(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 102065148 A
(43)申请公布日 2011.05.18

(21)申请号 201110004716.5

(22)申请日 2011.01.12

(71)申请人 无锡网芯科技有限公司
地址 214028 江苏省无锡市新区长江路 21-1 号 1102、1107 室
申请人 江苏华丽网络工程有限公司

(72)发明人 张启晨 郑有为 丁贤根 何慈康

(74)专利代理机构 无锡华源专利事务所 32228
代理人 聂汉钦

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
G06F 21/00(2006.01)

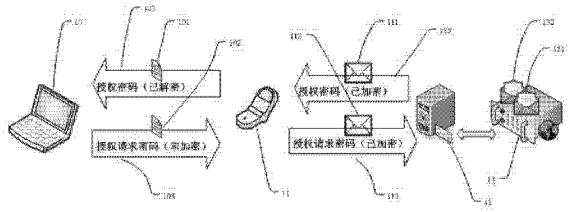
权利要求书 2 页 说明书 5 页 附图 2 页

(54)发明名称

基于通信网络的存储系统访问授权方法

(57)摘要

本发明涉及基于通信网络的存储系统访问授权方法，利用通信设备、被授权计算机和授权服务器作为现有授权技术的替代或补充；发送授权请求码和接收授权码的设备经过授权系统认证且与被授权的计算机设备隔离，授权请求码和授权码通过密文和独立于被授权计算机系统的通信技术传递；访问授权过程需要通过多重身份验证；授权请求码和授权码仅在有限的时间内有效。与现有的密码授权机制相比，被授权计算机无需接入任何通信网络，授权码在授权时生成且具有有限的生命周期，可避免授权码泄露所带来的风险；与现有的文件密钥授权机制相比，又可避免授权设备丢失损坏或者没有随身携带的不便，既具备足够安全性，又具有方便、灵活的特点。



CN 102065148 A

1. 一种基于通信网络的存储系统访问授权方法，其特征在于：将被授权计算机与授权服务器之间的互联网络隔离，并在两者之间设置第三方设备，所述第三方设备作为发送授权请求码和接收授权码的中间设备，其通过独立于互联网络的通信网络与被授权计算机及授权服务器进行授权过程以及接收授权过程的信息交互。

2. 根据权利要求 1 所述基于通信网络的存储系统访问授权方法，其特征在于包括请求授权过程以及接收授权过程，具体步骤如下：

请求授权过程依次执行以下步骤：

1）在被授权用户端设备上运行授权请求码生成程序；

2）授权请求码生成程序根据用户输入的身份识别密码验证用户身份的合法性；若身份识别密码验证结果表明该用户不符合请求授权的用户身份，则授权过程终止；

3）授权请求码生成程序生成授权请求码；

4）授权请求码通过近距离传输技术或用户输入至通信设备；

5）被授权用户端通信设备将授权请求码通过通信网络发送至授权服务器；

6）授权服务器端设备接收到通信设备发送的授权请求码；

7）授权服务器端设备验证发送授权请求码的通信设备的合法性；若验证检测结果表明该通信设备不合法，则授权过程终止；

8）授权服务器验证授权请求码的合法性；若验证检测结果表明该授权请求码不合法，则授权过程终止；

9）授权请求码通过验证后，授权服务器根据授权请求码生成授权码；

10）授权服务器端设备将授权码发送至发送相应请求的被授权用户端通信设备；

接收授权过程依次执行以下步骤：

11）被授权用户端通信设备接收到授权服务器发送的授权码；

12）授权码通过近距离传输技术或者用户输入至被授权用户端；

13）被授权用户端验证授权码的合法性；

14）若授权码验证成功，用户获得与被授权用户端设备连接的存储系统的访问许可；

15）若验证检测结果表明该授权码不合法，则授权失败。

3. 根据权利要求 2 所述基于通信网络的存储系统访问授权方法，其特征在于所述步骤 10 之后还包括如下步骤：10’）授权服务器记录此次访问请求。

4. 根据权利要求 2 或 3 所述基于通信网络的存储系统访问授权方法，其特征在于所述步骤 3 和步骤 9 生成授权请求码和授权码的过程中，被授权终端的硬件设备特征、用户身份信息以及当前时间都将作为生成算法的输入变量。

5. 根据权利要求 2 或 3 所述基于通信网络的存储系统访问授权方法，其特征在于所述步骤 3 和步骤 9 生成的授权请求码和授权码是一一对应的，都具有一的有效周期，仅在有效周期时间内有效；当授权请求码生成后在有效周期时间内还没有收到授权码，则该授权请求码将因超时自动作废；当授权码生成后在有效周期时间内未被输入至被授权终端，则该授权码也将因超时自动作废。

6. 根据权利要求 2 或 3 所述基于通信网络的存储系统访问授权方法，其特征在于所述步骤 8 和步骤 13 验证授权请求码和授权码的过程中，采用多重身份验证过程，对于使用者的用户身份、对被授权设备的硬件特征、发送授权请求码并接收授权码的通信设备的硬件

特征都要通过验证。

7. 根据权利要求 2 或 3 所述基于通信网络的存储系统访问授权方法，其特征在于所述步骤 8 和步骤 13 验证授权请求码和授权码的过程中，需要对授权请求码和授权码是否超时进行验证。

8. 根据权利要求 2 或 3 所述基于通信网络的存储系统访问授权方法，其特征在于所述发送授权请求码并接收授权码的通信设备独立于所述被授权终端，用于发送和接收授权请求码和授权码的通信网络也独立于被授权终端。

9. 根据权利要求 2 或 3 所述基于通信网络的存储系统访问授权方法，其特征在于所述发送授权请求码并接收授权码的通信设备是已在授权服务器系统中注册的设备；所述步骤 7 中授权服务器验证所述通信设备和授权服务器系统中注册设备信息的一致性，若收到的授权请求来自于未在授权服务器系统中注册的设备，则授权过程终止。

10. 根据权利要求 2 或 3 所述基于通信网络的存储系统访问授权方法，其特征在于所述授权请求码和授权码在传送过程中以加密的密文方式传送，授权请求码的加密过程以及授权码的解密过程由被授权用户端设备完成，授权请求码的解密过程以及授权码的加密过程由授权服务器端设备完成。

基于通信网络的存储系统访问授权方法

技术领域

[0001] 本发明涉及信息安全领域，特别涉及一种授权方法，具体地说是一种基于通信网络的存储系统访问授权方法。

背景技术

[0002] 现代企业的信息系统除了需要利用防火墙和防病毒产品抵御外部威胁外，数据加密也已经成为保护企业信息资产的主要工具。利用数据加密解决方案可保护笔记本电脑、工作站和服务器等设备的存储系统数据的安全。在没有经过授权的情况下，存储系统会处于加密保护状态，即使将其连接至网络或其它设备也无法存取该存储系统数据。采用存储系统数据加密技术的计算机设备，其存储系统上的所有数据将被保护起来，机密数据泄露的风险大大降低。

[0003] 每个存储系统加密产品都需要一个密钥来加密存储系统中的数据，常见的存储系统数据加密技术采用的访问授权方法通常有两种：基于文件的授权方法和基于密码的授权方法。

[0004] 基于文件的授权方法在对存储系统进行加密时，将某个文件作为加密存储系统的密钥文件的种子，若没有此文件或存储有此文件的媒介（如USB存储设备或智能卡），将无法解除文件系统加密；基于密码的授权方法，在输入正确的授权密码后，可以解除文件系统的加密。在现有的两种授权方法中，独立于授权终端系统的授权设备（如存储有密钥文件的智能卡或USB存储设备），在授权设备丢失损坏或者没有随身携带的情况下，将导致授权失败，可能影响正常企业业务的进行或外出办公人员远程办公；采用密码的授权方法，虽然在使用过程中不会受到解密授权设备的限制，但密码需要定期更换和规范管理，亦可能因密码泄露造成企业信息资产安全受到威胁。

[0005] 由此可知，现有授权方法对文件密钥／密码的管理和使用一直是信息安全保护方法中的薄弱环节。因此，数据加密技术在保护企业信息资产的同时，还需要为使用者提供安全且方便的授权方式，以此来降低因为用户网上冲浪、社会交际导致的密码泄露所带来的风险。

发明内容

[0006] 针对上述问题，申请人进行了改进研究，提供一种基于通信网络的存储系统访问授权方法，利用通信设备、被授权计算机、授权服务器作为替代密码、授权设备或作为现有授权设备的补充，在确保授权机制安全性的同时将使用的便利性最大化。

[0007] 本发明的技术方案如下：按照权利要求修改

一种基于通信网络的存储系统访问授权方法，将被授权计算机与授权服务器之间的互联网络隔离，并在两者之间设置第三方设备，所述第三方设备作为发送授权请求码和接收授权码的中间设备，其通过独立于互联网络的通信网络与被授权计算机及授权服务器进行授权过程以及接收授权过程的信息交互。

[0008] 其进一步的技术方案为：包括请求授权过程以及接收授权过程，具体步骤如下：

请求授权过程依次执行以下步骤：

1）在被授权用户端设备上运行授权请求码生成程序；

2）授权请求码生成程序根据用户输入的身份识别密码验证用户身份的合法性；若身份识别密码验证结果表明该用户不符合请求授权的用户身份，则授权过程终止；

3）授权请求码生成程序生成授权请求码；

4）授权请求码通过近距离传输技术或用户输入至通信设备；

5）被授权用户端通信设备将授权请求码通过通信网络发送至授权服务器；

6）授权服务器端设备接收到通信设备发送的授权请求码；

7）授权服务器端设备验证发送授权请求码的通信设备的合法性；若验证检测结果表明该通信设备不合法，则授权过程终止；

8）授权服务器验证授权请求码的合法性；若验证检测结果表明该授权请求码不合法，则授权过程终止；

9）授权请求码通过验证后，授权服务器根据授权请求码生成授权码；

10）授权服务器端设备将授权码发送至发送相应请求的被授权用户端通信设备；

接收授权过程依次执行以下步骤：

11）被授权用户端通信设备接收到授权服务器发送的授权码；

12）授权码通过近距离传输技术或者用户输入至被授权用户端；

13）被授权用户端验证授权码的合法性；

14）若授权码验证成功，用户获得与被授权用户端设备连接的存储系统的访问许可；

15）若验证检测结果表明该授权码不合法，则授权失败。

[0009] 其进一步的技术方案为：所述步骤 10 之后还包括如下步骤：10’）授权服务器记录此次访问请求。

[0010] 其进一步的技术方案为：所述步骤 3 和步骤 9 生成授权请求码和授权码的过程中，被授权终端的硬件设备特征、用户身份信息以及当前时间都将作为生成算法的输入变量。

[0011] 其进一步的技术方案为：所述步骤 3 和步骤 9 生成的授权请求码和授权码是一一对应的，都具有一的有效周期，仅在有效周期时间内有效；当授权请求码生成后在有效周期时间内还没有收到授权码，则该授权请求码将因超时自动作废；当授权码生成后在有效周期时间内未被输入至被授权终端，则该授权码也将因超时自动作废。

[0012] 其进一步的技术方案为：所述步骤 8 和步骤 13 验证授权请求码和授权码的过程中，采用多重身份验证过程，对于使用者的用户身份、对被授权设备的硬件特征、发送授权请求码并接收授权码的通信设备的硬件特征都要通过验证。

[0013] 其进一步的技术方案为：所述步骤 8 和步骤 13 验证授权请求码和授权码的过程中，需要对授权请求码和授权码是否超时进行验证。

[0014] 其进一步的技术方案为：所述发送授权请求码并接收授权码的通信设备独立于所述被授权终端，用于发送和接收授权请求码和授权码的通信网络也独立于被授权终端。

[0015] 其进一步的技术方案为：所述发送授权请求码并接收授权码的通信设备是已在授权服务器系统中注册的设备；所述步骤 7 中授权服务器验证所述通信设备和授权服务器系统中注册设备信息的一致性，若收到的授权请求来自于未在授权服务器系统中注册的设

备，则授权过程终止。

[0016] 其进一步的技术方案为：所述授权请求码和授权码在传送过程中以加密的密文方式传送，授权请求码的加密过程以及授权码的解密过程由被授权用户端设备完成，授权请求码的解密过程以及授权码的加密过程由授权服务器端设备完成。

[0017] 本发明的有益技术效果是：

本发明授权方法利用通信设备、被授权计算机和授权服务器作为现有授权技术的替代或补充。发送授权请求码和接收授权码的设备经过授权系统认证且与被授权的计算机设备隔离，授权请求码和授权码通过密文和独立的通信技术传递；访问授权过程需要通过多重身份验证；授权请求码和授权码仅在有限的时间内有效。与现有的密码授权机制相比，被授权计算机无需接入互联网，授权码在授权时生成且具有有限的生命周期，可避免密码泄露所带来的风险；与现有的文件密钥授权机制相比，又可避免授权设备丢失损坏或者没有随身携带的不便。因此本发明既具备足够安全性，又具有方便、灵活的特点。

附图说明

[0018] 图 1 是本发明的组成模块示意图。

[0019] 图 2 是本发明的请求授权过程的流程示意图。

[0020] 图 3 是本发明的接收授权过程的流程示意图。

[0021] 标号说明：图 1 中，10. 等待访问存储系统的被授权终端及运行其中的权请求码生成程序、授权码验证程序；101. 已解密的授权密码；102. 未加密的请求授权码；103. 近距离传输技术（如蓝牙），或用户输入；11. 通信设备；111. 已加密的授权码；112. 已加密的授权请求码；113. 移动通信网或其他远距离通信技术；12. 授权请求码接收和授权码发送设备；13. 授权服务器和授权码生成程序；131. 由授权服务器生成的未加密的授权码；132. 由授权服务器解密得到的授权请求码。

具体实施方式

[0022] 下面结合附图对本发明的具体实施方式做进一步说明。

[0023] 如图 1 所示，本发明的访问授权系统由以下几个部分协同组成，各部分的功能如下：

1、等待访问存储系统的被授权终端（如个人电脑或笔记本电脑）以及运行其中的授权请求码生成程序和授权码验证程序 10。

[0024] 在请求授权时，根据所运行终端的硬件特征码和系统日期时间（也可包含用户密码）等参数生成授权请求码 102，并通过近距离传输技术 103（或通过通信设备的键盘等输入设备）将授权请求码输入通信设备 11；在接受授权时，验证用户输入的或通过近距离传输技术 103（如蓝牙传输技术）从通信设备 11 接收到的授权码 101。

[0025] 2、用于发送授权请求码和接收授权码的在授权系统中注册过的通信设备 11。

[0026] 在请求授权时，通信设备 11（通常为移动电话，也可以是在授权系统中注册过的普通固定电话）通过近距离传输技术 103（或通过通信设备的键盘等输入设备）接收被授权终端 10 生成的未加密的授权请求码 102，再由运行在该通信设备上的加密软件生成已加密的

授权请求码 112(若采用在授权系统中注册过的普通固定电话作为通信设备,则授权请求码加密过程可由被授权终端完成),通过移动通信网或其他远距离通信技术 113 (如 GSM/CDMA 无线通信网络)发送至授权服务器端授权请求码接收设备 12 ;在接受授权时,该通信设备通过移动通信网或远距离通信技术 113 接收已加密的授权密码 111,并通过运行于该通信设备上的解密软件解密(若采用在授权系统中注册过的普通固定电话作为通信设备,则授权码解密过程可由被授权终端完成)。

[0027] 3、授权请求码接收和授权码发送设备 12。

[0028] 通过移动通信网或远距离通信技术 113 接收已加密的授权请求码 112 并传送至授权服务器 13 ;在授权码生成后,将已加密的授权码 111 通过移动通信网或远距离通信技术 113 发送至接收授权码的通信设备 11。

[0029] 4、授权服务器和运行在授权服务器端的基于授权请求码的授权码生成程序 13。

[0030] 在被授权终端请求授权时,授权服务器将已加密的授权请求码 112 解密,然后根据解密后的授权请求码 132,在验证其合法性的基础上,根据授权请求码和相关参数生成未加密的授权码 131 并加密传递给授权码发送装置 12。

[0031] 本发明根据上述访问授权系统,形成以下的请求授权过程以及接收授权过程 :

图 2 给出了请求授权过程的流程图,过程如下 :

1)用户在安装有存储系统(或外接存储系统,如 U 盘)的被授权计算机终端上运行授权请求码生成程序(步骤 201)。

[0032] 2)授权请求码生成程序根据用户输入的身份识别密码验证用户身份的合法性。若验证结果表明该用户不符合请求授权的用户身份,则授权过程终止(步骤 202)。

[0033] 3)授权请求码生成程序根据计算机终端的硬件特征序号、当前时间、日期等参数生成授权请求码。每次生成的授权请求码的具有一定的生命周期,当授权请求码生成后一定时间内还没有收到授权码,则该授权请求码将因超时自动作废(步骤 203)。

[0034] 4)授权请求码通过近距离传输技术(如蓝牙)或用户输入至移动通信设备(步骤 204)。

[0035] 5)运行在移动通信设备上的软件将授权请求码加密,并通过通信网络发送至授权服务器(步骤 205)。

[0036] 6)授权服务器接收到移动通信设备发送的授权请求码(步骤 206)。

[0037] 7)授权服务器验证发送授权请求码的移动通信设备的合法性。若收到的授权请求来自于未在授权系统中注册的设备,则授权过程终止(步骤 207)。

[0038] 8)授权服务器端的解密设备解密授权请求码(步骤 208)。

[0039] 9)授权服务器根据当前时间、请求授权的用户身份等参数检测授权请求码合法性。由于授权请求码的具有一定的生命周期,若授权请求码超时,则授权服务器将终止授权过程 ;若授权请求码检测结果表明授权请求码不合法(如不符合请求授权的用户身份、不符合被授权访硬件的特征或授权请求为伪造等),授权过程也将终止(步骤 209)。

[0040] 10)授权请求码通过验证后,授权服务器根据授权请求码生成授权码(步骤 210)。

[0041] 11)授权服务器端的加密设备加密授权码,并发送至发送相应请求的移动通信设备(图中步骤 211)。

[0042] 12)授权服务器记录此次访问请求(步骤 212)。此步骤可选。

[0043]

图 3 给出了接收授权过程的流程图，过程如下：

1）移动通信设备接收到授权服务器发送的加密过的授权码（步骤 301）。

[0044] 2）移动通信设备运行其上的解密软件解密授权码（步骤 302）。

[0045] 3）授权码通过近距离传输技术（如蓝牙无线传输技术）或者用户输入至被授权设备（步骤 303）。

[0046] 4）被授权终端根据当前时间及授权码中包含的信息检测授权码合法性（步骤 304）。

[0047] 5）若授权码验证成功，用户获得与被授权终端连接的存储系统的访问许可（步骤 305）。

[0048] 6）授权码具有一定的生命周期，若接收到的授权码超时，则授权失败；若授权请求码验证结果表明授权码不合法，则授权也将失败（步骤 306）。

[0049] 所述图 2、图 3 是针对采用移动通信设备作为通信设备的授权流程，若采用在授权系统中注册过的普通固定电话作为通信设备，则授权请求码加密过程以及授权码解密过程则由被授权终端完成。

[0050] 以上所述的仅是本发明的优选实施方式，本发明不限于以上实施例。可以理解，本领域技术人员在不脱离本发明的精神和构思的前提下直接导出或联想到的其他改进和变化，均应认为包含在本发明的保护范围之内。

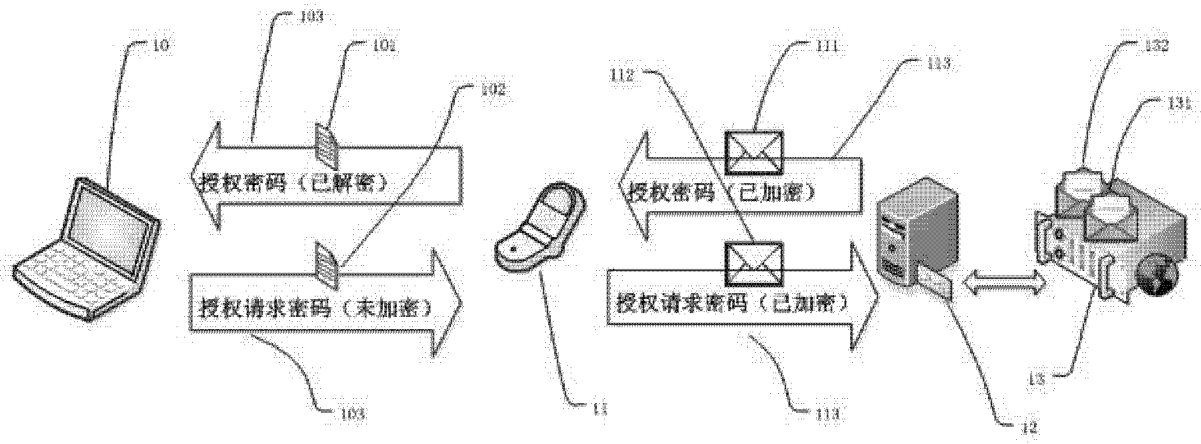

10
103
102
102
授权密码（已解密）
授权请求密码（未加密）
103
11
112
111
113
授权密码（已加密）
授权请求密码（已加密）
113
12
132
131
13

图 1

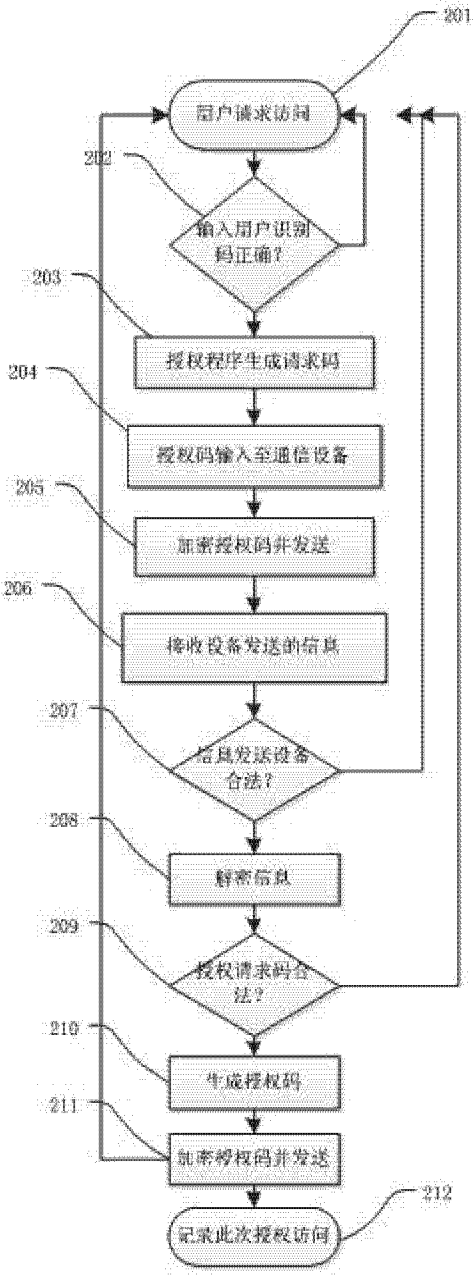

201
用户请求访问
202
输入用户识别码正确?
203
授权程序生成请求码
204
授权码输入至通信设备
205
加密授权码并发送
206
接收设备发送的结果
207
结果发送设备合法?
208
解密信息
209
授权请求码合法?
210
生成授权码
211
加密授权码并发送
212
记录此次授权访问

图 2

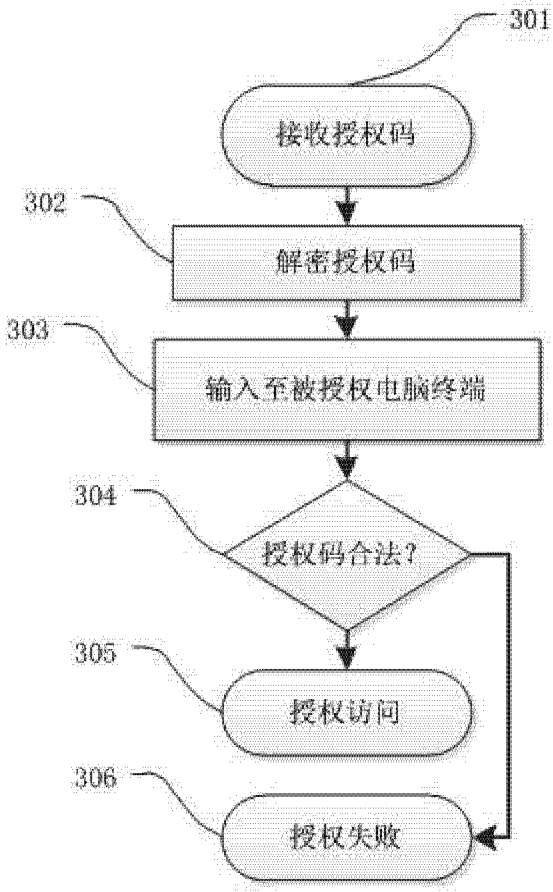

301
接收授权码
302
解密授权码
303
输入至被授权电脑终端
304
授权码合法?
305
授权访问
306
授权失败

图 3