(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104468096 B
(45)授权公告日 2018.01.05

(21)申请号 201410719446.X

(22)申请日 2014.12.01

(65)同一申请的已公布的文献号
申请公布号 CN 104468096 A

(43)申请公布日 2015.03.25

(73)专利权人 公安部第三研究所
地址 200031 上海市徐汇区岳阳路76号

(72)发明人 邹翔 杨明慧 倪力舜 胥怡心 黄俊

(74)专利代理机构 上海智信专利代理有限公司 31002
代理人 王洁 郑暄

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 102833239 A,2012.12.19,
CN 103249045 A,2013.08.14,
CN 103731268 A,2014.04.16,
CN 103856640 A,2014.06.11,
US 2014325628 A1,2014.10.30,

审查员 张超群

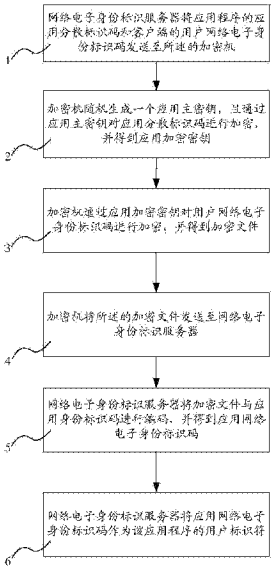
权利要求书2页 说明书6页 附图3页

(54)发明名称

基于密钥分散运算实现网络电子身份标识信息保护的方法

(57)摘要

本发明涉及一种基于密钥分散运算实现网络电子身份标识信息保护的方法，其中包括：网络电子身份标识服务器将应用程序的应用分散标识码和客户端的用户网络电子身份标识码发送至加密机；加密机随机生成一个应用主密钥，且对应用分散标识码进行加密得到应用加密密钥；加密机对用户网络电子身份标识码进行加密得到加密文件；网络电子身份标识服务器将加密文件与应用身份标识码进行编码得到应用网络电子身份标识码；网络电子身份标识服务器将应用网络电子身份标识码作为该应用程序的用户标识符。采用本发明的基于密钥分散运算实现网络电子身份标识信息保护的方法，对网络身份管理及个人隐私起到安全有效地保护，避免个人信息泄露，具有更广泛的应用范围。



CN 104468096 B

1.一种基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的方法基于网络电子身份标识服务系统，该系统包括客户端、加密机和网络电子身份标识服务器，所述的方法包括以下步骤：

(1)所述的网络电子身份标识服务器将应用程序的应用分散标识码和客户端的用户网络电子身份标识码发送至所述的加密机；

(2)所述的加密机随机生成一个应用主密钥，且通过所述的应用主密钥对所述的应用分散标识码进行加密，并得到应用加密密钥；

(3)所述的加密机通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密，并得到加密文件；

(4)所述的加密机将所述的加密文件发送至所述的网络电子身份标识服务器；

(5)所述的网络电子身份标识服务器将所述的加密文件与应用身份标识码进行编码，并得到应用网络电子身份标识码；

(6)所述的网络电子身份标识服务器将所述的应用网络电子身份标识码作为该应用程序的用户标识符。

2.根据权利要求1所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的步骤(1)之前，还包括以下步骤：

(0)所述的加密机生成一个包含数个应用主密钥的应用主密钥矩阵。

3.根据权利要求2所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的加密机随机生成一个应用主密钥，具体为：

所述的加密机从所述的应用主密钥矩阵中随机选取一个应用主密钥。

4.根据权利要求3所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的应用主密钥矩阵为16×16的矩阵。

5.根据权利要求1所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的通过所述的应用主密钥对所述的应用分散标识码进行加密，具体为：

所述的加密机通过所述的应用主密钥对所述的应用分散标识码的高8位进行加密得到所述的应用加密密钥的高8位，且所述的加密机通过所述的应用主密钥对所述的应用分散标识码的低8位进行加密得到所述的应用加密密钥的低8位。

6.根据权利要求1至5中任一项所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的通过所述的应用主密钥对所述的应用分散标识码进行加密，具体为：

所述的加密机采用对称加密算法通过所述的应用主密钥对所述的应用分散标识码进行加密。

7.根据权利要求6所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的对称加密算法为3DES加密算法、SM1加密算法或SM4加密算法。

8.根据权利要求1至5中任一项所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的加密机通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密，具体为：

所述的加密机采用对称加密算法通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密。

9.根据权利要求8所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的对称加密算法为3DES加密算法、SM1加密算法或SM4加密算法。

10.根据权利要求1所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的网络电子身份标识服务器将所述的加密文件与所述的应用身份标识码进行编码，具体为：

所述的网络电子身份标识服务器将所述的加密文件与所述的应用身份标识码进行拼接，并在所述的加密文件与所述的应用身份标识码拼接完成后进行Base64编码。

11.根据权利要求1所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的步骤(1)之前，还包括以下步骤：

(a)所述的网络电子身份标识服务器给各个已注册的应用程序分配一个应用身份标识码和一个应用分散标识码，并将所述的应用身份标识码和应用分散标识码保存至数据库中。

12.根据权利要求1所述的基于密钥分散运算实现网络电子身份标识信息保护的方法，其特征在于，所述的应用分散标识码为16字节二进制的标识码，所述的加密文件为32字节的文件，所述的应用身份标识码为4字节二进制的标识码，所述的应用网络电子身份标识码为48字节的标识码。

基于密钥分散运算实现网络电子身份标识信息保护的方法

技术领域

[0001] 本发明涉及网络身份管理与信息安全的交叉技术领域，具体是指一种基于密钥分散运算实现网络电子身份标识信息保护的方法。

背景技术

[0002] 网络时代人们的生活和工作方式发生根本性改变，个人的物质利益和精神利益都可以在信息网络中得到体现。互联网发展日新月异，各种应用层出不穷，用户常常具有相同的注册习惯，即在不同网站的账户使用相同的用户名和密码。因此用户在一个网站上的信息泄露，也许就是其在网络上其他应用的间接泄露，非常容易形成隐私信息泄露的蝴蝶效应，即互通关联账户间用户的姓名、身份证号码、地址、银行卡号、通讯录、短信、照片、GPS定位信息等隐私数据信息被复制、曝光、买卖等，导致用户遭受信息泄露带来的广告推销、垃圾短信轰炸、电话骚扰、恶性欺诈、勒索等问题。

[0003] 为此，2012年12月28日全国人大审议通过的《关于加强网络信息保护的决定》，表明网络身份管理已成为当前全国上下关注的焦点问题。实施网络身份管理，对整个社会公共领域而言，可以有效遏制互联网虚拟性滥用导致虚假信息、不良信息泛滥现象；对民生服务而言，可以提供社会公共服务，为公民提供便利；对于商业服务而言，可以解决网络交易诚信问题，已成为我国社会和谐发展的迫切需求。进入大数据时代，实现网络身份管理不仅需要能够识别和验证公民网络身份的真实性和有效性，也要阻止多个应用间由于主动(商业数据交换)或被动(被拖库)账户信息汇聚和数据分析所导致个人隐私信息泄露，以及由此造成的直接或间接损失。

[0004] 现有的各依赖方(即网络应用服务提供方)自建的账号管理系统在个人网络身份识别的准确性和身份信息保护方面均存在严重缺陷，导致了前面所述的大规模信息泄露，给依赖方自身及其用户造成了严重损失。

[0005] 目前广泛采用的“关联比对”等方案，在完成身份信息校验过程中，很容易造成个人身份信息的泄露，并且在大数据环境中将导致个人的所有网络行为全部暴露，其造成的损失将更加严重。

[0006] 网络电子身份标识(electronic IDentity，简称eID)是网络上远程证明个人身份的权威性电子信息文件，由“公安部公民网络身份识别系统”统一签发，其基于密码技术，以安全芯片为载体，用于公民在网络上远程证实身份，其编码在设计上已经对个人真实身份信息进行了保护。但面向所有依赖方如果使用唯一性编码在账户信息汇聚和数据分析情况下，仍然容易造成个人身份信息泄露。因此，必须设计一种面向依赖方的网络身份标识码生成方法，安全高效地解决大数据环境下的网络身份管理及个人隐私保护问题。

发明内容

[0007] 本发明的目的是克服了上述现有技术的缺点，提供了一种能够准确识别和验证公民网络身份的真实性和有效性，并且能够防止多个应用间由于主动或被动账户信息汇聚和

数据分析所导致个人隐私信息泄露，安全高效地解决大数据环境下的网络身份管理及个人隐私保护问题的基于密钥分散运算实现网络电子身份标识信息保护的方法。

[0008] 为了实现上述目的，本发明的基于密钥分散运算实现网络电子身份标识信息保护的方法具有如下构成：

[0009] 该基于密钥分散运算实现网络电子身份标识信息保护的方法，其主要特点是，所述的方法基于网络电子身份标识服务系统，该系统包括客户端、加密机和网络电子身份标识服务器，所述的方法包括以下步骤：

[0010] (1)所述的网络电子身份标识服务器将应用程序的应用分散标识码和客户端的用户网络电子身份标识码发送至所述的加密机；

[0011] (2)所述的加密机随机生成一个应用主密钥，且通过所述的应用主密钥对所述的应用分散标识码进行加密，并得到应用加密密钥；

[0012] (3)所述的加密机通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密，并得到加密文件；

[0013] (4)所述的加密机将所述的加密文件发送至所述的网络电子身份标识服务器；

[0014] (5)所述的网络电子身份标识服务器将所述的加密文件与所述的应用身份标识码进行编码，并得到应用网络电子身份标识码；

[0015] (6)所述的网络电子身份标识服务器将所述的应用网络电子身份标识码作为该应用程序的用户标识符。

[0016] 进一步地，所述的步骤(1)之前，还包括以下步骤：

[0017] (0)所述的加密机生成一个包含数个应用主密钥的应用主密钥矩阵。

[0018] 更进一步地，所述的加密机随机生成一个应用主密钥，具体为：

[0019] 所述的加密机从所述的应用主密钥矩阵中随机选取一个应用主密钥。

[0020] 更进一步地，所述的应用主密钥矩阵为16×16的矩阵。

[0021] 进一步地，所述的通过所述的应用主密钥对所述的应用分散标识码进行加密，具体为：

[0022] 所述的加密机通过所述的应用主密钥对所述的应用分散标识码的高8位进行加密得到所述的应用加密密钥的高8位，且所述的加密机通过所述的应用主密钥对所述的应用分散标识码的低8位进行加密得到所述的应用加密密钥的低8位。

[0023] 更进一步地，其特征在于，所述的通过所述的应用主密钥对所述的应用分散标识码进行加密，具体为：

[0024] 所述的加密机采用对称加密算法通过所述的应用主密钥对所述的应用分散标识码进行加密。

[0025] 更进一步地，所述的对称加密算法为3DES加密算法、SM1加密算法或SM4加密算法。

[0026] 更进一步地，所述的加密机通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密，具体为：

[0027] 所述的加密机采用对称加密算法通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密。

[0028] 更进一步地，所述的对称加密算法为3DES加密算法、SM1加密算法或SM4加密算法。

[0029] 进一步地，所述的网络电子身份标识服务器将所述的加密文件与所述的应用身份

标识码进行编码，具体为：

[0030] 所述的网络电子身份标识服务器将所述的加密文件与所述的应用身份标识码进行拼接，并在所述的加密文件与所述的应用身份标识码拼接完成后进行Base64编码。

[0031] 进一步地，所述的步骤(1)之前，还包括以下步骤：

[0032] (a)所述的网络电子身份标识服务器给各个已注册的应用程序分配一个应用身份标识码和一个应用分散标识码，并将所述的应用身份标识码和应用分散标识码保存至数据库中。

[0033] 进一步地，所述的应用分散标识码为16字节二进制的标识码，所述的加密文件为32字节的文件，所述的应用身份标识码为4字节二进制的标识码，所述的应用网络电子身份标识码为48字节的标识码。

[0034] 本发明的基于密钥分散运算实现网络电子身份标识信息保护的方法是面向依赖方(即网络应用服务提供方)的，不仅能够准确识别和验证公民网络身份的真实性和有效性，并且能够防止多个应用间由于主动(商业数据交换)或被动(被拖库)账户信息汇聚和数据分析所导致个人隐私信息泄露，安全高效地解决大数据环境下的网络身份管理及个人隐私保护问题，其具有以下积极的效益：

[0035] 1、应用网络电子身份标识码具有匿名性，不泄露用户的网络电子身份标识码和其它个人身份信息。经过密码算法(3DES/SM1/SM4)的加密保护，隐藏了用户真实身份相关信息；

[0036] 2、应用网络电子身份标识码具有唯一性，用户在每个应用上的编码是不同的，并且每个应用中所有用户的编码是不同的；

[0037] 3、应用网络电子身份标识码能够抗密码分析，无法通过密码分析得出相关明文信息。并且，每个应用的应用网络电子身份标识码生成密钥是由主密钥矩阵中随机选取的一个主密钥分散而成，各不相同，即使一个主密钥被泄露也可以将造成的危害控制在较小范围；

[0038] 4、应用网络电子身份标识码具有不可连结性，由于用户在每个应用上的编码是不同的，即使在账户信息汇聚和数据分析情况下，也无法对用户身份做跨应用确认。

附图说明

[0039] 图1为本发明的基于密钥分散运算实现网络电子身份标识信息保护的方法的流程图。

[0040] 图2为本发明的一个具体实施例的生成应用网络电子身份标识码的流程图。

[0041] 图3为本发明的一个具体实施例的生成加密密文的流程图。

具体实施方式

[0042] 为了能够更清楚地描述本发明的技术内容，下面结合具体实施例来进行进一步的描述。

[0043] 如图1所示，在一种实施方式中，该基于密钥分散运算实现网络电子身份标识信息保护的方法，其主要特点是，所述的方法基于网络电子身份标识服务系统，该系统包括客户端、加密机和网络电子身份标识服务器，所述的方法包括以下步骤：

[0044] (1)所述的网络电子身份标识服务器将应用程序的应用分散标识码和客户端的用户网络电子身份标识码发送至所述的加密机；

[0045] (2)所述的加密机随机生成一个应用主密钥，且通过所述的应用主密钥对所述的应用分散标识码进行加密，并得到应用加密密钥；

[0046] (3)所述的加密机通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密，并得到加密文件；

[0047] (4)所述的加密机将所述的加密文件发送至所述的网络电子身份标识服务器；

[0048] (5)所述的网络电子身份标识服务器将所述的加密文件与所述的应用身份标识码进行编码，并得到应用网络电子身份标识码；

[0049] (6)所述的网络电子身份标识服务器将所述的应用网络电子身份标识码作为该应用程序的用户标识符。

[0050] 其中，所述的应用分散标识码为16字节二进制的标识码，所述的加密文件为32字节的文件，所述的应用身份标识码为4字节二进制的标识码，所述的应用网络电子身份标识码为48字节的标识码。

[0051] 在一种优选的实施方式中，所述的步骤(1)之前，还包括以下步骤：

[0052] (0)所述的加密机生成一个包含数个应用主密钥的应用主密钥矩阵，其中，所述的应用主密钥矩阵为16×16的矩阵。

[0053] 在一种更优选的实施方式中，所述的加密机随机生成一个应用主密钥，具体为：

[0054] 所述的加密机从所述的应用主密钥矩阵中随机选取一个应用主密钥。

[0055] 在一种优选的实施方式中，所述的通过所述的应用主密钥对所述的应用分散标识码进行加密，具体为：

[0056] 所述的加密机通过所述的应用主密钥对所述的应用分散标识码的高8位进行加密得到所述的应用加密密钥的高8位，且所述的加密机通过所述的应用主密钥对所述的应用分散标识码的低8位进行加密得到所述的应用加密密钥的低8位。

[0057] 在一种更优选的实施方式中，其特征在于，所述的通过所述的应用主密钥对所述的应用分散标识码进行加密，具体为：

[0058] 所述的加密机采用对称加密算法通过所述的应用主密钥对所述的应用分散标识码进行加密，其中，所述的对称加密算法为3DES加密算法、SM1加密算法或SM4加密算法。

[0059] 在一种更优选的实施方式中，所述的加密机通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密，具体为：

[0060] 所述的加密机采用对称加密算法通过所述的应用加密密钥对所述的用户网络电子身份标识码进行加密，其中，所述的对称加密算法为3DES加密算法、SM1加密算法或SM4加密算法。

[0061] 在一种优选的实施方式中，所述的网络电子身份标识服务器将所述的加密文件与所述的应用身份标识码进行编码，具体为：

[0062] 所述的网络电子身份标识服务器将所述的加密文件与所述的应用身份标识码进行拼接，并在所述的加密文件与所述的应用身份标识码拼接完成后进行Base64编码。

[0063] 在一种优选的实施方式中，所述的步骤(1)之前，还包括以下步骤：

[0064] (a)所述的网络电子身份标识服务器给各个已注册的应用程序分配一个应用身份

标识码和一个应用分散标识码，并将所述的应用身份标识码和应用分散标识码保存至数据库中。

[0065] 本发明可广泛地应用于eID为载体的电子政务、电子商务、网银、网上支付等领域的应用中，并结合不同的应用密钥实现对个人隐私的安全保护。其中，不同的应用密钥是根据加密算法进行分散运算取得的。经过从种子数据、应用主密钥、地区分密钥、卡分散密钥等多层次逐级分散。密钥分散的目的是为了确保即使某个子密钥泄露了，也不会威胁到主密钥的安全管理，因为无法从子密钥和分散数据推导出主密钥，提高了系统的安全性、降低了安全风险和管理成本，以下为密钥分散运算的相关概念：

[0066] 1)主密钥：上一级管理中心的密钥称作主密钥；

[0067] 2)子密钥：由主密钥经过分散运算生成的密钥；

[0068] 3)密钥分散过程：由主密钥生成子密钥的运算过程；

[0069] 4)分散数据：用于密钥分散的计算数据。

[0070] 此外，本发明中的涉及的实体和相关关键定义如下：

[0071] eID服务系统：提供eID相关服务的后台系统。主要实现eID的生成、存储、使用及维护等全生命周期业务处理等。

[0072] 依赖方：依赖于eID服务系统给出的身份认证结果提供网络应用服务的实体。

[0073] eID码：根据相关算法为每个eID用户生成的唯一的标识码，长度为48字节，记为eID_code。而用户的eID_code(用户网络电子身份标识码)的未经过Base64编码之前，有效字段为32字节，记为eID_code_{32}。

[0074] 应用eID码(应用网络电子身份标识码)：根据用户eID_code产生的用于在依赖方中标识该用户的网络电子身份标识码，同一eID用户在不同应用中具有不同的标识码，长度为48字节，记为App_eIDCode。

[0075] 应用身份标识码：eID服务系统为第三方应用指定的4字节二进制代码，用于标识该第三方应用，记为App_ID。

[0076] 应用分散标识码：eID服务系统为第三方应用指定的16字节二进制码，保存在eID服务平台的数据库中，用来做密钥分散因子，记为App_code。

[0077] 应用主密钥矩阵：应用主密钥用于生成应用加密密钥，由加密机产生并保护存放，应用主密钥矩阵由一组应用主密钥组成，一般大小为16×16的矩阵。可由两个16进制字符标识应用主密钥在矩阵中的具体位置，记为MKeyMatrix。

[0078] 当某个应用App_i在eID服务系统注册后，eID服务系统分配给该应用App_i一个App_ID_i和App_code_i，并存入数据库中。此后，当该应用需要对该用户进行身份验证时，应用App_i将请求eID服务系统或自行对该用户进行身份验证。在完成身份验证后，eID服务系统为该用户生成$App_eIDCode_i$返回给该应用，即该eID用户在应用App_i上的用户标识符是$App_eIDCode_i$。

[0079] 以下结合图2和图3对本发明的关键技术进行说明：

[0080] 1.eID服务系统为用户生成App_eIDCode的流程，如图2所示，具体步骤如下：

[0081] 1)eID服务系统将应用的App_code和用户的eID_code_{32}作为密钥成分传入加密机；

[0082] 2)接收到加密机32字节的加密文件C_1；

[0083] 3)eID服务系统将加密文件C_1与4字节的App_ID拼接后进行Base64编码，为该应用

生成48字节的App_eIDCode,即:

[0084] $App\_eIDCode = Base_{64}(C_1 | App\_ID)$

[0085] 2.加密机生成加密文件的流程,如图3所示,具体步骤如下:

[0086] 1)加密机生成大小为16×16的应用主密钥矩阵MKeyMatrix[i,j]。

[0087] 2)加密机收到App_code和eID_code_{32}后,从应用主密钥矩阵中随机选取一个MKeyMatrix[a,b](其中i=a,j=b,a和b为自然数)作为应用主密钥,用对称加密算法(如3DES/SM1/SM4等)得到应用加密密钥cKey,即:

[0088] cKey=3DES/SM1/SM4(MKeyMatrix[a,b],App_code);

[0089] 3)根据应用加密密钥cKey,加密机对某用户的eID_code_{32}用对称加密算法(如3DES/SM1/SM4等)加密,得到该用户在这个应用上的生成的32字节加密文件C_1,即:

[0090] C_1=3DES/SM1/SM4(cKey,eID_code_{32});

[0091] 4)加密机将32字节加密文件C_1传给eID服务系统。

[0092] 此外,以下以3DES算法为例说明加密机如何用对称加密算法对用户的eID_code_{32}进行加密:

[0093] 加密机从应用主密钥矩阵中随机选取的一个应用主密钥,并采用3DES-128算法对16字节APP_Code进行分散运算,具体算法为:

[0094] 用该应用主密钥对APP_Code的前8字节加密作为应用加密密钥的前8字节,用该应用主密钥对APP_Code的后8字节加密作为应用加密密钥的后8字节,从而得到应用加密密钥cKey。

[0095] 本发明的基于密钥分散运算实现网络电子身份标识信息保护的方法是面向依赖方(即网络应用服务提供方)的,不仅能够准确识别和验证公民网络身份的真实性和有效性,并且能够防止多个应用间由于主动(商业数据交换)或被动(被拖库)账户信息汇聚和数据分析所导致个人隐私信息泄露,安全高效地解决大数据环境下的网络身份管理及个人隐私保护问题,其具有以下积极的效益:

[0096] 1、应用网络电子身份标识码具有匿名性,不泄露用户的网络电子身份标识码和其它个人身份信息。经过密码算法(3DES/SM1/SM4)的加密保护,隐藏了用户真实身份相关信息;

[0097] 2、应用网络电子身份标识码具有唯一性,用户在每个应用上的编码是不同的,并且每个应用中所有用户的编码是不同的;

[0098] 3、应用网络电子身份标识码能够抗密码分析,无法通过密码分析得出相关明文信息。并且,每个应用的应用网络电子身份标识码生成密钥是由主密钥矩阵中随机选取的一个主密钥分散而成,各不相同,即使一个主密钥被泄露也可以将造成的危害控制在较小范围;

[0099] 4、应用网络电子身份标识码具有不可连结性,由于用户在每个应用上的编码是不同的,即使在账户信息汇聚和数据分析情况下,也无法对用户身份做跨应用确认。

[0100] 在此说明书中,本发明已参照其特定的实施例作了描述。但是,很显然仍可以作出各种修改和变换而不背离本发明的精神和范围。因此,说明书和附图应被认为是说明性的而非限制性的。

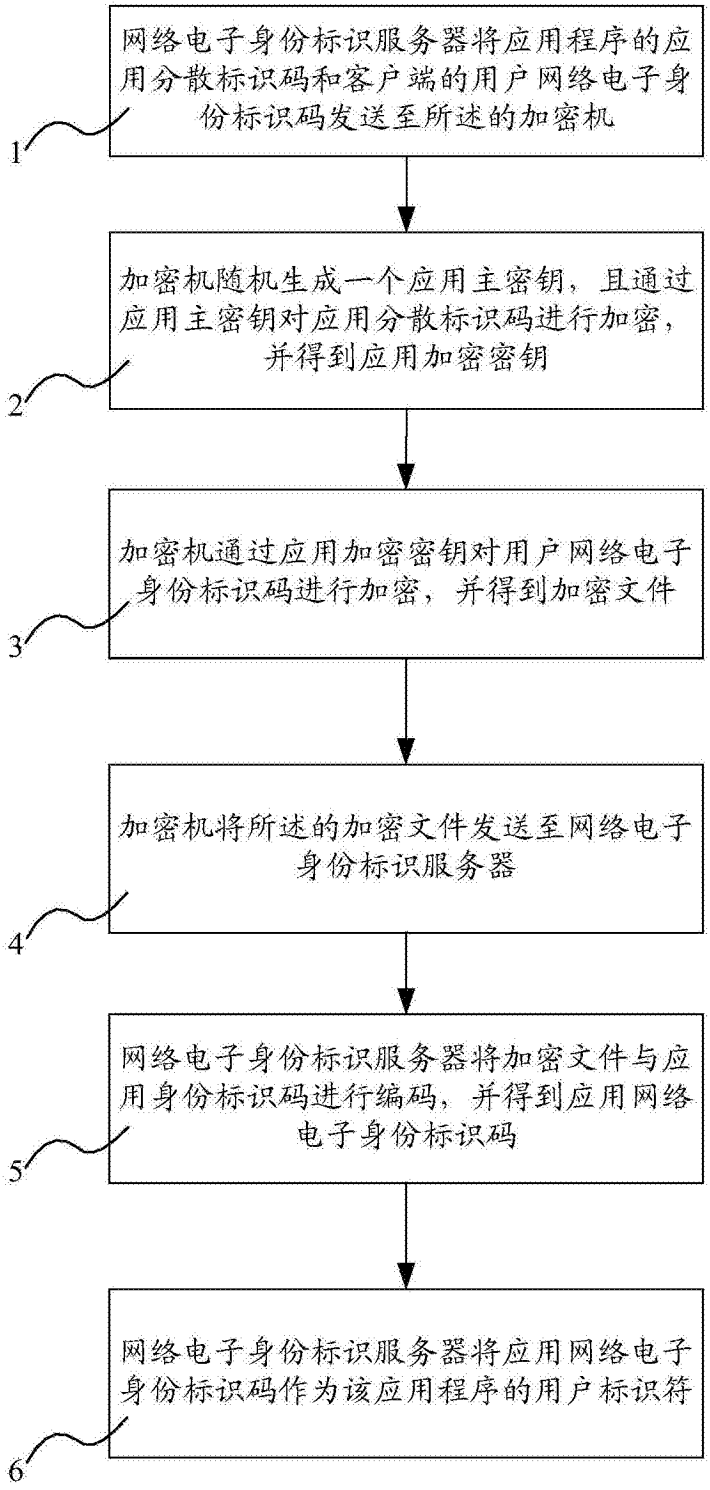

网络电子身份标识服务器将应用程序的应用分散标识码和客户端的用户网络电子身份标识码发送至所述的加密机
1
加密机随机生成一个应用主密钥，且通过应用主密钥对应用分散标识码进行加密，并得到应用加密密钥
2
加密机通过应用加密密钥对用户网络电子身份标识码进行加密，并得到加密文件
3
加密机将所述的加密文件发送至网络电子身份标识服务器
4
网络电子身份标识服务器将加密文件与应用身份标识码进行编码，并得到应用网络电子身份标识码
5
网络电子身份标识服务器将应用网络电子身份标识码作为该应用程序的用户标识符
6

图1

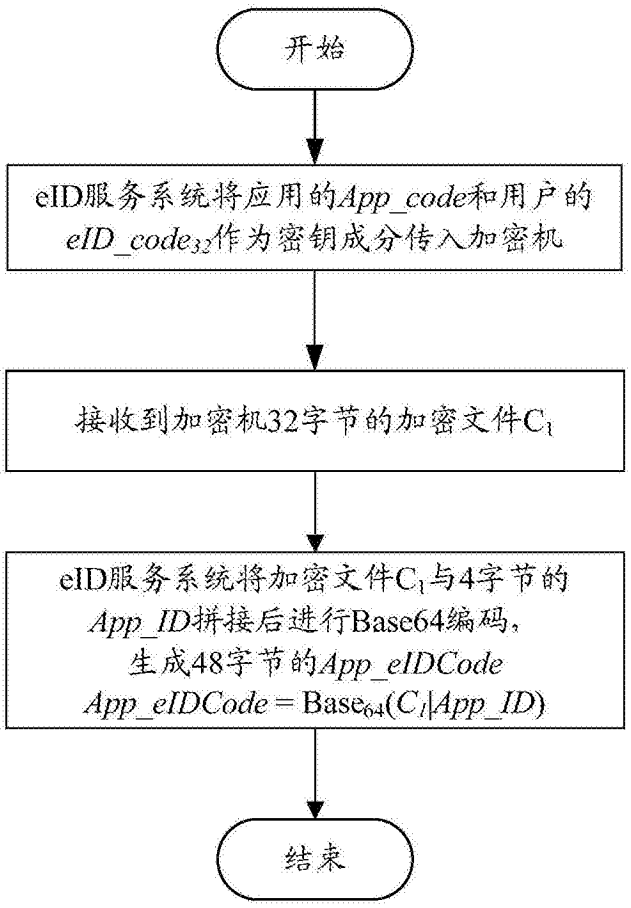

开始
eID服务系统将应用的App_code和用户的
eID_code32作为密钥成分传入加密机
接收到加密机32字节的加密文件C1
eID服务系统将加密文件C1与4字节的
App_ID拼接后进行Base64编码，
生成48字节的App_eIDCode
App_eIDCode = Base64(C1|App_ID)
结束

图2

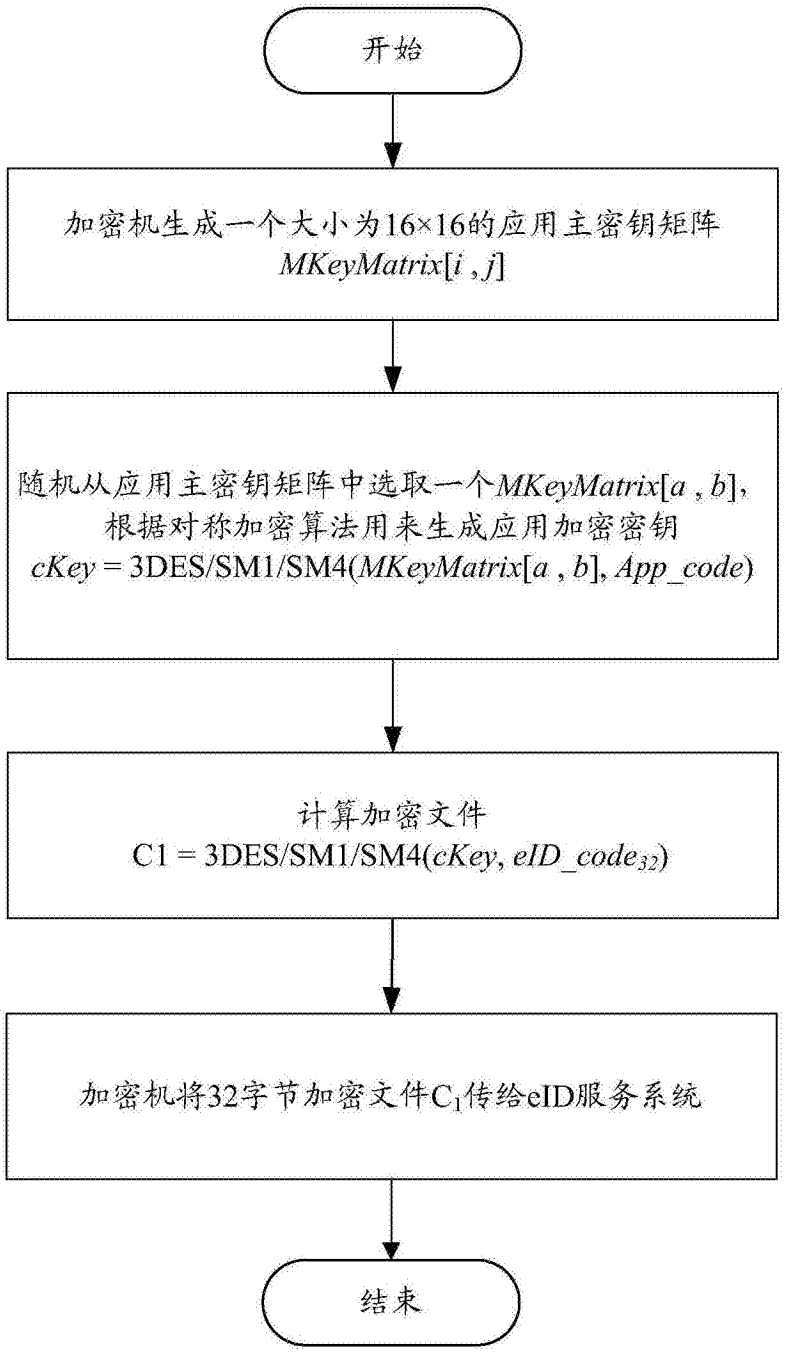

开始
加密机生成一个大小为16×16的应用主密钥矩阵
MKeyMatrix[i , j]
随机从应用主密钥矩阵中选取一个MKeyMatrix[a , b],
根据对称加密算法用来生成应用加密密钥
cKey = 3DES/SM1/SM4(MKeyMatrix[a , b], App_code)
计算加密文件
C1 = 3DES/SM1/SM4(cKey, eID_code32)
加密机将32字节加密文件C1传给eID服务系统
结束

图3