(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 101076109 B
(45)授权公告日 2010.05.19

(21)申请号 200710040557.8

(22)申请日 2007.05.11

(73)专利权人 天栢宽带网络科技(上海)有限公司
地址 200233 上海市宜山路 2016 号 9 楼

(72)发明人 吕品 陈德钊 刘玲

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈亮

(51)Int.Cl.
H04N 7/16(2006.01)
H04N 7/173(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 1254473 A,2000.05.24, 全文.
US 2005/0254648 A1,2005.11.17, 全文.
US 2006/0137015 A1,2006.06.22, 全文.
CN 1620137 A,2005.05.25, 全文.
CN 1753487 A,2006.03.29, 全文.
JP 2007-28519 A,2007.02.01, 全文.

审查员 梁军丽

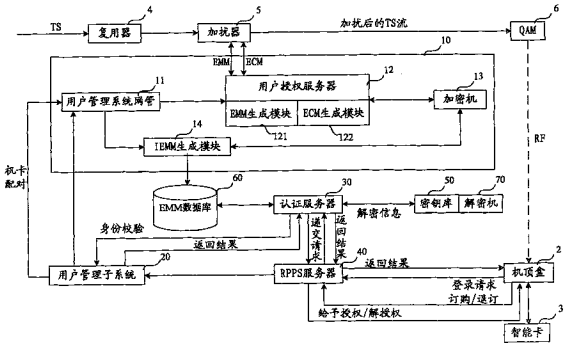
权利要求书 2 页 说明书 6 页 附图 2 页

(54)发明名称

数字电视双向 CA 系统和基于该系统的节目订购/取消方法

(57)摘要

本发明公开了数字电视中的双向 CA 系统和基于该系统的节目订购/取消方法,解决了数字电视中内容提供商、网络运营商和用户之间的安全认证,为交互式业务的开展提供便利的条件和极高的安全性,使得用户可掌握收视的主动权。其技术方案为:本发明基于客户端的主动认证进行双向认证,在认证过程中实现一次一密以提高安全。认证信息在机顶盒的智能卡中采用公钥进行加密,加密好的认证信息在前端的认证服务器中利用对应的私钥进行解密,进一步提升了系统的安全性。本发明的双向 CA 系统实现单/双向模式的兼容,在单向模式和双向模式之间平滑切换,实现网络资源的互补。本发明应用于数字电视领域。



CN 101076109 B

1. 一种数字电视中的双向 CA 系统，该双向 CA 系统包括：

双向条件接收子系统，一方面接收机卡配对信息，形成 EMM 信息后通过复用加扰设备以传输流的形式广播至机顶盒以完成配对，另一方面接收订购节目的授权指令或退订节目的解授权指令，产生 EMM 信息后通过 IP 网络发送；

用户管理子系统，连接该双向条件接收子系统，产生机卡配对信息并发送至该双向条件接收子系统，根据订购节目信息产生该节目的授权指令或根据退订节目信息产生该节目的解授权指令并发送至该双向条件接收子系统；

EMM 数据库，连接该双向条件接收子系统，接收该双向条件接收子系统子系统通过 IP 网络发送来的关于节目授权 / 解授权的 EMM 信息；

密钥库，产生公钥私钥对；

解密机，连接该密钥库，进行加密信息的解密过程；

认证服务器，一方面连接该密钥库和解密机，分配加解密的密钥，另一方面连接该 EMM 数据库，提取该 EMM 数据库中的节目授权 / 解授权的 EMM 信息；

回传通道服务器，一端通过网络连接客户端的机顶盒和智能卡，另一端连接该用户管理子系统和该认证服务器，将认证服务器分配的加密用的公钥传送至智能卡，智能卡完成对身份信息的加密后通过该回传通道服务器返回该认证服务器，该认证服务器将加密后的身份信息传送至该解密机，该解密机利用加密公钥对应的私钥进行解密，将解密后的身份信息通过该认证服务器传送至该用户管理子系统中加以校验，校验结果通过该认证服务器和该回传通道服务器传输至机顶盒，在身份校验验证合格后将对应的该认证服务器提取的节目授权 / 解授权的 EMM 信息通过该回传通道服务器传输至机顶盒。

2. 根据权利要求 1 所述的数字电视中的双向 CA 系统，其特征在于，该双向条件接收子系统进一步包括：

用户管理系统网管，连接该用户管理子系统，一方面将该用户管理子系统发送来的文本格式的机卡配对信息进行格式上的转换，另一方面接收该用户管理子系统发送来的订购节目的授权指令或退订节目的解授权指令；

加密机，对送入该加密机的授权信息和数据进行加密；

用户授权服务器，进一步包括：

EMM 生成模块，连接该用户管理系统网管，接收格式转换后的机卡配对信息，同时接收原始用户数据，与授权数据和业务密钥一起做授权处理，通过与该加密机加密操作的交互，形成 EMM 信息后插入复用设备以传输流的形式广播至机顶盒以完成配对；

ECM 生成模块，连接该用户管理系统网管和该加密机，根据控制字、业务密钥和节目收看条件的形式生成 ECM 信息，插入复用加扰设备以传输流的形式广播至机顶盒；

IEMM 生成模块，连接该用户管理系统网管和加密机，接收该用户管理系统网管传送来的订购节目的授权指令或退订节目的解授权指令，产生 EMM 信息，通过 IP 网络发送至该 EMM 数据库。

3. 根据权利要求 1 所述的数字电视中的双向 CA 系统，其特征在于，该密钥库随机产生公钥密钥对，且一次一密。

4. 根据权利要求 1 所述的数字电视中的双向 CA 系统，其特征在于，该密钥库的密钥对生成算法和产生的密钥对以及该解密机中的解密算法存储在破坏性氧化电荷易失存储电

路中。

5. 根据权利要求 1 所述的数字电视中的双向 CA 系统，其特征在于，该回传通道服务器获得机顶盒返回的对授权 / 解授权信息的确认后，自动删除该 EMM 数据库中对应的授权 / 解授权信息。

6. 根据权利要求 2 所述的数字电视中的双向 CA 系统，其特征在于，该回传通道服务器在预设时间内没有获得机顶盒应当返回的对授权 / 解授权信息的确认后，通知该用户管理子系统以单向广播的方式将授权 / 解授权信息发送至机顶盒；当该回传通道服务器获得机顶盒返回的对授权 / 解授权信息的确认后，通知用户管理子系统自动恢复到双向模式。

7. 一种基于双向 CA 系统的节目订购 / 取消方法，包括：

认证过程：

密钥库随机产生一对密钥，其中一个是公钥，一个是私钥，当机顶盒向认证服务器发送登陆请求时，认证服务器发送一个公钥信息至机顶盒；

智能卡使用该公钥对发送信息进行加密并发送至认证服务器；

认证服务器接收到该加密后的信息后，利用对应的私钥解密该信息，并进行身份信息的校验，并将校验结果返回至机顶盒，如果校验结果为该用户是合法用户，则进入下面的步骤，如果校验结果为该用户是非法用户，则流程结束；

节目授权 / 解授权过程：

接收机顶盒的节目订购 / 取消信息，形成 CA 授权 / 解授权指令，发送至双向条件接收子系统；

双向条件接收子系统将该授权 / 解授权指令加密成 EMM 信息，保存至 EMM 数据库，并返回确认信息；

通知认证服务器从 EMM 数据库中提取加密好的 EMM 信息，发送至机顶盒；

机顶盒获取授权指令后节目可以观看或者获取解授权指令后节目停止播放，并返回获取到指令的确认信息。

8. 根据权利要求 7 所述的基于双向 CA 系统的节目订购 / 取消方法，其特征在于，密钥库产生的密钥对是一次一密的，且加解密算法和密钥对存储在破坏性氧化电荷易失存储电路中。

9. 根据权利要求 7 所述的基于双向 CA 系统的节目订购 / 取消方法，其特征在于，该方法还包括：

在获得从机顶盒处返回的获取到指令的确认信息后，自动删除 EMM 数据库中对应的授权 / 解授权信息。

10. 根据权利要求 7 所述的基于双向 CA 系统的节目订购 / 取消方法，其特征在于，该方法还包括单向模式和双向模式的切换过程：

如果在预设时间内没有获得机顶盒应当返回的对授权 / 解授权信息的确认，则以单向广播的方式将授权 / 解授权信息发送至机顶盒；

如果获得机顶盒返回的对授权 / 解授权信息的确认，则自动恢复到双向模式。

数字电视双向CA系统和基于该系统的节目订购/取消方法

技术领域

[0001] 本发明涉及一种数字电视领域中的CA授权系统以及基于该授权系统的对电视节目的订购和取消方法，尤其涉及一种数字电视中的基于客户端主动认证的双向条件接收系统以及基于该双向条件接收系统的对节目进行订购和取消的方法。

背景技术

[0002] 在数字电视领域中，传统的CA授权系统（条件接收系统）保证用户通过单向的有线网络合法收看电视台运营商提供的加密付费电视节目。

[0003] 传统的CA系统一般采用三重密钥或者多层密钥对原始数据码流进行加扰控制。三重密钥一般是：加扰控制字(CW)、业务密钥(SK)和用户分配密钥(PDK)。控制字(CW)控制加扰器对视频、音频和数据进行加扰，控制字CW通过业务密钥SK加密成ECM（授权控制信息）信息后传输给用户。业务密钥SK再由用户分配密钥PDK加密成EMM（授权管理信息）后传输给用户。为了增强安全性，加扰控制字CW基本上在5秒到30秒频繁变化，业务密钥SK也定期变化。

[0004] 在接收端机顶盒STB的解扰过程中，机顶盒在授权密钥寻址分配数据包中查找与自己的用户分配密钥PDK相匹配的那个数据包，把它截获下来。然后机顶盒用用户分配密钥PDK解开EMM，获得业务密钥SK，再通过业务密钥SK解开ECM，获得控制字CW。最后由CW控制解扰器解扰，得到原始的数据码流。

[0005] 这种传统的CA系统存在以下主要缺陷：(1)造成资源的巨大浪费。为了保证用户能即时收到订购的服务，在单向网络中，必须根据一定的周期和发送频率在网络中重复发送这些EMM，造成系统处理能力和网络带宽的巨大浪费。(2)缺乏对用户设备的有效控制，CA系统关断机顶盒存在一定的问题。具体地说，当用户欠费时，CA系统向机顶盒发送关断信息，当机顶盒收到此信息后，就不再对相应信息进行解码。这里存在一个问题：当CA系统向机顶盒发送关断信息的时候，如果机顶盒处于关闭状态，即机顶盒没有收到关断信息，下一次用户开机时照样可以收看节目。更严重的是，可能有人会故意设计机顶盒忽略关断信息，这严重损害了运营商的利益。目前的解决方法是隔一段时间再次向机顶盒发送关断信息，这将造成系统资源的浪费，而且即使这样也仍然不能保证关断所有欠费的机顶盒。

发明内容

[0006] 本发明的目的在于解决上述问题，提供了一种数字电视中的双向CA系统，解决了数字电视中内容提供商、网络运营商和用户之间的安全认证，为交互式业务的开展提供便利的条件和极高的安全性，使得用户可掌握收视的主动权。

[0007] 本发明的另一目的在于基于这种双向CA系统，提供了一种电视节目的订购/取消方法，解决了数字电视中内容提供商、网络运营商和用户之间的安全认证，为交互式业务的开展提供便利的条件和极高的安全性，使得用户可掌握收视的主动权。

[0008] 本发明的技术方案为：本发明提出了一种数字电视中的双向CA系统，该双向CA系

统包括：

[0009] 双向条件接收子系统，一方面接收机卡配对信息，形成 EMM 信息后通过复用加扰设备以传输流的形式广播至机顶盒以完成配对，另一方面接收订购节目的授权指令或退订节目的解授权指令，产生 EMM 信息后通过 IP 网络发送；

[0010] 用户管理子系统，连接该双向条件接收子系统，产生机卡配对信息并发送至该双向条件接收子系统，根据订购节目信息产生该节目的授权指令或根据退订节目信息产生该节目的解授权指令并发送至该双向条件接收子系统；

[0011] EMM 数据库，连接该双向条件接收子系统，接收该双向条件接收子系统子系统通过 IP 网络发送来的关于节目授权 / 解授权的 EMM 信息；

[0012] 密钥库，产生公钥私钥对；

[0013] 解密机，连接该密钥库，进行加密信息的解密过程；

[0014] 认证服务器，一方面连接该密钥库和解密机，分配加解密的密钥，另一方面连接该 EMM 数据库，提取该 EMM 数据库中的节目授权 / 解授权的 EMM 信息；

[0015] 回传通道服务器，一端通过网络连接客户端的机顶盒和智能卡，另一端连接该用户管理子系统和该认证服务器，将认证服务器分配的加密用的公钥传送至智能卡，智能卡完成对身份信息的加密后通过该回传通道服务器返回该认证服务器，该认证服务器将加密后的身份信息传送至该解密机，该解密机利用加密公钥对应的私钥进行解密，将解密后的身份信息通过该认证服务器传送至该用户管理子系统中加以校验，校验结果通过该认证服务器和该回传通道服务器传输至机顶盒，在身份校验验证合格后将对应的该认证服务器提取的节目授权 / 解授权的 EMM 信息通过该回传通道服务器传输至机顶盒。

[0016] 上述的数字电视中的双向 CA 系统，其中，该双向条件接收子系统进一步包括：

[0017] 用户管理系统网管，连接该用户管理子系统，一方面将该用户管理子系统发送来的文本格式的机卡配对信息进行格式上的转换，另一方面接收该用户管理子系统发送来的订购节目的授权指令或退订节目的解授权指令；

[0018] 加密机，对送入该加密机的授权信息和数据进行加密；

[0019] 用户授权服务器，进一步包括：

[0020] EMM 生成模块，连接该用户管理系统网管，接收格式转换后的机卡配对信息，同时接收原始用户数据，与授权数据和业务密钥一起做授权处理，通过与该加密机加密操作的交互，形成 EMM 信息后插入复用设备以传输流的形式广播至机顶盒以完成配对；

[0021] ECM 生成模块，连接该用户管理系统网管和该加密机，根据控制字、业务密钥和节目收看条件的形式生成 ECM 信息，插入复用加扰设备以传输流的形式广播至机顶盒；

[0022] IEMM 生成模块，连接该用户管理系统网管和加密机，接收该用户管理系统网管传送来的订购节目的授权指令或退订节目的解授权指令，产生 EMM 信息，通过 IP 网络发送至该 EMM 数据库。

[0023] 上述的数字电视中的双向 CA 系统，其中，该密钥库随机产生公钥密钥对，且一次一密。

[0024] 上述的数字电视中的双向 CA 系统，其中，该密钥库的密钥对生成算法和产生的密钥对以及该解密机中的解密算法存储在破坏性氧化电荷易失存储电路中。

[0025] 上述的数字电视中的双向 CA 系统，其中，该回传通道服务器获得机顶盒返回的对

授权 / 解授权信息的确认后，自动删除该 EMM 数据库中对应的授权 / 解授权信息。

[0026] 上述的数字电视中的双向 CA 系统，其中，该回传通道服务器在预设时间内没有获得机顶盒应当返回的对授权 / 解授权信息的确认后，通知该用户管理子系统以单向广播的方式将授权 / 解授权信息发送至机顶盒；当该回传通道服务器获得机顶盒返回的对授权 / 解授权信息的确认后，通知用户管理子系统自动恢复到双向模式。

[0027] 基于上述的双向 CA 系统，本发明另外提出了一种基于双向 CA 系统的节目订购 / 取消方法，包括：

[0028] 认证过程：

[0029] 密钥库随机产生一对密钥，其中一个是公钥，一个是私钥，当机顶盒向认证服务器发送登陆请求时，认证服务器发送一个公钥信息至机顶盒；

[0030] 智能卡使用该公钥对发送信息进行加密并发送至认证服务器；

[0031] 认证服务器接收到该加密后的信息后，利用对应的私钥解密该信息，并进行身份信息的校验，并将校验结果返回至机顶盒，如果校验结果为该用户是合法用户，则进入下面的步骤，如果校验结果为该用户是非法用户，则流程结束；

[0032] 节目授权 / 解授权过程：

[0033] 接收机顶盒的节目订购 / 取消信息，形成 CA 授权 / 解授权指令，发送至双向条件接收子系统；

[0034] 双向条件接收子系统将该授权 / 解授权指令加密成 EMM 信息，保存至 EMM 数据库，并返回确认信息；

[0035] 通知认证服务器从 EMM 数据库中提取加密好的 EMM 信息，发送至机顶盒；

[0036] 机顶盒获取授权指令后节目可以观看或者获取解授权指令后节目停止播放，并返回获取到指令的确认信息。

[0037] 上述的基于双向 CA 系统的节目订购 / 取消方法，其中，密钥库产生的密钥对是一次一密的，且加解密算法和密钥对存储在破坏性氧化电荷易失存储电路中。

[0038] 上述的基于双向 CA 系统的节目订购 / 取消方法，其中，该方法还包括：

[0039] 在获得从机顶盒处返回的获取到指令的确认信息后，自动删除 EMM 数据库中对应的授权 / 解授权信息。

[0040] 上述的基于双向 CA 系统的节目订购 / 取消方法，其中，该方法还包括单向模式和双向模式的切换过程：

[0041] 如果在预设时间内没有获得机顶盒应当返回的对授权 / 解授权信息的确认，则以单向广播的方式将授权 / 解授权信息发送至机顶盒；

[0042] 如果获得机顶盒返回的对授权 / 解授权信息的确认，则自动恢复到双向模式。

[0043] 本发明对比现有技术有如下的有益效果：本发明基于客户端的主动认证进行双向认证，在认证过程中实现一次一密以提高安全。认证信息在机顶盒的智能卡中采用公钥进行加密，加密好的认证信息在前端的认证服务器中利用对应的私钥进行解密，进一步提升了系统的安全性。本发明的双向 CA 系统实现单 / 双向模式的兼容，在单向模式和双向模式之间平滑切换，实现网络资源的互补。

附图说明

[0044] 图 1 是本发明的双向 CA 系统的一个较佳实施例的原理图。

[0045] 图 2 是本发明的基于双向 CA 系统的节目订购 / 取消方法的一个较佳实施例的流程图。

具体实施方式

[0046] 下面结合附图和实施例对本发明作进一步的描述。

[0047] 图 1 示出了本发明的双向 CA 系统的一个较佳实施例的原理。请参见图 1，位于前端的双向 CA 系统 1 包括：BiCAS 子系统（即双向条件接收子系统）10、用户管理子系统 (SMS，Subscriber Management Server)20、认证服务器 (LS，LicenseServer)30、密钥库 50、解密机 (DS，Descryption Server)70、EMM（授权管理信息）数据库 60 和 RPPS 服务器 (Return Path Pool Server，回传通道服务器)40。BiCAS 子系统 10 又进一步包括：用户管理系统网管 (SMSGW，即 SMS Gateway)11、用户授权服务器 (SAS，Subscriber Authorization Server)12、加密机 (ES，Encryption Server)13、和 IEMM 生成模块 (IEMMG，Interactive EMM Generator)14。在用户授权服务器 12 中又包含 EMM 生成模块 (EMM Generator)121 和 ECM 生成模块 (ECM Generator)122。

[0048] 以下介绍双向 CA 系统 1 的双向模式的工作原理。系统对一个新的用户需要进行一次机卡配对的过程。用户管理系统 20 存有新用户的用户数据信息、对应的机顶盒编号和智能卡编号，其中机顶盒编号和智能卡编号绑定为文本形式的机卡配对信息。用户管理系统 20 将文本形式的机卡配对信息和用户数据信息发送至用户管理系统网管 11。在用户管理系统网管 11 中，对机卡配对信息做格式转换，转换成后面的用户授权服务器 12 能接受的格式。用户授权服务器 12 接收到格式正确的机卡配对信息后，其内部的 EMM 生成模块 121 同时接收到原始用户数据，并与授权数据和业务密钥一起做授权处理，通过与加密机 13 的加密操作的交互，形成 EMM 信息后插入加扰器 5 中。TS 流经过复用器 4 的复用，在控制字 CW 的控制下经加扰器 5 的处理变成加扰后的 TS 流，包含机卡配对信息的 EMM 信息被插入在加扰的 TS 流中，经 QAM6 调制后以 RF 的形式广播至客户端的机顶盒 2 和智能卡 3，在客户端完成两者的机卡配对。将智能卡与机顶盒绑定，可以防止智能卡的非法流动和盗版机顶盒的大范围使用。当节目需要机卡配对时，没有配对的智能卡将无法解扰节目。机顶盒在接收到前端发来的配对指令后也有两种处理方式：一种是通过手动输入该条配对指令包含的密码，才能配对成功；另一种方式是无需输入密码，自动完成配对过程。在机顶盒和智能卡之间是以加密方式来传送信息的，以提升系统的安全性。

[0049] 以下以用户订购一个节目为例来说明系统对身份认证和给机顶盒授权指令的处理。当用户订购一个节目时，系统首先对当前用户的身份进行校验。机顶盒 2 通过 IP 网络发送登陆请求至 RPPS 服务器 40，RPPS 服务器 40 完成机顶盒 2 与认证服务器 30 之间的交互，完成机顶盒 2 与用户管理子系统 20 之间的交互。登陆请求包含加密的身份信息，密钥库 50 随机产生一对公钥私钥对，其中的公钥经过认证服务器 30 和 RPPS 服务器 40 传送至机顶盒 2，在智能卡 3 中利用公钥对登陆用户的身份信息进行加密。RPPS 服务器 40 将包含加密的用户身份信息的登陆请求递交至认证服务器 30 中。认证服务器 30 将该加密的用户身份信息送至解密机 70，解密机 70 根据密钥库 50 中与当前公钥对应的私钥对加密信息进行解密操作，将解密信息返回给认证服务器 30。认证服务器 30 把解密后的用户身份信息通

过 RPPS 服务器 40 送入用户管理子系统 20 中进行身份校验，用户管理子系统 20 再将身份校验的结果返回至认证服务器 30。由 RPPS 服务器 40 通过网络将身份校验结果返还至机顶盒 2。如果校验结果是该用户为合法用户，则可进一步进行授权操作，否则用户非法，无法进行下一步操作。在认证过程中，安全性是考虑的重点。密钥库是随机产生公钥私钥对，而且每一次产生的公钥私钥对都是不同的。其核心算法和产生的密钥对存储在专用 IC 卡中，其存储方式是破坏性氧化电荷易失存储，保证破解者无法采用剖开芯片用电子显微镜分集集成电路。采用的加密算法是两重加密算法，里层可以采用 RSA 奇数密钥对算法，外层采用 DES3 揉密算法，使得黑容很难通过解析法得出一个明文和密文之间的函数关系。

[0050] 机顶盒 2 把需要订购的节目信息通过 IP 网络发送给 RPPS 服务器 40，RPPS 服务器 40 把订购信息发送给用户管理子系统 20。用户管理子系统 20 接收到订购信息后形成 CA 授权指令并发送给 BiCAS 子系统 10。用户管理系统网管 11 接收 CA 授权指令，并将其送至 IEMM 生成模块 14。IEMM 生成模块 14 接收 CA 授权指令并通过加密机 13 的加密，生成 EMM 信息，保存至 EMM 数据库 60 中，并返回确认信息（ACK 信息）给用户管理子系统 20。用户管理子系统 20 同时把确认信息返回给 RPPS 服务器 40。同时，ECM 生成模块 122 根据接收到的控制字 CW、业务密钥 SK 和节目收看条件 AC（通过 AC 设置可以完成对 PPC、IPPV、节目级别、水印、条件限播和区域等的区分控制）生成 ECM 信息，通过加扰机 5 插入加扰后的 TS 流中以广播方式传送至机顶盒 2。RPPS 服务器 40 在接收到返回的确认信息后与认证服务器 30 通讯，认证服务器 30 从 EMM 数据库中提取包含授权信息的 EMM 信息并传送至 RPPS 服务器 40，再由 RPPS 服务器 40 发送给机顶盒 2。机顶盒 2 在获得授权指令后，返回一个收到授权指令的确认信息至 RPPS 服务器 40，此时节目可以观看。当 RPPS 服务器 40 接收到该确认后，可以自动删除 EMM 数据库 60 中的授权信息，这样就有效降低了由于用户增长带来对码流带宽和响应速度的压力，也使得数据库容量不会因为用户数增加而直线增大。

[0051] 机顶盒在接收节目时，首先分析 ECM 数据包，根据权限对照自己的授权信息，判定是否有权限收看。在有权限收看的基础上，对 ECM 数据包进行解析，得到控制字 CW 后对视频进行解扰。

[0052] 用户取消一个节目的原理和订购大致是一样的，唯一的差别在于：用户取消节目的信息生成一个解授权指令，当机顶盒最终接收到解授权指令后，节目将被关闭。

[0053] 上述描述是系统始终处于双向模式下的工作原理，双向 CA 系统 1 也可以工作在单向模式下。当 RPPS 服务器 40 在一个预设时间内（例如设为 5 秒）没有获得机顶盒 2 应当返回的对授权或者解授权信息的确认时，就通知用户管理子系统 20 以单向广播的方式将授权或者解授权信息发送至机顶盒 2。

[0054] 单向模式和传统的 CA 系统的工作原理是相同的，由 EMM 生成模块 121 生成授权信息或解授权信息的 EMM 包，通过加扰器 5 插入在加扰后的 TS 流中，最后通过 RF 广播至机顶盒 2。

[0055] 在双向 CA 系统的双向模式和单向模式之间可以平滑切换，例如系统当前处于单向模式，如果 RPPS 服务器 40 接收到机顶盒 2 返回的授权或解授权信息的确认后，通知用户管理子系统 20 自动恢复到双向模式。

[0056] 基于双向 CA 系统，本发明还提出了一种节目订购 / 取消方法，图 2 示出了该方法的一个较佳实施例的流程，下面结合图 2 对该流程中的各步骤给予较为详细的描述。

[0057] 步骤 S10 :密钥库随机产生一对密钥,其中一个是公钥,一个是私钥,当机顶盒向认证服务器发送登陆请求时,认证服务器发送公钥至机顶盒。这种密钥对是一次一密的,每次产生的密钥对都是不同的。

[0058] 步骤 S11 :智能卡使用公钥对发送信息(主要是身份信息)进行加密并发送至认证服务器。

[0059] 步骤 S12 :认证服务器接收到加密信息后利用对应的私钥解密该信息,并进行身份信息的校验,将校验结果返回至机顶盒。

[0060] 上述步骤的密钥对和算法均存储在 IC 芯片中,并以破坏性氧化电荷易失的存储方式来存储。

[0061] 步骤 S13 :校验结果中该用户是否合法,如果用户合法,则进入下一步,否则流程结束。

[0062] 步骤 S14 :接收机顶盒发送的节目订购 / 取消信息,形成 CA 授权 / 解授权指令,发送至 BiCAS 子系统。

[0063] 步骤 S15 :BiCAS 子系统将 CA 授权 / 解授权指令加密成 EMM 信息,保存至 EMM 数据库中,并返回确认信息。

[0064] 步骤 S16 :根据确认信息通知认证服务器从 EMM 数据库中提取加密好的 EMM 信息,将该 EMM 信息发送至机顶盒。

[0065] 步骤 S17 :机顶盒在获取到授权 / 解授权指令返回确认信息,同时节目可以收看或者停止播放。

[0066] 步骤 S18 :认证服务器在获得上一步返回的确认信息后,自动删除 EMM 数据库中对应的授权 / 解授权指令。

[0067] 上述方法均以双向模式下的节目订购 / 取消为基础。上述方法还可以包括一个切换单向模式和双向模式的过程。可以预先设定一个时间,在设定的时间内没有获得机顶盒应当返回的对授权 / 解授权指令的确认,则以单向广播的方式将授权 / 解授权指令发送至机顶盒,这种单向广播模式是传统 CA 系统就已经具备的。当再次获得返回的确认时,又自动恢复到上述的双向模式。

[0068] 上述实施例是提供给本领域普通技术人员来实现或使用本发明的,本领域普通技术人员可在不脱离本发明的发明思想的情况下,对上述实施例做出种种修改或变化,因而本发明的保护范围并不被上述实施例所限,而应该是符合权利要求书提到的创新性特征的最大范围。

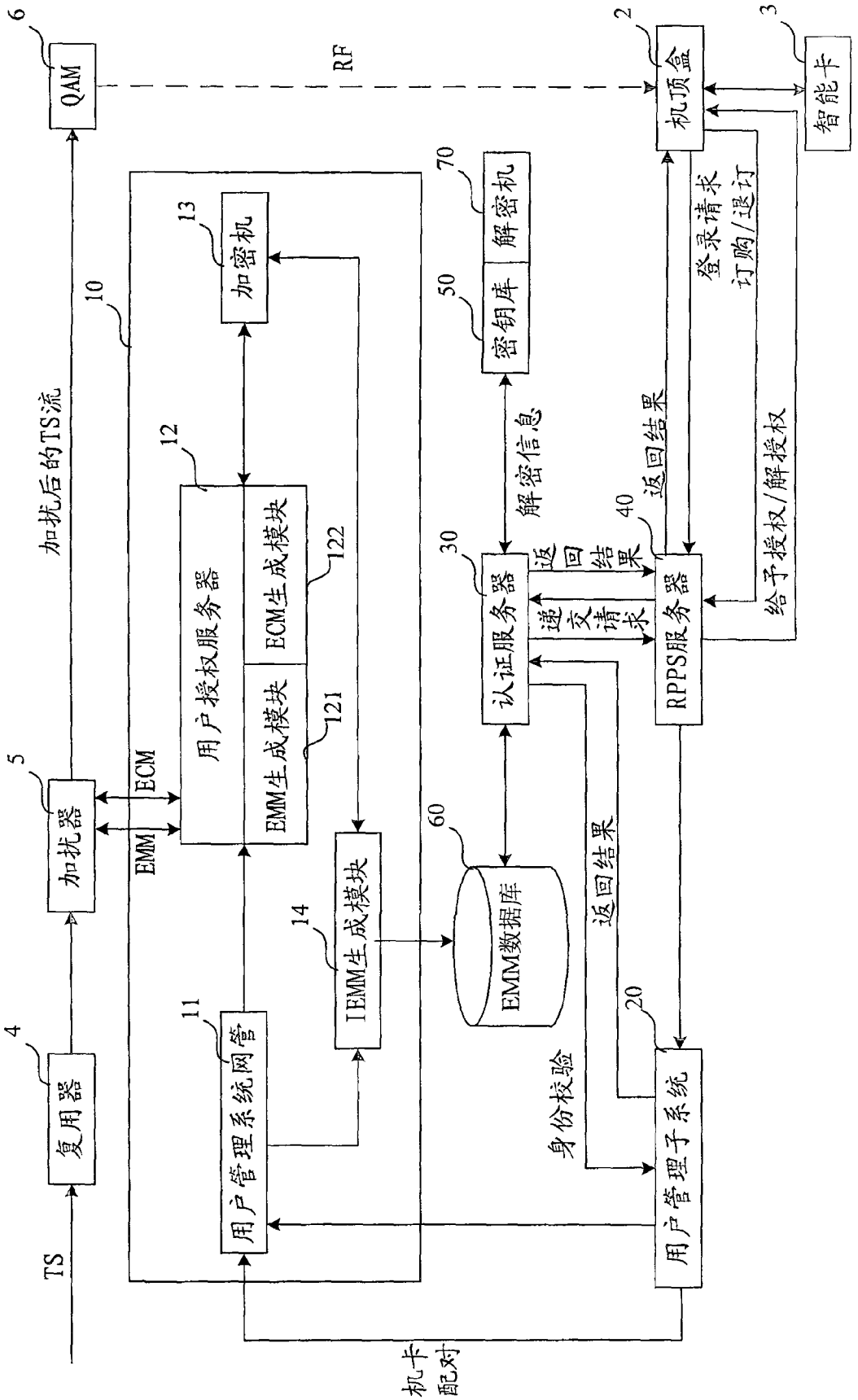

6
QAM
RF
2
机顶盒
3
智能卡
加扰后的TS流
10
70
解密机
13
加密机
50
密钥库
12
用户授权服务器
ECM生成模块
122
EMM生成模块
121
解密信息
返回结果
40
30
认证服务器
返回结果
递交请求
RPPS服务器
登录请求
订购/退订
给予授权/解授权
5
加扰器
ECM
EMM
60
EMM数据库
14
IEMM生成模块
返回结果
身份校验
20
4
复用器
11
用户管理系统网管
用户管理子系统
TS
机卡配对

图 1

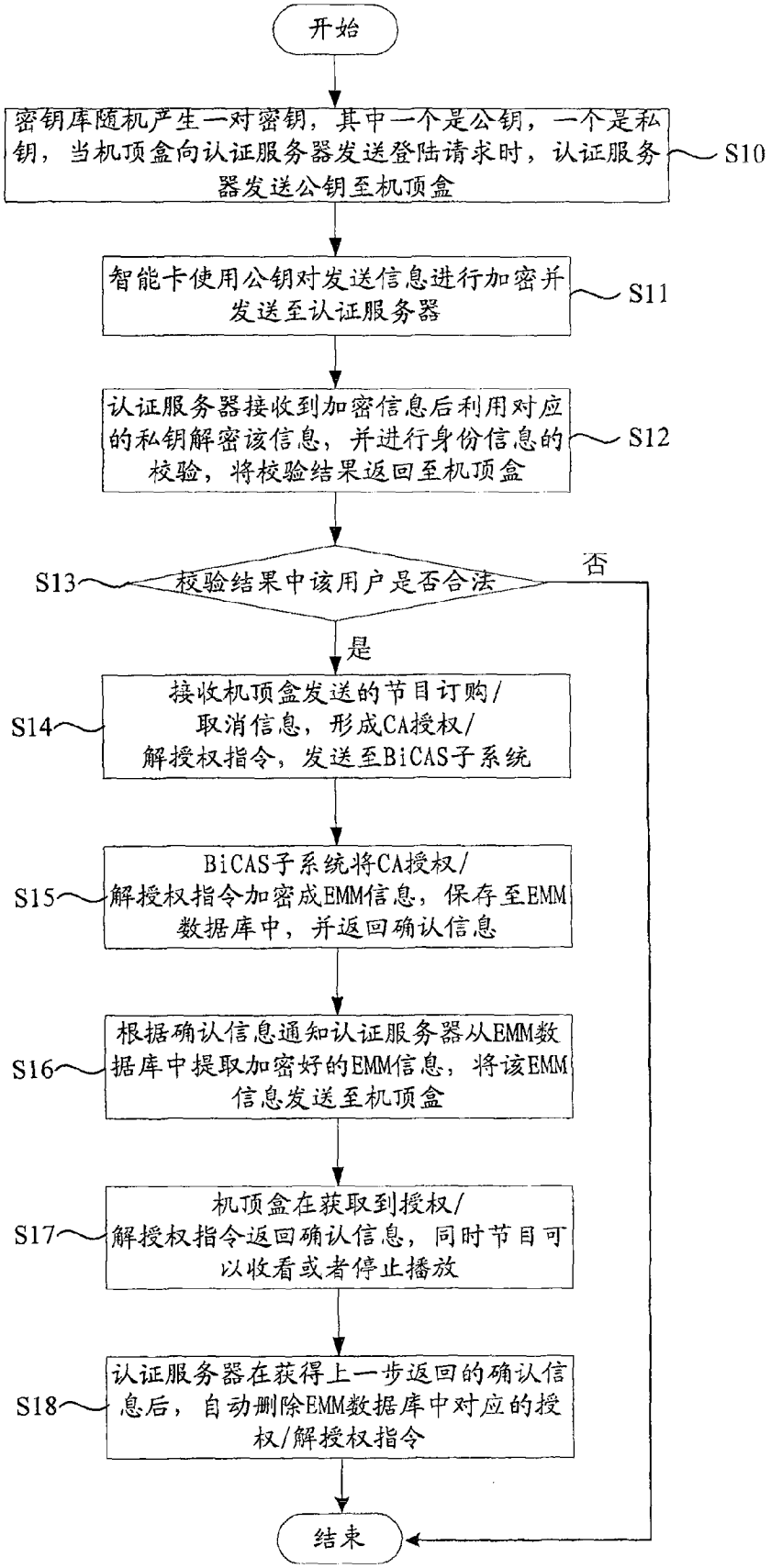

开始
密钥库随机产生一对密钥，其中一个是公钥，一个是私钥，当机顶盒向认证服务器发送登陆请求时，认证服务器发送公钥至机顶盒
S10
智能卡使用公钥对发送信息进行加密并发送至认证服务器
S11
认证服务器接收到加密信息后利用对应的私钥解密该信息，并进行身份信息的校验，将校验结果返回至机顶盒
S12
S13
校验结果中该用户是否合法
否
是
S14
接收机顶盒发送的节目订购/取消信息，形成CA授权/解授权指令，发送至BiCAS子系统
S15
BiCAS子系统将CA授权/解授权指令加密成EMM信息，保存至EMM数据库中，并返回确认信息
S16
根据确认信息通知认证服务器从EMM数据库中提取加密好的EMM信息，将该EMM信息发送至机顶盒
S17
机顶盒在获取到授权/解授权指令返回确认信息，同时节目可以收看或者停止播放
S18
认证服务器在获得上一步返回的确认信息后，自动删除EMM数据库中对应的授权/解授权指令
结束

图 2