[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
H04L 9/00

[12] 发明专利申请公开说明书

[21] 申请号 03156489.5

[43] 公开日 2005 年 3 月 9 日

[11] 公开号 CN 1592197A

[22] 申请日 2003.9.1 [21] 申请号 03156489.5

[71] 申请人 台均实业有限公司
地址 台湾省桃园县中坜市环北路 400 号 10F 之 7
[72] 发明人 施宣明

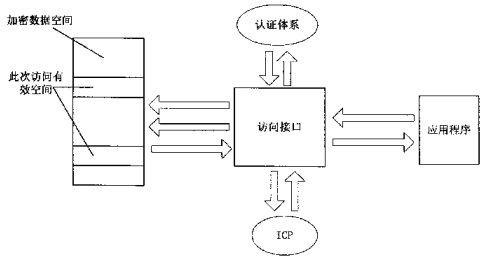
[74] 专利代理机构 北京同立钧成知识产权代理有限公司
代理人 刘 薇 刘 芳

权利要求书 4 页 说明书 7 页 附图 2 页

[54] 发明名称 用户端设备与本地客户端应用或远程网络服务间鉴权的方法

[57] 摘要

本发明提供一种用户端设备与本地客户端应用/远程网络服务间鉴权的方法，在用户端设备内设置认证信息以及安全机制接口，在应用或服务内设置与认证信息匹配的认证文件和访问安全机制接口的路径；安全机制接口为两者通信的特定协议，当用户需求某应用或服务时，通过用户端设备与应用或服务之间设置的安全机制接口，将两者的认证文件交认证机制进行鉴权，鉴权通过的用户端设备可获得软件应用或服务；没有通过的，则拒绝该用户。通过本发明可以实现信息安全存放、信息管理以及信息安全交互，从而衍生出：硬件设备识别、用户身份验证、用户权限管理、用户数据共享、安全数据存放及管理、软件版权保护、定制应用服务等一系列功能。



ISSN1008-4274

知识产权出版社出版

1、 一种用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：在用户端设备内设置认证信息以及安全机制接口，在应用或服务内设置与认证信息匹配的认证文件和访问安全机制接口的路径；安全机制接口为两者通信的特定协议，当用户需求某应用或服务时，通过用户端设备与应用或服务之间设置的安全机制接口，将两者的认证文件交认证机制进行鉴权，鉴权通过的用户端设备可获得软件应用或服务；没有通过的，则拒绝该用户。

2、 根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：用户端设备为 USB 闪存、键盘读取设备、MP3 读取设备、PDA 读取设备、STB 读取设备、磁盘读取设备、智能 PDA 读取设备、数据银行、电子词典、多功能无线设备、数码相机、录音笔。

3、 根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：实现鉴权过程的认证机制设置在用户端设备或客户端，或者通过两者结合进行。

4、 根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：认证机制进行鉴权是由应用或服务向用户端设备进行，即应用或服务认证用户端设备是否有使用权限。

5、 根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：用户端设备内设置的认证信息是服务包的集合，用于实现与应用或服务之间认证鉴权。

6、 根据权利要求 5 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：所述服务包集合含有一个或一个以上服务包信息。

7、 根据权利要求 6 所述的用户端设备与本地客户端应用/远程网络服

务间鉴权的方法，其特征在于：所述服务包信息包括有效标志和/或有效时间，其中有效标志标示用户端设备对于某应用或服务的使用权限信息；有效时间标志了此类服务使用的有效时间。

8、 根据权利要求 7 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：服务包信息可通过网络远程下载动态更新。

9、 根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：用户端设备内设置认证信息可通过软件或网络远程控制方式进行修改。

10、 根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务设置的认证文件中包括认证文件版本、有效区域名称和有效区域长度；所述认证文件版本，用于记录认证文件的版本信息；所述有效区域名称，用于标示授权的应用或服务在硬件设备安全加密数据区中可以访问的区域；所述有效区域长度，用于标示授权的应用或服务在硬件设备安全加密数据区中可以访问的区域的长度。

11、 根据权利要求 10 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务设置的认证文件中还包括有效期限，用于限定证书的有效时间。

12、 根据权利要求 10 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务设置的认证文件中还包括服务类别，用于标志该认证文件对应的服务类型。

13、 根据权利要求 10 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务设置的认证文件中还包括认证文件删除，用于删除认证文件。

14、 根据权利要求 10 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务设置的认证文件中还包括保密串，用于认证证书拥有者的合法性。

15、根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务认证文件的设置通过网络获取或制作时生成。

16、根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务由本地客户端或远程网络提供。

17、根据权利要求 1 至 16 任一所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：用户端设备与应用或服务之间鉴权的具体步骤为：当授权的服务或应用需要访问用户端设备信息时，发出访问请求，同时将认证文件提交到认证机制；认证机制读取用户端设备的认证信息，也就是服务包信息；验证该用户端设备是否有权限使用此项应用或服务；认证机制读取认证文件中的“服务类别”，判断在硬件的认证服务包信息中此项“服务类别”是否为有效服务；如不是，证明该用户端设备无权限使用此项应用或服务，返回错误信息，结束；如是，认证机制判断在硬件的服务包信息中该“服务类别”是否过期；若过期，证明该用户端设备无权限使用此项应用或服务，返回错误信息，结束；如未过期，认证机制分析认证文件，验证此项应用或服务对硬件信息的访问权限；读取认证文件中的“有效时间”，判断认证文件是否过期；若过期，返回错误信息，结束；如未过期，读取认证文件中的“保密串”，判断使用者身份是否合法；若不合法，返回错误信息，结束；如合法，则用户端设备获得该应用或服务。

18、根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：用户端设备内设置安全机制，通过加密算法实现设备加密数据空间的保护。

19、根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：用户端设备内还设有身份信息和/或类型识别信息。

20、根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服

务间鉴权的方法，其特征在于：所述认证机制进行鉴权包括由用户端设备对应用或服务进行，即用户端设备认证应用或服务是否有使用权限。

21、根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：用户端设备内设有安全数据存储区，设置安全机制，包括内建的密钥表，用于加解密安全加密数据存储区的数据。

22、根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务认证文件包括设备安全数据存储区访问的权限，有效数据区域名称或区域大小，用于限定该应用或服务只能够访问对应的数据存储区。

23、根据权利要求 1 所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：应用或服务认证文件包括设备使用方法，用于制定对于安全数据存储区的访问方式，获取相应的密钥，实现数据加解密。

24、根据权利要求 20 至 23 任一所述的用户端设备与本地客户端应用/远程网络服务间鉴权的方法，其特征在于：用户端设备对于应用或服务进行，即用户端设备认证应用或服务是否有使用权限时，认证机制读取认证文件中的“有效区域名称”，判断使用者希望访问的空间与有效访问空间是否一致；如不一致，返回错误信息，结束；如一致，读取认证文件中的“有效区域大小”，判断访问空间是否溢出；如溢出，返回错误信息，结束；如不溢出，此项应用或服务有权限访问它想要访问的用户端设备信息；读取认证文件中的“使用方法”，取得讲演使用的密钥 ID，通过安全机制接口访问用户端设备上的信息。

用户端设备与本地客户端应用或远程网络服务间鉴权的方法

技术领域

本发明涉及计算机技术领域，具体地说，涉及用户端设备与本地客户端应用或远程网络服务间鉴权的方法，尤其是在用户端基于软硬件结合方式实现的与客户端应用服务间鉴权的方法。

背景技术

应用软件和网络服务的不断发展，必将导致用户和应用服务之间的信息交互。这种信息交互不可能是无约束的，必须是在安全机制之下进行。一方面，需要知道哪些用户有权使用哪些应用或服务；另一方面，用户也需要知道哪些应用或服务可以访问用户的哪部分个人信息。

对于信息交互过程中，用户和应用服务双方之间的鉴权和认证，已经有一些方法来实现，但这些方法都存在自身的缺陷。例如软加密的技术，是不依靠特别硬件实现的对软件的保护技术，主要有密码法、计算机硬件校验法、钥匙盘法，这类方法的缺陷是加密方法比较容易被破解，另外其验证条件是固定不变的，一旦被破解，将迅速蔓延。目前基于软件发行和网络服务应用的需求，不得不广泛地采取该项技术，但是该加密鉴权方法常常出现尴尬的局面，难以实现诸如版权保护等目的。对于特定的应用，还可以采用硬加密技术，例如硬件加密狗，这种方式的缺点是：一个硬件只能针对一个应用服务进行保护，并且被限制在某一固定的本地终端或远程服务器上使用。这样过于“固定”的硬加密方式，虽然安全性较高，但是灵活性、普适性以及移动性较差，远远不能满足实际情况中被授权用户对于不同应用、不同本地终端或远程服务的通用授权和移动使用的要求。

发明内容

本发明的目的在于提供一种用户端设备与本地客户端应用或远程网络

服务间鉴权的方法，实现用户对授权的客户端应用使用权限的认证，以及用户对网络服务的使用权限的认证。

本发明的再一目的在于提供一种用户端设备与本地客户端应用或远程网络服务间鉴权的方法，实现客户端应用或网络服务对用户的访问权限的认证。

本发明的另一目的在于提供一种用户端设备与本地客户端应用或远程网络服务间鉴权的方法，可以由同一个硬件设备完成用户与多个客户端应用或网络服务之间的认证。

本发明的又一目的在于提供一种用户端设备与本地客户端应用或远程网络服务间鉴权的方法，用户端设备与本地客户端应用或远程网络服务可根据需要动态地更改、控制认证条件，灵活地保障数据安全。

为此，本发明通过如下技术方案实现上述目的：在用户端设备内设置认证信息以及安全机制接口，在应用或服务内设置与所述认证信息匹配的认证文件和访问安全机制接口的路径；安全机制接口为两者通信的特定协议，当用户需求某应用或服务时，通过用户端设备与应用或服务之间设置的安全机制接口，将两者的认证文件交认证机制进行鉴权，鉴权通过的用户端设备可获得软件应用或服务；没有通过的，则拒绝该用户。

本发明通过带有安全机制的硬件设备存储、管理用户和客户端应用或网络服务所需的交互信息，实现信息安全存放、信息管理以及信息安全交互，从而衍生出：硬件设备识别、用户身份验证、用户权限管理、用户数据共享、安全数据存放及管理、软件版权保护、定制应用服务等一系列功能。

附图说明

图 1 为本发明认证体系的结构示意图；

图 2 为本发明认证内容的流程示意图；

图 3 为本发明鉴权和访问的流程图。

具体实施方式

下面根据附图和实施例，对本发明的技术方案做进一步的详细描述。

参见图 1，本发明为一种硬件和软件相结合的用户与客户端应用或网络服务之间的鉴权机制。通过硬件设备内建立的安全机制、授权客户端应用或网络服务的认证文件(AKF)、遵循的安全机制接口、对硬件设备和软件应用服务之间进行鉴权的认证体系，可以实现用户与客户端应用或网络服务之间的鉴权，实现信息安全存放、信息管理以及信息安全交互，从而衍生出：硬件设备识别、用户身份验证、用户权限管理、用户数据共享、安全数据存放及管理、软件版权保护、定制应用服务等一系列功能。

如图 2 所示，本发明的方法包含 3 方面的内容:

第一、具有安全机制的硬件设备。这个设备具有安全的加密数据空间、加密及认证的算法、自身的认证信息和特性信息。这个设备可具体表现为不同的电子产品，如：USB 闪存、键盘读取设备、MP3 读取设备、PDA 读取设备、STB 读取设备、磁盘读取设备、智能 PDA 读取设备、数据银行、电子图书、多功能无线设备 E-phone、数码相机、录音笔等。

第二、遵循安全机制接口的应用或服务。这些应用和服务都具有认证文件，并且通过既定的安全机制接口访问硬件设备。

第三、认证体系。认证体系完成鉴权的过程，用于硬件设备和应用服务双方进行合法性和权限的互相认证。认证体系可以由硬件设备的 IC 实现，也可以由软件方式实现，也可以是二者的结合。

当应用或服务需要访问硬件设备时，其简要过程如下:

应用或服务发送访问请求，同时将认证文件提交到认证体系;

认证体系获取应用或服务的认证文件，同时获取硬件设备自身的认证信息和特性信息;

认证体系认证该硬件设备是否有权使用该应用或服务，如无权，返回错

误信息，终止访问；否则，继续；

认证体系认证该应用或服务是否有权访问该硬件设备，如无权，返回错误信息，终止访问；否则，继续；

认证体系对该应用或服务对该硬件设备的有效访问信息（有效空间、大小等等）进行认证；

认证通过后，该应用或服务通过既定的安全机制接口访问硬件设备。

又参见图 3，本发明用户硬件设备具有安全机制结构和特点。硬件设备芯片具有该设备的特性信息，包括唯一的设备 ID 号和设备类型的标示。硬件设备包括 MP3，PDA 数据银行，数码相机，录音笔等类型，每一种类型又细分为不同的型号、不同的厂商，具有相同型号、相同厂商的移动存储设备为同一类别。在用户硬件设备内建有加、解密的密钥表，用于对安全加密数据区存储的信息进行加、解密，还具有执行信息加解密的功能模块。对于信息进行加密解密，可利用软件或者硬件独立或者结合的方式实现。上述加密解密算法可以是符合条件的任何算法，例如 DES 算法、RSA 算法，并且用户硬件设备还具有一组命令集，用于实现硬件设备和应用或服务之间的认证过程。

用户硬件设备内设有一定容量的安全加密数据区。在该数据区内，存有该硬件设备的认证信息，这些信息是一个服务包的集合，每一个服务包的内容包括：有效标志，用于标志此类服务是否被开启，通过标示该硬件设备可以接受哪些类别的认证文件，就标示了该硬件设备可以使用哪些类别的应用或服务；有效时间，用于标志此类服务的有效截至时间。

如果要访问安全加密数据区中的数据，必须通过证书认证，而且只能通过安全机制接口进行访问。

本发明另一方面，授权的应用或服务可以是客户端应用，也可以是远端的网络服务应用，该本地客户端或远程网络可以调用安全机制接口，并具有认证文件。该认证文件在授权时颁发，每一个被授权的应用或服务都具有自

己的认证文件。该认证文件包括：认证文件版本，用于记录认证文件的版本信息；有效区域名称，用于标示授权的应用或服务在硬件设备安全加密数据区中可以访问的区域；有效区域长度，用于标示授权的应用或服务在硬件设备安全加密数据区中可以访问的区域的长度。上述认证文件还包括保密串，用于验证证书拥有者的合法性；有效期限，用于限定该证书的有效时间；服务类别，用于标示该认证文件对应的服务类型；使用方法，用于制定对有效区域的访问方式，如使用哪一把密钥进行加解密；认证文件删除，用于删除该认证文件。

本发明的认证体系从硬件设备处取得硬件的认证信息，从授权的应用或服务处取得认证文件，作为进行鉴权认证的依据。认证体系可利用硬件设备IC所带的认证机制算法和/或软件实现的认证机制算法对硬件认证信息和认证文件进行认证。

具体地，本发明的步骤为：

首先，为每一个硬件设备设定认证信息，也就是服务包信息。每一个硬件设备在出厂时都进行认证信息的设定，认证信息还可以通过软件或网络远程控制的方式进行修改。

其次，为每一个授权的服务或应用生成特定的AKF认证文件，通过颁发渠道交付给使用者。AKF认证文件具有有效期限，需定期更换。

当授权的服务或应用要访问硬件设备信息时，发出访问请求，同时将AKF文件提交到认证体系。此时由认证体系读取硬件的认证信息，也就是服务包信息。

认证体系首先验证该硬件设备是否有权限使用此项应用或服务，即该硬件设备的用户是否有权限使用此项应用或服务。具体是：认证体系读取AKF认证文件中的“服务类别”，判断在硬件的认证服务包信息中此项“服务类别”是否为有效服务。如不是，证明该硬件设备无权限使用此项应用或服务，返回错误信息，结束；如是，继续。认证体系判断硬件的服务包信息中该“服

务类别”是否过期。若过期， 证明该硬件设备无权限使用此项应用或服务，返回错误信息，结束；如未过期，继续。

然后认证体系分析 AKF 认证文件，验证此项应用或服务对硬件设备信息的访问权限。具体是：认证体系读取 AKF 文件中的“有效时间”，判断 AKF 文件是否过期，若过期，返回错误信息，结束；如未过期，继续。读取 AKF 文件中的“保密串”，判断使用者身份是否合法，如不合法，返回错误信息，结束；如合法，则继续。读取 AKF 文件中的“有效区域名称”，判断使用者希望访问的空间与有效访问空间是否一致，如不一致，返回错误信息，结束；如一致，继续。读取 AKF 文件中的“有效区域大小”，判断访问空间是否溢出，如溢出，返回错误信息，结束；如不溢出，则表明此项应用或服务有权限访问它想要访问的硬件设备信息。最后读取 AKF 文件中的“使用方法”，取得讲演使用的密钥 ID，并通过安全机制接口访问硬件设备上的信息。

采用本发明，实现双向认证的过程如下：

认证体系从硬件设备处取得硬件认证信息，从授权的应用或服务处取得认证文件，作为认证的依据。

其中，用户设备硬件认证信息是一个服务包的集合，标志了该硬件设备对授权的应用或服务的使用权限。对硬件认证信息的认证，也就是对硬件设备设备权限的认证。

认证文件则标志了授权的应用或服务对硬件设备的使用权限。对认证文件的认证，也就是对授权的应用或服务的权限的认证。

采用本发明实现一个硬件设备和多个服务应用之间的认证时，用户设备硬件认证信息是一个服务包的集合，包含了多个服务包，每一个服务包可以标志该硬件设备对某一类授权的应用或服务的使用权限，所以通过硬件认证信息即可验证该硬件设备和多个服务应用之间的认证。

本发明实现动态控制认证的条件是：用户设备硬件认证信息是可以通过软件或网络远程控制的方式进行修改的；同时 AKF 认证文件是可以更换的。

所以双方的认证条件都是可以动态控制的。

最后所应说明的是，以上实施例仅用以说明本发明的技术方案而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或者等同替换，而不脱离本发明技术方案的精神和范围，其均应涵盖在本发明的权利要求范围当中。

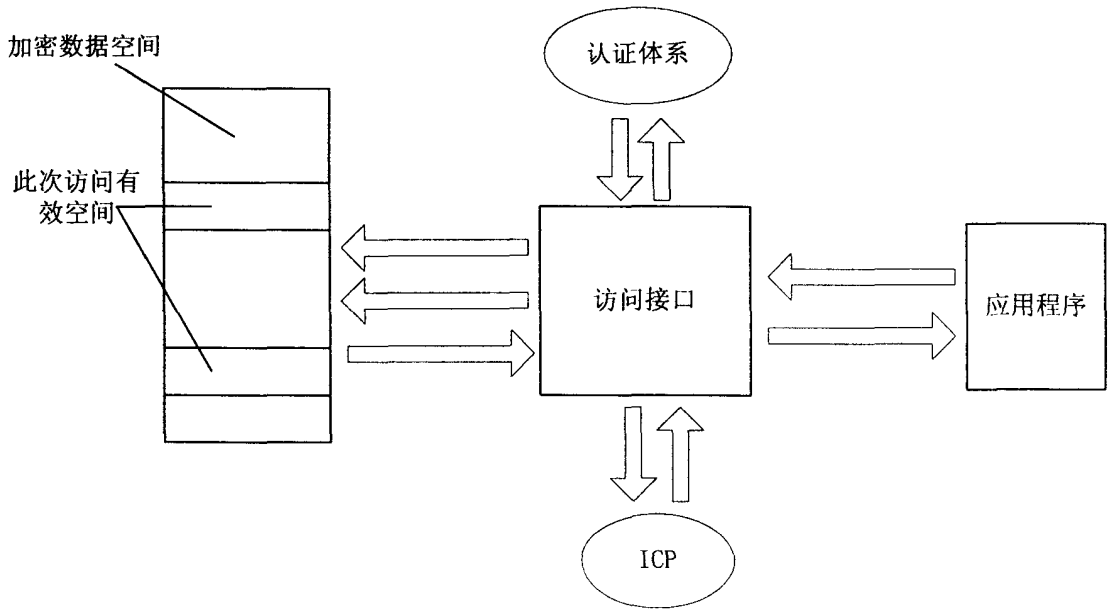

加密数据空间
此次访问有效空间
认证体系
访问接口
应用程序
ICP

图 1

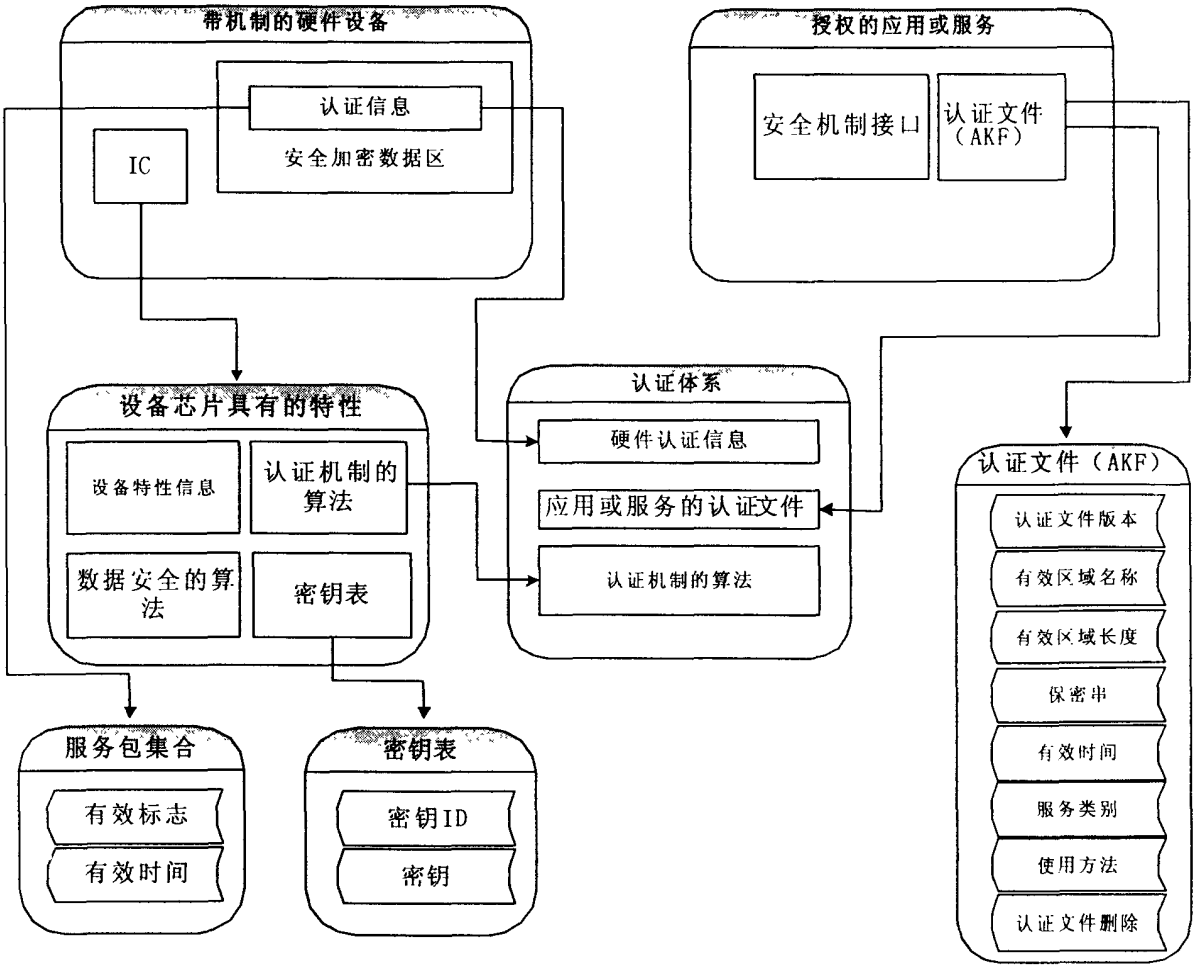

带机制的硬件设备
认证信息
安全加密数据区
IC
授权的应用或服务
安全机制接口
认证文件（AKF）
设备芯片具有的特性
设备特性信息
认证机制的算法
数据安全的算法
密钥表
认证体系
硬件认证信息
应用或服务的认证文件
认证机制的算法
认证文件（AKF）
认证文件版本
有效区域名称
有效区域长度
保密串
有效时间
服务类别
使用方法
认证文件删除
服务包集合
有效标志
有效时间
密钥表
密钥ID
密钥

图 2

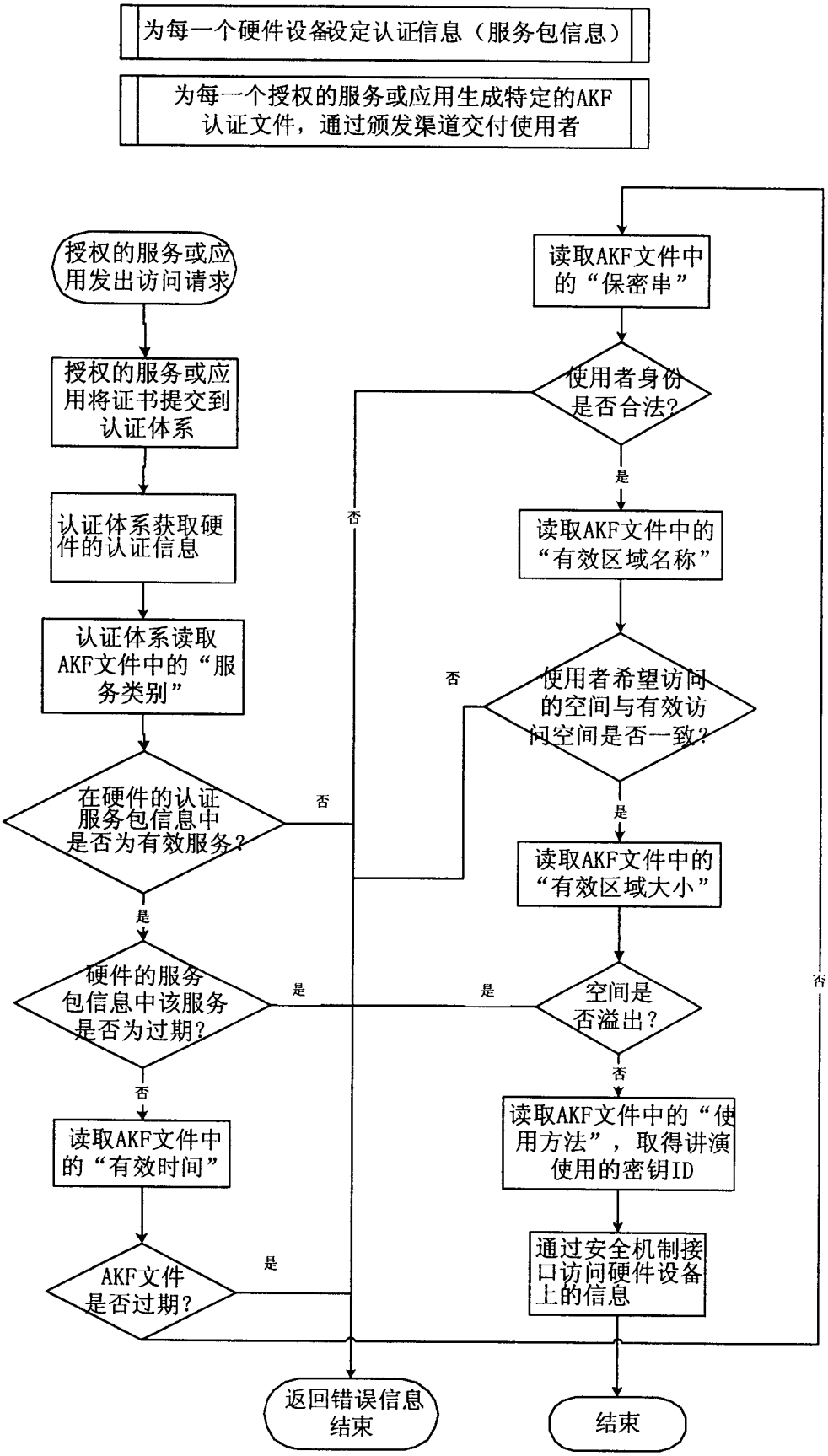

为每一个硬件设备设定认证信息（服务包信息）
为每一个授权的服务或应用生成特定的AKF认证文件，通过颁发渠道交付使用者
授权的服务或应用发出访问请求
授权的服务或应用将证书提交到认证体系
认证体系获取硬件的认证信息
认证体系读取AKF文件中的“服务类别”
在硬件的认证服务包信息中是否为有效服务?
否
是
硬件的服务包信息中该服务是否为过期?
是
否
读取AKF文件中的“有效时间”
AKF文件是否过期?
是
返回错误信息结束
读取AKF文件中的“保密串”
使用者身份是否合法?
否
是
读取AKF文件中的“有效区域名称”
使用者希望访问的空间与有效访问空间是否一致?
否
是
读取AKF文件中的“有效区域大小”
空间是否溢出?
是
否
读取AKF文件中的“使用方法”，取得讲演使用的密钥ID
通过安全机制接口访问硬件设备上的信息
否
结束

图 3