[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610113237.6

[43] 公开日 2007 年 3 月 14 日

[11] 公开号 CN 1929381A

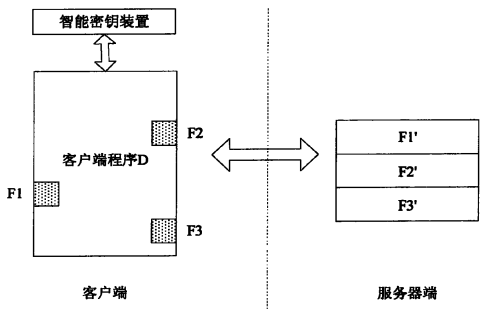
[22] 申请日 2006.9.20
[21] 申请号 200610113237.6
[71] 申请人 北京飞天诚信科技有限公司
地址 100083 北京市海淀区学院路 40 号研 7 楼 5 层
[72] 发明人 陆 舟 于华章
[74] 专利代理机构 北京众合诚成知识产权代理有限公司
代理人 李光松
权利要求书 2 页 说明书 8 页 附图 5 页

[54] 发明名称

一种基于网络的软件保护方法

[57] 摘要

本发明提供一种基于网络的软件保护方法，该方法是客户端程序与智能密钥装置结合，并以 C/S 或 B/S 结构与服务器端进行通信，客户端程序利用智能密钥装置对用户进行身份认证，实现对软件的保护；其具体步骤为：运行客户端程序；客户端程序利用智能密钥装置对用户进行身份认证；通过后，客户端程序结合服务器端继续执行。 客户端程序结合服务器端的方式可以为客户端程序需要服务器端响应特定的服务或提供特定的数据或客户端程序缺少部分代码需要服务器端提供。 本发明针对现有的网络身份验证方式用户名和密码以明文的方式在网络上传输容易被截获的缺点，在客户端结合智能密钥装置并使客户端程序有服务器的参与才能运行，增大破解难度，提高安全性。



1.一种基于网络的软件保护方法，该方法是客户端程序与智能密钥装置相结合，并以C/S或B/S结构与服务器端进行网络通信，客户端程序利用智能密钥装置对用户进行身份认证，实现对软件的保护；其特征在于，该方法的客户端程序与服务器端以网络通信的形式结合，客户端程序利用智能密钥装置对用户进行身份认证，实现对软件的保护，其具体步骤为：

1)运行客户端程序；

2)客户端程序利用智能密钥装置对用户进行身份认证；

3)身份认证通过后，客户端程序结合服务器端继续运行。

2.根据权利要求1所述基于网络的软件保护方法，其特征在于：所述客户端程序为一个完整程序或是经过处理的客户端程序，处理后的客户端程序需要服务器端响应特定的服务；或处理后的客户端程序需要服务器端提供特定的数据；或处理后的客户端程序为缺少部分代码的不完整程序，当客户端程序运行至缺少代码的位置时需要服务器端返回相应缺少的代码；或是上述三种情况的任意组合。

3.根据权利要求1所述基于网络的软件保护方法，其特征在于：所述利用智能密钥装置对用户身份认证的方法为通过用户名和PIN码进行验证，或是基于公钥体制进行验证，或采用冲击响应的方法进行验证。

4.根据权利要求2所述的基于网络的软件保护方法，其特征在于：所述客户端程序需要服务器端响应特定的服务是当客户端程序运行至需要服务器端提供特定服务的位置时，客户端程序向服务器端请求服务，服务器端将相应服务的结果返回客户端程序。

5. 根据权利要求4所述的基于网络的软件保护方法，其特征在于：所述服务的结果以密文形式传递。

6.根据权利要求2所述基于网络的软件保护方法，其特征在于：所述客户端程序需要服务器端提供特定的数据是当客户端程序运行至需要服务器端提供数据的位置时，客户端程序向服务器端请求数据，服务器端将相应数据返回客户端。

7.根据权利要求6所述的基于网络的软件保护方法，其特征在于：所述数据以密文形式传递。

8.根据权利要求2所述基于网络的软件保护方法，其特征在于：如果客户端程序缺少部分代码，当客户端程序运行至缺少代码的位置时，客户端程序向服务器端请求下载相应代码，服务器端向客户端程序返回相应代码来填充客户端程序缺少部分。

9.根据权利要求8所述的基于网络的软件保护方法，其特征在于：所述代码以密文形式传递。

一种基于网络的软件保护方法

技术领域

本发明属于软件保护领域，具体涉及结合智能密钥装置的一种基于网络的软件保护方法。

背景技术

软件作为一种无形的产品，凝聚了开发者的辛勤劳动，然而，开放平台上的软件几乎从一开始就受到盗版问题的困扰，盗版者常常会让软件厂商血本无归。

基于网络（包括局域网和因特网）的软件系统，其系统结构主要包括C/S结构和B/S结构两种类型：C/S （Client/Server）结构，即客户端/服务器端结构；B/S（Browser/Server）结构，即浏览器端/服务器端结构。其中B/S结构是在C/S结构基础上发展而来的，浏览器端实质上也是一种客户端程序，它将 HTML 脚本转换成可视的界面。通过这两种结构可以充分利用两端硬件环境的优势，将任务合理分配到客户端或浏览器端和服务器端来实现，降低了系统的通讯开销。目前大多数应用软件系统都是C/S或B/S形式的两层结构。

对于上述两种结构的软件系统，对于客户端或浏览器端应用程序的安装程序一直没有行之有效的机制和手段来保障版权不受侵犯，安装程序被盗版者肆意的拷贝和散播，给软件开发商的权益造成了巨大的伤害，而且也给服务器端应用及数据的安全性带来了巨大的挑战。

在中国专利 200310111755.0 中公开了一种利用指纹进行软件保护的方法及其应用装置。其以指纹鉴定软件使用者合法身份并以安装在认证服务器上的软件加密开发包模块来保护软件的关键代码和数据。

在中国专利 0211355.0 和 200510109229.x 中，公开了一种软件保护方法。是将编译后的程序文件中的代码分解为两部分，其中分解出的代码块在加密装置中运行，其余部分代码在计算机中运行。

在目前众多的软件保护类产品中，智能密钥装置是被普遍使用的产品。智能密钥装置是一种带有处理器和存储器的小型硬件装置，它可通过计算机的数据通

讯接口与计算机连接，实现控制软件运行和限制软件功能的功能。其内部可以保存私钥，可预置加密算法，同时也可后期自行定制部分算法。当为一个软件产品安装了智能密钥装置对其进行保护后，软件产品与智能密钥装置硬件就被绑定在一起，离开智能密钥装置软件就无法正常运行。智能密钥装置内置的私钥具有对外不可见性，与密钥相关的运算完全在装置内部运行，且智能密钥装置具有物理抗攻击的特性，安全性极高。

以往的网络身份验证方式，用户名和密码会以明文的方式在网络上传输，很容易被恶意分子截获，非对称密钥体制和冲击响应机制可以用来解决这个问题。非对称密钥体制是目前应用最广泛的一种身份验证体制，在这一体制中，加密密钥与解密密钥各不相同。公钥体制的数字签名既保证了信息的机密性，又保证了信息具有不可抵赖性，其原理是：首先将明文用被验证方私钥签名，得到数字签名，然后将数字签名发向验证方，验证方用被验证方的公钥进行解密，最后与原文进行比较，进行验证。

HMAC-Hash 是常用的冲击响应认证方式。HMAC-Hash 是对 Hash 算法的加强，Hash 算法是一种无需密钥参与的单向加密算法，可以将任意长度的数据进行加密，输出成固定长度的密文。HMAC(keyed-Hashing Message Authentication Code)将密钥结合 Hash 运算，并且每次运算都有随机数据参与，以保证每次认证过程产生的结果数据不同，这样即使有恶意分子截获了某一次认证数据，也无法通过下一次的认证。同时，密钥并没有在网络中传递，从根本上避免了密钥的泄漏，提供一种更安全的身份验证方式。

发明内容

本发明的目的是提供一种基于网络的软件保护方法，该方法是客户端程序与智能密钥装置相结合，并以 C/S 或 B/S 结构与服务器端进行网络通信，客户端程序与服务器端以网络通信的形式结合，客户端程序利用智能密钥装置对用户进行身份认证，实现对软件的保护，防止了用户名和密码以明文的方式在网络上传输，增大软件破解的难度，提高软件的安全性。

其具体步骤为：

1)运行客户端程序；

2)客户端程序利用智能密钥装置对用户进行身份认证；

3)身份认证通过后，客户端程序结合服务器端继续运行。

所述客户端程序为一个完整程序或是经过处理的客户端程序，处理后的客户端程序需要服务器端响应特定的服务；或处理后的客户端程序需要服务器端提供特定的数据；或处理后的客户端程序为缺少部分代码的不完整程序，当客户端程序运行至缺少代码的位置时需要服务器端返回相应缺少的代码；或是上述三种情况的任意组合。

所述利用智能密钥装置对用户身份认证的方法为通过用户名和PIN码进行验证，或是基于公钥体制进行验证，或采用冲击响应的方法。

上述方法中，所述客户端程序需要服务器端响应特定的服务是当客户端程序运行至需要服务器端提供特定服务的位置时，客户端程序向服务器端请求服务，服务器端将相应服务的结果返回客户端程序，所述服务的结果以密文形式传递。

上述方法中，所述客户端程序需要服务器端提供特定的数据是当客户端程序运行至需要服务器端提供数据的位置时，客户端程序向服务器端请求数据，服务器端将相应数据返回客户端程序，所述数据以密文形式传递。

上述方法中，如果客户端程序缺少部分代码，当客户端程序运行至缺少代码的位置时，客户端程序向服务器端请求下载相应代码，服务器端向客户端程序返回相应代码来填充客户端程序缺少部分，所述代码以密文形式传递。

本发明与现有技术相比，其优点在于：由于智能密钥装置是能够防止篡改和盗取内部信息的安全载体，智能密钥装置能实现只在设备内部使用私钥，这样私钥就不能被复制和攻击，本发明采用智能密钥装置保护软件的方法安全性极高；

另外，本发明的客户端软件是不完整的软件，运行时需服务器的参与而不能单独运行，从而增大破解方法的难度，使安全性更高。

附图说明

图 1 为第一种认证方式的流程图。

图 2 为第二种认证方式的流程图。

图 3 为第三种认证方式的流程图。

图 4 为客户端程序需要服务器端提供服务或数据时的运行流程图。

图 5 为客户端程序缺少部分代码的的软件系统示意图。

图 6 为客户端程序需要下载缺少代码时的运行流程图。

具体实施方式

本发明是针对现有技术的不足提供一种基于网络的软件保护方法，该方法是客户端程序与智能密钥装置相结合，并以 C/S 或 B/S 结构与服务器端进行网络通信，客户端程序与服务器端以网络通信的形式结合，客户端程序利用智能密钥装置对用户进行身份认证，实现对软件的保护，避免了用户名和密码以明文的方式在网络上传输，增大软件破解的难度，提高软件的安全性。

其具体步骤为:

1)运行客户端程序;

2)客户端程序利用智能密钥装置对用户进行身份认证;

3)身份认证通过后，客户端程序结合服务器端继续运行。

所述客户端程序为一个完整程序或是经过处理的客户端程序，处理后的客户端程序需要服务器端响应特定的服务；或处理后的客户端程序需要服务器端提供特定的数据；或处理后的客户端程序为缺少部分代码的不完整程序，当客户端程序运行至缺少代码的位置时需要服务器端返回相应缺少的代码；或是上

述三种情况的任意组合。

所述缺少特定的服务指客户端程序的缺少一个或多个重要函数（服务），当客户端运行到缺少函数的位置时，向服务器端发送请求，服务器端运行与客户端相应的缺少的函数，并将运行后的结果返回给客户端，由于函数的概念可能不能包括我们要限定的所有这种情况，所以用服务一词概括。

所述特定的数据是指在客户端程序运行的过程中需要访问一些与程序运行相关的数据，例如专利查询软件，用户想要看到专利的具体内容，这些具体内容需要通过服务器端发给客户端，用户才能看到，这些具体内容就是本发明中所说的数据。

下面结合附图和具体实施方式进一步说明本发明，但不作为对本发明的限定。

由于B/S结构中的浏览器实质上也是一种客户端程序，所以以下说明中的客户端程序泛指C/S结构中的客户端程序和B/S结构中的浏览器程序。

用户购买客户端程序时销售商会针对每一个用户生成一对公钥和私钥，例如公私钥对与客户端程序的序列号对应（在具体实现时公私钥对只要能够与用户的唯一标识对应即可），公钥存储在服务器端，私钥存储于智能密钥装置中发放给用户。

在本发明中服务器端对客户端的身份验证可以采用多种方式，现选用三种最优的实施方式加以描述。

第一种实施方式是利用PIN码进行身份验证，参见图1，验证的具体步骤如下：

步骤101，客户端程序运行；

步骤102，客户端程序首先向服务器端发送登录请求；

步骤103，服务器端向客户端发送身份认证请求；

步骤104，客户端程序检测智能密钥装置是否存在，如果不存在则步骤111提示错误并退出，如果存在则执行步骤105；

步骤105，客户端程序将身份认证请求转发至智能密钥装置中；

步骤106，智能密钥装置要求用户输入PIN码；

步骤107，智能密钥装置对用户输入的PIN码进行验证，PIN码错误则步骤111客户端程序提示错误并退出，PIN码正确则执行步骤108；

步骤108，智能密钥装置将验证成功信息通过客户端程序发送至服务器端；

步骤109，服务器端接收验证成功信息后允许客户端程序对服务器端的数据和资源等的访问；

步骤110，客户端程序继续运行；

步骤111，提示错误并退出。

第二种实施方式利用公钥体制进行身份验证，参见图2，验证的具体步骤如

下：

步骤 201，客户端程序运行；

步骤 202，客户端程序首先向服务器端发送登录请求；

步骤 203，服务器端向客户端发送身份验证请求，即向客户端程序发送一个随机字符串；

步骤 204，客户端程序检测智能密钥装置是否存在，如果不存在则步骤 211 提示错误并退出，如果存在则执行步骤 205；

步骤 205，客户端程序将上述随机字符串转发至智能密钥装置；

步骤 206，智能密钥装置利用其内置的算法和私钥签名随机字符串；

步骤 207，智能密钥装置将此签名通过客户端程序发送给服务器端；

步骤 208，服务器端利用与客户端程序对应的公钥验证签名，签名验证失败则步骤 211 提示错误并退出，验证成功则执行步骤 209；

步骤 209，服务器端允许客户端程序对服务器端的数据和资源等的访问；

步骤 210，客户端程序继续运行；

步骤 211，提示错误并退出。

第三种实施方式采用冲击响应的方法验证用户身份，为了实现这种验证方法，需要在服务器端和智能密钥装置中预置 HMAC-Hash 算法和对称密钥，参见图 3，验证的具体步骤如下：

步骤 301，客户端程序运行；

步骤 302，客户端程序首先向服务器端发送登录请求；

步骤 303，服务器端向客户端发送身份验证请求，即向客户端程序发送一个随机字符串；

步骤 304，客户端程序检测智能密钥装置是否存在，如果不存在，则步骤 312 提示错误并退出，如果存在则执行步骤 305；

步骤 305，客户端程序将上述随机字符串转发至智能密钥装置；

步骤 306，智能密钥装置利用预置的密钥和 HMAC-Hash 算法处理上述随机字符串得到客户端运算结果；

步骤307，智能密钥装置将客户端运算结果通过客户端程序返回给服务器端；

步骤 308，服务器端收到客户端运算结果后利用客户端对应的密钥和HMAC-Hash 算法处理上述随机字符串得到服务器端运算结果；

步骤 309，服务器端程序将服务器端运算结果和客户端运算结果相比较，如果不一致则步骤 312 提示错误并退出，如果一致则执行步骤 310；

步骤 310，服务器端允许客户端程序对服务器端的数据和资源等的访问；

步骤 311，客户端程序继续运行；

步骤 312，提示错误并退出。

上述三种验证身份的方式也可以互相结合使用，这样可以进一步提升客户端程序的安全程度。

用户通过上述三种情况的身份认证后，客户端程序继续运行，客户端程序的运行需要服务器端响应特定的服务、提供特定的数据或提供客户端程序缺少的代码：

首先描述客户端程序需要服务器端响应特定服务或提供特定数据的情况，

如图 4 所示：

当客户端程序通过服务器端的上述身份验证后继续运行，

步骤 401，当运行至需要服务器端提供特定服务或数据的位置时，向服务器端发送请求；

步骤 402，服务器端响应客户端的请求，利用与客户端对应的公钥将服务的运行结果或数据加密后返回客户端程序；

步骤 403，客户端程序将收到的密文转发至智能密钥装置；

步骤 404，智能密钥装置利用其私钥解密服务的运行结果或数据，并返回客户端程序；

步骤 405，客户端程序利用返回的服务的运行结果或数据继续运行；

步骤 406，客户端程序再次运行至需要服务器端提供特定服务或数据的位置时重复步骤 401～405；

步骤 407，当运行至程序尾部时结束。

再描述客户端程序缺少部分代码，需要服务器端提供相应缺少代码的情况，如图 5 所示，客户端程序是经过处理后缺少部分代码 F 的不完整程序（如图中的客户端的 F1、F2 和 F3 为缺少代码的位置），缺少代码的部分用跳转语句填充，相应的客户端程序缺少的代码利用与客户端对应的公钥加密后以密文形式存储在服务器端（如图中的服务器端的 F1’、F2’和 F3’）。

如图 6 所示，客户端程序恢复的流程，具体描述如下：

当客户端程序通过服务器端的上述身份验证后继续运行，

步骤 601，当运行至缺少代码的位置时向服务器端发送下载相应代码的请求；

步骤 602，服务器端响应客户端程序的请求，将相应代码的密文发送给客户端程序；

步骤 603，客户端程序将密文代码转发至智能密钥装置；

步骤 604，智能密钥装置利用其私钥解密密文的代码成明文返回客户端程序；

步骤 605，客户端程序利用上述代码继续运行；

步骤 606，客户端程序再次运行至缺少代码的位置时重复步骤 601～605；

步骤 607，当运行至程序尾部时结束。

以上所述实施方式仅为本发明的优选实施例，本发明不限于上述实施例，对于本领域一般技术人员而言，在不背离本发明原理的前提下对它所做的任何显而易见的改动，都属于本发明的构思和所附权利要求的保护范围。

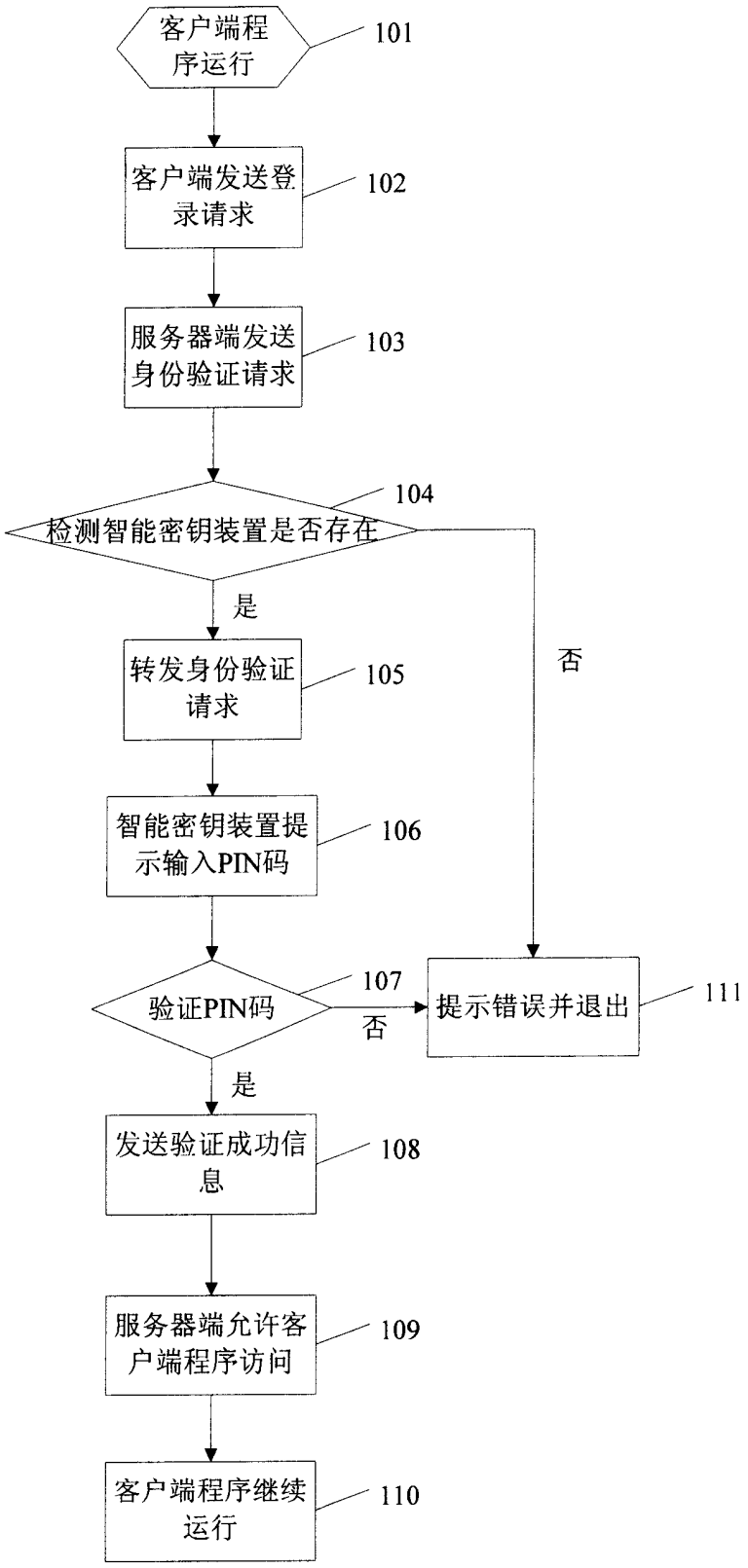

客户端程序运行
101
客户端发送登录请求
102
服务器端发送身份验证请求
103
检测智能密钥装置是否存在
104
是
否
转发身份验证请求
105
智能密钥装置提示输入PIN码
106
验证PIN码
107
否
提示错误并退出
111
是
发送验证成功信息
108
服务器端允许客户端程序访问
109
客户端程序继续运行
110

图 1

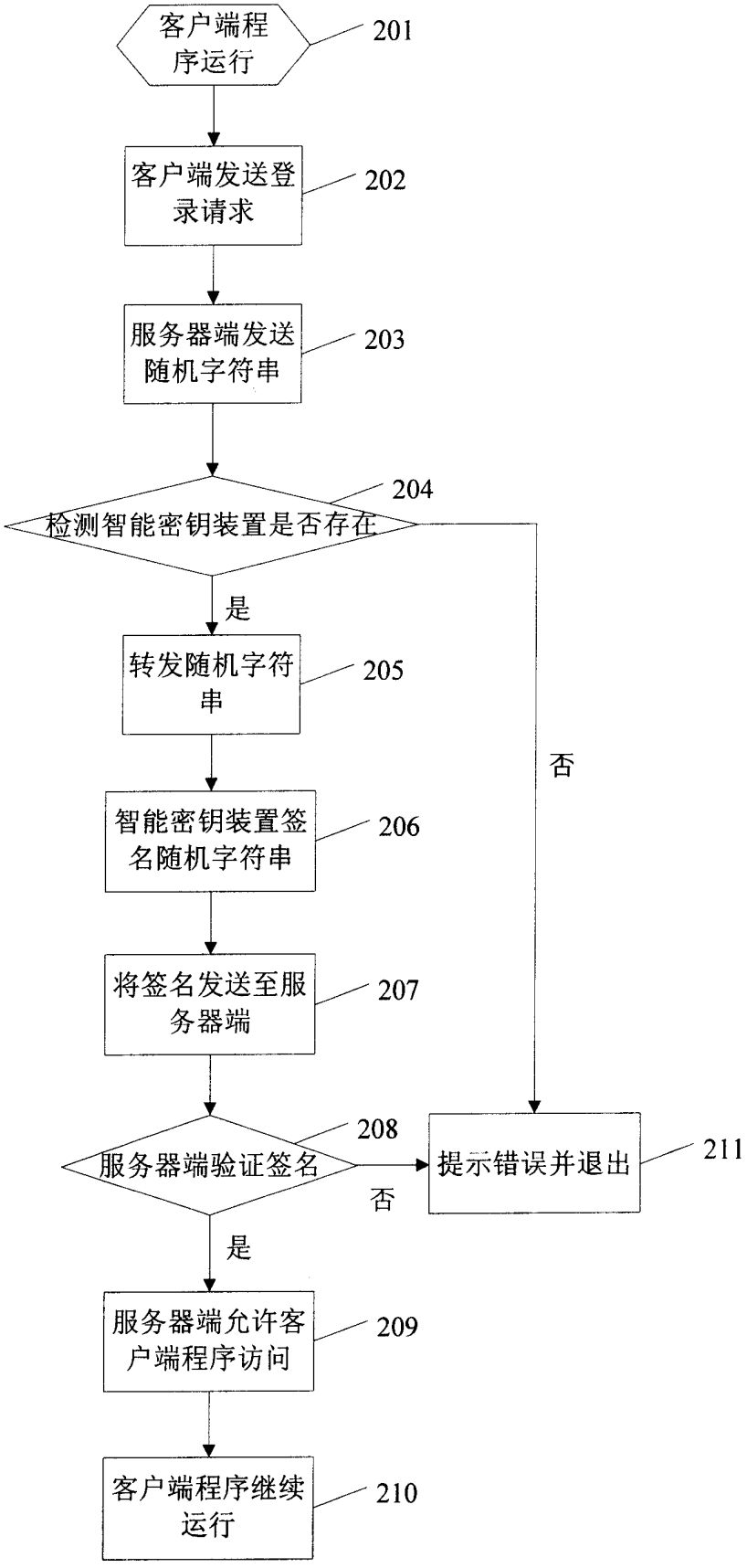

客户端程序运行
201
客户端发送登录请求
202
服务器端发送随机字符串
203
检测智能密钥装置是否存在
204
是
否
转发随机字符串
205
智能密钥装置签名随机字符串
206
将签名发送至服务器端
207
服务器端验证签名
208
否
提示错误并退出
211
是
服务器端允许客户端程序访问
209
客户端程序继续运行
210

图 2

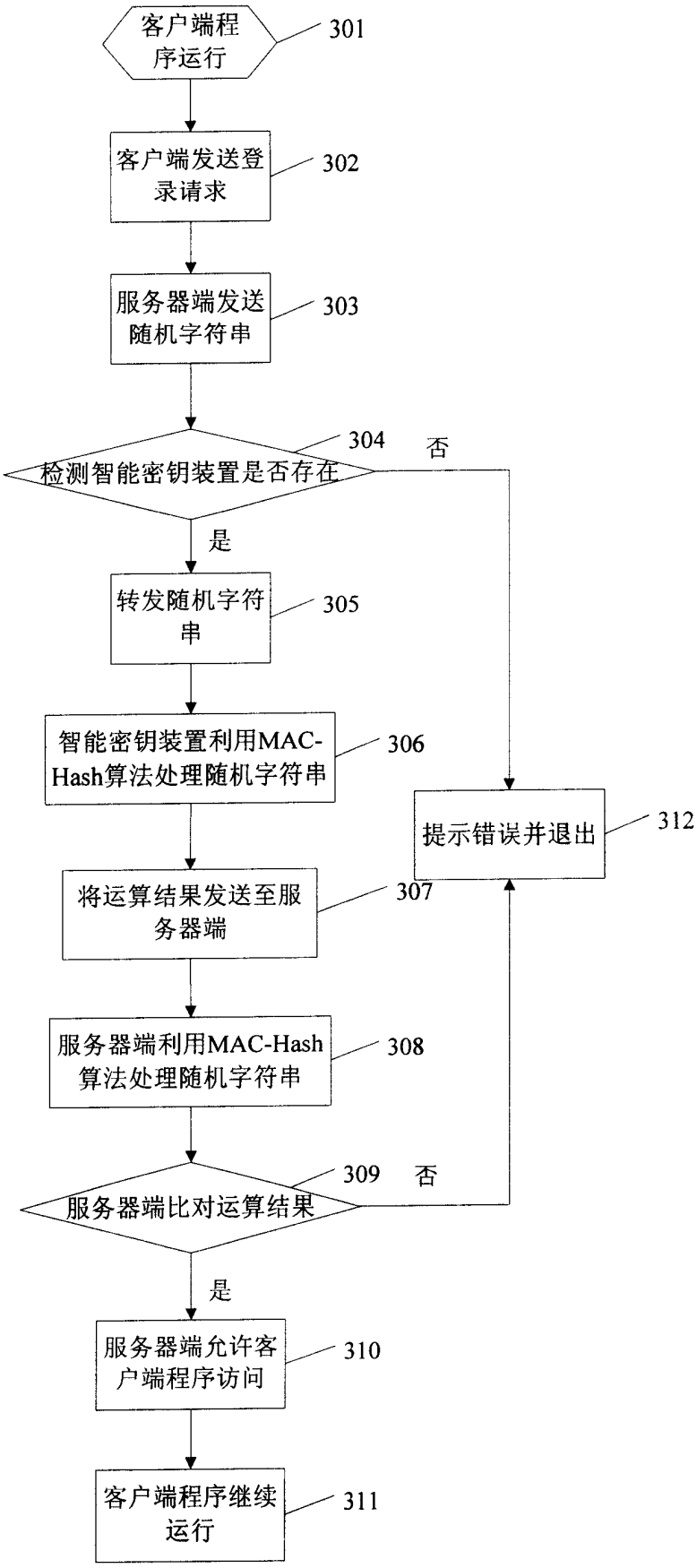

客户端程序运行
301
客户端发送登录请求
302
服务器端发送随机字符串
303
检测智能密钥装置是否存在
304
否
是
转发随机字符串
305
智能密钥装置利用MAC-Hash算法处理随机字符串
306
提示错误并退出
312
将运算结果发送至服务器端
307
服务器端利用MAC-Hash算法处理随机字符串
308
服务器端比对运算结果
309
否
是
服务器端允许客户端程序访问
310
客户端程序继续运行
311

图 3

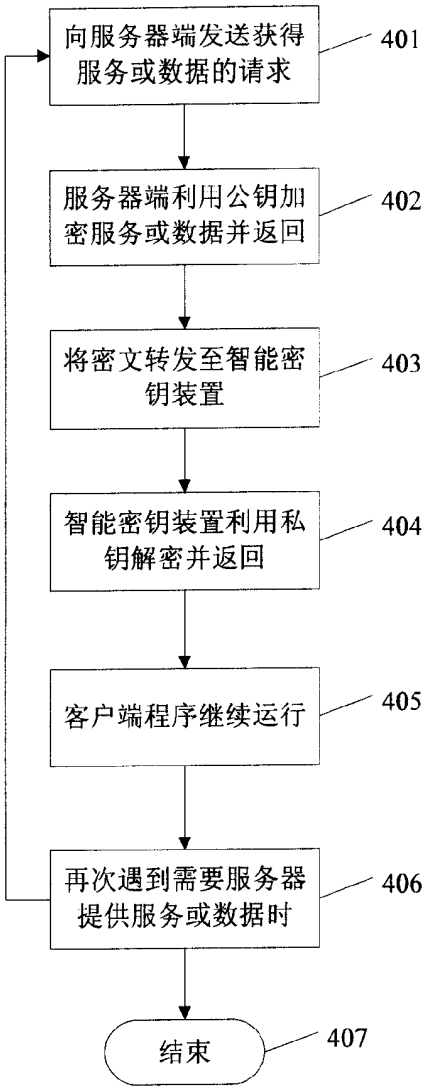

向服务器端发送获得服务或数据的请求
401
服务器端利用公钥加密服务或数据并返回
402
将密文转发至智能密钥装置
403
智能密钥装置利用私钥解密并返回
404
客户端程序继续运行
405
再次遇到需要服务器提供服务或数据时
406
结束
407

图 4

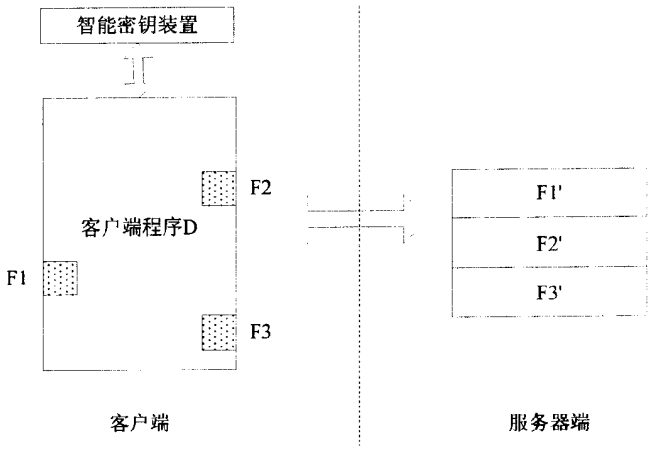

智能密钥装置
F2
客户端程序D
F1
F3
F1'
F2'
F3'
客户端
服务器端

图 5

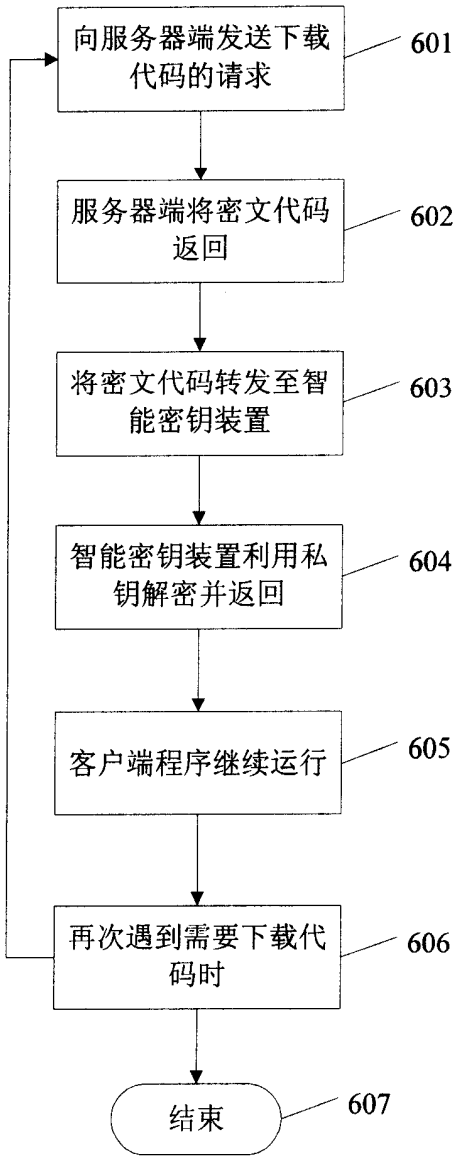

向服务器端发送下载代码的请求
601
服务器端将密文代码返回
602
将密文代码转发至智能密钥装置
603
智能密钥装置利用私钥解密并返回
604
客户端程序继续运行
605
再次遇到需要下载代码时
606
结束
607

图 6