(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 101119194 B
(45)授权公告日 2010.04.14

(21)申请号 200710121064.7

(22)申请日 2007.08.29

(73)专利权人 北京数码视讯科技股份有限公司
地址 100085 北京市海淀区上地东路 1 号盈创动力大厦 A2 座 6F

(72)发明人 宿玉文 陈德权 戴成 熊彬

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 周国城

(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
WO 2006/067677 A2,2006.06.29, 全文.
CN 101018317 A,2007.08.15, 全文.
CN 101014922 A,2007.08.08, 全文.
WO 2007/028099 A2,2007.03.08, 全文.
CN 101019427 A,2007.08.15, 附图 1-4、说明书第 2 页第 26 行到第 15 页第 7 行.

审查员 张凡

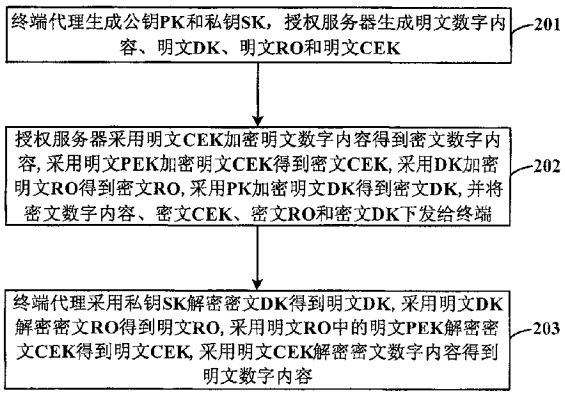
权利要求书 2 页 说明书 6 页 附图 2 页

(54)发明名称

一种对数字内容及授权进行加密和解密的方法

(57)摘要

本发明公开了一种对数字内容及授权进行加密和解密的方法,包括:终端代理生成公钥 PK 和私钥 SK,授权服务器生成明文数字内容、DK、RO 和 CEK;授权服务器采用 CEK 加密明文数字内容得到密文数字内容,采用 PEK 加密明文 CEK 得到密文 CEK,采用 DK 加密明文 RO 得到密文 RO,采用 PK 加密明文 DK 得到密文 DK,将密文数字内容、密文 CEK、密文 RO 和密文 DK 下发给终端;终端代理采用 SK 解密密文 DK 得到明文 DK,采用明文 DK 解密密文 RO 得到明文 RO,采用明文 RO 中的明文 PEK 解密密文 CEK 得到明文 CEK,采用明文 CEK 解密密文数字内容得到明文数字内容。本发明实现了对 DRM 系统数字内容及授权的版权保护。



CN 101119194 B

1. 一种对数字内容及授权进行加密和解密的方法，其特征在于，该方法包括：

终端代理生成公钥 PK 和私钥 SK，授权服务器生成明文数字内容、明文分发密钥 DK、明文权利对象 RO 和明文内容加密密钥 CEK，明文 RO 中包括明文产品密钥 PEK；

授权服务器采用明文 CEK 加密明文数字内容得到密文数字内容，采用明文 PEK 加密明文 CEK 得到密文 CEK，采用 DK 加密明文 RO 得到密文 RO，采用公钥 PK 加密明文 DK 得到密文 DK，并将密文数字内容、密文 CEK、密文 RO 和密文 DK 下发给终端；

终端代理采用私钥 SK 解密密文 DK 得到明文 DK，采用明文 DK 解密密文 RO 得到明文 RO，采用明文 RO 中的明文 PEK 解密密文 CEK 得到明文 CEK，采用明文 CEK 解密密文数字内容得到明文数字内容；

其中，所述授权服务器生成明文 DK 和明文 RO，以及对明文 DK 和明文 RO 进行加密的步骤包括：

终端需要观看数字内容但没有得到该数字内容的许可信息时，通过终端代理生成许可申请信息，并将许可申请信息发送给授权服务器；

授权服务器接收并验证终端代理的许可申请信息，通过验证后，授权服务器生成随机的明文 DK；

授权服务器利用终端代理的证书公钥 PK 对明文 DK 进行加密处理，得到密文 DK；

授权服务器生成明文 RO，采用明文 DK 对明文 RO 进行加密处理，得到密文 RO。

2. 根据权利要求 1 所述的对数字内容及授权进行加密和解密的方法，其特征在于，所述终端代理生成公钥 PK 和私钥 SK 的步骤包括：

终端代理在本地按照一定策略和要求生成一个非对称的公私密钥对，包括公钥 PK 和私钥 SK；

终端代理生成注册请求信息，并将生成的注册请求信息发送给授权服务器；

授权服务器对注册请求信息中的用户身份识别信息进行验证，通过验证后签发用户的公钥证书。

3. 根据权利要求 2 所述的对数字内容及授权进行加密和解密的方法，其特征在于，所述注册请求信息包括证书公钥 PK 和用户身份识别信息。

4. 根据权利要求 1 所述的对数字内容及授权进行加密和解密的方法，其特征在于，所述授权服务器得到密文数字内容和密文 CEK 后，进一步将密文 CEK 嵌入到密文数字内容中，与密文数字内容一起下发给终端。

5. 根据权利要求 1 所述的对数字内容及授权进行加密和解密的方法，其特征在于，所述授权服务器得到密文 DK 和密文 RO 后，进一步将密文 DK 和密文 RO 一起下发给终端。

6. 根据权利要求 1 所述的对数字内容及授权进行加密和解密的方法，其特征在于，所述许可申请信息包括用户标识、节目标识、所申请的许可和辅助信息。

7. 根据权利要求 1 所述的对数字内容及授权进行加密和解密的方法，其特征在于，所述终端代理采用明文 DK 解密密文 RO 得到明文 RO 后，进一步包括：

终端代理在需要使用明文数字内容时，验证 RO 中包含的许可规则，在验证通过后，终端代理接收嵌入到密文数字内容中的密文 CEK，采用数字内容对应的 PEK 对密文 CEK 进行解密。

8. 根据权利要求 1 所述的对数字内容及授权进行加密和解密的方法，其特征在于，所

述终端代理为用户端的一部分，每个终端用户对应一个终端代理；所述终端代理为如下形式之一：以软件模块的形式嵌入到操作系统、集成于专用卡 MMC 卡和 SIM 卡、采用专用的集成电路芯片。

9. 根据权利要求 1 所述的对数字内容及授权进行加密和解密的方法，其特征在于，

所述明文 DK 是用户首次申请许可时与授权服务器协商的分发密钥，具有一定的有效期，失效之后需要与授权服务器重新协商；

所述明文 PEK 与数字内容相对应，是按照一定策略随机生成的，并且不发生变化；

所述明文 CEK 是按照一定策略随机生成的，并且随着时间的变化而变化。

一种对数字内容及授权进行加密和解密的方法

技术领域

[0001] 本发明涉及数字媒体版权保护技术领域，尤其涉及一种对数字内容及授权进行加密和解密的方法。

背景技术

[0002] 随着信息社会的不断发展，数字媒体变得极其丰富，数字媒体的版权保护问题也越来越受到关注。

[0003] 在数字版权管理 (Digital Rights Management，DRM) 系统中，对数字内容和授权的加密是一个关键的问题，需要利用一套完善的密钥体系对数字内容和授权进行加密，限制终端用户使用受保护的数字内容，实现数字版权保护的目的。

[0004] 为了解决上述问题，结合当前的技术发展情况，本发明提出了一种用于 DRM 系统的多层密钥体系，并基于该多层密钥体系提供了一种对数字内容及授权进行加密和解密的方法，有效的满足了 DRM 系统对数字内容和授权安全加密的需求。

发明内容

[0005] （一）要解决的技术问题

[0006] 有鉴于此，本发明的主要目的在于提供一种对数字内容及授权进行加密和解密的方法，以满足 DRM 系统对数字内容和授权安全加密的需求，实现对 DRM 系统数字内容及授权的版权保护。

[0007] （二）技术方案

[0008] 为达到上述目的，本发明提供了一种对数字内容及授权进行加密和解密的方法，该方法包括：

[0009] 终端代理生成公钥 PK 和私钥 SK，授权服务器生成明文数字内容、明文分发密钥 DK、明文权利对象 RO 和明文内容加密密钥 CEK，明文 RO 中包括明文产品密钥 PEK；

[0010] 授权服务器采用明文 CEK 加密明文数字内容得到密文数字内容，采用明文 PEK 加密明文 CEK 得到密文 CEK，采用 DK 加密明文 RO 得到密文 RO，采用公钥 PK 加密明文 DK 得到密文 DK，并将密文数字内容、密文 CEK、密文 RO 和密文 DK 下发给终端；

[0011] 终端代理采用私钥 SK 解密密文 DK 得到明文 DK，采用明文 DK 解密密文 RO 得到明文 RO，采用明文 RO 中的明文 PEK 解密密文 CEK 得到明文 CEK，采用明文 CEK 解密密文数字内容得到明文数字内容；

[0012] 其中，所述授权服务器生成明文 DK 和明文 RO，以及对明文 DK 和明文 RO 进行加密的步骤包括：

[0013] 终端需要观看数字内容但没有得到该数字内容的许可信息时，通过终端代理生成许可申请信息，并将许可申请信息发送给授权服务器；

[0014] 授权服务器接收并验证终端代理的许可申请信息，通过验证后，授权服务器生成随机的明文 DK；

[0015] 授权服务器利用终端代理的证书公钥 PK 对明文 DK 进行加密处理，得到密文 DK；

[0016] 授权服务器生成明文 RO，采用明文 DK 对明文 RO 进行加密处理，得到密文 RO。

[0017] 上述方案中，所述终端代理生成公钥 PK 和私钥 SK 的步骤包括：

[0018] 终端代理在本地按照一定策略和要求生成一个非对称的公私密钥对，包括公钥 PK 和私钥 SK；

[0019] 终端代理生成注册请求信息，并将生成的注册请求信息发送给授权服务器；

[0020] 授权服务器对注册请求信息中的用户身份识别信息进行验证，通过验证后签发用户的公钥证书。

[0021] 上述方案中，所述注册请求信息包括证书公钥 PK 和用户身份识别信息。

[0022] 上述方案中，所述授权服务器得到密文数字内容和密文 CEK 后，进一步将密文 CEK 嵌入到密文数字内容中，与密文数字内容一起下发给终端。

[0023] 上述方案中，所述授权服务器得到密文 DK 和密文 RO 后，进一步将密文 DK 和密文 RO 一起下发给终端。

[0024] 上述方案中，所述许可申请信息包括用户标识、节目标识、所申请的许可和辅助信息。

[0025] 上述方案中，所述终端代理采用明文 DK 解密密文 RO 得到明文 RO 后，进一步包括：终端代理在需要使用明文数字内容时，验证 RO 中包含的许可规则，在验证通过后，终端代理接收嵌入到密文数字内容中的密文 CEK，采用数字内容对应的 PEK 对密文 CEK 进行解密。

[0026] 上述方案中，所述终端代理为用户端的一部分，每个终端用户对应一个终端代理；

[0027] 所述终端代理为如下形式之一：以软件模块的形式嵌入到操作系统、集成于专用卡 MMC 卡和 SIM 卡、采用专用的集成电路芯片。

[0028] 上述方案中，所述明文 DK 是用户首次申请许可时与授权服务器协商的分发密钥，具有一定的有效期，失效之后需要与授权服务器重新协商；

[0029] 所述明文 PEK 与数字内容相对应，是按照一定策略随机生成的，并且不发生变化；

[0030] 所述明文 CEK 是按照一定策略随机生成的，并且随着时间的变化而变化。

[0031] （三）有益效果

[0032] 从上述技术方案可以看出，本发明具有以下有益效果：

[0033] 本发明提供的这种对数字内容及授权进行加密和解密的方法，通过采用多层密钥体系对数字内容及授权进行加密和解密，有效地保证了数字内容及授权的安全使用，最大限度的限制了终端用户使用受保护的数字内容，满足了 DRM 系统对数字内容和授权安全加密的需求，实现了对 DRM 系统数字内容及授权的版权保护。

附图说明

[0034] 图 1 为本发明提供的多层密钥体系的结构示意图；

[0035] 图 2 为本发明提供的对数字内容及授权进行加密和解密的方法流程图；

[0036] 图 3 为依照本发明实施例对数字内容及授权进行加密和解密的方法流程图。

具体实施方式

[0037] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本发明进一步详细说明。

[0038] 如图 1 所示，图 1 为本发明提供的多层密钥体系的结构示意图，该多层密钥体系包括注册层、授权管理层、内容密钥层和内容加密层四个结构层。

[0039] 其中，在注册层，终端代理生成公私密钥对，并向授权服务器提出注册请求，授权服务器签发用户公钥证书。

[0040] 在终端代理生成公私密钥对时，终端代理在本地按照一定策略和要求生成一个非对称的公私密钥对，包括公钥 (Public Key，PK) 和私钥 (SecretKey，SK)。然后，终端代理生成注册请求信息，注册请求信息包括证书公钥 PK 和用户身份识别信息。终端代理向给授权服务器发送注册请求信息，授权服务器对注册请求信息中的用户身份识别信息进行验证，验证通过后签发该用户的公钥证书。

[0041] 在授权管理层，终端代理生成许可申请信息，并向授权服务器提出许可申请，授权服务器生成并返回权利对象 (Right Object，RO)，终端代理解密权利对象。

[0042] 在用户需要观看数字内容但没有得到该数字内容的许可信息时，通过终端代理生成许可申请信息，许可申请信息包括用户标识、节目标识、所申请的许可、以及其他辅助信息。终端代理将许可申请信息发送给授权服务器，授权服务器接收并验证终端代理的许可申请信息，验证通过后，授权服务器生成随机的分发密钥 (Distribution Key，DK)。授权服务器利用终端代理的证书公钥 PK 对 DK 进行加密处理得到密文 DK，授权服务器生成 RO，RO 包括用户申请数字内容所对应的产品密钥 (Product EncryptionKey，PEK)。授权服务器利用 DK 对 RO 进行加密处理得到密文 RO，授权服务器将密文 DK 和密文 RO 一起下发给终端用户；终端代理接收到密文 DK 和密文 RO 后，利用证书私钥 SK 解密密文 DK，得到明文 DK，然后利用 DK 解密密文 RO，得到明文 RO，获得 PEK。

[0043] 在内容密钥层，授权服务器生成密文内容加密密钥 (ContentEncryption Key，CEK) 信息，将密文 CEK 嵌入到密文数字内容中并下发给终端用户，终端代理接收并解密密文 CEK，得到明文 CEK。授权服务器利用 PEK 加密 CEK 和其他相关信息，得到密文 CEK。授权服务器将密文 CEK 嵌入到密文数字内容中，与密文数字内容一起下发给终端用户；终端代理接收嵌入到密文数字内容中的密文 CEK，利用数字内容对应的 PEK 解密密文 CEK，得到明文 CEK。

[0044] 在内容加密层，授权服务器生成密文数字内容，将密文数字内容发送到终端用户，终端代理解密密文数字内容，得到明文数字内容。授权服务器利用 CEK 对明文数字内容进行加密，得到密文数字内容。授权服务器将密文数字内容发送到终端用户。用户需要使用该数字内容时，终端代理验证 RO 中包含的许可规则，验证通过后，利用明文 CEK 解密密文数字内容，得到明文数字内容。

[0045] 上述授权管理层的 DK，是用户首次申请许可时与授权服务器协商的分发密钥，具有一定的有效期，失效之后需要与授权服务器重新协商。用户申请许可时，如果 DK 处于有效期，则可以继续使用，否则用户需要与授权服务器协商新的 DK。

[0046] 上述授权管理层所述 PEK，是与数字内容对应的，是按照一定策略随机生成的，一般是固定的，不会发生变化。

[0047] 上述内容密钥层所述 CEK，是按照一定策略随机生成的，并且随着时间的变化而变化。

[0048] 基于上述图 1 所示的多层密钥体系，图 2 示出了本发明提供的对数字内容及授权进行加密和解密的方法流程图，该方法包括以下步骤：

[0049] 步骤 201：终端代理生成公钥 (PK) 和私钥 (SK)，授权服务器生成明文数字内容、明文分发密钥 (DK)、明文权利对象 (RO) 和明文内容加密密钥 (CEK)，明文 RO 中包括明文产品密钥 (PEK)；

[0050] 步骤 202：授权服务器采用明文 CEK 加密明文数字内容得到密文数字内容，采用明文 PEK 加密明文 CEK 得到密文 CEK，采用 DK 加密明文 RO 得到密文 RO，采用公钥 PK 加密明文 DK 得到密文 DK，并将密文数字内容、密文 CEK、密文 RO 和密文 DK 下发给终端；

[0051] 步骤 203：终端代理采用私钥 SK 解密密文 DK 得到明文 DK，采用明文 DK 解密密文 RO 得到明文 RO，采用明文 RO 中的明文 PEK 解密密文 CEK 得到明文 CEK，采用明文 CEK 解密密文数字内容得到明文数字内容。

[0052] 上述终端代理生成公钥 PK 和私钥 SK 的步骤包括：

[0053] 步骤 a1：终端代理在本地按照一定策略和要求生成一个非对称的公私密钥对，包括公钥 PK 和私钥 SK；

[0054] 步骤 a2：终端代理生成注册请求信息，并将生成的注册请求信息发送给授权服务器；所述注册请求信息包括证书公钥 PK 和用户身份识别信息；

[0055] 步骤 a3：授权服务器对注册请求信息中的用户身份识别信息进行验证，通过验证后签发该用户的公钥证书。

[0056] 上述授权服务器得到密文数字内容和密文 CEK 后，进一步将密文 CEK 嵌入到密文数字内容中，与密文数字内容一起下发给终端。

[0057] 上述授权服务器生成明文 DK 和明文 RO，以及对明文 DK 和明文 RO 进行加密的步骤包括：

[0058] 步骤 b1：终端需要观看数字内容但没有得到该数字内容的许可信息时，通过终端代理生成许可申请信息，并将许可申请信息发送给授权服务器；所述许可申请信息包括用户标识、节目标识、所申请的许可和辅助信息；

[0059] 步骤 b2：授权服务器接收并验证终端代理的许可申请信息，通过验证后，授权服务器生成随机的明文 DK；

[0060] 步骤 b3：授权服务器利用终端代理的证书公钥 PK 对明文 DK 进行加密处理，得到密文 DK；

[0061] 步骤 b4：授权服务器生成明文 RO，采用明文 DK 对明文 RO 进行加密处理，得到密文 RO。

[0062] 上述步骤 b3 和步骤 b4 授权服务器得到密文 DK 和密文 RO 后，进一步将密文 DK 和密文 RO 一起下发给终端。

[0063] 上述终端代理采用明文 DK 解密密文 RO 得到明文 RO 后，进一步包括：终端代理在需要使用明文数字内容时，验证 RO 中包含的许可规则，在验证通过后，终端代理接收嵌入到密文数字内容中的密文 CEK，采用数字内容对应的 PEK 对密文 CEK 进行解密。

[0064] 上述终端代理为用户端的一部分，每个终端用户对应一个终端代理；所述终端代理包括但不局限于如下形式：以软件模块的形式嵌入到操作系统、集成于专用卡 MMC 卡和

SIM 卡、采用专用的集成电路芯片。

[0065] 基于图 2 所述的对数字内容及授权进行加密和解密的方法流程图，以下结合具体的实施例对本发明提供的对数字内容及授权进行加密和解密的方法进一步详细说明。

[0066] 如图 3 所示，图 3 为依照本发明实施例对数字内容及授权进行加密和解密的方法流程图，该方法包括以下步骤：

[0067] 步骤 301：终端代理生成公私密钥对，向授权服务器提出注册请求，授权服务器签发用户公钥证书。具体包含以下步骤：

[0068] A1、终端代理在本地按照一定策略和要求生成一个非对称的公私密钥对，包括公钥 PK 和私钥 SK；

[0069] A2、终端代理生成注册请求信息，注册请求信息包括证书公钥 PK 和用户身份识别信息；

[0070] A3、终端代理向给授权服务器发送注册请求信息；

[0071] A4、授权服务器对注册请求信息中的用户身份识别信息进行验证，通过验证后签发该用户的公钥证书。

[0072] 步骤 302：授权服务器生成密文数字内容和密文 CEK，将密文 CEK 嵌入到密文数字内容中，并下发到终端用户。具体包括以下步骤：

[0073] B1、授权服务器利用 CEK 对明文数字内容进行加密，得到密文数字内容；

[0074] B2、授权服务器利用 PEK 加密 CEK 和其他相关信息，得到密文 CEK；

[0075] B3、授权服务器将密文 CEK 嵌入到密文数字内容中，与密文数字内容一起发送到终端用户。

[0076] 步骤 303：终端代理生成许可申请信息，向授权服务器提出许可申请，授权服务器生成并返回 RO，终端代理解密 RO。具体包括以下步骤：

[0077] C1、用户需要观看数字内容但是没有得到该数字内容的许可信息时，通过终端代理生成许可申请信息，许可申请信息包括用户标识、节目标识、所申请的许可、以及其他辅助信息；

[0078] C2、终端代理将许可申请信息发送给授权服务器；

[0079] C3、授权服务器接收并验证终端代理的许可申请信息，通过验证后，授权服务器生成随机的分发密钥 (Distribution Key，简称 DK)；

[0080] C4、授权服务器利用终端代理的证书公钥 PK 对 DK 进行加密处理，得到密文 DK；

[0081] C5、授权服务器生成 RO，RO 包括用户申请数字内容所对应的产品密钥 (Product Encryption Key，简称 PEK)；

[0082] C6、授权服务器利用 DK 对 RO 进行加密处理，得到密文 RO；

[0083] C7、授权服务器将密文 DK 和密文 RO 一起发送给终端用户；

[0084] C8、终端代理接收到密文 DK 和密文 RO 后，利用证书私钥 SK 解密密文 DK，得到明文 DK，然后利用 DK 解密密文 RO，得到明文 RO，获得 PEK。

[0085] 步骤 304：终端代理解密密文数字内容，获得明文数字内容。具体包括以下步骤：

[0086] D1、用户需要使用该数字内容时，终端代理验证 RO 中包含的许可规则；

[0087] D2、通过验证后，终端代理接收嵌入到密文数字内容中的密文 CEK，利用数字内容对应的 PEK 解密密文 CEK，得到明文 CEK；

[0088] D3、终端代理利用明文 CEK 解密密文数字内容，得到明文数字内容。

[0089] 本发明提供的这种对数字内容及授权进行加密和解密的方法，不仅适用于 DRM 系统，也适用于其他加密系统、安全保护等系统。用于上述加密或安全保护系统的与本发明类似的，或在本发明基础上本领域普通技术人员能够不必付出创造性劳动而得到的密钥体系结构或加密方法，均应包含在本发明的保护范围之内。

[0090] 本发明提供的这种对数字内容及授权进行加密和解密的方法，其他与本发明类似的、在本发明基础上进行修改的、删减的、增加的密钥体系结构或加密方法，如果使用了本发明提出的思想，均应包含在本发明的保护范围之内。

[0091] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

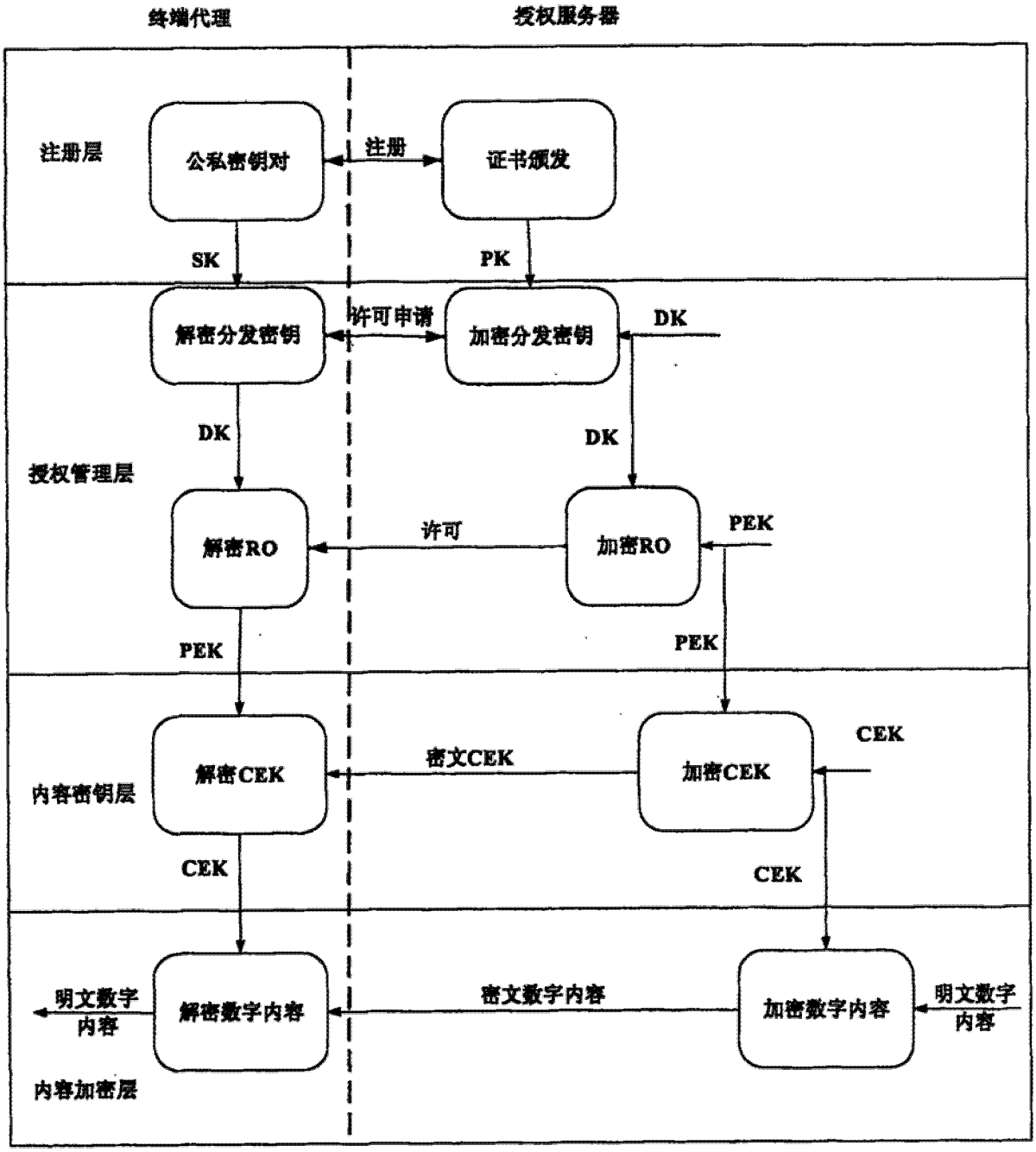

终端代理
授权服务器
注册层
公私密钥对
注册
证书颁发
SK
PK
解密分发密钥
许可申请
加密分发密钥
DK
DK
DK
授权管理层
解密RO
许可
加密RO
PEK
PEK
PEK
内容密钥层
解密CEK
密文CEK
加密CEK
CEK
CEK
CEK
明文数字内容
解密数字内容
密文数字内容
加密数字内容
明文数字内容
内容加密层

图 1

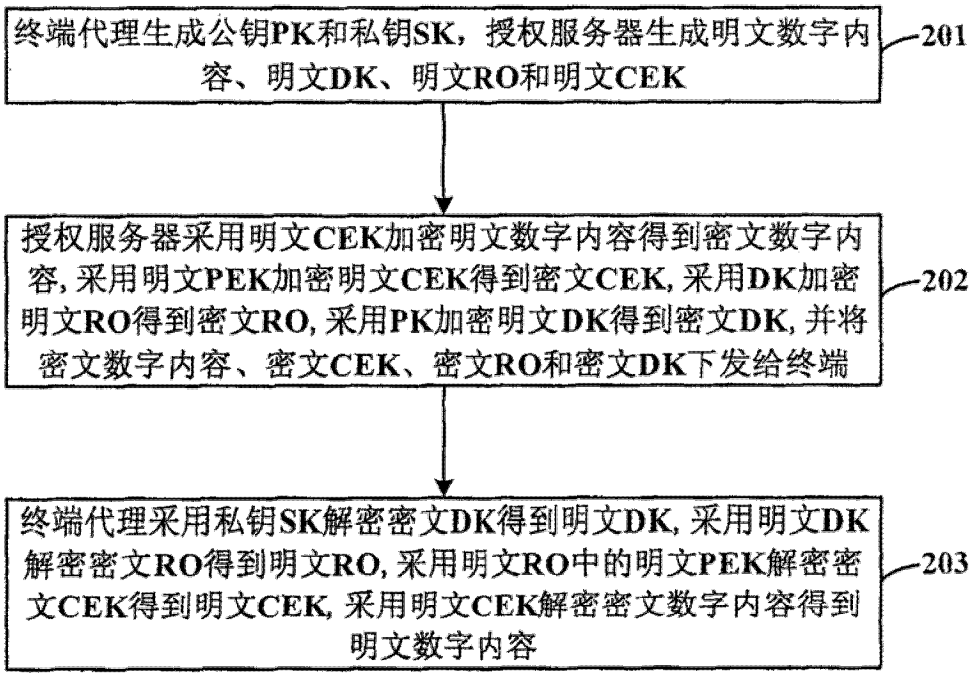

终端代理生成公钥PK和私钥SK，授权服务器生成明文数字内容、明文DK、明文RO和明文CEK
201
授权服务器采用明文CEK加密明文数字内容得到密文数字内容，采用明文PEK加密明文CEK得到密文CEK，采用DK加密明文RO得到密文RO，采用PK加密明文DK得到密文DK，并将密文数字内容、密文CEK、密文RO和密文DK下发给终端
202
终端代理采用私钥SK解密密文DK得到明文DK，采用明文DK解密密文RO得到明文RO，采用明文RO中的明文PEK解密密文CEK得到明文CEK，采用明文CEK解密密文数字内容得到明文数字内容
203

图 2

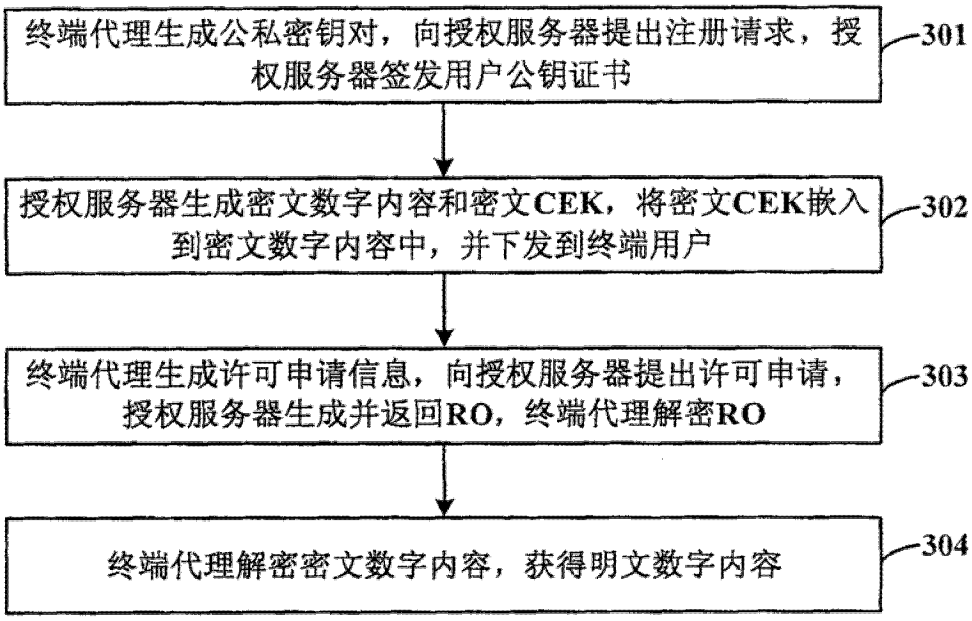

终端代理生成公私密钥对，向授权服务器提出注册请求，授权服务器签发用户公钥证书
301
授权服务器生成密文数字内容和密文CEK，将密文CEK嵌入到密文数字内容中，并下发到终端用户
302
终端代理生成许可申请信息，向授权服务器提出许可申请，授权服务器生成并返回RO，终端代理解密RO
303
终端代理解密密文数字内容，获得明文数字内容
304

图 3