加密后的所述第二随机加密参数发送至所述移动终端；

所述移动银行服务器将所述第二验证信息以短信的形式发送至所述移动终端。

6. 根据权利要求 5 所述的方法，其特征在于，将所述第二随机加密参数和所述第二验证信息发送至所述移动终端的步骤之后，步骤 f 之前，所述方法还包括：

所述移动终端根据所述第一随机加密参数对加密后的所述第二随机加密参数进行解密，获得所述第二随机加密参数；并接收用户输入的第二验证信息。

7. 根据权利要求 3 所述的方法，其特征在于，所述步骤 f 包括：

所述移动终端根据所述第一随机加密参数和第二随机加密参数对所述第二验证信息和所述用户公钥进行加密以生成所述第三验证信息，并根据所述用户私钥对所述硬件特征信息进行签名以生成第一签名信息，并将所述第三验证信息、用户公钥和第一签名信息发送至所述移动银行服务器；或

所述移动终端根据所述第一随机加密参数和第二随机加密参数对所述第二验证信息和所述用户公钥进行加密以生成所述第三验证信息，并根据所述用户私钥对所述硬件特征信息的哈希值进行签名以生成第一签名信息，并将所述第三验证信息、用户公钥和第一签名信息发送至所述移动银行服务器。

8. 根据权利要求 7 所述的方法，其特征在于，所述步骤 g 中所述移动银行服务器对来自所述移动终端的所述第三验证信息进行验证的步骤包括：

所述移动银行服务器根据存储的所述第一随机加密参数和第二随机加密参数对所述第二验证信息和所述用户公钥进行加密以生成第四验证信息，并根据所述用户公钥对所述第一签名信息进行验签，并判断所述第三验证信息与所述第四验证信息是否一致，所述第一签名信息是否通过验签；如果一致并通过验签，则验证通过。

9. 根据权利要求 1 或 7 所述的方法，其特征在于，步骤 f 中所述生成第三验证信息的步骤包括：

利用所述第一随机加密参数和所述第二随机加密参数对所述第二验证信息和所述用户公钥进行分段做 MAC。

10. 一种数字证书的生成系统，其特征在于，该系统包括：移动终端、移动银行服务器和银行综合前置服务器，其中，

所述移动终端，用于接收注册指令，并根据所述注册指令与所述移动银行服务器建立连接，以及生成一对用户公钥和私钥，并利用预存的所述移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至所述移动银行服务器；

所述移动银行服务器，用于利用所述移动银行服务器的私钥对来自所述移动终端的信息进行解密，以获得所述账号信息、所述第一验证信息以及第一随机加密参数，并对所述第一验证信息进行验证，验证通过后将所述账号信息发送至银行综合前置服务器；

所述银行综合前置服务器，用于对来自所述移动银行服务器的所述账号信息进行验证，发送验证结果至所述移动银行服务器；

所述移动银行服务器还用于在所述验证结果为正确时生成第二随机加密参数和第二验证信息，并将所述第二随机加密参数和所述第二验证信息发送至所述移动终端，所述移动终端利用所述第一随机加密参数和第二随机加密参数加密第二验证信息和所述用户公钥生成第三验证信息，并将第三验证信息发送至所述移动银行服务器，所述移动银行服务器对来自所述移动终端的所述第三验证信息进行验证，并在验证通过后将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书。

11. 根据权利要求 10 所述的系统，其特征在于，所述移动终端还从所加载的软件中获取移动银行服务器的公钥和银行综合前置服务器的公钥，对所述移动银行服务器的公钥和所述银行综合前置服务器的公钥进行验证，以及在验证通过之后根据所述注册指令与所述移动银行服务器建立连接。

12. 根据权利要求 10 所述的系统，其特征在于，所述移动终端还利用预存的所述移动银行服务器的公钥对所述移动终端的硬件特征信息或者所述移动终端的硬件特征信息的哈希值进行加密，并将加密之后的信息发送至所述移动银行服务器，其中，所述硬件特征信息包括设备序列号和 / 或网卡的 MAC 地址。

13. 根据权利要求 12 所述的系统，其特征在于，所述账号信息包括手机号码、银行卡号和登录密码，所述移动终端还用于：

接收所述移动银行服务器生成的所述第一验证信息，其中所述第一验证信息为图形验证码，以及根据所述移动银行服务器的公钥对所述手机号码、银行卡号、登录密码、硬件特征信息、第一随机加密参数和第一验证信息进行加密，并将加密之后的信息发送至所述移动银行服务器，其中所述第一随机加密参数由所述移动终端生成；

或者

所述移动终端根据所述移动银行服务器的公钥对接收的所述手机号码、接收的所述银行卡号、计算得到的所述登录密码的哈希值、计算得到的所述硬件特征信息的哈希值、生成的所述第一随机加密参数和接收的所述第一验证信息进行加密，并将加密之后的信息发送至所述移动银行服务器。

14. 根据权利要求 10 所述的系统，其特征在于，所述移动银行服务器还用于：

根据所述第一随机加密参数对所述第二随机加密参数进行加密，并将加密后的所述第二随机加密参数发送至所述移动终端，并将所述第二验证信息以短信的形式发送至所述移动终端。

15. 根据权利要求 14 所述的系统，其特征在于，所述移动终端还用于：

根据所述第一随机加密参数对加密后的所述第二随机加密参数进行解密，获得所述第二随机加密参数；并接收用户输入的第二验证信息。

16. 根据权利要求 12 所述的系统，其特征在于，所述移动终端还用于：

根据所述第一随机加密参数和第二随机加密参数对所述第二验证信息和所述用户公钥进行加密以生成所述第三验证信息，并根据所述用户私钥对所述硬件特征信息进行签名以生成第一签名信息，并将所述第三验证信息、用户公钥和第一签名信息发送至所述移动银行服务器；或

所述移动终端根据所述第一随机加密参数和第二随机加密参数对所述第二验证信息和所述用户公钥进行加密以生成所述第三验证信息，并根据所述用户私钥对所述硬件特征信息的哈希值进行签名以生成第一签名信息，并将所述第三验证信息、用户公钥和第一签名信息发送至所述移动银行服务器。

17. 根据权利要求 16 所述的系统，其特征在于，所述移动银行服务器还用于：

根据存储的所述第一随机加密参数和第二随机加密参数对所述第二验证信息和所述用户公钥进行加密以生成第四验证信息，并根据所述用户公钥对所述第一签名信息进行验签，并判断所述第三验证信息与所述第四验证信息是否一致，所述第一签名信息是否通过验签；如果一致并通过验签，则验证通过。

数字证书的生成方法和系统

技术领域

[0001] 本发明涉及信息安全技术领域，特别涉及一种数字证书的生成方法和一种数字证书的生成系统。

背景技术

[0002] 近年来，伴随互联网以及金融信息化的快速发展，网上银行因其便利、高效等优点迅速得到用户和银行业界的普遍推崇，其中数字证书是通过网上银行进行交易时用户和银行服务器的身份标识，可以保证网上交易的安全。

[0003] 目前，用户数字证书的生成均由银行服务器完成，经过第三方电子商务认证服务器认证之后再下发给用户所使用的终端。存在的问题是，银行服务器在下发的数字证书给终端的过程中，银行服务器可能不知道所发送的具体终端，从而有可能遭到拦截，数字证书在下发的过程中存在被盗取的安全隐患。

发明内容

[0004] 本发明的目的旨在至少解决上述技术缺陷之一。

[0005] 为达到上述目的，本发明第一个目的在于提出一种数字证书的生成方法，该方法包括以下步骤：a、移动终端接收注册指令，并根据所述注册指令与移动银行服务器建立连接，以及生成一对用户公钥和私钥；b、移动终端利用预存的所述移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至所述移动银行服务器；c、所述移动银行服务器利用所述移动银行服务器的私钥对来自所述移动终端的信息进行解密，以获得所述账号信息、所述第一验证信息以及第一随机加密参数，并对所述第一验证信息进行验证，验证通过后将所述账号信息发送至银行综合前置服务器；d、所述银行综合前置服务器对来自所述移动银行服务器的所述账号信息进行验证，发送验证结果至所述移动银行服务器；e、在所述验证结果为正确时，所述移动银行服务器生成第二随机加密参数和第二验证信息，并将所述第二随机加密参数和所述第二验证信息发送至所述移动终端；f、所述移动终端利用所述第一随机加密参数和第二随机加密参数加密第二验证信息和所述用户公钥生成第三验证信息，并将第三验证信息发送至所述移动银行服务器；以及 g、所述移动银行服务器对来自所述移动终端的所述第三验证信息进行验证，并在验证通过后将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书。

[0006] 根据本发明实施例的数字证书的生成方法，在移动终端生成用户公钥和私钥，将用户信息和用户公钥发送至移动银行服务器之前，移动终端与移动银行服务器和银行综合前置服务器多方进行验证，并在验证之后以数字证书的方式存储在移动银行服务器，保证用户公钥传输通路的安全性，增加攻击的难度。同时移动银行服务器经过对移动终端进行验证，可以明确知道与自己通信的是哪个移动终端，防止假冒移动终端与移动银行服务器进行交互，保证了安全。

[0007] 为达到上述目的，本发明第二个目的在于提出一种数字证书的生成系统，该系统包括：移动终端、移动银行服务器和银行综合前置服务器，其中，所述移动终端，用于接收注册指令，并根据所述注册指令与所述移动银行服务器建立连接，以及生成一对用户公钥和私钥，并利用预存的所述移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至所述移动银行服务器；所述移动银行服务器，用于利用所述移动银行服务器的私钥对来自所述移动终端的信息进行解密，以获得所述账号信息、所述第一验证信息以及第一随机加密参数，并对所述第一验证信息进行验证，验证通过后将所述账号信息发送至银行综合前置服务器；所述银行综合前置服务器，用于对来自所述移动银行服务器的所述账号信息进行验证，发送验证结果至所述移动银行服务器；所述移动银行服务器还用于在所述验证结果为正确时生成第二随机加密参数和第二验证信息，并将所述第二随机加密参数和所述第二验证信息发送至所述移动终端，所述移动终端利用所述第一随机加密参数和第二随机加密参数加密第二验证信息和所述用户公钥生成第三验证信息，并将第三验证信息发送至所述移动银行服务器，所述移动银行服务器对来自所述移动终端的所述第三验证信息进行验证，并在验证通过后将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书。

[0008] 根据本发明实施例的数字证书的生成系统，在移动终端生成用户公钥和私钥，将用户信息和用户公钥发送至移动银行服务器之前，移动终端与移动银行服务器和银行综合前置服务器多方进行验证，并在验证之后以数字证书的方式存储在移动银行服务器，保证用户公钥传输通路的安全性，增加攻击的难度。同时移动银行服务器经过对移动终端进行验证，可以明确知道与自己通信的是哪个移动终端，防止假冒移动终端与移动银行服务器进行交互，保证了安全。

[0009] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0010] 本发明上述的和 / 或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0011] 图 1 为本发明实施例 1 的数字证书的生成方法的流程图；

[0012] 图 2 为本发明实施例 2 的数字证书的生成方法的流程图；

[0013] 图 3 为本发明实施例 3 的数字证书的生成系统的结构示意图。

具体实施方式

[0014] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

[0015] 在本发明的描述中，需要理解的是，术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性。在本发明的描述中，需要说明的是，除非另有明确的规定

和限定，术语“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。此外，在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。

[0016] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0017] 下面参考附图描述根据本发明实施例的数字证书的生成方法和系统。

[0018] 实施例 1

[0019] 图 1 为本发明实施例 1 的数字证书的生成方法的流程图。

[0020] 如图 1 所示，根据本发明实施例的数字证书的生成方法包括下述步骤：

[0021] 步骤 S101，移动终端接收注册指令，并根据注册指令与移动银行服务器建立连接，以及生成一对用户公钥和私钥。

[0022] 具体的，移动终端下载银行客户端软件，在安装客户端软件时，从所加载的软件中获取移动银行服务器的公钥和银行综合前置服务器的公钥，并根据注册指令对移动银行服务器的公钥和银行综合前置服务器的公钥进行验证，以及在验证通过之后根据注册指令与移动银行服务器建立连接。具体地，银行客户端软件在进行安装时，移动银行服务器的公钥和银行综合前置服务器的公钥的根证书提前预置在移动终端中，在发送注册请求时，可以根据预置的根证书验证移动银行服务器的公钥和银行综合前置服务器的公钥是否正确，其中在移动银行服务器的公钥和银行综合前置服务器的公钥正确时才可以继续执行下述步骤，在移动银行服务器的公钥和银行综合前置服务器的公钥错误时提示错误信息。

[0023] 其中，移动银行服务端的私钥存储在移动银行服务器中，移动银行服务器的公钥和私钥用于对移动终端与移动银行服务端之间的通讯数据进行加密；银行服务端的私钥存储在银行综合前置服务器中，银行综合前置服务器的公钥和私钥用于对交易过程中的银行卡等敏感信息进行加密。

[0024] 当然，本实施例中，可以在用户点击注册后，触发移动终端根据预设的非对称加密算法的密钥生成规则生成用户的公私钥对，移动终端生成用户的公私钥对以便后续执行交易时通过该公私钥对与移动银行服务器进行交互。

[0025] 步骤 S102，移动终端利用预存的移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器。

[0026] 具体的，第一验证信息由移动银行服务器生成，并下发至移动终端并显示出来，以供用户查看并输入，该第一验证信息可以为图形验证码，从而可以防止攻击。

[0027] 移动终端接收用户输入的第一验证信息(例如图形验证码中的字符)。

[0028] 另外，本实施例中，第一随机加密参数由移动终端随机生成。

[0029] 账号信息包括：手机号码、银行卡号、注册完毕后的登录密码；或者

[0030] 账号信息包括：手机号码、银行卡号、注册完毕后的登录密码的哈希值。

[0031] 步骤 S103，移动银行服务器利用移动银行服务器的私钥对来自移动终端的信息进

行解密，以获得账号信息、第一验证信息以及第一随机加密参数，并对第一验证信息进行验证，验证通过后将账号信息发送至银行综合前置服务器。

[0032] 具体的，移动银行服务器验证移动终端发送的第一验证信息与自身生成的第一验证信息是否一致，一致则通过验证。

[0033] 另外，移动银行服务器获取解密信息后，保存账号信息中的手机号码以及第一随机加密参数。

[0034] 步骤 S104，银行综合前置服务器对来自移动银行服务器的账号信息进行验证，发送验证结果至移动银行服务器。

[0035] 具体的，银行综合前置服务器验证账号信息中的手机号码和银行卡号是否正确，发送验证结果至移动银行服务器。

[0036] 步骤 S105，在验证结果为正确时，移动银行服务器生成第二随机加密参数和第二验证信息，并将第二随机加密参数和第二验证信息发送至移动终端。

[0037] 具体的，在验证结果为正确时，移动银行服务器根据第一随机加密参数对第二随机加密参数进行加密，并将加密后的第二随机加密参数发送至移动终端；并且利用存储的手机号码将第二验证信息以短信的形式发送至移动终端。

[0038] 步骤 S106，移动终端利用第一随机加密参数和第二随机加密参数加密第二验证信息和用户公钥生成第三验证信息，并将第三验证信息发送至移动银行服务器。

[0039] 具体的，移动终端根据第一随机加密参数对加密后的第二随机加密参数进行解密，获得第二随机加密参数；并接收用户输入的第二验证信息；

[0040] 移动终端再根据第一随机加密参数和第二随机加密参数对用户输入的第二验证信息和用户公钥进行加密以生成第三验证信息，将第三验证信息和用户公钥发送至移动银行服务器。

[0041] 在本实施例中，可以利用第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行分段做 MAC 以生成第三验证信息。

[0042] 步骤 S107，移动银行服务器对来自移动终端的第三验证信息进行验证，并在验证通过后将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书。

[0043] 移动银行服务器根据存储的第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行加密以生成第四验证信息，并判断接收到的第三验证信息与生成的第四验证信息是否一致，如果一致，则验证通过。

[0044] 具体地，第三方电子商务认证服务器对用户的公钥进行认证签名，可以防止用户公钥被冒充，并将签名之后的用户公钥储存在移动银行服务器中，移动银行服务器存储签名的用户公钥之后提示用户公钥证书生成成功。

[0045] 根据本发明实施例的数字证书的生成方法，在移动终端生成用户公钥和私钥，将用户信息和用户公钥发送至移动银行服务器之前，移动终端与移动银行服务器和银行综合前置服务器多方进行验证，并在验证之后以数字证书的方式存储在移动银行服务器，保证用户公钥传输通路的安全性，增加攻击的难度。

[0046] 实施例 2

[0047] 图 2 为本发明实施例 2 的数字证书的生成方法的流程图。

[0048] 如图 2 所示，根据本发明实施例的数字证书的生成方法包括下述步骤：

[0049] 步骤 S201，移动终端接收注册指令，并根据注册指令与移动银行服务器建立连接，以及生成一对用户公钥和私钥。

[0050] 具体的，移动终端下载银行客户端软件，在安装客户端软件时，从所加载的软件中获取移动银行服务器的公钥和银行综合前置服务器的公钥，并根据注册指令对移动银行服务器的公钥和银行综合前置服务器的公钥进行验证，以及在验证通过之后根据注册指令与移动银行服务器建立连接。银行客户端软件在进行安装时，移动银行服务器的公钥和银行综合前置服务器的公钥的根证书提前预置在移动终端中，在发送注册请求时，可以根据预置的根证书验证移动银行服务器的公钥和银行综合前置服务器的公钥是否正确，其中在移动银行服务器的公钥和银行综合前置服务器的公钥正确时才可以继续执行下述步骤，在移动银行服务器的公钥和银行综合前置服务器的公钥错误时提示错误信息。

[0051] 其中，移动银行服务端的私钥存储在移动银行服务器中，移动银行服务器的公钥和私钥用于对移动终端与移动银行服务端之间的通讯数据进行加密；银行服务端的私钥存储在银行综合前置服务器中，银行综合前置服务器的公钥和私钥用于对交易过程中的银行卡等敏感信息进行加密。

[0052] 当然，本实施例中，可以在用户点击注册后，触发移动终端根据预设的非对称加密算法的密钥生成规则生成用户的公私钥对，移动终端生成用户的公私钥对以便后续执行交易时通过该公私钥对与移动银行服务器进行交互。

[0053] 步骤 S202，移动终端利用预存的移动银行服务器的公钥对账号信息、硬件信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器。

[0054] 具体的，第一验证信息由移动银行服务器生成，并下发至移动终端并显示出来，以供用户查看并输入，该第一验证信息可以为图形验证码，从而可以防止攻击。

[0055] 移动终端接收用户输入的第一验证信息(例如图形验证码中的字符)。

[0056] 另外，本实施例中，第一随机加密参数由移动终端随机生成。

[0057] 账号信息包括：手机号码、银行卡号、注册完毕后的登录密码；或者

[0058] 账号信息包括：手机号码、银行卡号、注册完毕后的登录密码的哈希值。

[0059] 硬件信息为：硬件特征信息或者硬件特征信息的哈希值，其中，硬件特征信息包括设备序列号和 / 或网卡的 MAC 地址。

[0060] 具体的，移动终端根据移动银行服务器的公钥对手机号码、银行卡号、登录密码、硬件信息、第一随机加密参数和第一验证信息进行加密，并将加密之后的信息发送至移动银行服务器，其中第一随机加密参数由移动终端生成。

[0061] 具体地，移动终端提取移动终端自身的硬件特征信息(或者计算提取的硬件特征信息的哈希值)，同时生成第一随机加密参数，接收用户录入的手机号码、银行卡号、登录密码(可以提示用户输入两次)、图形验证码显示的字符，通过点击提交之后移动终端通过移动银行服务器的公钥对获取的信息(包括手机号码、银行卡号、登录密码、硬件特征信息 / 硬件特征信息的哈希值、第一随机加密参数和图形验证码)进行加密并发送给移动银行服务器。

[0062] 当然，此时，移动终端还可以计算登录密码的哈希值，通过点击提交之后移动终端

通过移动银行服务器的公钥对获取的信息(包括手机号码、银行卡号、登录密码的哈希值、硬件特征信息/硬件特征信息的哈希值、第一随机加密参数和图形验证码)进行加密并发送给移动银行服务器。

[0063] 步骤S203,移动银行服务器利用移动银行服务器的私钥对来自移动终端的信息进行解密,以获得账号信息、硬件信息、第一验证信息以及第一随机加密参数,并对第一验证信息进行验证,验证通过后将账号信息发送至银行综合前置服务器。

[0064] 具体的,移动银行服务器验证移动终端发送的第一验证信息与自身生成的第一验证信息是否一致,一致则通过验证。

[0065] 另外,移动银行服务器获取解密信息后,保存账号信息中的手机号码、硬件信息以及第一随机加密参数。

[0066] 步骤S204,银行综合前置服务器对来自移动银行服务器的账号信息进行验证,发送验证结果至移动银行服务器。

[0067] 具体的,银行综合前置服务器验证账号信息中的手机号码和银行卡号是否正确,发送验证结果至移动银行服务器。

[0068] 步骤S205,在验证结果为正确时,移动银行服务器生成第二随机加密参数和第二验证信息,并将第二随机加密参数和第二验证信息发送至移动终端。

[0069] 具体的,在验证结果为正确时,移动银行服务器根据第一随机加密参数对第二随机加密参数进行加密,并将加密后的第二随机加密参数发送至移动终端;并且利用存储的手机号码将第二验证信息以短信的形式发送至移动终端。

[0070] 步骤S206,移动终端根据第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行加密以生成三验证信息,并根据用户私钥对硬件信息进行签名以生成第一签名信息,并将第三验证信息、用户公钥和第一签名信息发送至移动银行服务器。

[0071] 具体的,移动终端根据第一随机加密参数对加密后的第二随机加密参数进行解密,获得第二随机加密参数;并接收用户输入的第二验证信息;

[0072] 移动终端再根据第一随机加密参数和第二随机加密参数对用户输入的第二验证信息和用户公钥进行加密以生成第三验证信息,并根据用户私钥对硬件特征信息或者硬件特征信息的哈希值进行签名以生成第一签名信息,将第三验证信息、用户公钥以及第一签名信息发送至移动银行服务器。

[0073] 在本实施例中,可以利用第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行分段做MAC以生成第三验证信息。

[0074] 步骤S207,移动银行服务器对来自移动终端的第三验证信息和第一签名信息进行验证,并在验证通过后将用户公钥发送至第三方电子商务认证服务器进行认证签名,以生成用户公钥证书。

[0075] 具体的,移动银行服务器根据存储的第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行加密以生成第四验证信息,并根据用户公钥对第一签名信息进行验签,并判断第三验证信息与第四验证信息是否一致,第一签名信息是否通过验签;如果一致并通过验签,则验证通过。

[0076] 具体地,第三方电子商务认证服务器对用户的公钥进行认证签名,可以防止用户公钥被冒充,并将签名之后的用户公钥储存在移动银行服务器中,移动银行服务器存储签

名的用户公钥之后提示用户公钥证书生成成功。

[0077] 根据本发明实施例的数字证书的生成方法，在移动终端生成用户公钥和私钥，将用户信息和用户公钥发送至移动银行服务器之前，移动终端与移动银行服务器和银行综合前置服务器多方进行验证，并在验证之后以数字证书的方式存储在移动银行服务器，保证用户公钥传输通路的安全性，增加攻击的难度。同时移动银行服务器经过对移动终端的硬件信息进行验证，可以明确知道与自己通信的是哪个移动终端，防止假冒移动终端与移动银行服务器进行交互，保证了安全。

[0078] 实施例 3

[0079] 图 3 为本发明实施例 3 的数字证书的生成系统的结构框图。

[0080] 如图 3 所示，根据本发明实施例的数字证书的生成系统包括 ：移动终端 10、移动银行服务器 20、银行综合前置服务器 30 和第三方电子商务认证服务器 40。

[0081] 具体地，移动终端 10 用于接收注册指令，并根据注册指令与移动银行服务器 20 建立连接，以及生成一对用户公钥和私钥，并利用预存的移动银行服务器 20 的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器 20 ；或者

[0082] 移动终端 10 接收注册指令，并根据注册指令与移动银行服务器 20 建立连接，以及生成一对用户公钥和私钥，并利用预存的移动银行服务器 20 的公钥对账号信息、硬件信息(硬件特征信息或者硬件特征信息的哈希值)、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器 20。其中，硬件特征信息包括设备序列号和 / 或网卡的 MAC 地址。

[0083] 移动银行服务器 20 利用移动银行服务器 20 的私钥对来自移动终端 10 的信息进行解密，以获得账号信息、第一验证信息以及第一随机加密参数，并对第一验证信息进行验证，验证通过后将账号信息发送至银行综合前置服务器 30 ；或者

[0084] 移动银行服务器 20 利用移动银行服务器 20 的私钥对来自移动终端 10 的信息进行解密，以获得账号信息、硬件信息、第一验证信息以及第一随机加密参数，并对第一验证信息进行验证，验证通过后将账号信息发送至银行综合前置服务器 30。

[0085] 银行综合前置服务器 30 用于对来自移动银行服务器 20 的账号信息进行验证，发送验证结果至移动银行服务器 20，移动银行服务器 20 还用于在验证结果为正确时生成第二随机加密参数和第二验证信息，并将第二随机加密参数和第二验证信息发送至移动终端 10。

[0086] 移动终端 10 利用第一随机加密参数和第二随机加密参数加密第二验证信息和用户公钥生成第三验证信息，并将第三验证信息发送至移动银行服务器 20，移动银行服务器 20 对来自移动终端 10 的第三验证信息进行验证，并在验证通过后将用户公钥发送至第三方电子商务认证服务器 40 进行认证签名，以生成用户公钥证书 ；或者

[0087] 移动终端 10 根据第一随机加密参数和第二随机加密参数对用户输入的第二验证信息和用户公钥进行加密以生成第三验证信息，并根据用户私钥对硬件特征信息或者硬件特征信息的哈希值进行签名以生成第一签名信息，将第三验证信息、用户公钥以及第一签名信息发送至移动银行服务器 20，移动银行服务器 20 对来自移动终端 10 的第三验证信息和第一签名信息进行验证，并在验证通过后将用户公钥发送至第三方电子商务认证服务器

40 进行认证签名，以生成用户公钥证书。

[0088] 在本实施例中，可以利用第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行分段做 MAC 以生成第三验证信息。

[0089] 根据本发明实施例的数字证书的生成系统，在移动终端生成用户公钥和私钥，将用户信息和用户公钥发送至移动银行服务器之前，移动终端与移动银行服务器和银行综合前置服务器多方进行验证，并在验证之后以数字证书的方式存储在移动银行服务器，保证用户公钥传输通路的安全性，增加攻击的难度。同时移动银行服务器经过对移动终端的硬件信息进行验证，可以明确知道与自己通信的是哪个移动终端，防止假冒移动终端与移动银行服务器进行交互，保证了安全。

[0090] 在本发明的一个实施例中，移动终端 10 还用于：从所加载的软件中获取移动银行服务器 20 的公钥和银行综合前置服务器 30 的公钥，并根据注册指令对移动银行服务器 20 的公钥和银行综合前置服务器 30 的公钥进行验证，以及在验证通过之后根据注册指令与移动银行服务器 20 建立连接。

[0091] 移动银行服务器 20 还用于：根据验证通过信息生成第二随机加密参数和第二验证信息，并根据第一随机加密参数对第二随机加密参数进行加密，并将第二验证信息和加密后的第二随机加密参数发送至移动终端 10。其中，第二验证信息以短信的形式发送至移动终端 10，移动终端 10 根据第一随机加密参数对第二随机加密参数进行解密。

[0092] 移动银行服务器 20 还用于：根据存储的第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行加密以生成第四验证信息，并根据用户公钥对第一签名信息进行验签，并判断第三验证信息与第四验证信息是否一致，第一签名信息是否通过验签一致，如果一致并通过验签，则验证通过。

[0093] 尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同限定。

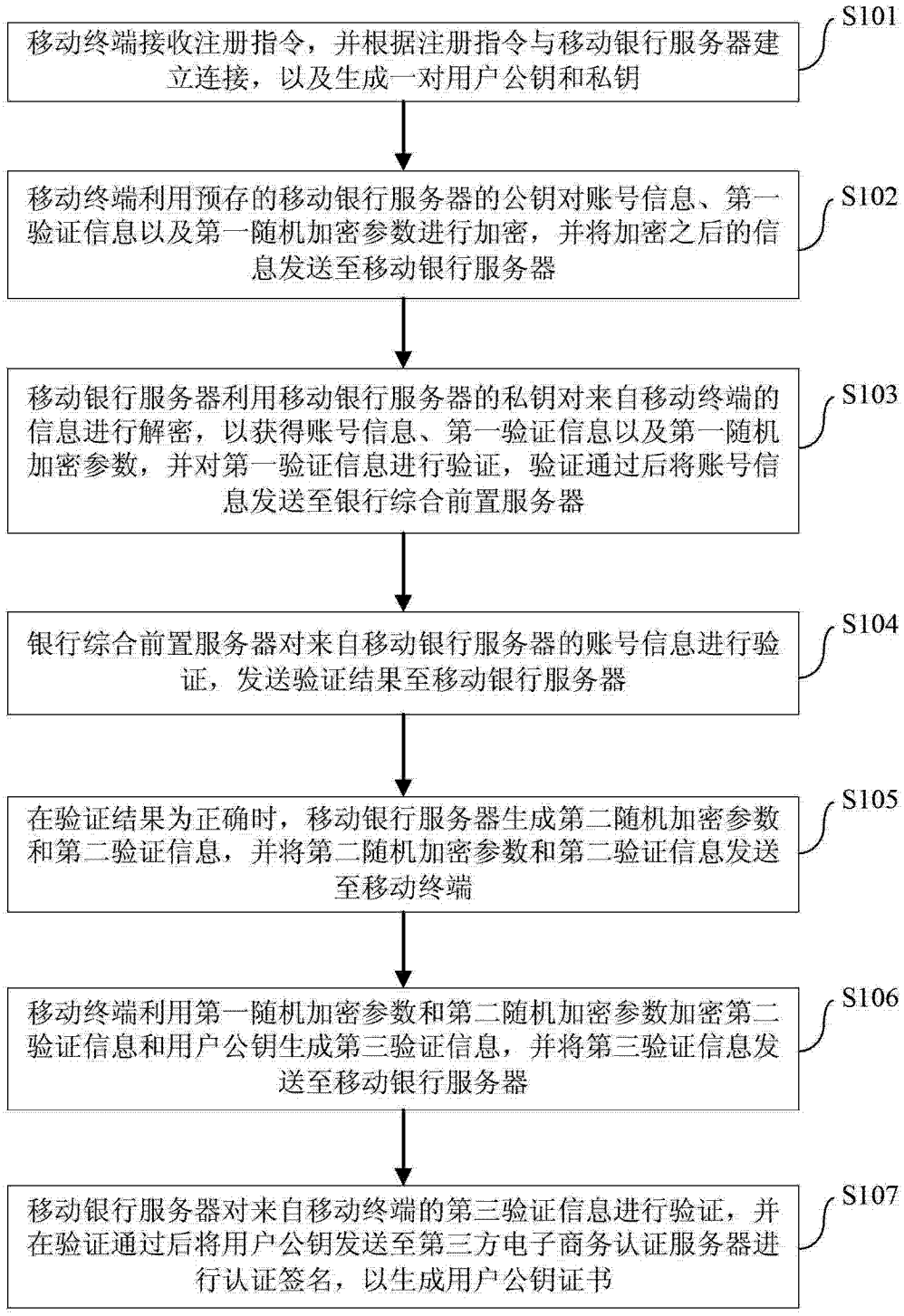

移动终端接收注册指令，并根据注册指令与移动银行服务器建立连接，以及生成一对用户公钥和私钥
S101
移动终端利用预存的移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器
S102
移动银行服务器利用移动银行服务器的私钥对来自移动终端的信息进行解密，以获得账号信息、第一验证信息以及第一随机加密参数，并对第一验证信息进行验证，验证通过后将账号信息发送至银行综合前置服务器
S103
银行综合前置服务器对来自移动银行服务器的账号信息进行验证，发送验证结果至移动银行服务器
S104
在验证结果为正确时，移动银行服务器生成第二随机加密参数和第二验证信息，并将第二随机加密参数和第二验证信息发送至移动终端
S105
移动终端利用第一随机加密参数和第二随机加密参数加密第二验证信息和用户公钥生成第三验证信息，并将第三验证信息发送至移动银行服务器
S106
移动银行服务器对来自移动终端的第三验证信息进行验证，并在验证通过后将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书
S107

图 1

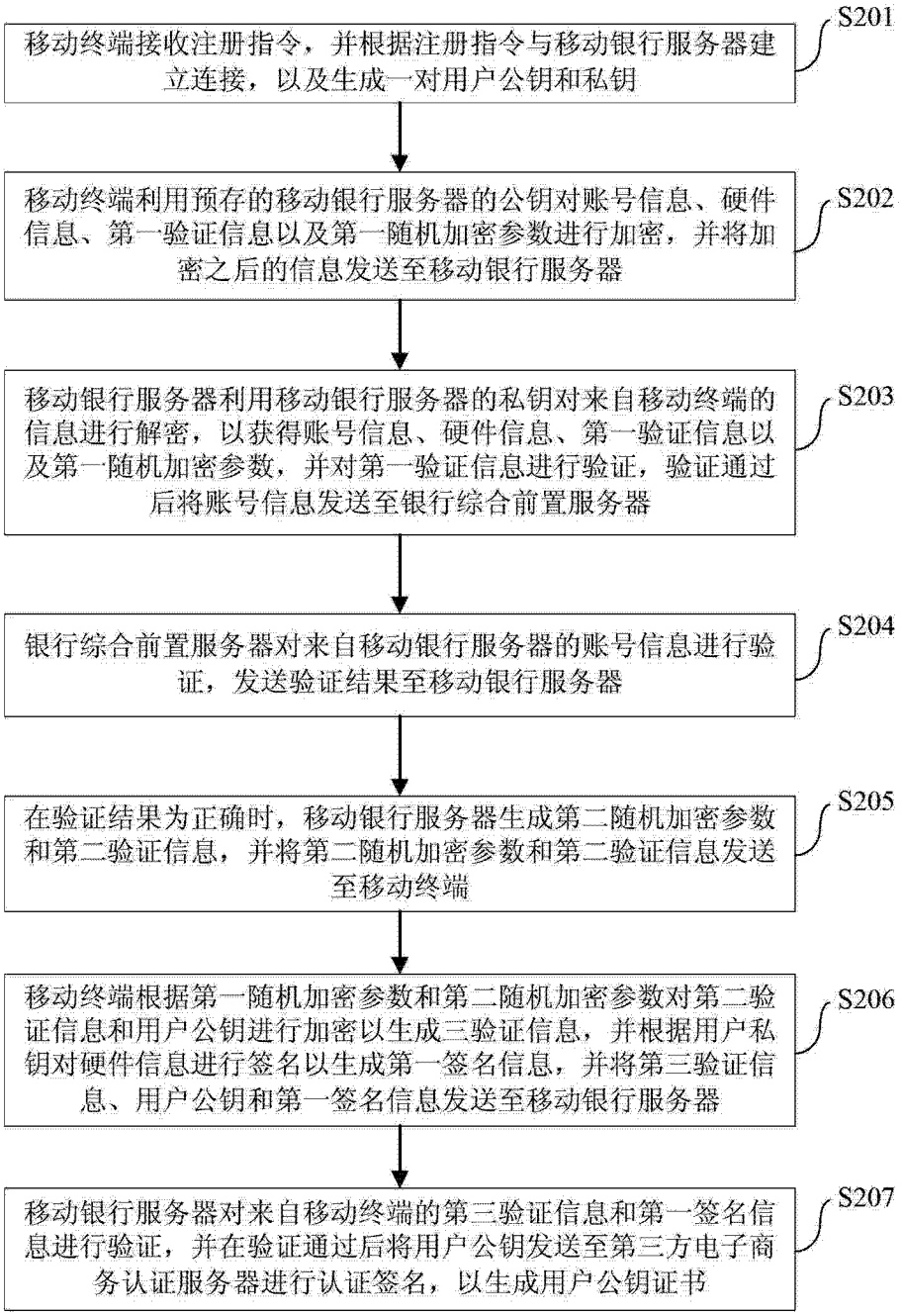

移动终端接收注册指令，并根据注册指令与移动银行服务器建立连接，以及生成一对用户公钥和私钥
S201
移动终端利用预存的移动银行服务器的公钥对账号信息、硬件信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器
S202
移动银行服务器利用移动银行服务器的私钥对来自移动终端的信息进行解密，以获得账号信息、硬件信息、第一验证信息以及第一随机加密参数，并对第一验证信息进行验证，验证通过后将账号信息发送至银行综合前置服务器
S203
银行综合前置服务器对来自移动银行服务器的账号信息进行验证，发送验证结果至移动银行服务器
S204
在验证结果为正确时，移动银行服务器生成第二随机加密参数和第二验证信息，并将第二随机加密参数和第二验证信息发送至移动终端
S205
移动终端根据第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行加密以生成三验证信息，并根据用户私钥对硬件信息进行签名以生成第一签名信息，并将第三验证信息、用户公钥和第一签名信息发送至移动银行服务器
S206
移动银行服务器对来自移动终端的第三验证信息和第一签名信息进行验证，并在验证通过后将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书
S207

图 2

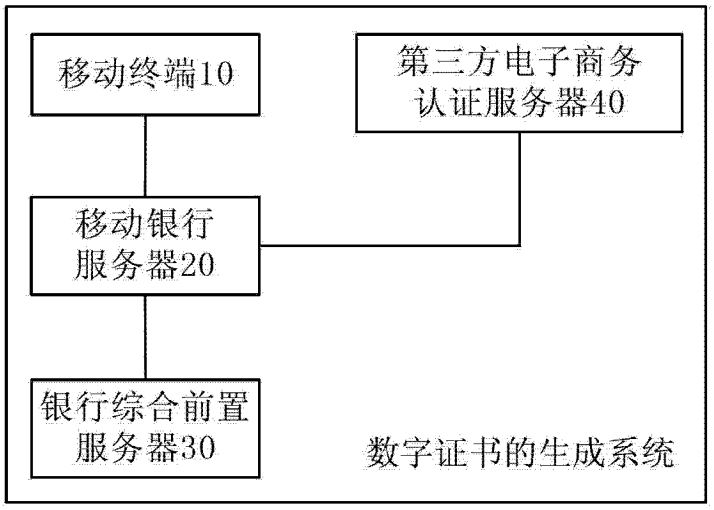


图 3