(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 102281143 B
(45)授权公告日 2015.04.01

(21)申请号 201110253400.X

(22)申请日 2011.08.30

(73)专利权人 公安部第三研究所
地址 200031 上海市徐汇区岳阳路76号

(72)发明人 王兴 胡善学 杭强伟 张勇 胥怡心

(74)专利代理机构 上海天翔知识产权代理有限公司 31224
代理人 刘粉宝

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 1901443 A,2007.01.24,
EP 1463351 A1,2004.09.29,
CN 101645124 A,2010.02.10,
CN 101917691 A,2010.12.15,
CN 101996446 A,2011.03.30,
CN 102083058 A,2011.06.01,

审查员 莫伟

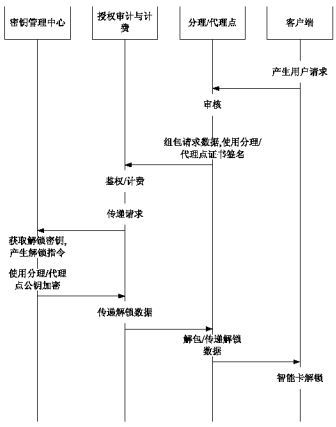
权利要求书2页 说明书5页 附图2页

(54)发明名称

智能卡远程解锁系统

(57)摘要

本发明公开了智能卡远程解锁系统及解锁方法，该解锁系统中客户端用于产生智能卡解锁请求，提交身份校验数据，接收解锁指令并执行智能卡解锁操作；分理/代理单元与客户端进行数据传输，用于审核客户端提交的身份校验数据和相应的智能卡解锁请求；授权审计与计费单元与分理/代理单元进行数据传输，用于校验来自分理/代理单元的解锁请求；密钥管理单元与授权审计与计费单元进行数据传输，用于管理解锁密钥。解锁时解锁请求由智能卡产生，经各级分理/代理点传递至授权中心，授权中心的解锁应答亦由各级分理/代理点传回卡片；解锁指令加密传输。本发明可有效降低传统智能卡解锁模式和方法中存在的密钥泄露、失控等安全隐患。



CN 102281143 B

1. 智能卡远程解锁系统，其特征在于，所述系统包括：

客户端，用于产生智能卡解锁请求，提交身份校验数据，接收解锁指令并执行智能卡解锁操作；

分理 / 代理单元，与客户端进行数据传输，用于审核客户端提交的身份校验数据和相应的智能卡解锁请求；

授权审计与计费单元，与分理 / 代理单元进行数据传输，用于校验来自分理 / 代理单元的解锁请求，并通过设定规则进行审计和计费；

密钥管理单元，与授权审计与计费单元进行数据传输，用于管理解锁密钥，并使相应解锁密钥可备份、可恢复和不可明文导出；

由此形成授权中心 - 分理 / 代理点 - 用户的多级可扩展模式，一次一密、全程加密传递解锁指令序列；集中管理解锁核心密钥，统一解锁操作入口；

所述解锁系统的工作过程如下：

(1) 用户通过客户端产生智能卡解锁请求，并提交相应的身份校验数据，将智能卡解锁请求和身份校验数据签名后传至分理 / 代理单元；所述智能卡解锁请求的基本信息数据包主要包含：待解锁智能卡的序列号、智能卡卡片软硬件版本以及智能卡内产生的随机数；

(2) 分理 / 代理单元验证客户端提供的数据，并根据自定规则审核用户身份，检查客户端提交的解锁请求数据包的完整性，并附加自身身份标示信息，重新封装解锁请求数据包并签名并传至授权审计与计费单元，其形成的数据结构主要包含：分理 / 代理点标示、操作人员身份标示、解锁请求基本信息数据、数字签名；

(3) 授权审计与计费单元验证分理 / 代理单元提交请求数据的合法性，在验证通过后，解析出卡片序列号、卡片软硬件版本和卡内产生随机数，形成密码服务请求数据，对相应的请求数据进行签名发送至密钥管理单元，并对相应的解锁请求进行审计和计费；所述密码服务请求数据包含：操作类型、卡内产生的随机数、接收端加密公钥；

(4) 密钥管理单元验证授权审计与计费单元提交的请求数据的合法性，相应解锁请求，获取解锁密钥产生一次一密解锁指令，形成密码服务响应数据，并加密后传至授权审计与计费单元；所述密码服务响应数据包含：使用接收端公钥加密、一次一密解锁指令以及数字签名；

(5) 授权审计与计费单元在解密并验证签名后将解锁指令再次签名加密后传至分理 / 代理单元；

(6) 分理 / 代理单元在解密并验证签名后，解包解锁指令，并对其签名加密后传至客户端；

(7) 客户端在解密并验证签名后获取相应的解锁指令，并根据解锁指令对智能卡进行解锁。

2. 根据权利要求 1 所述的智能卡远程解锁系统，其特征在于，所述分理 / 代理单元由多级的上级分理 / 代理点和下级分理 / 代理点组成，所述下级分理 / 代理点与客户端和上级分理 / 代理点之间进行数据传输，所述下级分理 / 代理点用于审核客户端提交的身份校验数据和相应的智能卡解锁请求，所述上级分理 / 代理点用于审核下级分理 / 代理点提交的身份校验数据和相应的智能卡解锁请求。

3. 根据权利要求 1 所述的智能卡远程解锁系统，其特征在于，所述系统中的分理 / 代理

单元、授权审计与计费单元、密钥管理单元之间进行数据传输之前还包括相互身份鉴别步骤。

智能卡远程解锁系统

技术领域

[0001] 本发明涉及一种智能卡技术，具体涉及一种智能卡远程解锁系统以及与该系统相配合的解锁方法。

背景技术

[0002] 智能卡的芯片操作系统在设计之时，均会为敏感操作提供身份鉴别机制，以防卡片被误用或是敏感信息泄露。通常做法是要求持卡人在敏感操作之前输入 PIN 码，卡片内校验通过之后才允许敏感操作执行。如果不通过，持卡人尝试次数是受到限制的，以防穷举破解。那么重试次数超过限制之后，卡片会进入锁定状态，不再允许尝试。

[0003] 当卡片遵循安全机制设定进入锁定状态时，需要专用解锁指令进行解锁。在卡片生产或发行时，会预共享一段密钥，用于解除 PIN 码锁定。常见的 PIN 码解锁装置、程序等会根据此密钥产生解锁指令，当需要时传入卡内进行卡片解锁。但是这种做法存在巨大的安全隐患：

[0004] 1) 卡片解锁不可控。同批次同类型卡片可以使用专用解锁工具任意解锁，无法控制和限制使用范围。

[0005] 2) 解锁操作不可审计，不可追踪。由于缺乏紧密结合的有效管理手段，无法统计卡片解锁操作，也无法认定执行卡片解锁操作的个人。

[0006] 3) 解锁密钥泄露风险增大。解锁工具内置预共享解锁密钥，一旦被反编译或是破解，该密钥泄露的概率极高。

[0007] 采用专用设备、专人定点为持卡人解锁，可以提高安全性，但是操作极不方便，增加了持卡人的用卡成本。

[0008] 由此，如何提高智能卡解锁的可操行和安全性，是本领域亟需解决的技术问题。

发明内容

[0009] 本发明针对现有技术存在的缺陷，提供了一种智能卡远程解锁系统，该系统采用授权中心 - 分理 / 代理点 - 用户多级可扩展的安全解锁模式，既提高了安全性，又保证解锁服务广泛可达、易于获取。

[0010] 为了达到上述目的，本发明采用如下的技术方案：

[0011] 智能卡远程解锁系统，所述系统包括：

[0012] 客户端，用于产生智能卡解锁请求，提交身份校验数据，接收解锁指令并执行智能卡解锁操作；

[0013] 分理 / 代理单元，与客户端进行数据传输，用于审核客户端提交的身份校验数据和相应的智能卡解锁请求；

[0014] 授权审计与计费单元，与分理 / 代理单元进行数据传输，用于校验来自分理 / 代理单元的解锁请求，并通过设定规则进行审计和计费；

[0015] 密钥管理单元，与授权审计与计费单元进行数据传输，用于管理解锁密钥，并使相

应解锁密钥可备份、可恢复和不可明文导出。

[0016] 进一步的，所述分理 / 代理单元由多级的上级分理 / 代理点和下级分理 / 代理点组成，所述下级分理 / 代理点与客户端和上级分理 / 代理点之间进行数据传输，所述下级分理 / 代理点用于审核客户端提交的身份校验数据和相应的智能卡解锁请求，所述上级分理 / 代理点用于审核下级分理 / 代理点提交的身份校验数据和相应的智能卡解锁请求。

[0017] 再进一步的，所述数据传输采用一次一密模式。

[0018] 基于上述解锁系统，本发明还提供一种智能卡远程解锁方法，该方法包括如下步骤：

[0019] (1) 用户通过客户端产生智能卡解锁请求，并提交相应的身份校验数据，将智能卡解锁请求和身份校验数据签名后传至分理 / 代理单元；

[0020] (2) 分理 / 代理单元验证客户端提供的数据，并根据身份校验数据鉴别智能卡持有者身份，审核智能卡解锁请求，在审核通过后对其进行签名并传至授权审计与计费单元；

[0021] (3) 授权审计与计费单元验证分理 / 代理单元提交请求数据的合法性，在验证通过后对相应的请求数据进行签名发送至密钥管理单元，并对相应的解锁请求进行审计和计费；

[0022] (4) 密钥管理单元验证授权审计与计费单元提交的请求数据的合法性，相应解锁请求，获取解锁密钥产生解锁指令，并对解锁指令进行签名加密后传至授权审计与计费单元；

[0023] (5) 授权审计与计费单元在解密并验证签名后将解锁指令再次签名加密后传至分理 / 代理单元；

[0024] (6) 分理 / 代理单元在解密并验证签名后，解包解锁指令，并对其签名加密后传至客户端；

[0025] (7) 客户端在解密并验证签名后获取相应的解锁指令，并根据解锁指令对智能卡进行解锁。

[0026] 进一步的，在上述各个单元之间进行数据传输之前还包括相互身份鉴别步骤。

[0027] 根据上述方案形成的本发明与现有技术相比具有以下优势：

[0028] (1) 采用授权中心 - 分理 / 代理点 - 用户的多级可扩展模式，一次一密、全程加密传递解锁指令序列；集中管理解锁核心密钥，统一解锁操作入口，可有效降低传统智能卡解锁模式和方法中存在的密钥泄露、失控等安全隐患；

[0029] (2) 解锁操作可控、人员操作可追踪、总体使用情况可审计；

[0030] (3) 部署灵活易于扩展等。

附图说明

[0031] 以下结合附图和具体实施方式来进一步说明本发明。

[0032] 图 1 为本发明的系统框图；

[0033] 图 2 为本发明解锁的原理图；

[0034] 图 3 为本发明中解锁请求基本信息数据结构示意图；

[0035] 图 4 为本发明中解锁请求数据结构示意图；

[0036] 图 5 为本发明中密码服务请求数据结构示意图；

[0037] 图 6 为本发明中密码服务响应数据结构示意图。

具体实施方式

[0038] 为了使本发明实现的技术手段、创作特征、达成目的与功效易于明白了解，下面结合具体图示，进一步阐述本发明。

[0039] 参见图 1，本发明提供的智能卡远程解锁系统，整个解锁系统包括客户端 100、分理 / 代理单元 200、授权审计与计费单元 300 以及密钥管理单元 400。

[0040] 其中，客户端 100 用于产生智能卡解锁请求，提交身份校验数据，接收解锁指令并执行智能卡解锁操作。

[0041] 分理 / 代理单元 200 与客户端 100 进行数据传输，主要用于审核客户端提交的身份校验数据和相应的智能卡解锁请求。分理 / 代理单元 200 与客户端 100 之间的数据传输采用数字签名进行安全保护。

[0042] 同时分理 / 代理单元 200 由多级的上级分理 / 代理点 201 和下级分理 / 代理点 202 组成，下级分理 / 代理点 202 与客户端 100 和上级分理 / 代理点 201 之间进行数据传输。其中下级分理 / 代理点 202 用于审核客户端提交的身份校验数据和相应的智能卡解锁请求，上级分理 / 代理点 201 用于审核下级分理 / 代理点提交的身份校验数据和相应的智能卡解锁请求。

[0043] 授权审计与计费单元 300 与分理 / 代理单元 200 进行数据传输，并采用数字签名进行安全保护。其主要用于校验来自分理 / 代理单元的解锁请求，并通过设定规则进行审计和计费。

[0044] 密钥管理单元 400 与授权审计与计费单元 300 进行数据传输，并采用数字签名进行安全保护。其主要用于管理解锁密钥，并使相应解锁密钥可备份、可恢复和不可明文导出。

[0045] 上述方案形成的解锁系统采用授权中心 - 分理 / 代理点 - 用户的多级可扩展模式，由密钥管理单元集中管理解锁核心密钥，统一解锁服务入口，具有极高的安全性。

[0046] 再者，各个单元之间均采用全程加密传输模式所有数据请求与回应均有数字证书签名保护，进一步提高其数据传输的安全性。

[0047] 基于上述解锁系统，进行智能卡远程解锁方法具体包括如下步骤（参见图 2）：

[0048] (1) 用户通过客户端产生智能卡解锁请求，并提交相应的身份校验数据，将智能卡解锁请求和身份校验数据签名后传至分理 / 代理单元；

[0049] (2) 分理 / 代理单元验证客户端提供的数据，并根据身份校验数据鉴别智 能卡持有者身份，审核智能卡解锁请求，在审核通过后对其进行签名并传至授权审计与计费单元；

[0050] (3) 授权审计与计费单元验证分理 / 代理单元提交请求数据的合法性，在验证通过后对相应的请求数据进行签名发送至密钥管理单元，并对相应的解锁请求进行审计和计费；

[0051] (4) 密钥管理单元验证授权审计与计费单元提交的请求数据的合法性，相应解锁请求，获取解锁密钥产生解锁指令，并对解锁指令进行签名加密后传至授权审计与计费单

元；

[0052] (5) 授权审计与计费单元在解密并验证签名后将解锁指令再次签名加密后传至分理 / 代理单元；

[0053] (6) 分理 / 代理单元在解密并验证签名后，解包解锁指令，并对其签名加密后传至客户端；

[0054] (7) 客户端在解密并验证签名后获取相应的解锁指令，并根据解锁指令对智能卡进行解锁。

[0055] 在上述步骤中，在客户端与分理 / 代理单元之间、分理 / 代理单元与授权审计与计费单元之间以及授权审计与计费单元与密钥管理单元之间进行数据传输之前可进行相互身份鉴别的操作，具体方法可以采用多种方法，只要能够达到识别传输数据双方的身份即可。

[0056] 基于上述方案，本发明实现远程解锁操作的流程如下：

[0057] 1) 持卡客户端产生用户请求

[0058] 客户端根据持卡用户的要求产生包含相应基本信息的解锁请求数据包，并将相应的解锁请求数据包进行提交。

[0059] 参见图 3，客户端产生的解锁请求基本信息数据包主要包含：待解锁智能卡的序列号、智能卡卡片软硬件版本以及智能卡内产生的随机数。

[0060] 2) 分理 / 代理点鉴别用户请求数据，重新组包、传递请求

[0061] 分理 / 代理点根据自定规则审核用户身份，检查客户端提交的解锁请求数据包的完整性，并附加自身身份标示信息，重新封装解锁请求数据包并签名。如图 4 所示，其形成的数据结构主要包含：分理 / 代理点标示、操作人员身份标示、解锁请求基本信息数据、数字签名。

[0062] 3) 授权中心（即授权审计与计费单元）鉴别请求数据，发送密钥服务请求至密钥管理中心（即密钥管理单元）

[0063] 授权中心校验分理 / 代理点请求合法性，解析出卡片序列号、卡片软硬件版本和卡内产生随机数等基本信息数据，形成密码服务请求数据，并发送到密钥管理中心。

[0064] 参见图 5，密码服务请求数据主要包含：操作类型、卡内产生的随机数、接收端加密公钥。

[0065] 4) 密钥管理中心（即密钥管理单元）响应密码服务请求，产生一次一密解锁指令，形成密码服务响应数据，并加密传回。

[0066] 参见图 6，密码服务响应数据主要包含：使用接收端公钥加密、一次一密解锁指令以及数字签名。

[0067] 5) 授权中心回传响应数据。

[0068] 6) 代理 / 分理点解包数据，发送解锁指令至客户端。

[0069] 7) 客户端发送解锁指令到卡片，完成解锁。

[0070] 以上显示和描述了本发明的基本原理、主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的只是说明本发明的原理，在不脱离本发明精神和范围的前提下，本发明还会有各种变化和改进，这些变化和改进都落入要求保护的本发明范围内。本发明要求保护范围由所附的权利要求书及其

等效物界定。


400
300
200
100
密钥管理单元
授权审计与计费单元
分理/代理单元
客户端

图 1

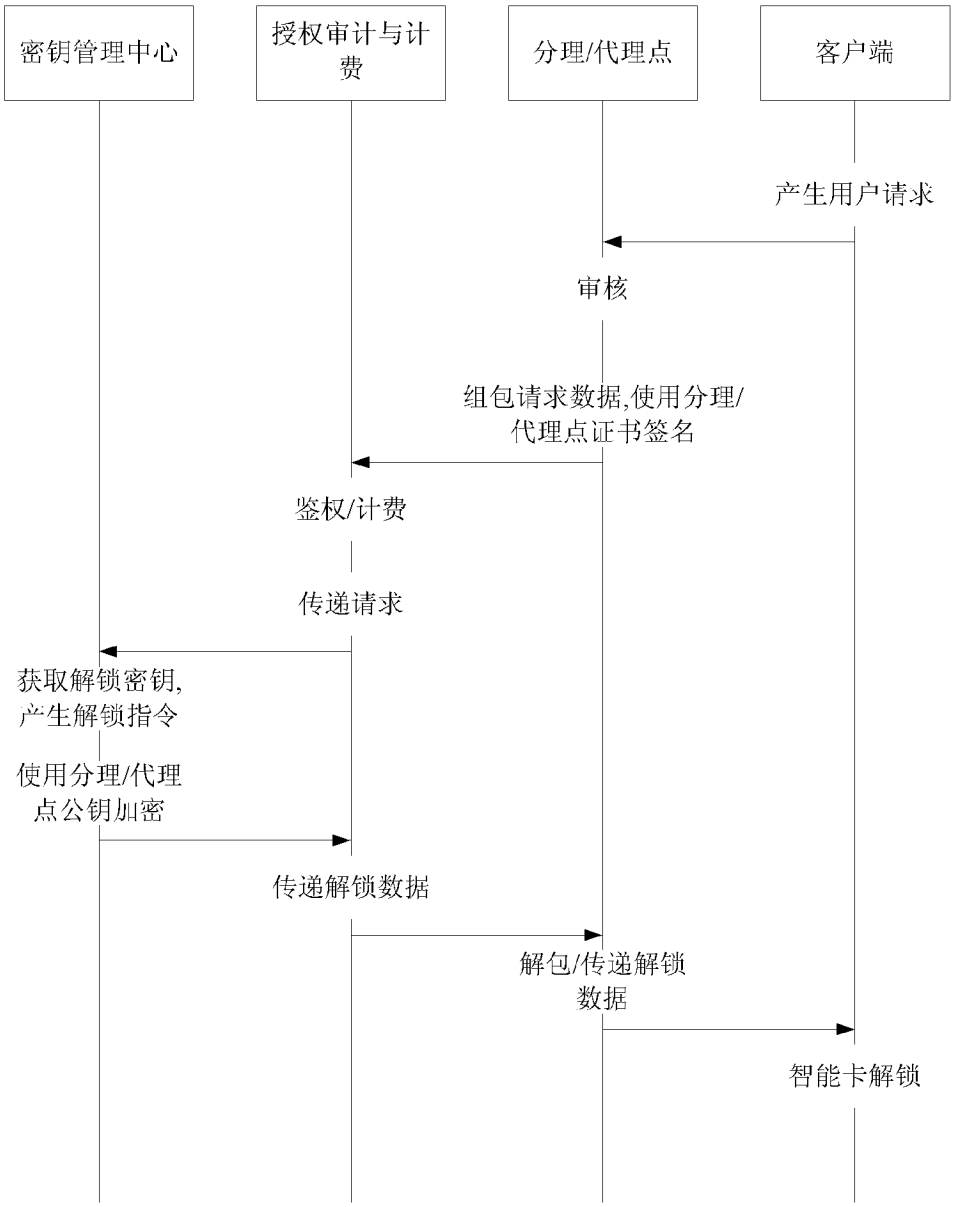

密钥管理中心
授权审计与计费
分理/代理点
客户端
产生用户请求
审核
组包请求数据,使用分理/代理点证书签名
鉴权/计费
传递请求
获取解锁密钥,产生解锁指令
使用分理/代理点公钥加密
传递解锁数据
解包/传递解锁数据
智能卡解锁

图 2

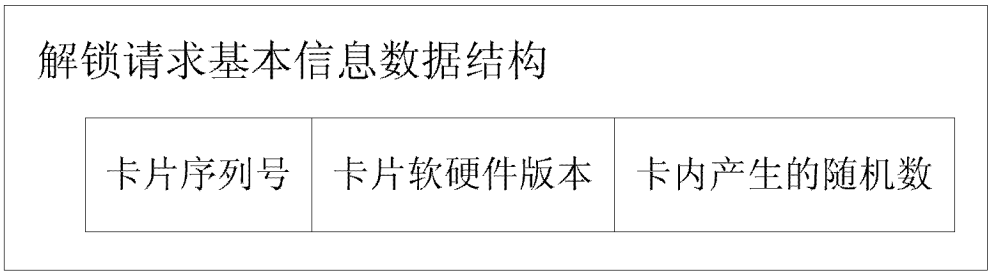

解锁请求基本信息数据结构
卡片序列号
卡片软硬件版本
卡内产生的随机数

图 3

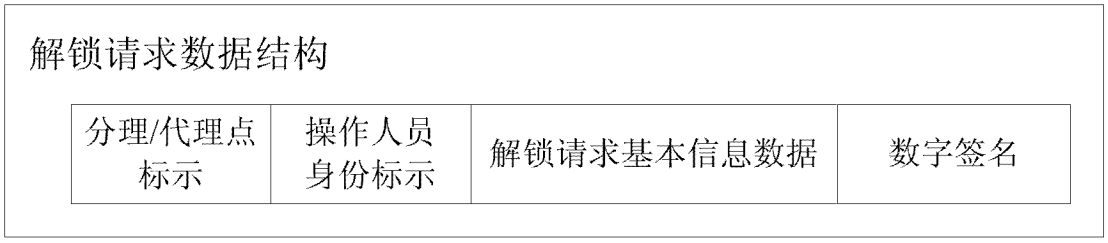

解锁请求数据结构
分理/代理点标示
操作人员身份标示
解锁请求基本信息数据
数字签名

图 4

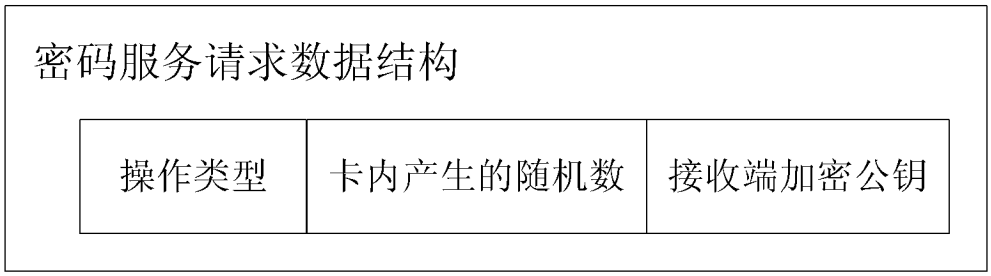

密码服务请求数据结构
操作类型
卡内产生的随机数
接收端加密公钥

图 5

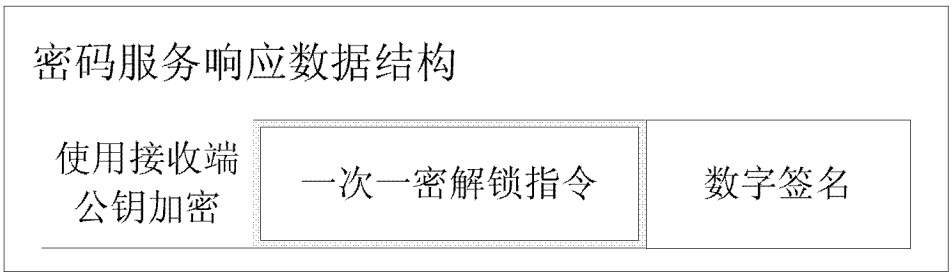

密码服务响应数据结构
使用接收端公钥加密
一次一密解锁指令
数字签名

图 6