(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2006 年2 月9 日 (09.02.2006)

PCT

(10) 国际公布号
WO 2006/012788 A1

(51) 国际专利分类号[7]: H04N 7/167, 7/173
(21) 国际申请号: PCT/CN2005/001092
(22) 国际申请日: 2005 年7 月21 日 (21.07.2005)
(25) 申请语言: 中文
(26) 公布语言: 中文
(30) 优先权:
200410070382.1
2004 年8 月2 日 (02.08.2004) CN

(71) 申请人 (对除美国外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

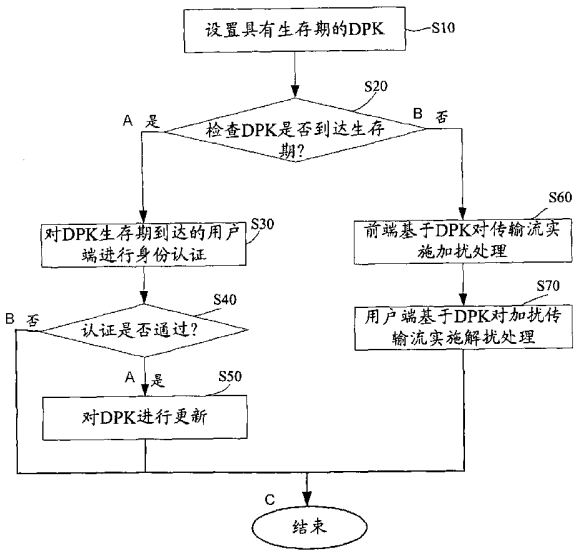
(75) 发明人/申请人 (仅对美国): 刘进明(LIU, Jinming) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 鞠德刚(JU, Degang) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 胡峻岭(HU, Junling) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 许永红(XU, Yonghong) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 姚峻(YAO, Jun) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京集佳知识产权代理有限公司(UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

[见续页]

(54) Title: SUBSCRIBER AUTHORIZATING METHOD AND AUTHORIZATING SYSTEM

(54) 发明名称: 用户授权方法及授权系统



S10 SETTING THE DPK WITH A SURVIVAL TERM
S20 CHECKING IF THE SURVIVAL TERM IS ENDING
S30 CARRYING OUT THE IDENTITY AUTHENTICATION FOR THE SUBSCRIBER TERMINAL OF WHICH THE SURVIVAL TERM IS EXPIRED
S40 IF THE AUTHENTICATION IS PASSED?
S50 UPDATING THE DPK
S60 THE HEADEND IMPLEMENTS SCRAMBLING FOR TRANSPORT STREAM ON THE BASIS OF THE DPK
S70 SUBSCRIBER TERMINALS IMPLEMENT UNSCRAMBLING FOR THE SCRAMBLED TRANSPORT STREAM ON THE BASIS OF THE DPK
A YES
B NO
C END

(57) Abstract: Subscriber authorizating method comprises the steps as following: setting the dynamic personal keys with a survival term which are shared by the headend and subscriber terminal; checking if the survival term reachs the ending time, if so, returning and sequentially checking the survival term of the dynamic personal keys after updating the dynamic personal keys of which the survival term is expired; or else, the headend implements encrypting, scrambling and authorizing for transport stream on the basis of the dynamic personal keys, subscriber terminals implement decrypting and unscrambling for the scramble transport stream on the basis of the dynamic personal keys. Accordingly, the present invention also provides a subscriber authorizing system. The invention can reduce the probability that unauthorized users watch the television programs using the cloned smart card, while the invention can reduce the economy loss resulted from maintaining the smart card by the operators.

[见续页]

WO 2006/012788 A1

(81) **指定国**（除另有指明，要求每一种可提供的国家保护）：AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW。

(84) **指定国**（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(57) **摘要：**

本发明提供了一种用户授权方法，包括设置前端和用户端共享的具有生存期的动态个人密钥；检查动态个人密钥的生存期是否到达终止时间，如果是，更新生存期到达的动态个人密钥后返回继续检查动态个人密钥的生存期；否则前端基于动态个人密钥对传输流实施加密、加扰及授权处理，用户端基于动态个人密钥对加扰传输流实施解密及解扰处理。相应地，本发明还提供了一种用户授权系统。本发明可以降低非法用户使用克隆智能卡收看电视节目的概率，同时降低运营商为维护智能卡所造成的经济损失。

用户授权方法及授权系统

技术领域

本发明涉及广播电视领域的有线电视技术，尤其涉及一种用户授权方法及授权系统。

背景技术

目前，随着广播电视系统面向数字化、产业化的发展，用户为自身收看的电视节目内容付费已成为这一发展的必然，而要实现用户为自身收看的电视节目内容付费的目的，首要解决的技术问题是应该对收看电视节目的用户进行有效管理。

条件接收系统（CAS，Conditional Access System）就是在现有广播电视网中实施的用于对用户进行有效管理的方式之一，而由 CAS 技术实现的对用户进行管理的主要过程如下：

广播电视网的前端（HE，Head End）对要发送给用户的电视节目数据进行加扰处理，然后再对用户能够收看的节目进行授权，并且授权处理后的授权数据还要进行加密处理后才能传送到最终用户端；

用户端接收到电视节目后，只有合法用户才能对加密处理的授权数据进行解密，得到相应的授权数据，然后使用授权数据对加扰处理的电视节目进行解扰处理，以正常收看电视节目；而非法用户或者没有正常接收到自身授权数据的用户由于无法对加扰处理的电视节目进行解扰，因此就不能正常收看电视节目，这样就到达了对用户收看的电视节目内容进行控制和管理的目的，进而驱使用户为自己所收看的电视节目内容进行付费。

参照图 1，该图是现有技术在广播电视网中实现对电视节目进行加解扰及加解密处理的原理示意图；其对电视节目数据进行加解扰处理及加解密处理的过程如下：

在广播电视网的前端 HE 10 中进行如下操作：

1）电视节目在播出前，加扰器使用控制字（CW，Control Words）对

电视节目数据复用处理后传输流（TS，Transport Stream）进行加扰处理，可以表示为：

TS + CW -> TS';

2）CAS 技术的核心实际上是对控制字 CW 的传输进行控制，因此在前端 HE 10 中还要使用业务密钥（SK，Service Key）对控制字 CW 进行加密处理，形成授权控制信息（ECM，Entitlement Control Message），可以表示为：

CW + SK -> ECM;

其中由业务密钥 SK 加密处理后的控制字 CW 封装在 ECM 中传送，其中 ECM 中还包括节目来源、内容分类和节目收费价格等信息；

3）前端 HE 10 再根据用户注册时的授权信息，使用用户的个人分配密钥（PDK，Personal Distribute Keyword）对业务密钥 SK 进行加密处理，形成授权管理信息（EMM，Entitlement Management Message），可以表示为：

SK + PDK -> EMM;

其中由个人分配密钥 PDK 加密处理的业务密钥 SK 封装在 EMM 中传送，EMM 中还包括接收方地址信息、用户授权信息和用户可以收看的电视节目时间段信息等。

其中上述的 EMM 数据主要针对用户而生成，ECM 数据主要针对电视节目数据而生成，生成的 EMM 数据和 ECM 数据与电视节目数据一起复用在传输流 TS 里通过光纤同轴混合有线电视网络（HFC，Hybrid Fiber-Coaxial）传输到用户端。

用户端的机顶盒（STB，Set-Top Box）20 接收到广播电视网的前端 HE 10 发来的传输流 TS 后，使用智能卡（Smart Card）中存有的用户注册授权数据对传输流 TS 进行如下的解密及解扰处理：

4）STB 20 从传输流 TS 中过滤出 ECM 数据和 EMM 数据；

5）通过智能卡的接口将 ECM 数据和 EMM 数据送到智能卡内部；

6）智能卡读取自身存有的授权数据中的个人分配密钥 PDK，利用 PDK

对 EMM 数据进行解密，得到业务密钥 SK，可以表示为：

EMM + PDK -> SK;

7）智能卡利用得到的业务密钥 SK 对 ECM 数据进行解码，得到控制字 CW，可以表示为：

ECM + SK -> CW;

智能卡将得到的 CW 通过相应接口发送给 STB 的解扰引擎;

8）机顶盒 STB 20 的解扰引擎利用控制字 CW 对进行了加扰处理的传输流 TS 进行解扰处理，以得到电视节目数据的明文形式，可以表示为：

TS' + CW -> TS;

解扰处理后的节目数据经过解复用和解调等处理后，就可以恢复出原始的音视频图像信息，以播放给用户进行收看。

由此可见，上述使用 CAS 技术能够实现对电视节目数据进行加解密及加解扰处理，以驱使用户对自身收看的电视节目进行付费，从而实现了使广播电视运营商能够为自身提供的业务进行合理性收费的目的。

但是由于在用户端，用户的授权数据（最主要的是个人分配密钥 PDK）都保存在用户手持的智能卡中，这样就容易导致在经济利益的驱使下，不法分子可以采用各种方法对合法用户手持的智能卡进行克隆（包括对个人分配密钥 PDK 的复制），再通过非法渠道大量出售克隆的智能卡以牟取暴利，从而导致了广播电视运营商大量客户的流失，造成了不可估量的经济损失。

因为传统的广播电视系统是一个单向传输的广播网络，广播电视运营商根本无法获知用户是否在线的情况，因此就无法对用户身份的合法性与唯一性进行鉴权，所以即使大量持有非法智能卡的身份信息相同的用户同时在线收看电视节目，运营商也无能为力。

目前，广播电视运营商为防止非法用户对智能卡进行克隆，提供了两种处理措施：

第一，加强智能卡本身的物理安全，以降低智能卡被克隆的可能性，但是这种方式必将会增加智能卡的烧制成本;

第二，在发现智能卡被克隆后及时进行智能卡升级处理，即更换智能卡中存储的用户授权数据（最主要是更换个人分配密钥 PDK），以使非法用户克隆的智能卡在进行了智能卡升级处理后，不能再正常使用。但是这种处理方式却面临着即使一张智能卡被克隆，广播电视运营商也要将整个系统中的所有智能卡全部进行升级处理，并更换全部用户端的智能卡，其主要原因在于运营商并不太容易知道哪些智能卡被克隆了，而哪些智能卡没有被克隆；其次即使只有一张智能卡被克隆，则其他智能卡也存在被克隆的可能性，因此必须更换整个智能卡系统才能避免这种风险。但是如果更换整个系统的所有智能卡，也同样会增加运营商为升级所有智能卡而带来的经济损失。

发明内容

本发明提出一种用户授权方法及其授权系统，以解决现有广播电视系统中因授权技术的不完善而存在的大量非法用户使用克隆智能卡收看电视节目的问题。

为解决上述问题，本发明提出了一种用户授权方法，包括步骤：

（1）设置前端和用户端共享的具有生存期的动态个人密钥；

（2）检查所述动态个人密钥的生存期是否到达终止时间，如果是继续步骤（3）；否则转至步骤（4）；

（3）更新生存期到达终止时间的所述动态个人密钥后返回步骤（2）；

（4）前端基于所述动态个人密钥对传输流实施加密、加扰及授权处理，用户端基于所述动态个人密钥对加扰传输流实施解密及解扰处理。

所述步骤（2）中以周期规律检查动态个人密钥的生存期。

所述步骤（2）具体包括如下步骤：

（21）设置一固定时长值；

（22）判断当前检测时间点距动态个人密钥生存期到达时间点的时长值是否小于所述固定时长值，如果是，判定动态个人密钥的生存期已到达；否则判定未到达。

所述步骤（3）在更新动态个人密钥之前还包括对动态个人密钥生存

期到达的用户端进行身份认证的步骤，如果认证通过继续更新动态个人密钥处理，否则结束。

所述步骤（2）中检查动态个人密钥的生存期是由前端完成。

所述步骤（3）对动态个人密钥生存期到达的用户端进行身份认证的过程具体包括步骤：

（31）所述前端发送认证指示命令到动态个人密钥生存期到达的用户端，指示用户端到前端进行身份认证；

（32）用户端将自身标识信息上传到前端；

（33）前端根据用户端的标识信息对用户端进行身份认证。

所述步骤（31）之前还包括前端判断动态个人密钥生存期到达的用户端是否在线的步骤。

所述步骤（2）中检查动态个人密钥的生存期由用户端完成。

所述步骤（3）对动态个人密钥生存期到达的用户端进行身份认证的过程具体包括步骤：

（3a）动态个人密钥生存期到达的用户端将自身标识信息上传到广播电视网前端；

（3b）前端根据用户端的标识信息对用户端进行身份认证。

所述步骤（3）更新动态个人密钥的过程具体包括：

（3-1）前端利用与用户端共享的个人分配密钥对更新的动态个人密钥进行加密后下发给用户端；

（3-2）用户端利用用户身份识别模块中存储的个人分配密钥对加密的动态个人密钥数据进行解密，得到更新的动态个人密钥。

所述步骤（3-1）中广播电视网前端将加密后的动态个人密钥数据通过有线通信网的有线传输线路或无线通信网的无线传输线路下发到用户端。

所述用户端标识信息包括：

用户端机顶盒的 ID 标识信息；或

用户端用户身份识别模块中存储的用户身份标识信息；或

用户端机顶盒 ID 标识信息和用户端用户身份识别模块中存储的用户

身份标识信息的绑定关系。

其中步骤（4）中所述基于动态个人密钥对传输流实施加密、加扰及授权处理的过程具体包括:

（41）所述前端使用控制字对传输流进行加扰处理;

（42）使用业务密钥对控制字进行加密处理，得到授权控制信息;

（43）使用动态个人密钥对业务密钥进行加密处理，得到授权管理信息;

（44）将授权控制信息和授权管理信息复用到传输流中下发到用户端;

所述基于动态个人密钥对加扰传输流实施解密及解扰处理的过程具体包括:

（45）所述用户端使用动态个人密钥对授权管理信息进行解密处理，得到业务密钥;

（46）使用业务密钥对授权控制信息进行解密处理，得到控制字;

（47）使用控制字对加扰传输流进行解扰处理。

相应地，本发明还提出了一种用户授权系统，包括用于广播节目流的前端和用于接收节目流的用户端，所述用户端包括用于处理节目流信息的机顶盒和用于存储用户授权数据的用户身份识别模块，所述的系统还包括:

在所述用户端设置有与机顶盒连接的双向通信模块，用于将用户端标识信息上传到所述前端，并用于接收前端发来的更新的用户授权数据;

在所述前端设置有认证服务器，与所述双向通信模块通过双向传输线路连接，用于根据用户端上传的标识信息对用户端进行身份认证处理，并在认证通过后更新用户端的用户授权数据，并将更新的用户授权数据发送到用户端的双向通信模块。

所述双向通信模块通过设置在机顶盒内部实现与机顶盒的连接。

所述双向通信模块为无线通信模块，通过无线通信网的无线传输线路与所述认证服务器连接; 或

所述双向通信模块为有线通信模块，通过有线通信网的有线传输线路与所述认证服务器连接。

本发明能够到达如下有益效果:

由于本发明基于广播电视网的用户授权方法通过在前端和用户端分别设置动态个人密钥，前端和用户端基于动态个人密钥对传输流实施加解密及加解扰处理，并在动态个人密钥的生存期到达时，及时对动态个人密钥进行更新，这样由于动态个人密钥的定时更新就可以限制非法用户克隆智能卡的有效时间，为非法用户克隆智能卡带来了操作难度，从而降低了非法用户使用克隆智能卡收看电视节目的机率，同时降低了运营商为维护智能卡所造成的经济损失。

同时，由于本发明基于广播电视网的用户授权系统在用户端设置有双向通信模块，同时在前端设置有认证服务器，认证服务器和双向通信模块之间通过双向传输线路连接，这样可以实现广播电视网前端和用户端双方之间相互传递用户端标识信息和动态更新的用户授权数据，从而为前端动态更新用户端的用户授权数据提供了平台，因此降低了非法用户使用克隆智能卡收看电视节目的机率，并降低了运营商为维护智能卡所造成的经济损失。

附图说明

图 1 是现有技术在广播电视网中实现对电视节目进行加解扰及加解密处理的原理示意图；

图 2 是本发明基于广播电视网的用户授权系统的基本组成结构框图；

图 3 是本发明基于广播电视网的用户授权方法的基本实现原理流程图；

图 4 是在本发明基于广播电视网的用户授权方法中，由前端发起的对用户端进行身份认证处理的过程示意图；

图 5 是在本发明基于广播电视网的用户授权方法中，由用户端发起的对用户端进行身份认证处理的过程示意图。

具体实施方式

本发明基于广播电视网的用户授权方法及其授权系统的设计思想是：能够在广播电视网络正常运营过程中，以一种用户不可察觉的方式更换智能卡（智能卡只是用户身份识别模块中的一种特例，为了说明本发明要求

的保护范围，下面以用户身份识别模块进行说明，其中现有技术中已存在的智能卡是这里所述的用户身份识别模块中的一种典型的例子）中保存的用户授权数据，从而减少非法分子克隆用户身份识别模块所带来的非法经济利益，并降低广播电视网络运营商为维护整个用户身份识别模块系统而造成的经济损失。但是本发明基于广播电视网的用户授权方法及其授权系统只是相对现有技术而言，能够减少非法用户克隆用户身份识别模块的机率，而并不能从根本上杜绝用户身份识别模块被非法克隆的可能性。

下面首先结合附图对本发明提出的基于广播电视网的用户授权系统的基本原理进行详细阐述。参照图 2，该图是本发明基于广播电视网的用户授权系统的基本组成结构框图，其中用户授权系统的工作原理如下：

由于目前的广播电视网是由用于广播节目流的前端 HE 2 和用于接收节目流的用户端所组成的，其中用户端一般包括用于处理节目流信息的机顶盒 4 和用于存储用户授权数据和用户身份标识信息的用户身份识别模块 5，而目前广播电视网的工作模式都是由前端 HE 2 通过广播信道单向对所有用户端来进行广播节目流信息的，而用户端并不能通过广播信道向前端 HE 2 来发送反向通信信息，因此为增加广播电视网的前端 HE 2 和用户端之间的双向认证功能，需作如下设置：

在用户端设置一个与机顶盒 4 连接的双向通信模块 3，以用于将用户端标识信息上传到前端 HE 2，同时还用于接收前端 HE 2 发来的更新的用户授权数据；其中双向通信模块 3 可以通过设置在机顶盒 4 的内部来实现与机顶盒 4 的连接，这样就会构成一个带交互通信模块功能的机顶盒；当然双向通信模块 3 也可以通过设置在机顶盒 4 的外部来实现与机顶盒 4 的外置连接；

同时在广播电视网的前端 HE 2 设置一个认证服务器 1，该设置的认证服务器 1 与用户端侧的双向通信模块 3 之间通过双向传输线路进行连接，其用于根据用户端上传的标识信息对用户端进行身份认证处理，并在认证通过后更新用户端的用户授权数据，并将更新的用户授权数据发送到用户端的双向通信模块 3。

其中用于连接广播电视网前端设置的认证服务器 1 和用户端机顶盒 4

处设置的双向通信模块 3 的双向传输线路的物理形态可以为无线传输线路，如为 GSM 通信网中的无线传输信道或为 3G 通信网中的无线传输信道等，这时双向通信模块 3 为具有无线通信功能的无线通信模块；也可以为有线传输线路，如为 PSTN 通信网中的有线传输信道或为广播电视网中的有线传输信道（即 Cable 信道）等，这时双向通信模块 3 就为有线通信模块。

基于上述在广播电视网上建立的用户授权系统，广播电视网前端 HE 2 就可以通过单向广播信道单向广播传输流 TS 到所有用户端的机顶盒 4，而用户端需要到前端 HE 2 进行身份认证时，就可以通过设置的双向通信模块 3 将自身的标识信息通过双向传输线路上传到前端 HE 2 侧的认证服务器 1，由认证服务器 1 对用户端的身份合法性进行认证，并在用户端身份认证通过后，将对其更新的用户授权数据通过认证服务器 1 和双向通信模块 3 之间的双先传输线路下发到用户端侧的双向通信模块 3，用户端根据双向通信模块 3 接收的更新后的用户授权数据来实现对自身用户授权数据的更新。

相应地，本发明还提出了一种基于广播电视网的用户授权方法，下面结合附图对本发明基于广播电视网的用户授权方法的基本实现原理进行详细阐述。参照图 3，该图是本发明基于广播电视网的用户授权方法的基本实现原理流程图；其基本实现过程如下：

步骤 S10，设置具有生存期的动态个人密钥（DPK，Dynamic Personal Key），即广播电视网的前端为每个用户分别设置一个 DPK，其中 DPK 是有生存期的，需要在其生存一段时间后对其进行更新处理；其中为每个用户设置的 DPK，前端和用户端都共享这个 DPK，即针对每一用户，前端存有为该用户设置的 DPK，用户端也存有该设置的 DPK，一般用户端会将该设置的 DPK 存放在自身携带的用户身份识别模块中。

步骤 S20，检测每个用户的 DPK 是否到达其生存期，其中可以采取周期规律对每个用户的 DPK 生存期进行检查，如果某个用户的 DPK 到达了其生存期，执行步骤 S30；否则执行步骤 S60；其中判断每个 DPK 是否到达其生存期的方法可以采取如下方式：

1）预先设置一个固定时长值（如 1 小时）;

2）判断当前检测时间点距动态个人密钥 DPK 生存期到达时间点的时长值是否小于 1）中设置的固定时长值，如果是，则可以判定动态个人密钥 DPK 的生存期已到达；否则可以判定 DPK 的生存期未到达（其中当前检测时间点可以在 DPK 生存期到达时间点的前面，也可以在到达时间点的后面，即在检测 DPK 生存期时，其 DPK 可能即将到达生存期或已经到达了生存期）。

另外，根据具体情况，可以选择由广播电视网的前端来检查每个 DPK 的生存期；也可以选择由广播电视网的用户端来检查每个 DPK 的生存期。

步骤 S30，广播电视网的前端对 DPK 生存期到达的用户端进行身份认证，一般情况下，前端可以通过对用户端的 ID 标识信息进行认证，来判断用户端的身份是否合法，如前端可以通过对用户端机顶盒的 ID 标识信息进行认证，来判定用户端是否为合法用户；也可以通过对用户端用户身份识别模块中存储的用户身份标识信息进行认证，来判定用户端是否为合法用户；当然更为安全的认证方式是前端通过认证用户端的机顶盒 ID 标识信息和用户身份识别模块中存储的用户身份标识信息的绑定关系，来判断用户端是否为合法用户。

步骤 S40，如果前端对用户端进行身份认证通过，执行步骤 S50，否则结束，执行下一次的 DPK 生存期检测。

步骤 S50，广播电视网前端更新生存期已经到达的 DPK 后，到达结束程序，等待执行下一次的 DPK 生存期检测。其中广播电视网前端对到达生存期的 DPK 进行更新的过程如下:

a. 前端利用与用户端共享的个人分配密钥 PDK（其中 PDK 是在用户入网注册时，由网络运营商为其分配的静态个人授权数据，PDK 也分别保存在前端和用户端手持的用户身份识别模块中）对更新后的动态个人密钥 DPK 进行加密处理后下发给用户端;

b. 用户端接收到 a 中的加密数据后，利用自身用户身份识别模块中存储的个人分配密钥 PDK 对加密的动态个人密钥数据进行解密处理，得到更新后的动态个人密钥 DPK。

利用这种方式传输更新的DPK，可以保证更新的DPK的安全性，其中加密处理的DPK数据可以选择通过有线通信网的有线传输线路或者无线通信网的无线传输线路来传输下发到用户端，这样其安全性也会得到较好的保证；当然也可以选择使用广播信道（Cable信道）来传输下发加密处理后的DPK数据到用户端，但是这样传输数据的安全性保证会稍差一些。

步骤S60，广播电视网前端基于动态个人密钥DPK对传输流TS实施加密、加扰及授权处理，对应地用户端基于该共享的动态个人密钥DPK对前端通过广播信道下发的加扰传输流TS实施解密及解扰处理，以得到解扰后的TS，然后用户端的机顶盒对解扰处理的TS进行解复用及解码等处理，以显示给用户观看，然后到达结束程序，等待执行下一次的DPK生存期检测。

其中广播电视网前端基于动态个人密钥DPK对要发送到用户端机顶盒的传输流TS实施加密、加扰及授权处理的过程如下：

A、广播电视网前端使用控制字CW对传输流TS进行加扰处理，得到加扰传输流TS'；可以表示为：TS + CW ->TS'；

B、前端再使用业务密钥SK对控制字CW进行加密处理，得到授权控制信息ECM，可以表示为：CW+SK ->ECM;

C、前端再使用动态个人密钥DPK对业务密钥SK进行加密处理，得到授权管理信息EMM，可以表示为：SK + DPK ->EMM;

相应地，广播电视网用户端基于动态个人密钥DPK对接收的加扰传输流TS'实施解密及解扰处理的过程如下：

D、用户端将接收到的ECM和EMM数据发送到用户身份识别模块中，用户身份识别模块通过自身存储的DPK对EMM进行解密，得到SK，可以表示为：EMM + DPK->SK;

E、用户端的用户身份识别模块利用得到的SK对ECM进行解密，得到CW，可以表示为：ECM + SK->CW;

F、用户端的用户身份识别模块将得到的CW反馈给用户端的机顶盒，机顶盒中的解扰引擎利用得到的CW对加扰传输流TS'实施解扰处理，得到传输流TS，可以表示为：TS' + CW->TS。

由上述可见，本发明基于广播电视网的用户授权方法是在传统 CAS 三层加密的体系下，增加了一层动态个人密钥（DPK）作为工作密钥，同时按照一定的有效期限制与更新策略对这个工作密钥进行更新，从而完成了对用户身份识别模块中存储的用户授权数据的更新；在双向传输线路传递 DPK 的时候再利用用户的个人分配密钥（PDK）对其进行加密，即密钥体系变为四层，如下：

TS + CW -> TS'

CW + SK -> ECM

SK + DPK -> EMM

这三层加密体制用于传输流的加密及加扰处理；

DPK + PDK -> EMM2

这层加密体制用于动态个人密钥 DPK 更新传输时的加密处理，其中 EMM2 优选使用双向传输线路进行传输。

其中由广播电视网前端对用户端进行身份认证的过程可以由前端发起，也可以由用户端发起，下面对这两种情况进行详细说明。

参照图 4，该图是在本发明基于广播电视网的用户授权方法中，由前端发起的对用户端进行身份认证处理的过程示意图；其处理过程如下：

步骤 S100，广播电视网的前端检测下一个用户的 DPK 生存期，其中对于初始状态，该下一个用户即为第一个用户，后续逐一对每一用户端的 DPK 进行生存期检查处理，其中可以采用周期规律对每一用户端的 DPK 进行一次轮回检查操作；

步骤 S110，前端判断检测的该用户的 DPK 生存期是否到达，如果是，执行步骤 S130，否则执行步骤 S120；

步骤 S120，前端再次判断检测的该用户的 DPK 距离其生存期的到达是否小于 1 小时，如果是执行步骤 S130，否则转至执行步骤 S195；

步骤 S130，前端再判断该 DPK 已到达其生存期的用户是否在线，如果在线，执行步骤 S140；否则转至执行步骤 S195；其中判断 DPK 已到达生存期的用户是否在线的实现方式如下：

前端对上次认证通过的用户，将默认这个用户是在线用户，并为每一

个用户保存一个关于是否在线的状态变量，直到下次认证过程用户端无响应或者认证失败，前端将认定当前用户为离线状态。

步骤 S140，前端发送认证指示命令到 DPK 生存期已到达的该用户端；

步骤 S150，该用户端接收到前端发来的认证指示命令后，将自身的标识信息通过双向传输线路上传到前端，其中用户端上传的标识信息可以为用户端机顶盒的 ID 标识信息，也可以为用户端用户身份识别模块中存储的用户身份标识信息，也可以为机顶盒 ID 标识信息和用户身份识别模块中存储的用户身份标识信息的绑定关系；

步骤 S160，前端根据该用户端发来的标识信息，采用认证服务器对其身份进行认证处理；

步骤 S170，前端根据步骤 S160 的认证结果，判断该用户端的身份认证是否通过，如果认证通过执行步骤 S180，否则转至执行步骤 S195；

步骤 S180，前端对生存期到达的 DPK 进行更新，并用前端和用户端共享的 PDK 对更新后的 DPK 进行加密处理，即 DPK + PDK->EMM2，得到加密数据 EMM2，然后将 EMM2 发送到相应的用户端；

步骤 S190，用户端机顶盒接收到前端发来的加密数据 EMM2 后，将其发送至用户身份识别模块，用户身份识别模块利用自身存储的 PDK 对 EMM2 数据进行解密处理，得到更新的 DPK，并将其存储，其解密过程可以表示为：EMM2 + PDK->DPK；

步骤 S195，前端判断该次轮回检测每个用户的 DPK 是否到达其生存期的操作是否完成，即判断每个用户端的 DPK 是否都已检测到，如果是则结束，以等待下一轮的对每个用户端的 DPK 生存期进行检测的操作；否则返回执行步骤 S100，继续检测下一个用户的 DPK 的生存期是否到达。

参照图 5，该图是在本发明基于广播电视网的用户授权方法中，由用户端发起的对用户端进行身份认证处理的过程示意图；其处理过程如下：

步骤 S200，用户端将自身机顶盒 STB 开机后，用户端将自动检查自身的 DPK 生存期；用户端可以采用周期规律对自身的 DPK 生存期进行检查；

步骤 S210，用户端判断自身的 DPK 是否到达其生存期，如果是，执行步骤 S230；否则执行步骤 S220；

步骤 S220，用户端再次判断自身 DPK 距离其生存期到达时长值是否小于 1 小时，如果是，执行步骤 S230；否则结束，以等待下一次 DPK 生存期是否到达的检测；

步骤 S230，为避免同时有大量 DPK 到达生存期的 STB 同时发起认证流程而导致前端认证服务器过载，所以用户端在这里将采取退避一段时间的处理方式；

步骤 S240，退避时间过后，用户端将自身的标识信息通过双向传输线路上传到前端，其中用户端上传的标识信息可以为用户端机顶盒的 ID 标识信息，也可以为用户端用户身份识别模块中存储的用户身份标识信息，当然也可以为机顶盒 ID 标识信息和用户身份识别模块中存储的用户身份标识信息的绑定关系；

步骤 S250，前端根据用户端发来的标识信息，采用认证服务器对其身份进行认证处理；

步骤 S260，前端根据步骤 S250 的认证结果，判断用户端的身份认证是否通过，如果认证通过执行步骤 S270，否则结束，以等待下一次 DPK 生存期是否到达的检测；

步骤 S270，前端对生存期到达的 DPK 进行更新，并用前端和用户端共享的 PDK 对更新后的 DPK 进行加密处理，即 DPK + PDK->EMM2，得到加密数据 EMM2，然后将 EMM2 发送到发起认证的用户端；

步骤 S280，用户端机顶盒接收到前端发来的加密数据 EMM2 后，将其发送至用户身份识别模块，用户身份识别模块利用自身存储的 PDK 对 EMM2 数据进行解密处理，得到更新的 DPK，并将其存储，其解密过程可以表示为：EMM2 + PDK->DPK；然后结束，以等待下一次 DPK 生存期是否到达的检测。

综上所述，本发明基于广播电视网的用户授权方法及其授权系统的基本思想就是广播电视网的前端依旧利用单向的广播信道（Cable 信道）广播电视节目传输流 TS，而单独使用在用户端机顶盒中设置的双向通信模块和前端与用户端之间设置的双向传输线路来完成用户端的身份认证处理和动态个人密钥 DPK 的更新处理；从而可以实现通过周期性更改动态个人

密钥DPK来降低非法用户利用克隆用户身份识别模块来获得非法经济利益的目的，即只要控制DPK的更新周期就能够有效限制非法用户克隆用户身份识别模块的有效时间，而使非法用户克隆用户身份识别模块的操作难度系数加大。同时也降低了运行商为维护整个用户身份识别模块系统所造成的成本损失，因为只要通过周期更新每个用户身份识别模块的DPK，就不再需要在部分用户身份识别模块被克隆的情况下，还要更换所有实际的物理用户身份识别模块，所以其经济成本一定会降低。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权 利 要 求

1、一种用户授权方法，其特征在于，包括步骤:

（1）设置前端和用户端共享的具有生存期的动态个人密钥;

（2）检查所述动态个人密钥的生存期是否到达终止时间，如果是继续步骤（3）; 否则转至步骤（4）;

（3）更新生存期到达终止时间的所述动态个人密钥后返回步骤（2）;

（4）前端基于所述动态个人密钥对传输流实施加密、加扰及授权处理，用户端基于所述动态个人密钥对加扰传输流实施解密及解扰处理。

2、根据权利要求 1 所述的用户授权方法，其特征在于，所述步骤（2）中以周期规律检查动态个人密钥的生存期。

3、根据权利要求 1 所述的基于广播电视网的用户授权方法，其特征在于，所述步骤（2）具体包括如下步骤:

（21）设置一固定时长值;

（22）判断当前检测时间点距动态个人密钥生存期到达时间点的时长值是否小于所述固定时长值，如果是，判定动态个人密钥的生存期已到达; 否则判定未到达。

4、根据权利要求 1 所述的用户授权方法，其特征在于，所述步骤（3）在更新动态个人密钥之前还包括对动态个人密钥生存期到达的用户端进行身份认证的步骤，如果认证通过继续更新动态个人密钥处理，否则结束。

5、根据权利要求 4 所述的用户授权方法，其特征在于，所述步骤（2）中检查动态个人密钥的生存期是由前端完成。

6、根据权利要求 5 所述的基于广播电视网的用户授权方法，其特征在于，所述步骤（3）对动态个人密钥生存期到达的用户端进行身份认证的过程具体包括步骤:

（31）所述前端发送认证指示命令到动态个人密钥生存期到达的用户端，指示用户端到前端进行身份认证；

（32）用户端将自身标识信息上传到前端；

（33）前端根据用户端的标识信息对用户端进行身份认证。

7、根据权利要求 6 所述的用户授权方法，其特征在于，所述步骤（31）之前还包括前端判断动态个人密钥生存期到达的用户端是否在线的步骤。

8、根据权利要求 4 所述的用户授权方法，其特征在于，所述步骤（2）中检查动态个人密钥的生存期由用户端完成。

9、根据权利要求 8 所述的用户授权方法，其特征在于，所述步骤（3）对动态个人密钥生存期到达的用户端进行身份认证的过程具体包括步骤：

（3a）动态个人密钥生存期到达的用户端将自身标识信息上传到广播电视网前端；

（3b）前端根据用户端的标识信息对用户端进行身份认证。

10、根据权利要求 1 所述的用户授权方法，其特征在于，所述步骤（3）更新动态个人密钥的过程具体包括：

（3-1）前端利用与用户端共享的个人分配密钥对更新的动态个人密钥进行加密后下发给用户端；

（3-2）用户端利用用户身份识别模块中存储的个人分配密钥对加密的动态个人密钥数据进行解密，得到更新的动态个人密钥。

11、根据权利要求 10 所述的用户授权方法，其特征在于，所述步骤（3-1）中广播电视网前端将加密后的动态个人密钥数据通过有线通信网的有线传输线路或无线通信网的无线传输线路下发到用户端。

12、根据权利要求 6 或 9 所述的用户授权方法，其特征在于，所述用户端标识信息包括：

用户端机顶盒的 ID 标识信息；或

用户端用户身份识别模块中存储的用户身份标识信息；或

用户端机顶盒 ID 标识信息和用户端用户身份识别模块中存储的用户身份标识信息的绑定关系。

13、根据权利要求 1 所述的用户授权方法，其特征在于，

步骤（4）中所述基于动态个人密钥对传输流实施加密、加扰及授权处理的过程具体包括:

（41）所述前端使用控制字对传输流进行加扰处理;

（42）使用业务密钥对控制字进行加密处理，得到授权控制信息;

（43）使用动态个人密钥对业务密钥进行加密处理，得到授权管理信息;

（44）将授权控制信息和授权管理信息复用到传输流中下发到用户端;

所述基于动态个人密钥对加扰传输流实施解密及解扰处理的过程具体包括:

（45）所述用户端使用动态个人密钥对授权管理信息进行解密处理，得到业务密钥;

（46）使用业务密钥对授权控制信息进行解密处理，得到控制字;

（47）使用控制字对加扰传输流进行解扰处理。

14、一种用户授权系统，包括用于广播节目流的前端和用于接收节目流的用户端，所述用户端包括用于处理节目流信息的机顶盒和用于存储用户授权数据的用户身份识别模块，其特征在于，所述的系统还包括:

在所述用户端设置有与机顶盒连接的双向通信模块，用于将用户端标识信息上传到所述前端，并用于接收前端发来的更新的用户授权数据;

在所述前端设置有认证服务器，与所述双向通信模块通过双向传输线路连接，用于根据用户端上传的标识信息对用户端进行身份认证处理，并在认证通过后更新用户端的用户授权数据，并将更新的用户授权数据发送到用户端的双向通信模块。

15、根据权利要求 14 所述的用户授权系统，其特征在于，所述双向通信模块通过设置在机顶盒内部实现与机顶盒的连接。

16、根据权利要求 14 所述的用户授权系统，其特征在于，

所述双向通信模块为无线通信模块，通过无线通信网的无线传输线路与所述认证服务器连接；或

所述双向通信模块为有线通信模块，通过有线通信网的有线传输线路与所述认证服务器连接。

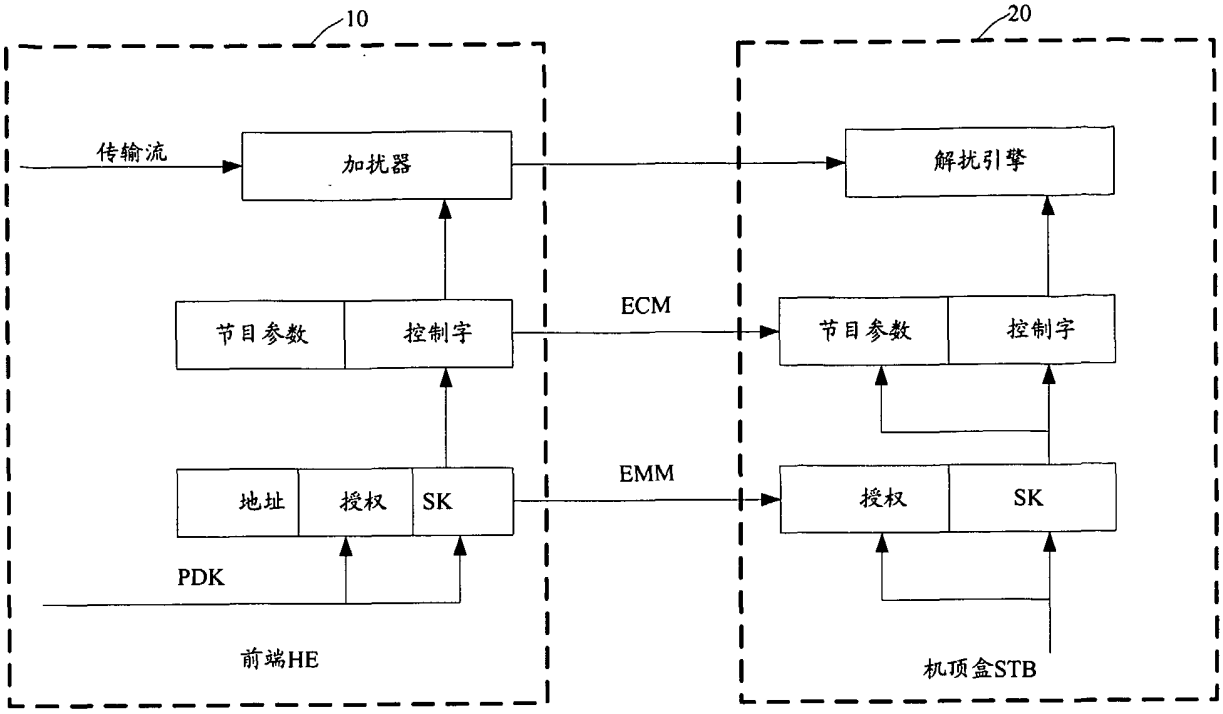

10
20
传输流
加扰器
解扰引擎
节目参数
控制字
ECM
节目参数
控制字
地址
授权
SK
EMM
授权
SK
PDK
前端HE
机顶盒STB

图 1

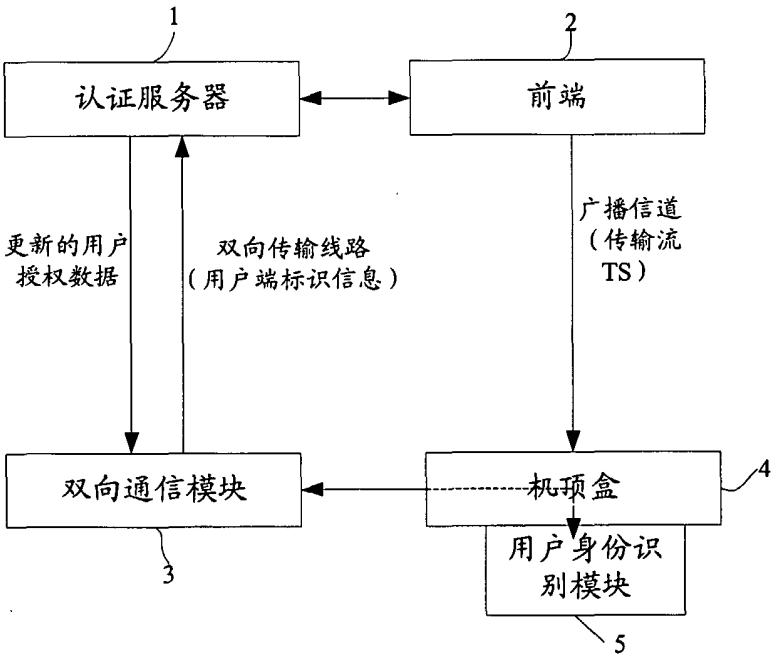

1
2
认证服务器
前端
更新的用户授权数据
双向传输线路（用户端标识信息）
广播信道（传输流TS）
双向通信模块
机顶盒
4
用户身份识别模块
3
5

图 2

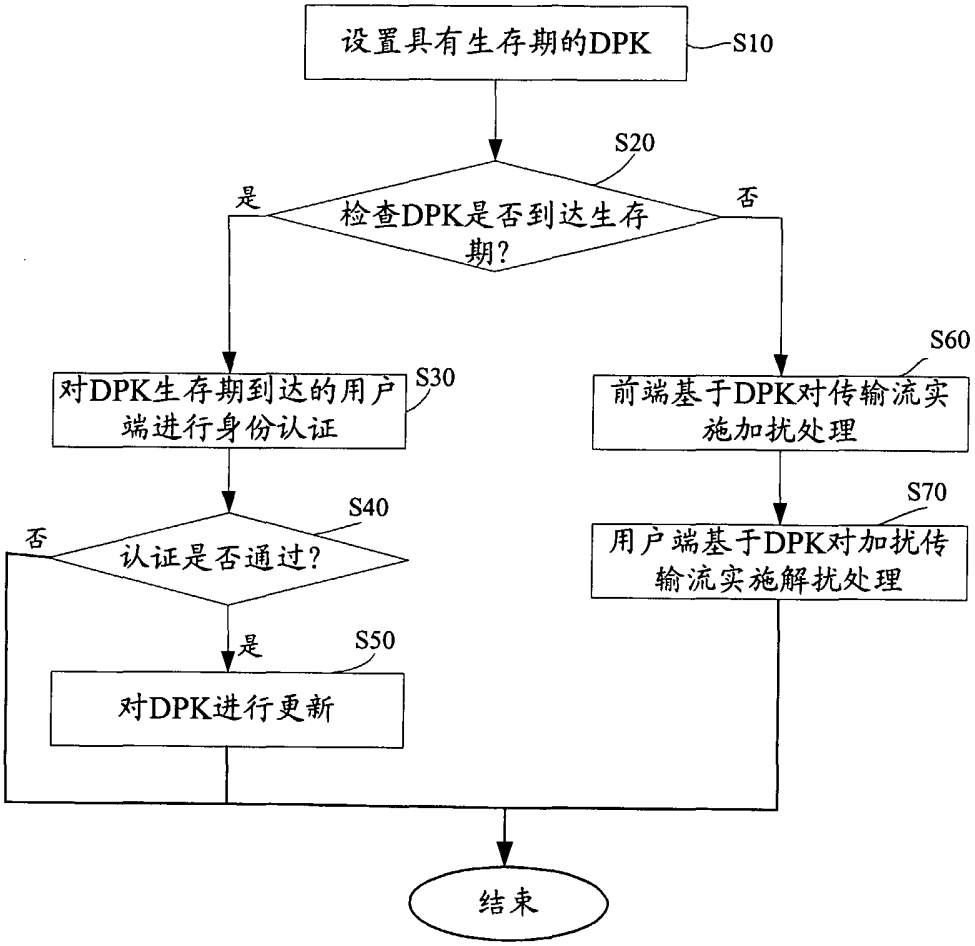

设置具有生存期的DPK
S10
S20
检查DPK是否到达生存期?
是
否
对DPK生存期到达的用户端进行身份认证
S30
前端基于DPK对传输流实施加扰处理
S60
S40
认证是否通过?
否
是
S50
对DPK进行更新
S70
用户端基于DPK对加扰传输流实施解扰处理
结束

图 3

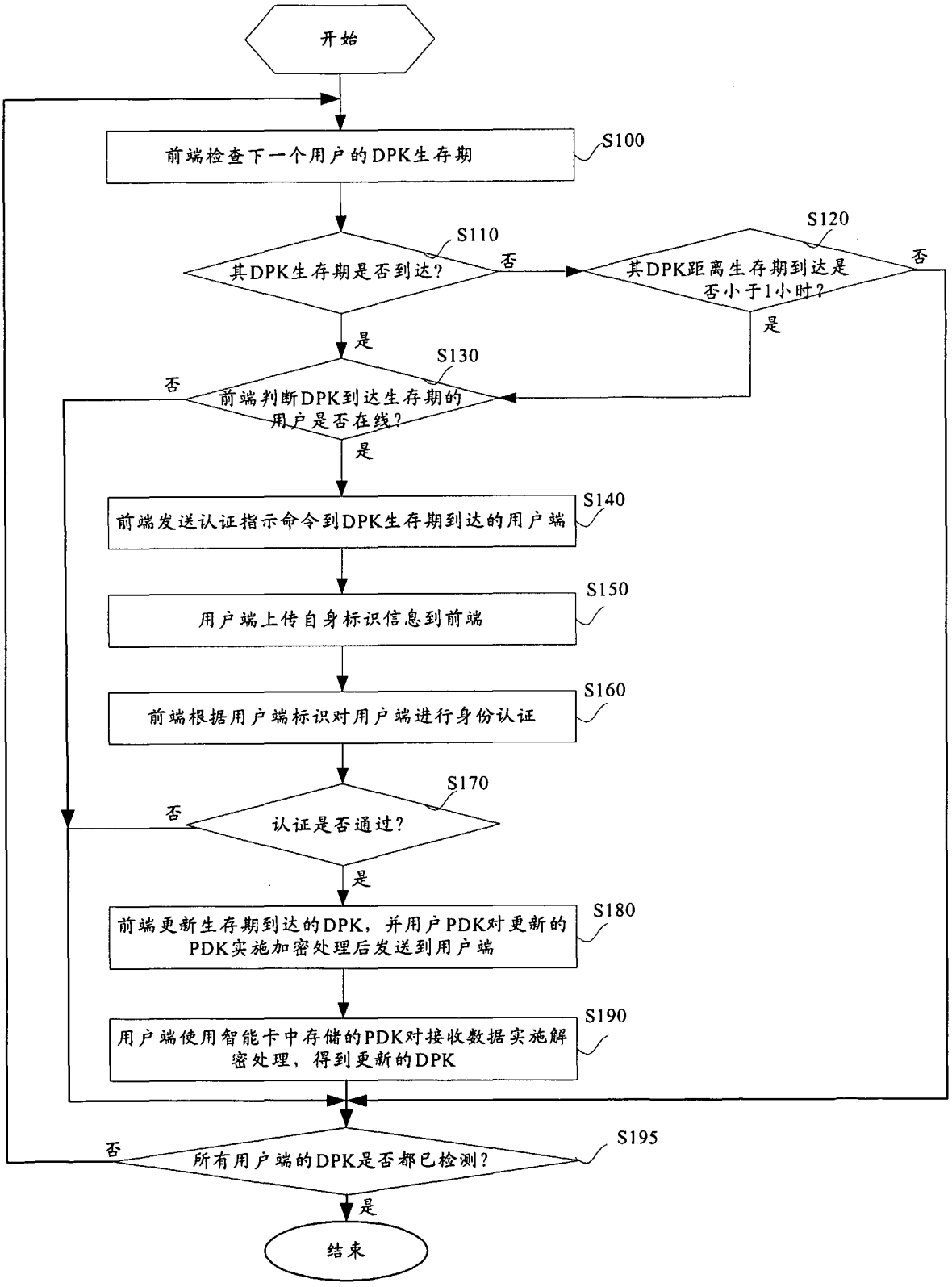

开始
前端检查下一个用户的DPK生存期
S100
其DPK生存期是否到达?
S110
否
其DPK距离生存期到达是否小于1小时?
S120
否
是
是
前端判断DPK到达生存期的用户是否在线?
S130
否
是
前端发送认证指示命令到DPK生存期到达的用户端
S140
用户端上传自身标识信息到前端
S150
前端根据用户端标识对用户端进行身份认证
S160
认证是否通过?
S170
否
是
前端更新生存期到达的DPK，并用户PDK对更新的PDK实施加密处理后发送到用户端
S180
用户端使用智能卡中存储的PDK对接收数据实施解密处理，得到更新的DPK
S190
所有用户端的DPK是否都已检测?
S195
否
是
结束

图 4

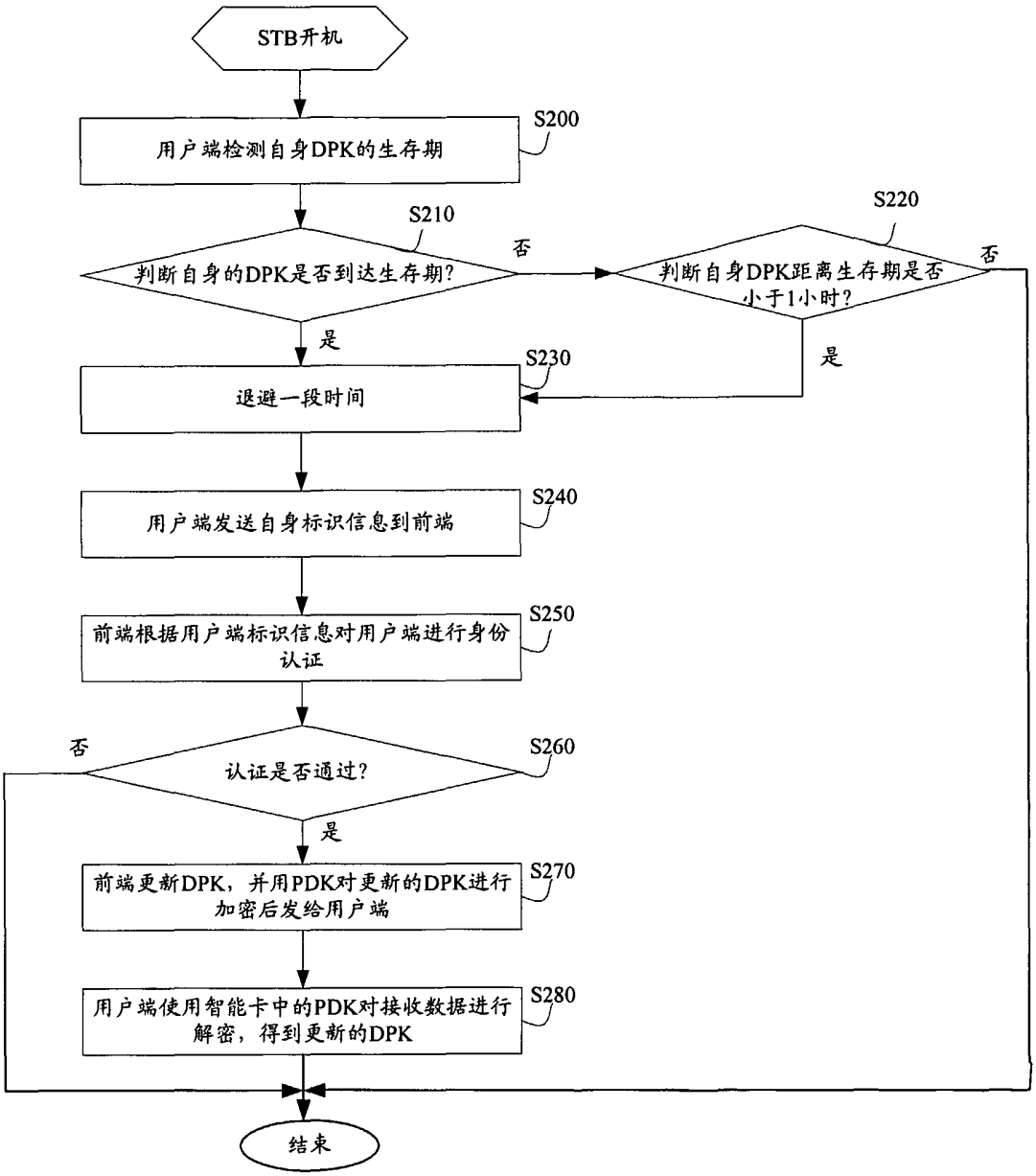

STB开机
用户端检测自身DPK的生存期
S200
判断自身的DPK是否到达生存期?
S210
否
判断自身DPK距离生存期是否小于1小时?
S220
否
是
是
退避一段时间
S230
用户端发送自身标识信息到前端
S240
前端根据用户端标识信息对用户端进行身份认证
S250
否
认证是否通过?
S260
是
前端更新DPK，并用PDK对更新的DPK进行加密后发给用户端
S270
用户端使用智能卡中的PDK对接收数据进行解密，得到更新的DPK
S280
结束

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/001092

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7] H04N7/167 H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7] H04N7/167 H04N7/173

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

CN

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRS: the Chinese words of "encrypt, decrypt, scramble, uncramble, update, time, term, bidirection, set top box, server"; WPI;EPODOC;PAJ: encrypt+, dencrypt+, scrambl+, unscrambl+, update, time, term, period, bidirection? ?, set top box, STB, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO03067888A1(NOKIA CORP)14.Aug.2003(14.08.2003) Description page3 line15-page16 last line	1-13
X	WO 02058398A2(GEN INSTR CORP) 25.Jul.2002(25.07.2002)	14—16
A	Description page 13 line 8—page 17 line 8 and fig.1	1-13
A	CN 1249621 A(MATSUSHITA ELECTRIC IND CO LTD) 05.Apr.2002(05.04.2000) The whole document	1-13
A	CN1372766A (PREDIWAVE CORP) 02.Oct.2002 (02.10.2002) The whole document	14—16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search
26.Oct.2005(26.10.2005)

Date of mailing of the international search report
17 · NOV 2005 (17 · 11 · 2005)

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer
Ma Guili

Telephone No. 86-10-62084643

Form PCT/ISA /210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/001092

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Two groups of inventions as claims1－13 and claims 14－16.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2005/001092

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO03067888A1	14.08.2003	KR2004083504 A	02.10.2004
		US2003147532 A1	07.08.2003
		AU2003202118 A1	02.09.2003
		EP1483912 A1	08.12.2004
WO02058398A2	25.07.2002	AU2002354779 A1	21.01.2003
		US2002087971 A1	04.07.2002
		WO03005724 A2	16.01.2003
		EP1354476 A2	22.10.2003
		AU2002241876 A1	30.07.2002
		EP1415472 A2	06.05.2004
CN1249621 A	05.04.2000	JP3565715B2	15.09.2004
		EP0969667 A2	05.01.2000
		AU3794999 A	20.01.2000
		JP2000023137 A	21.01.2000
		SG71930 A1	18.04 .2000
		KR2000011441 A	25.02.2000
		TW416246 A	21.12.2000
		AU741900 B	13.12.2001
		KR304806 B	01.11.2001
		US6714649 B1	30.03.2004
CN1372766A	02.10.2002	IN200201636 P3	11.12.2004
		WO0239747 A1	16.05.2002
		AU0170263 A	21.05.2002
		EP1340380 A1	03.09.2003
		KR2003051799 A	25.06.2003
		US2003208561 A1	06.11.2003
		JP2004523146 T	29.07.2004

国际检索报告

国际申请号
PCT/CN2005/001092

A. 主题的分类

IPC[7] H04N7/167 H04N7/173

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[7] H04N7/167 H04N7/173

包含在检索领域中的除最低限度文献以外的检索文献

CN

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CPRS：加密，解密，加扰，解扰，刷新，更新，时间，期限，双向，机顶盒，服务器； WPI;EPODOC;PAJ：encrypt+，dencrypt+，scrambl+，unscrambl+，update，time，term，period，bidirection??，set top box，STB，server

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	WO03067888 A1（诺基亚有限公司）14.8 月 2003（14.08.2003） 说明书第 3 页第 15 行－第 16 页最后一行	1－13
X	WO 02058398 A2（通用仪器公司）25.7 月 2002（25.07.2002）	14－16
A	说明书第 13 页第 8 行－第 17 页第 8 行及图 1	1－13
A	CN1249621A（松下电器产业株式会社）05.4 月 2000（05.04.2000）全文	1－13
A	CN1372766A（派威公司）02.10 月.2002（02.10.2002）全文	14－16

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
26.10 月 2005（26.10.2005）	17·11月 2005 (17·11·2005)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 马桂丽 电话号码：(86-10)62084643

国际检索报告

国际申请号
PCT/CN2005/001092

第II栏　关于某些权利要求不能作为检索主题的意见(接第 1 页第 2 项)

按条约 17(2)(a)对某些权利要求未作国际检索报告的理由如下：

1. ☐ 权利要求：

因为它们涉及到不要求本国际检索单位进行检索的主题，即：

2. ☐ 权利要求：

因为它们涉及到国际申请中不符合规定的要求的部分，以致不能进行任何有意义的国际检索，

具体地说：

3. ☐ 权利要求：

因为它们是从属权利要求，并且没有按照细则 6.4(a)第 2 句和第 3 句的要求撰写。

第III栏　关于缺乏发明单一性时的意见(接第 1 页第 3 项)

本国际检索单位在该国际申请中发现多项发明，即：

权利要求 1－13 和权利要求 14－16 两项发明。

1. ☒ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告针对全部可作检索的权利要求。

2. ☐ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本国际检索单位未通知缴纳任何附加费。

3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求。具体地说，是权利要求：

4. ☐ 申请人未按时缴纳被要求的附加检索费。因此，本国际检索报告仅涉及权利要求中首次提及的发明；包含该发明的权利要求是：

关于异议的说明： ☐ 申请人缴纳了附加检索费，同时提交了异议书，缴纳了异议费。

☐ 申请人缴纳了附加检索费，同时提交了异议书，但未缴纳异议费。

☐ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2005/001092

检索报告中引用的专利文件	公布日期	同族专利	公布日期
WO03067888A1	14.08.2003	KR2004083504 A	02.10.2004
		US2003147532 A1	07.08.2003
		AU2003202118 A1	02.09.2003
		EP1483912 A1	08.12.2004
WO02058398A2	25.07.2002	AU2002354779 A1	21.01.2003
		US2002087971 A1	04.07.2002
		WO03005724 A2	16.01.2003
		EP1354476 A2	22.10.2003
		AU2002241876 A1	30.07.2002
		EP1415472 A2	06.05.2004
CN1249621 A	05.04.2000	JP3565715B2	15.09.2004
		EP0969667 A2	05.01.2000
		AU3794999 A	20.01.2000
		JP2000023137 A	21.01.2000
		SG71930 A1	18.04 .2000
		KR2000011441 A	25.02.2000
		TW416246 A	21.12.2000
		AU741900 B	13.12.2001
		KR304806 B	01.11.2001
		US6714649 B1	30.03.2004
CN1372766A	02.10.2002	IN200201636 P3	11.12.2004
		WO0239747 A1	16.05.2002
		AU0170263 A	21.05.2002
		EP1340380 A1	03.09.2003
		KR2003051799 A	25.06.2003
		US2003208561 A1	06.11.2003
		JP2004523146 T	29.07.2004