(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 106027473 B
(45)授权公告日 2019.05.21

(21)申请号 201610041669.4

(22)申请日 2016.01.21

(65)同一申请的已公布的文献号
申请公布号 CN 106027473 A

(43)申请公布日 2016.10.12

(73)专利权人 李明
地址 100086 北京市海淀区太月园12号楼603室

(72)发明人 李明

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/31(2013.01)

审查员 周天豪

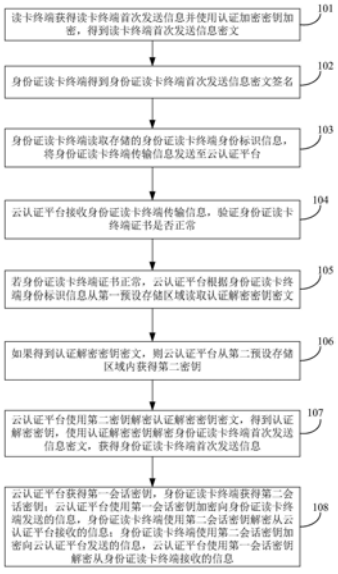
权利要求书4页 说明书23页 附图2页

(54)发明名称

身份证读卡终端与云认证平台数据传输方法和系统

(57)摘要

本发明提供一种身份证读卡终端与云认证平台数据传输方法和系统，包括：身份证读卡终端获得身份证读卡终端首次发送信息，使用认证加密密钥加密得到身份证读卡终端首次发送信息密文；对身份证读卡终端首次发送信息密文进行签名得到身份证读卡终端首次发送信息密文签名，将身份证读卡终端传输信息发送至云认证平台；云认证平台验证身份证读卡终端证书是否正常；若正常根据身份证读卡终端身份标识信息读取认证解密密钥密文并获得第二密钥，使用第二密钥解密认证解密密钥密文得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文获得身份证读卡终端首次发送信息；云认证平台获得第一会话密钥，身份证读卡终端获得第二会话密钥。



CN 106027473 B

1.一种身份证读卡终端与云认证平台数据传输方法,其特征在于,包括:

身份证读卡终端获得身份证读卡终端首次发送信息和认证加密密钥,使用所述认证加密密钥加密所述身份证读卡终端首次发送信息,得到身份证读卡终端首次发送信息密文;

所述身份证读卡终端对所述身份证读卡终端首次发送信息密文进行散列计算,得到身份证读卡终端首次发送信息密文摘要,并调用所述身份证读卡终端的身份证读卡终端私钥加密所述身份证读卡终端首次发送信息密文的摘要,得到身份证读卡终端首次发送信息密文签名;

所述身份证读卡终端读取存储的身份证读卡终端身份标识信息,将身份证读卡终端传输信息发送至所述云认证平台,所述身份证读卡终端传输信息至少包括所述身份证读卡终端身份标识信息、所述身份证读卡终端首次发送信息密文、所述身份证读卡终端首次发送信息密文签名和身份证读卡终端证书;

所述云认证平台接收所述身份证读卡终端传输信息,验证所述身份证读卡终端证书是否正常;若所述身份证读卡终端证书正常,所述云认证平台根据所述身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文,如果得到认证解密密钥密文,则所述云认证平台从第二预设存储区域内获得第二密钥,使用所述第二密钥解密所述认证解密密钥密文,得到认证解密密钥,使用所述认证解密密钥解密所述身份证读卡终端首次发送信息密文,获得所述身份证读卡终端首次发送信息;

所述云认证平台获得第一会话密钥,所述身份证读卡终端获得第二会话密钥;

所述云认证平台使用所述第一会话密钥加密向所述身份证读卡终端发送的信息,所述身份证读卡终端使用所述第二会话密钥解密从所述云认证平台接收的信息;

所述身份证读卡终端使用所述第二会话密钥加密向所述云认证平台发送的信息,所述云认证平台使用所述第一会话密钥解密从所述身份证读卡终端接收的信息。

2.根据权利要求1所述的方法,其特征在于,所述云认证平台验证所述身份证读卡终端证书是否正常,包括:

所述云认证平台接收对身份证读卡终端证书或所述身份证读卡终端证书编号进行查询的查询结果,所述查询结果为数字证书在线查询服务器对身份证读卡终端证书或所述身份证读卡终端证书编号进行在线查询是否有效得到的;

如果查询结果为无效,所述云认证平台获得身份证读卡终端证书异常提示,根据所述身份证读卡终端证书异常提示对所述身份证读卡终端发送的信息进行处理;

如果查询结果为有效,所述云认证平台获得身份证读卡终端证书有效提示,所述云认证平台使用根证书验证所述身份证读卡终端证书是否合法,如果所述身份证读卡终端证书合法,则所述云认证平台获得身份证读卡终端证书正常提示,如果所述身份证读卡终端证书不合法,则所述云认证平台获得身份证读卡终端证书异常提示。

3.根据权利要求1所述的方法,其特征在于,若所述身份证读卡终端证书正常,所述方法还包括:

所述云认证平台对所述身份证读卡终端首次发送信息密文进行散列计算,得到身份证读卡终端首次发送信息密文摘要,调用所述身份证读卡终端证书中的身份证读卡终端公钥解密所述身份证读卡终端首次发送信息密文签名,得到身份证读卡终端首次发送信息密文签名的明文,通过判断所述身份证读卡终端首次发送信息密文签名的明文与所述身份证读

卡终端首次发送信息密文摘要是否相同，判断验签是否通过；

若不相同，所述云认证平台判断验签没有通过，所述云认证平台获得身份证读卡终端签名异常提示；

若相同，所述云认证平台判断验签通过，所述云认证平台根据所述身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

4.根据权利要求1所述的方法，其特征在于，

所述身份证读卡终端首次发送信息包括安全控制信息；

在所述云认证平台获得所述终端首次发送信息之后，所述方法还包括：

所述云认证平台根据所述安全控制信息进行调度服务。

5.根据权利要求1所述的方法，其特征在于，所述云认证平台获得第一会话密钥，所述身份证读卡终端获得第二会话密钥，包括：

所述云认证平台生成会话随机因子，将所述会话随机因子作为第一会话密钥，使用所述身份证读卡终端的公钥加密所述第一会话密钥，得到第一会话密钥密文，将云认证平台第一传输信息发送至所述身份证读卡终端，所述云认证平台第一传输信息至少包括所述第一会话密钥密文；

所述身份证读卡终端接收所述云认证平台第一传输信息，调用所述身份证读卡终端私钥解密所述第一会话密钥密文，得到第二会话密钥。

6.根据权利要求1所述的方法，其特征在于，所述云认证平台获得第一会话密钥，所述身份证读卡终端获得第二会话密钥，包括：

所述云认证平台将云认证平台第二传输信息发送至所述身份证读卡终端，所述云认证平台第二传输信息中至少包括认证证书、认证验签信息和对认证验签信息进行签名得到的认证签名；

所述身份证读卡终端接收所述云认证平台第二传输信息，根据根证书判断所述认证证书是否合法，如果合法，使用认证证书公钥和所述认证验签信息对所述认证签名进行验签计算，如果验签通过，则生成第二随机因子，将所述第二随机因子作为第二会话密钥，使用所述认证证书公钥加密所述第二会话密钥，得到第二会话密钥密文；

所述身份证读卡终端将所述第二会话密钥密文发送至所述云认证平台，所述云认证平台使用所述认证证书私钥解密所述第二会话密钥密文，得到第一会话密钥。

7.一种身份证读卡终端与云认证平台数据传输系统，其特征在于，包括：

所述身份证读卡终端，用于获得身份证读卡终端首次发送信息和认证加密密钥，使用所述认证加密密钥加密所述身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文；对所述身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，并调用所述身份证读卡终端的身份证读卡终端私钥加密所述身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名；读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至所述云认证平台，所述身份证读卡终端传输信息至少包括所述身份证读卡终端身份标识信息、所述身份证读卡终端首次发送信息密文、所述身份证读卡终端首次发送信息密文签名、和身份证读卡终端证书；获得第二会话密钥，使用所述第二会话密钥解密从所述云认证平台接收的信息，使用所述第二会话密钥加密向所述云认证平台发送的信息；

所述云认证平台，用于接收所述身份证读卡终端传输信息，验证所述身份证读卡终端证书是否正常；若所述身份证读卡终端证书正常，所述云认证平台根据所述身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文；如果得到认证解密密钥密文，从第二预设存储区域内获得第二密钥，使用所述第二密钥解密所述认证解密密钥密文，得到认证解密密钥，使用所述认证解密密钥解密所述身份证读卡终端首次发送信息密文，获得所述身份证读卡终端首次发送信息；获得第一会话密钥，使用所述第一会话密钥加密向所述身份证读卡终端发送的信息，使用所述第一会话密钥解密从所述身份证读卡终端接收的信息。

8.根据权利要求7所述的系统，其特征在于：

所述云认证平台，具体用于接收对身份证读卡终端证书或所述身份证读卡终端证书编号进行查询的查询结果，所述查询结果为数字证书在线查询服务器对身份证读卡终端证书或所述身份证读卡终端证书编号进行在线查询是否有效得到的；如果查询结果为无效，所述云认证平台获得身份证读卡终端证书异常提示，根据所述身份证读卡终端证书异常提示对所述身份证读卡终端发送的信息进行处理；如果查询结果为有效，所述云认证平台获得身份证读卡终端证书有效提示，所述云认证平台使用根证书验证所述身份证读卡终端证书是否合法，如果所述身份证读卡终端证书合法，则所述云认证平台获得身份证读卡终端证书正常提示，如果所述身份证读卡终端证书不合法，则所述云认证平台获得身份证读卡终端证书异常提示。

9.根据权利要求7所述的系统，其特征在于：

所述云认证平台，还用于对所述身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，调用所述身份证读卡终端证书中的身份证读卡终端公钥解密所述身份证读卡终端首次发送信息密文签名，得到身份证读卡终端首次发送信息密文签名的明文，通过判断所述身份证读卡终端首次发送信息密文签名的明文与所述身份证读卡终端首次发送信息密文摘要是否相同，判断验签是否通过；若不相同，所述云认证平台判断验签没有通过，所述云认证平台获得身份证读卡终端签名异常提示；若相同，所述云认证平台判断验签通过，所述云认证平台根据所述身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

10.根据权利要求7所述的系统，其特征在于，所述身份证读卡终端首次发送信息包括安全控制信息；所述云认证平台，还用于根据所述安全控制信息进行调度服务。

11.根据权利要求7所述的系统，其特征在于，

所述云认证平台，具体用于生成会话随机因子，将所述会话随机因子作为第一会话密钥，使用所述身份证读卡终端的公钥加密所述第一会话密钥，得到第一会话密钥密文，将云认证平台第一传输信息发送至所述身份证读卡终端，第一传输信息至少包括所述第一会话密钥密文；

所述身份证读卡终端，具体用于接收所述云认证平台第一传输信息，调用所述身份证读卡终端私钥解密所述第一会话密钥密文，得到第二会话密钥。

12.根据权利要求7所述的系统，其特征在于，

所述云认证平台，具体用于将云认证平台第二传输信息发送至所述身份证读卡终端，所述云认证平台第二传输信息中至少包括认证证书、认证验签信息和对认证验签信息进行

签名得到的认证签名;使用所述认证证书私钥解密所述第二会话密钥密文,得到第一会话密钥;

所述身份证读卡终端,具体用于接收所述云认证平台第二传输信息,根据根证书判断所述认证证书是否合法,如果合法,使用认证证书公钥和所述认证验签信息对所述认证签名进行验签计算,如果验签通过,则生成第二随机因子,将所述第二随机因子作为第二会话密钥,使用所述认证证书公钥加密所述第二会话密钥,得到第二会话密钥密文;将所述第二会话密钥密文发送至所述云认证平台。

身份证读卡终端与云认证平台数据传输方法和系统

技术领域

[0001] 本发明涉及一种电子技术领域，尤其涉及身份证读卡终端与云认证平台数据传输方法和系统。

背景技术

[0002] 居民二代身份证中存储的是身份证信息的密文，需要经过公安部授权的安全控制模块才能解密居民身份证中存储的身份证信息的密文。现有的身份证读卡器具有至少两个模块，包括读模块以及居民身份证验证安全控制模块。由于每个身份证读卡器均设置居民身份证验证安全控制模块，因此，现有的身份证读卡器的制造成本高；并且，一个居民身份证验证安全控制模块只能对一个读模块读取的居民身份证信息进行身份验证，因此，现有的身份证读卡器利用率较低，为解决该问题，目前出现了改进方案：身份证读卡器不再包括居民身份证验证安全控制模块，将居民身份证验证安全控制模块设于后台服务器，从而提升居民身份证验证安全控制模块的利用率。在这种情况下，身份证读卡器需要与后台服务器进行信息交互，才能获得身份证的明文信息。然而由于后台处于的网络环境为公开网络，任何读卡器均能够请求后台服务器使其接入居民身份证验证安全控制模块，这就大大提高了后台服务器的居民身份证验证安全控制模块的安全隐患，因此，如何对后台服务器的居民身份证验证安全控制模块进行有效保护，并防止虚假的读卡器接入后台，并保障后台服务器与读卡器之间信息交互的安全，是本领域技术人员亟待解决的技术问题。

发明内容

[0003] 本发明旨在解决上述问题之一。

[0004] 本发明的主要目的在于提供一种身份证读卡终端与云认证平台数据传输方法，包括：身份证读卡终端获得身份证读卡终端首次发送信息和认证加密密钥，使用认证加密密钥加密身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文；身份证读卡终端对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，并调用身份证读卡终端的身份证读卡终端私钥加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名；身份证读卡终端读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台，身份证读卡终端传输信息至少包括身份证读卡终端身份标识信息、身份证读卡终端首次发送信息密文、身份证读卡终端首次发送信息密文签名和身份证读卡终端证书；云认证平台接收身份证读卡终端传输信息，验证身份证读卡终端证书是否正常；若身份证读卡终端证书正常，云认证平台根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文，如果得到认证解密密钥密文，则云认证平台从第二预设存储区域内获得第二密钥，使用第二密钥解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，获得身份证读卡终端首次发送信息；云认证平台获得第一会话密钥，身份证读卡终端获得第二会话密钥；云认证平台使用第一会话密钥加密向身份证

读卡终端发送的信息，身份证读卡终端使用第二会话密钥解密从云认证平台接收的信息；身份证读卡终端使用第二会话密钥加密向云认证平台发送的信息，云认证平台使用第一会话密钥解密从身份证读卡终端接收的信息。

[0005] 此外，身份证读卡终端首次发送信息至少包括寻卡请求；在身份证读卡终端获得身份证读卡终端首次发送信息之前，还包括：身份证读卡终端发送寻卡指令至身份证，身份证接收到寻卡指令后发送确认寻卡指令信息至身份证读卡终端；身份证读卡终端接收确认寻卡指令，身份证读卡终端生成寻卡请求。

[0006] 此外，云认证平台验证身份证读卡终端证书是否正常，包括：云认证平台接收对身份证读卡终端证书或身份证读卡终端证书编号进行查询的查询结果，查询结果为数字证书在线查询服务器对身份证读卡终端证书或身份证读卡终端证书编号进行在线查询是否有效得到的；如果查询结果为无效，云认证平台获得身份证读卡终端证书异常提示，根据身份证读卡终端证书异常提示对身份证读卡终端发送的信息进行处理；如果查询结果为有效，云认证平台获得身份证读卡终端证书有效提示，云认证平台使用根证书验证身份证读卡终端证书是否合法，如果身份证读卡终端证书合法，则云认证平台获得身份证读卡终端证书正常提示，如果身份证读卡终端证书不合法，则云认证平台获得身份证读卡终端证书异常提示。

[0007] 此外，若身份证读卡终端证书正常，方法还包括：云认证平台对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，调用身份证读卡终端证书中的身份证读卡终端公钥解密身份证读卡终端首次发送信息密文签名，得到身份证读卡终端首次发送信息密文签名的明文，通过判断身份证读卡终端首次发送信息密文签名的明文与身份证读卡终端首次发送信息密文摘要是否相同，判断验签是否通过；若不相同，云认证平台判断验签没有通过，云认证平台获得身份证读卡终端签名异常提示；若相同，云认证平台判断验签通过，云认证平台根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

[0008] 此外，如果云认证平台从第一预设存储区域无法得到认证解密密钥密文，云认证平台获取身份证读卡终端解密密钥异常提示。

[0009] 此外，身份证读卡终端首次发送信息包括安全控制信息；在云认证平台获得终端首次发送信息之后，方法还包括：云认证平台根据安全控制信息进行调度服务。

[0010] 此外，云认证平台获得第一会话密钥，身份证读卡终端获得第二会话密钥，包括：云认证平台生成会话随机因子，将会话随机因子作为第一会话密钥，使用身份证读卡终端的公钥加密第一会话密钥，得到第一会话密钥密文，将云认证平台第一传输信息发送至身份证读卡终端，云认证平台第一传输信息至少包括第一会话密钥密文；身份证读卡终端接收云认证平台第一传输信息，调用身份证读卡终端私钥解密第一会话密钥密文，得到第二会话密钥。

[0011] 此外，云认证平台获得第一会话密钥，身份证读卡终端获得第二会话密钥，包括：云认证平台将云认证平台第二传输信息发送至身份证读卡终端，云认证平台第二传输信息中至少包括认证证书、认证验签信息和对认证验签信息进行签名得到的认证签名；身份证读卡终端接收云认证平台第二传输信息，根据根证书判断认证证书是否合法，如果合法，使用认证证书公钥和认证验签信息对认证签名进行验签计算，如果验签通过，则生成第二随

机因子，将第二随机因子作为第二会话密钥，使用认证证书公钥加密第二会话密钥，得到第二会话密钥密文；身份证读卡终端将第二会话密钥密文发送至云认证平台，云认证平台使用认证证书私钥解密第二会话密钥密文，得到第一会话密钥。

[0012] 本发明的另一目的在于提供一种身份证读卡终端与云认证平台数据传输系统，包括：身份证读卡终端，用于获得身份证读卡终端首次发送信息和认证加密密钥，使用认证加密密钥加密身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文；对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，并调用身份证读卡终端的身份证读卡终端私钥加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名；读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台，身份证读卡终端传输信息至少包括身份证读卡终端身份标识信息、身份证读卡终端首次发送信息密文、身份证读卡终端首次发送信息密文签名、和身份证读卡终端证书；获得第二会话密钥，使用第二会话密钥解密从云认证平台接收的信息，使用第二会话密钥加密向云认证平台发送的信息；云认证平台，用于接收身份证读卡终端传输信息，验证身份证读卡终端证书是否正常；若身份证读卡终端证书正常，云认证平台根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文；如果得到认证解密密钥密文，从第二预设存储区域内获得第二密钥，使用第二密钥解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，获得身份证读卡终端首次发送信息；获得第一会话密钥，使用第一会话密钥加密向身份证读卡终端发送的信息，使用第一会话密钥解密从身份证读卡终端接收的信息。

[0013] 此外，系统还包括身份证；身份证读卡终端首次发送信息至少包括寻卡请求；身份证读卡终端，还用于在身份证读卡终端获得身份证读卡终端首次发送信息之前，发送寻卡指令至身份证；终端接收身份证发送的确认寻卡指令，身份证读卡终端生成寻卡请求；身份证，用于接收到寻卡指令后发送确认寻卡指令信息至身份证读卡终端。

[0014] 此外，云认证平台，具体用于接收对身份证读卡终端证书或身份证读卡终端证书编号进行查询的查询结果，查询结果为数字证书在线查询服务器对身份证读卡终端证书或身份证读卡终端证书编号进行在线查询是否有效得到的；如果查询结果为无效，云认证平台获得身份证读卡终端证书异常提示，根据身份证读卡终端证书异常提示对身份证读卡终端发送的信息进行处理；如果查询结果为有效，云认证平台获得身份证读卡终端证书有效提示，云认证平台使用根证书验证身份证读卡终端证书是否合法，如果身份证读卡终端证书合法，则云认证平台获得身份证读卡终端证书正常提示，如果身份证读卡终端证书不合法，则云认证平台获得身份证读卡终端证书异常提示。

[0015] 此外，云认证平台，还用于对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，调用身份证读卡终端证书中的身份证读卡终端公钥解密身份证读卡终端首次发送信息密文签名，得到身份证读卡终端首次发送信息密文签名的明文，通过判断身份证读卡终端首次发送信息密文签名的明文与身份证读卡终端首次发送信息密文摘要是否相同，判断验签是否通过；若不相同，云认证平台判断验签没有通过，云认证平台获得身份证读卡终端签名异常提示；若相同，云认证平台判断验签通过，云认证平台根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密

文。

[0016] 此外，如果云认证平台从第一预设存储区域无法得到认证解密密钥密文，云认证平台获取身份证读卡终端解密密钥异常提示。

[0017] 此外，身份证读卡终端首次发送信息包括安全控制信息；云认证平台，还用于根据安全控制信息进行调度服务。

[0018] 此外，云认证平台，具体用于生成会话随机因子，将会话随机因子作为第一会话密钥，使用身份证读卡终端的公钥加密第一会话密钥，得到第一会话密钥密文，将云认证平台第一传输信息发送至身份证读卡终端，第一传输信息至少包括第一会话密钥密文；身份证读卡终端，具体用于接收云认证平台第一传输信息，调用身份证读卡终端私钥解密第一会话密钥密文，得到第二会话密钥。

[0019] 此外，云认证平台，具体用于将云认证平台第二传输信息发送至身份证读卡终端，云认证平台第二传输信息中至少包括认证证书、认证验签信息和对认证验签信息进行签名得到的认证签名；使用认证证书私钥解密第二会话密钥密文，得到第一会话密钥。身份证读卡终端，具体用于接收云认证平台第二传输信息，根据根证书判断认证证书是否合法，如果合法，使用认证证书公钥和认证验签信息对认证签名进行验签计算，如果验签通过，则生成第二随机因子，将第二随机因子作为第二会话密钥，使用认证证书公钥加密第二会话密钥，得到第二会话密钥密文；将第二会话密钥密文发送至云认证平台。

[0020] 由上述本发明提供的技术方案可以看出，本发明提供了一种身份证读卡终端与云认证平台数据传输方法和系统，身份证读卡终端首次发送信息使用认证加密密钥进行加密，云认证平台接收到身份证读卡终端首次发送信息密文后，根据身份证读卡终端身份标识信息获得认证解密密钥，获得身份证读卡终端首次发送信息，即只有拥有认证加密密钥的身份证读卡终端才能与云认证平台进行数据传输，而只有拥有认证解密密钥的设备才能获得身份证读卡终端发送的数据，保障了身份证读卡终端与云认证平台的信息交互安全。在获得身份证读卡终端首次发送信息之后，云认证平台和身份证读卡终端分别生成第一会话密钥和第二会话密钥，并使用第一会话密钥和第二会话密钥对身份证读卡终端与云认证平台后续传输的数据进行加密，减少使用认证加密密钥和认证解密密钥的使用，提高认证加密密钥和认证解密密钥的安全性。

附图说明

[0021] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他附图。

[0022] 图1为本发明实施例1提供的身份证读卡终端与云认证平台数据传输方法的流程图；

[0023] 图2为本发明实施例4提供的身份证读卡终端与云认证平台数据传输系统的结构示意图；

[0024] 图3为本发明实施例5提供的身份证读卡终端与云认证平台数据传输系统的另一结构示意图；

[0025] 图4为本发明实施例6提供的身份证读卡终端与云认证平台数据传输系统的又一结构示意图。

具体实施方式

[0026] 下面结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明的保护范围。

[0027] 在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或数量或位置。

[0028] 在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。

[0029] 下面将结合附图对本发明实施例作进一步地详细描述。

[0030] 实施例1

[0031] 图1为本实施例提供的一种身份证读卡终端与云认证平台数据传输方法，如图1所示，本实施例提供的身份证读卡终端与云认证平台数据传输方法主要包括以下步骤(101-108)。

[0032] 步骤101：身份证读卡终端获得身份证读卡终端首次发送信息和认证加密密钥，使用认证加密密钥加密身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文；

[0033] 在本实施例中，需要说明的是，一般的身份证读卡终端中设置有公安部授权的安全控制模块，用以解密身份证读卡终端读取的加密身份证信息，但是身份证读卡终端中集成有公安部授权的安全控制模块的成本高，本实施例中，身份证读卡终端未设置有公安部授权的安全控制模块，安全控制模块设置在远端，如可以设置在本实施例的云认证平台中，身份证读卡终端与云认证平台通过有线(例如，身份证读卡终端通过有线方式接入互联网或局域网)连接，也可以通过无线(例如，身份证读卡终端通过WIFI，无线通信网络(如2G、3G、4G网络等)等与云认证平台连接)，具体本实施例不作限定。通过将身份证读卡终端与公安部授权的安全控制模块分开设置，可以多个身份证读卡终端共用一个公安部授权的安全控制模块，从而可以节约成本。

[0034] 在本实施例的一个可选实施方式中，身份证读卡终端内部可以具有安全芯片，该安全芯片内部拥有独立的处理器和存储单元，可存储PKI数字证书和密钥以及其他特征数据，对数据进行加解密运算，为用户提供数据加密和身份安全认证服务，保护商业隐私和数

据安全。因此，本可选实施方式中身份证读卡终端需要进行加解密、签名、验签、数字证书验证的数据均需经过身份证读卡终端内部的安全芯片，以保证身份证读卡终端与云认证平台之间的交互安全。可选地，认证加密密钥可以存储在安全芯片的文件系统中，认证加密密钥无法从安全芯片中导出，保障认证加密密钥的安全。可选地，安全芯片调用安全芯片的安全算法库中的预设加密算法使用认证加密密钥加密身份证读卡终端首次发送信息得到身份证读卡终端首次发送信息密文，确保身份证读卡终端首次发送信息密文可被顺利解密。

[0035] 在本实施例的一个可选实施方式中，预设第一存储区域内存储有认证加密密钥密文，预设第二存储区域内存储有第二预设密钥，身份证读卡终端根据身份证读卡终端身份标识从预设第二存储区域内获取第二预设密钥，从预设第一存储区域内获取认证加密密钥密文，使用第二预设密钥解密认证加密密钥密文，获得认证加密密钥。本可选实施方式中，预设第一存储区域可以是身份证读卡终端的安全芯片的文件系统，预设第二存储区域可以是读卡终端授权设备，该读卡终端授权设备可以是一个电子签名设备。采用认证加密密钥密文与第二预设密钥分开存放的方式，可以提高认证加密密钥的安全性，即没有读卡终端授权设备的授权，身份证读卡终端无法获得认证加密密钥，防止身份证读卡终端被非法使用，进一步提高了身份证信息的安全性。

[0036] 在本实施例中，身份证读卡终端首次发送信息可以是身份证读卡终端在读取一个新的身份证的信息的时候或读取一个新的身份证之前向云认证平台第一次发送的信息，该信息根据身份证读卡终端的操作的不同而不同，可以是认证信息、读卡请求、使用者身份确定请求等等，本实施例不做限制。

[0037] 在本实施例的一个可选实施方式中，身份证读卡终端首次发送信息至少包括寻卡请求；在身份证读卡终端获得身份证读卡终端首次发送信息之前，还包括：身份证读卡终端发送寻卡指令至身份证，身份证接收到寻卡指令后发送确认寻卡指令信息至身份证读卡终端；身份证读卡终端接收确认寻卡指令，身份证读卡终端生成寻卡请求。在本可选实施方式中，身份证读卡终端首次发送信息包括寻卡请求，在发送寻卡请求前获取确认寻卡指令信息，保障身份证读卡终端在后续操作中顺利读取身份证信息。

[0038] 步骤102：身份证读卡终端对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，并调用身份证读卡终端的身份证读卡终端私钥加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名；

[0039] 在本实施例的一个可选实施方式中，身份证读卡终端的安全芯片调用存储在文件系统中的身份证读卡终端私钥并使用安全算法库中的预设加密算法加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名。身份证读卡终端首次发送信息密文签名是使用身份证读卡终端不可导出的私钥签名获得的，以便云认证平台确认该身份证读卡终端的身份，且该身份具有不可抵赖性。

[0040] 步骤103：身份证读卡终端读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台，身份证读卡终端传输信息至少包括身份证读卡终端身份标识信息、身份证读卡终端首次发送信息密文、身份证读卡终端首次发送信息密文签名和身份证读卡终端证书；

[0041] 在本实施例中，身份证读卡终端身份标识信息可以是存储在身份证读卡终端的安

全芯片中的，身份证读卡终端身份标识信息可以是身份证读卡终端序列号和/或身份证读卡终端证书号，且身份证读卡终端序列号与身份证读卡终端证书号具备映射关系，云认证平台存储有身份证读卡终端序列号与身份证读卡终端证书号的映射关系，云认证平台收到身份证读卡终端序列号后，能够通过查询身份证读卡终端序列号与身份证读卡终端证书号的映射关系，获取身份证读卡终端证书号，反之亦然，通过身份证读卡终端序列号和/或身份证读卡终端证书号。可选地，通过身份证读卡终端身份标识信息，云认证平台还可以定位识别该身份证读卡终端，并获取身份证读卡终端的出厂信息、历史读卡信息、历史错误信息、历史举报信息和历史交易信息等信息，以便于云认证平台进一步利用收到的身份证读卡终端身份标识信息实现风险管理。

[0042] 步骤104：云认证平台接收身份证读卡终端传输信息，验证身份证读卡终端证书是否正常；

[0043] 在本实施例的一个可选实施方式中，身份证读卡终端证书至少包括：身份证读卡终端证书内容信息，对身份证读卡终端内容信息进行签名得到的身份证读卡终端证书签名信息，其中，身份证读卡终端内容信息至少包括：身份证读卡终端证书编号；云认证平台验证身份证读卡终端证书是否为正常证书的步骤，包括：云认证平台接收对身份证读卡终端证书或身份证读卡终端证书编号进行查询的查询结果，查询结果为数字证书在线查询服务器对身份证读卡终端证书或身份证读卡终端证书编号进行在线查询是否有效得到的；如果查询结果为无效，云认证平台获得身份证读卡终端证书异常提示，根据身份证读卡终端证书异常提示对身份证读卡终端发送的信息进行处理；如果查询结果为有效，云认证平台获得身份证读卡终端证书有效提示。云认证平台获得身份证读卡终端证书有效提示，使用预存的根证书的公钥对身份证读卡终端证书签名信息进行解密，得到身份证读卡终端证书内容信息第一摘要，对身份证读卡终端证书内容信息进行散列计算，得到身份证读卡终端证书内容信息第二摘要，判断身份证读卡终端证书内容信息第一摘要与身份证读卡终端证书内容信息第二摘要是否相同，如果相同，则判断身份证读卡终端证书正常，可选地，如果不相同，则云认证平台可以判断身份证读卡终端证书不正常，接收身份证读卡终端证书异常提示。达到云认证平台对身份证读卡终端进行证书认证的效果，保障了没有证书、证书失效或虚假身份证读卡终端不能访问云认证平台。

[0044] 在上述可选实施方式中，为云认证平台提供查询结果的数字证书在线查询服务器可以设置在云认证平台内部，也可以设置在云认证平台外部。数字证书在线查询服务器可以存储所有身份证读卡终端的证书状态，通过身份证读卡终端证书或身份证读卡终端证书编号可以查找到该身份证读卡终端的证书处于有效状态或无效状态(可进一步包括过期状态、暂停使用状态和废止状态等等)，数字证书在线查询服务器的身份证读卡终端证书或身份证读卡终端证书编号与该证书的状态可通过列表等形式存储，例如将所有有效状态的身份证读卡终端证书信息存储在一个有效列表中，当该身份证读卡终端处于该有效列表，即该身份证读卡终端有效。本实施例对数字证书在线查询服务器的具体工作方式不做限制。

[0045] 在上述可选实施方式中，在数字证书在线查询服务器查询到身份证读卡终端证书有效后，使用根证书验证身份证读卡终端证书的合法性，以防止非法分子篡改身份证读卡终端的公钥，实现对身份证读卡终端证书的进一步验证，提高安全性。云认证平台可以从认证中心(Certificate Authority，简称CA)下载根证书或预设根证书，根证书是CA与云认证

平台建立信任关系的基础。如果验证通过，则认为身份证读卡终端证书合法，进而判断身份证读卡终端证书正常。云认证平台可获取身份证读卡终端证书正常的信息，对该身份证读卡终端发送的信息进行进一步的操作，如果验证不通过，身份证读卡终端证书不合法，则可以在此时结束流程，减少非法攻击对云认证平台的占用。

[0046] 在上述可选实施方式中，云认证平台可设置身份证读卡终端黑名单，在云认证平台收到该身份证读卡终端发送的信息时，查看身份证读卡终端是否在黑名单中，如果在，可拒绝处理该身份证读卡终端的信息，与其断开连接。云认证平台在接收到身份证读卡终端证书异常提示后，可将该身份证读卡终端列入黑名单中，拒绝处理该身份证读卡终端发送的信息，直接与身份证读卡终端断开连接，也可向身份证读卡终端返回证书异常提示，还可以对身份证读卡终端进行初步异常标记，综合其他判断信息后(如时间戳信息、计数器信息等)根据预设规则判断是否将身份证读卡终端列入黑名单中，与其断开连接，并不再处理该身份证读卡终端发送的任何数据，本实施例在此不做限制。在本实施例中，云认证平台接收到身份证读卡终端异常提示后，将该身份证读卡终端列入黑名单，拒绝处理该身份证读卡终端的信息或身份证读卡终端断开连接的情况下，从身份证读卡终端向云认证平台发送数据开始，到身份证读卡终端证书被判定为异常证书，耗时非常短暂，云认证平台可迅速判断身份证读卡终端并非可信终端，释放与身份证读卡终端的连接通道，因此，当非法设备伪装为身份证读卡终端对云认证平台进行攻击时，可迅速断开与非法设备的连接通道，减少非法攻击对云认证平台的占用，保证云认证平台的正常使用。

[0047] 在本实施例的一个可选实施方式中，若身份证读卡终端证书正常，本实施例还包括：云认证平台对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，调用身份证读卡终端证书中的身份证读卡终端公钥解密身份证读卡终端首次发送信息密文签名，得到身份证读卡终端首次发送信息密文签名的明文，通过判断身份证读卡终端首次发送信息密文签名的明文与身份证读卡终端首次发送信息密文摘要是否相同，判断验签是否通过；若不相同，云认证平台判断验签没有通过，云认证平台获得身份证读卡终端签名异常提示；若相同，云认证平台判断验签通过，云认证平台根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。即云认证平台进一步验证身份证读卡终端首次发送信息密文签名，若没有通过验签，云认证平台可以根据身份证读卡终端签名异常提示，根据该身份证读卡终端签名异常提示进行处理，若验签通过，则可进一步确认身份证读卡终端的身份，进一步保障云认证平台的安全。

[0048] 步骤105：若身份证读卡终端证书正常，云认证平台根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

[0049] 在本实施例的一个可选实施方式中，第一预设存储区域为认证解密密钥密文数据库，该数据库中存储有身份证读卡终端身份标识信息与认证解密密钥密文的映射关系，认证解密密钥密文数据库在至少接收到身份证读卡终端身份标识信息后，通过该身份证读卡终端身份标识信息查找对应的认证解密密钥密文，云认证平台获得认证解密密文。

[0050] 在本实施例的一个可选实施方式中，如果云认证平台从第一预设存储区域无法得到认证解密密钥密文，云认证平台获取身份证读卡终端解密密钥异常提示。在本实施方式中，若云认证平台无法得到认证解密密钥，说明身份证读卡终端存在异常，云认证平台可进一步根据异常提示处理身份证读卡终端传输的信息。

[0051] 步骤106:如果得到认证解密密钥密文,则云认证平台从第二预设存储区域内获得第二密钥。

[0052] 在本实施例的一个可选实施方式中,第二预设存储区域可以为授权设备,该授权设备可以是一个授权电子签名设备,该授权设备中存储有云认证平台的第二密钥,即若没有该授权设备的授权,云认证平台无法获得第二密钥,无法正常运行,即进一步保障身份证信息的安全。

[0053] 步骤107:云认证平台使用第二密钥解密认证解密密钥密文,得到认证解密密钥,使用认证解密密钥解密身份证读卡终端首次发送信息密文,获得身份证读卡终端首次发送信息;

[0054] 在本实施例的一个可选实施方式中,云认证平台可以使用预设解密算法和第二密钥解密认证解密密钥密文,进而得到认证解密密钥密文。认证解密密钥与认证加密密钥是密钥对。

[0055] 在本实施例的一个可选实施方式中,身份证读卡终端首次发送信息包括安全控制信息;在云认证平台获得终端首次发送信息之后,方法还包括:云认证平台根据计数器信息进行调度服务。可选地,安全控制信息可以是计数器信息,还可以是时间戳信息,身份证读卡终端根据向云认证平台发送信息的次数获得计数器信息,自身生成时间戳信息或从与身份证读卡终端连接的设备中读取时间戳信息。云认证平台接收到安全控制信息后,根据安全控制进行调度服务可以为,若相同身份证读卡终端针对读取不同身份证发送的计数器信息无变化,可以判定该身份证读卡终端可能被破解,将该身份证读卡终端列入黑名单中,不再处理该身份证读卡终端发送的信息,还可以为,若相同身份证读卡终端针对读取不同身份证发送的时间戳信息无变化,可以判定该身份证读卡终端可能被破解,将该身份证读卡终端列入黑名单中,不再处理该身份证读卡终端发送的信息,本实施例不做具体限制。

[0056] 步骤108:云认证平台获得第一会话密钥,身份证读卡终端获得第二会话密钥;云认证平台使用第一会话密钥加密向身份证读卡终端发送的信息,身份证读卡终端使用第二会话密钥解密从云认证平台接收的信息;身份证读卡终端使用第二会话密钥加密向云认证平台发送的信息,云认证平台使用第一会话密钥解密从身份证读卡终端接收的信息。

[0057] 在本实施例中,第一会话密钥和第二会话密钥为对称密钥对。

[0058] 在本实施例的一个可选实施方式中,云认证平台获得第一会话密钥,身份证读卡终端获得第二会话密钥,包括:云认证平台生成会话随机因子,将会话随机因子作为第一会话密钥,使用身份证读卡终端的公钥加密第一会话密钥,将云认证平台第一传输信息发送至身份证读卡终端,云认证平台第一传输信息至少包括第一会话密钥密文;身份证读卡终端接收云认证平台第一传输信息,调用身份证读卡终端私钥解密第一会话密钥密文,得到第二会话密钥。在本实施方式中,第一会话密钥由云认证平台生成,使用身份证读卡终端公钥加密后发送至身份证读卡终端,由于解密第一会话密钥密文的解密密钥为身份证读卡终端私钥,而身份证读卡终端私钥是存储在身份证读卡终端的安全芯片之中的,身份证读卡终端私钥是无法被导出的,也就是说,只有该身份证读卡终端可以解密第一会话密钥密文,其他身份证读卡终端或设备是无法解密第一会话密钥密文,无法得到第二会话密钥的,保障了第一会话密钥和第二会话密钥的安全性,保障了身份证读卡终端与云认证平台的通信安全。

[0059] 在上述可选实施方式中，还包括：云认证平台获得身份证读卡终端首次发送信息之后，云认证平台获取第一会话密钥生成提示，云认证平台根据第一会话密钥生成提示生成请求产生会话随机因子，云认证平台将会话随机因子存储为第一会话密钥；可选地，会话随机因子可以包括随机书和/或随机字符，在此不做限制。该会话随机因子也可以为一个或一串随机数，或者可以为一个或一串随机字符，或者一串随机数和随机字符组合的任意组合。云认证平台每次生成的会话随机因子都是随机生成的，与上一次生成的会话随机因子是不同的，将会话随机因子存储为第一会话密钥加密待发送信息，可以防止非法终端破解固定密钥，提高了身份证读卡终端与云认证平台之间信息传输的安全性。

[0060] 在上述可选实施方式中，云认证平台将云认证平台第一传输信息发送至身份证读卡终端之前，还包括：云认证平台对第一会话密钥密文进行散列计算，得到第一会话密钥密文摘要，使用云认证平台私钥加密第一会话密钥密文摘要，得到认证签名；云认证平台第一传输信息还包括认证证书和认证签名。进一步地，身份证读卡终端在将解密第一会话密钥密文得到的数据存储为第二会话密钥的步骤之前，还包括：身份证读卡终端对第一会话密钥密文进行散列计算，得到第一会话密钥密文第一摘要，使用认证证书公钥解密认证签名，得到第一会话密钥密文第二摘要，判断第一会话密钥密文第一摘要与第一会话密钥密文第二摘要是否相同，如果相同，则通过验签，将解密第一会话密钥密文得到的数据存储为第二会话密钥。身份证读卡终端对认证签名进行验签，避免其他设备仿冒为云认证平台，保护身份证读卡终端与云认证平台信息交互的安全性。

[0061] 在本实施例的一个可选实施方式中，还包括：云认证平台将云认证平台第二传输信息发送至身份证读卡终端，云认证平台第二传输信息中至少包括认证证书、认证验签信息和对认证验签信息进行签名得到的认证签名；身份证读卡终端接收云认证平台第二传输信息，根据根证书判断认证证书是否合法，如果合法，使用认证证书公钥和认证验签信息对认证签名进行验签计算，如果验签通过，则生成第二随机因子，将第二随机因子作为第二会话密钥，使用认证证书公钥加密第二会话密钥，得到第二会话密钥密文；身份证读卡终端将第二会话密钥密文发送至云认证平台，云认证平台使用认证证书私钥解密第二会话密钥密文，得到第一会话密钥。在本可选实施方式中，身份证读卡终端首先验证云认证平台的身份，可避免其他设备仿冒云认证平台，验证通过后再生成第二会话密钥密文，并使用认证证书公钥加密，得到第一会话密钥，使得只有云认证平台拥有认证证书私钥时才可解密第二会话密钥密文，保障了第二会话密钥的安全。

[0062] 在本实施例的一个可选实施方式中，第二会话密钥可存储身份证读卡终端的安全芯片的缓存或闪存中，当该安全芯片完成本次身份证信息读取工作，可以通过强制清除或强制断电重启等方法清楚该第二会话密钥，保障第二会话密钥的安全。

[0063] 在本实施例的一个可选实施方式中，云认证平台可以包括一个安全主控芯片，将云认证平台获得第一会话密钥后，可以将该第一会话密钥存储在安全主控芯片中，每次使用第一会话密钥进行信息加密，均可以在安全主控芯片中进行，进一步地，该第一会话密钥可以存储在安全主控芯片的缓存或闪存中，当该安全主控芯片完成本次与身份证读卡终端的身份证信息读取工作，可以清除该第一会话密钥，保障第一会话密钥的安全。

[0064] 在本实施例的一个可选实施方式中，云认证平台与身份证读卡终端可设置为身份证读卡终端每次读取不同的身份证，均需重新获取第一会话密钥或第二会话密钥，即一次

一密，保障身份证用户的身份证信息安全。

[0065] 本实施例提供的身份证读卡终端与云认证平台的数据传输方法中，身份证读卡终端首次发送信息使用认证加密密钥进行加密，云认证平台接收到身份证读卡终端首次发送信息密文后，根据身份证读卡终端身份标识信息获得认证解密密钥，获得身份证读卡终端首次发送信息，即只有拥有认证加密密钥的身份证读卡终端才能与云认证平台进行数据传输，而只有拥有认证解密密钥的设备才能获得身份证读卡终端发送的数据，保障了身份证读卡终端与云认证平台的信息交互安全。在获得身份证读卡终端首次发送信息之后，云认证平台和身份证读卡终端分别生成第一会话密钥和第二会话密钥，并使用第一会话密钥和第二会话密钥对身份证读卡终端与云认证平台后续传输的数据进行加密，减少使用认证加密密钥和认证解密密钥的使用，提高认证加密密钥和认证解密密钥的安全性。

[0066] 实施例2

[0067] 本实施例提供的一种身份证读卡终端与云认证平台数据传输方法，与实施例1属于同一构思，与实施例1相同之处不再赘述，以下仅针对本实施例与实施例1不同之处进行说明：

[0068] 在本实施例中，云认证平台进一步包括至少一个调度服务器和至少一个认证安全控制模块，调度服务器接收身份证读卡终端首次发送信息，并验证身份证读卡终端证书是否正常，若身份证读卡终端证书正常，调度服务器根据身份证读卡终端身份标识信息读取解密密钥密文和第二密钥，将认证解密密钥密文和第二密钥以及身份证读卡终端首次发送信息密文发送至符合预设条件的认证安全控制模块，认证安全控制模块获得认证解密密钥并使用认证解密密钥解密身份证读卡终端首次发送信息密文，得到身份证读卡终端首次发送信息。认证安全控制模块获得第一会话密钥。本实施例提供的身份证读卡终端与云认证平台数据传输方法，主要包括以下步骤：

[0069] 步骤201：身份证读卡终端获得身份证读卡终端首次发送信息和认证加密密钥，使用认证加密密钥加密身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文。

[0070] 步骤202：身份证读卡终端对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，并调用身份证读卡终端的身份证读卡终端私钥加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名。

[0071] 步骤203：身份证读卡终端读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台的调度服务器，身份证读卡终端传输信息至少包括身份证读卡终端身份标识信息、身份证读卡终端首次发送信息密文、身份证读卡终端首次发送信息密文签名和身份证读卡终端证书。

[0072] 在本实施例的一个可选实施方式中，云认证平台可进一步包括边界路由器和负载均衡器，身份证读卡终端将身份证读卡终端传输信息发送至调度服务器，可进一步包括：身份证读卡终端发送身份证读卡终端传输信息至边界路由器；边界路由器接收身份证读卡终端传输信息，判断身份证读卡终端传输信息是否符合预设标准，如果符合预设标准，则将身份证读卡终端传输信息发送至负载均衡器；负载均衡器接收身份证读卡终端传输信息，将身份证读卡终端传输信息发送至符合预设标准的调度服务器。在本可选实施方式中，边界

路由器是在一个或多个局域网络(LAN)和主干网络之间路由设备，是一个主要的接入点，经过设置，可阻挡部分对云认证平台的攻击；负载均衡器可以解决数据流量过大、网络负荷过重的问题，避免服务器单点故障造成数据流量的损失，把数据流量合理地分配给调度服务器。云认证平台更加安全，数据处理更加高效。

[0073] 步骤204：调度服务器接收身份证读卡终端传输信息，验证身份证读卡终端证书是否正常。

[0074] 在本实施例中，调度服务器验证身份证读卡终端证书是否正常，调度服务器接收数字证书在线查询服务器发送的身份证读卡终端证书状态查询结果，调度服务器在接收到身份证读卡终端证书异常提示后，可拒绝处理该身份证读卡终端发送的信息，直接与身份证读卡终端断开连接，也可向身份证读卡终端返回证书异常提示，还可以对身份证读卡终端进行初步异常标记，综合其他判断信息后(如时间戳信息、计数器信息等)根据预设规则判断是否与身份证读卡终端断开连接，本实施例在此不做限制。在本实施例中，调度服务器接收到身份证读卡终端异常提示后，即拒绝处理该身份证读卡终端的信息与身份证读卡终端断开连接的情况下，从身份证读卡终端向调度服务器发送数据开始，到身份证读卡终端证书被判定为异常证书，耗时非常短暂，调度服务器可迅速判断身份证读卡终端的证书错误，释放与身份证读卡终端的连接通道，因此，当非法设备伪装为身份证读卡终端对云认证平台进行攻击时，可迅速断开与非法设备的连接通道，减少攻击对云认证平台的占用，保证云认证平台的正常使用。

[0075] 在本实施例中，如果查询结果为有效，调度服务器获得身份证读卡终端证书有效提示；调度服务器使用预存的根证书的公钥对身份证读卡终端证书签名信息进行解密，得到身份证读卡终端证书内容信息第一摘要，对身份证读卡终端证书内容信息进行散列计算，得到身份证读卡终端证书内容信息第二摘要，判断身份证读卡终端证书内容信息第一摘要与身份证读卡终端证书内容信息第二摘要是否相同，如果相同，则判断身份证读卡终端证书合法，身份证读卡终端证书正常；

[0076] 在本实施例的一个可选实施方式中，身份证读卡终端传输信息还包括身份证读卡终端签名信息；方法还包括步骤204a：调度服务器至少使用身份证读卡终端证书对身份证读卡终端签名信息进行验签操作；如果验签不通过，则生成身份证读卡终端签名异常提示；调度服务器还根据身份证读卡终端签名异常提示对身份证读卡终端发送的信息进行处理。

[0077] 步骤205：若身份证读卡终端证书正常，调度服务器根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

[0078] 步骤206：如果得到认证解密密钥密文，则调度服务器从第二预设存储区域内获得第二密钥。

[0079] 步骤207：调度服务器将认证解密密钥密文、第二密钥和身份证读卡终端首次发送信息密文发送至符合预设条件的认证安全控制模块，认证安全控制模块使用第二密钥解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，获得身份证读卡终端首次发送信息。

[0080] 在本实施例的一个可选实施方式中，调度服务器在获得身份证读卡终端证书正常的提示后，为身份证读卡终端分配一个符合预设条件的认证安全控制模块，该认证安全控制模块用于处理该身份证读卡终端发送的信息，实现身份证读卡终端与认证安全控制模块

一对一的连接，保障身份证读卡终端的信息得到及时处理。进一步地，调度服务器可记录其负责调度的认证安全控制模块的状态，如空闲、忙碌、暂停使用等等，调度服务器分配认证安全控制模块的预设条件可以是认证安全控制模块处于空闲状态，本实施例在此不做限制。

[0081] 步骤208：认证安全控制模块获得第一会话密钥，身份证读卡终端获得第二会话密钥；认证安全控制模块使用第一会话密钥加密向身份证读卡终端发送的信息，身份证读卡终端使用第二会话密钥解密从认证安全控制模块接收的信息；身份证读卡终端使用第二会话密钥加密向认证安全控制模块发送的信息，认证安全控制模块使用第一会话密钥解密从身份证读卡终端接收的信息。

[0082] 在本实施例的一个可选实施方式中，认证安全控制模块获得第一会话密钥，身份证读卡终端获得第二会话密钥，包括：

[0083] 认证安全控制模块生成会话随机因子，将会话随机因子作为第一会话密钥，使用身份证读卡终端的公钥加密第一会话密钥，得到第一会话密钥密文，将云认证平台第一传输信息发送至身份证读卡终端，云认证平台第一传输信息至少包括第一会话密钥密文；身份证读卡终端接收云认证平台第一传输信息，调用身份证读卡终端私钥解密第一会话密钥密文，得到第二会话密钥。

[0084] 在本实施例的一个可选实施方式中，认证安全控制模块获得第一会话密钥，身份证读卡终端获得第二会话密钥，包括：认证安全控制模块将云认证平台第二传输信息发送至身份证读卡终端，云认证平台第二传输信息中至少包括认证证书、认证验签信息和对认证验签信息进行签名得到的认证签名(在本实施例中，认证证书为认证安全控制模块的证书，对认证验签信息进行签名也在认证安全控制模块中进行)；身份证读卡终端接收云认证平台第二传输信息，根据根证书判断认证证书是否合法，如果合法，使用认证证书公钥和认证验签信息对认证签名进行验签计算，如果验签通过，则生成第二随机因子，将第二随机因子作为第二会话密钥，使用认证证书公钥加密第二会话密钥，得到第二会话密钥密文；身份证读卡终端将第二会话密钥密文发送至认证安全控制模块，认证安全控制模块使用认证证书私钥解密第二会话密钥密文，得到第一会话密钥。

[0085] 在本实施例的一个可选实施方式中，认证安全控制模块可以是安全芯片，该安全芯片内部拥有独立的处理器和存储单元，可存储PKI数字证书和密钥，以及其他特征数据，对数据进行加解密运算并身份安全认证服务，保护商业隐私和数据安全。因此，本实施例中由认证安全控制模块解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，并生成第一会话密钥，可以进一步保证身份证读卡终端与云认证平台之间的交互安全。

[0086] 在本实施例中，步骤204中还可以有如下可选实施方式：调度服务器获得针对身份证读卡终端证书是否有效的查询结果，如果查询结果为有效，调度服务器获得身份证读卡终端证书有效提示；认证安全控制模块至少接收身份证读卡终端证书，使用预存的根证书的公钥对身份证读卡终端证书签名信息进行解密，得到身份证读卡终端证书内容信息第一摘要，对身份证读卡终端证书内容信息进行散列计算，得到身份证读卡终端证书内容信息第二摘要，判断身份证读卡终端证书内容信息第一摘要与身份证读卡终端证书内容信息第二摘要是否相同，如果相同，则判断身份证读卡终端证书合法，身份证读卡终端证书正常；

认证安全控制模块将身份证读卡终端证书正常提示发送至调度服务器。

[0087] 步骤205还可以有如下可选实施方式:若身份证读卡终端证书正常,认证安全控制模块根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

[0088] 步骤206还可以有如下可选实施方式:如果得到认证解密密钥密文,则认证安全控制模块从第二预设存储区域内获得第二密钥。

[0089] 在本实施例中,步骤204a还可以有如下可选实施方式:认证安全控制模块至少使用身份证读卡终端证书对身份证读卡终端签名信息进行验签操作;如果验签不通过,则生成身份证读卡终端签名异常提示,并发送至调度服务器;调度服务器还根据身份证读卡终端签名异常提示对身份证读卡终端发送的信息进行处理。

[0090] 需要说明的是,以上步骤204、步骤204a、步骤205和步骤206之间并不具有对应关系,也就是说,身份证读卡终端证书的有效性的结果由调度服务器接收的情况下,对该证书的合法性验证还可以由认证安全控制模块进行;在合法性验证由认证安全控制模块进行的情况下,对身份证读卡终端签名信息的验签操作可以由调度服务器进行,也可以由认证安全控制模块进行,获得认证解密密钥密文的操作可以由调度服务器进行,也可以由认证安全控制模块进行,获得第二密钥的操作可以由调度服务器进行,也可以由认证安全控制模块进行。本实施例并不做限制。在认证安全控制模块可以是安全芯片的情况下,使用根证书验证身份证读卡终端证书的合法性或验证身份证读卡终端签名信息更具有安全性更高。

[0091] 本实施例提供的身份证读卡终端与云认证平台的数据传输方法,云认证平台至少包括至少一个调度服务器和至少一个认证安全控制模块,由调度服务器完成身份证读卡终端的证书认证,并为身份证读卡终端提供认证安全控制模块调度服务,调度服务器根据身份证读卡终端身份标识信息获得认证解密密钥密文,认证安全控制模块获得认证解密密钥后获得身份证读卡终端首次发送信息,即只有拥有认证加密密钥的身份证读卡终端才能与云认证平台进行数据传输,而只有拥有认证解密密钥的设备才能获得身份证读卡终端发送的数据,保障了身份证读卡终端与云认证平台的信息交互安全。在获得身份证读卡终端首次发送信息之后,云认证平台和身份证读卡终端分别生成第一会话密钥和第二会话密钥,并使用第一会话密钥和第二会话密钥对身份证读卡终端与云认证平台后续传输的数据进行加密,减少使用认证加密密钥和认证解密密钥的使用,提高认证加密密钥和认证解密密钥的安全性。

[0092] 实施例3

[0093] 本实施例提供的一种身份证读卡终端与云认证平台数据传输方法,与实施例1和实施例2属于同一构思,与实施例1或实施例2相同之处不再赘述,以下仅针对本实施例与实施例1和实施例2不同之处进行说明:

[0094] 在本实施例中,云认证平台进一步包括至少一个调度服务器和至少一个认证安全控制模块,调度服务器接收身份证读卡终端首次发送信息,将身份证读卡终端首次发送信息至符合预设条件的认证安全控制模块,认证安全控制模块验证身份证读卡终端证书是否正常,若身份证读卡终端证书正常,认证安全控制模块根据身份证读卡终端身份标识信息读取认证解密密钥密文和第二密钥,认证安全控制模块获得认证解密密钥并使用认证解密密钥解密身份证读卡终端首次发送信息密文,得到身份证读卡终端首次发送信息。认证安全控制模块获得第一会话密钥。本实施例提供的身份证读卡终端与云认证平台数据传输方

法，主要包括以下步骤：

[0095] 步骤301：身份证读卡终端获得身份证读卡终端首次发送信息和认证加密密钥，使用认证加密密钥加密身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文。

[0096] 步骤302：身份证读卡终端对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，并调用身份证读卡终端的身份证读卡终端私钥加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名。

[0097] 步骤303：身份证读卡终端读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台的调度服务器，身份证读卡终端传输信息至少包括身份证读卡终端身份标识信息、身份证读卡终端首次发送信息密文、身份证读卡终端首次发送信息密文签名和身份证读卡终端证书。

[0098] 步骤304：调度服务器接收身份证读卡终端传输信息，将身份证读卡终端传输信息发送至符合预设条件的认证安全控制模块，认证安全控制模块验证身份证读卡终端证书是否正常。

[0099] 在本实施例的一个可选实施方式中，身份证读卡终端传输信息还包括身份证读卡终端签名信息；方法还包括步骤304a：认证安全控制模块至少使用身份证读卡终端证书对身份证读卡终端签名信息进行验签操作；如果验签不通过，则生成身份证读卡终端签名异常提示并发送至调度服务器；调度服务器还根据身份证读卡终端签名异常提示对身份证读卡终端发送的信息进行处理。

[0100] 步骤305：若身份证读卡终端证书正常，认证安全控制模块根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

[0101] 在本实施例的一个可选实施方式中，若身份证读卡终端证书异常，认证安全控制模块发送身份证读卡终端证书异常提示至调度服务器，调度服务器根据身份证读卡终端证书异常提示进行调度服务。

[0102] 步骤306：如果得到认证解密密钥密文，则认证安全控制模块从第二预设存储区域内获得第二密钥。

[0103] 步骤307：认证安全控制模块使用第二密钥解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，获得身份证读卡终端首次发送信息。

[0104] 步骤308：认证安全控制模块获得第一会话密钥，身份证读卡终端获得第二会话密钥；认证安全控制模块使用第一会话密钥加密向身份证读卡终端发送的信息，身份证读卡终端使用第二会话密钥解密从认证安全控制模块接收的信息；身份证读卡终端使用第二会话密钥加密向认证安全控制模块发送的信息，认证安全控制模块使用第一会话密钥解密从身份证读卡终端接收的信息。

[0105] 在本实施例中，步骤304中还可以有如下可选实施方式：认证安全控制模块获得针对身份证读卡终端证书是否有效的查询结果，如果查询结果为有效，认证安全控制模块获得身份证读卡终端证书有效提示；调度服务器至少接收身份证读卡终端证书，使用预存的根证书的公钥对身份证读卡终端证书签名信息进行解密，得到身份证读卡终端证书内容信

息第一摘要，对身份证读卡终端证书内容信息进行散列计算，得到身份证读卡终端证书内容信息第二摘要，判断身份证读卡终端证书内容信息第一摘要与身份证读卡终端证书内容信息第二摘要是否相同，如果相同，则判断身份证读卡终端证书合法，身份证读卡终端证书正常；调度服务器获得身份证读卡终端证书正常提示。

[0106] 步骤305还可以有如下可选实施方式：若身份证读卡终端证书正常，调度服务器根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

[0107] 步骤306还可以有如下可选实施方式：如果得到认证解密密钥密文，则调度服务器从第二预设存储区域内获得第二密钥。

[0108] 在本实施例中，步骤304a还可以有如下可选实施方式：调度服务器至少使用身份证读卡终端证书对身份证读卡终端签名信息进行验签操作；如果验签不通过，则获得身份证读卡终端签名异常提示；调度服务器还根据身份证读卡终端签名异常提示对身份证读卡终端发送的信息进行处理。

[0109] 需要说明的是，以上步骤304、步骤304a、步骤305和步骤306之间并不具有对应关系，也就是说，身份证读卡终端证书的有效性的结果由认证安全控制模块接收的情况下，对该证书的合法性验证还可以由调度服务器进行；在合法性验证由调度服务器进行的情况下，对身份证读卡终端签名信息的验签操作可以由调度服务器进行，也可以由认证安全控制模块进行，获得认证解密密钥密文的操作可以由调度服务器进行，也可以由认证安全控制模块进行，获得第二密钥的操作可以由调度服务器进行，也可以由认证安全控制模块进行。本实施例并不做限制。

[0110] 本实施例提供的身份证读卡终端与云认证平台的数据传输方法，云认证平台至少包括至少一个调度服务器和至少一个认证安全控制模块，由认证安全控制模块完成身份证读卡终端的证书认证，由调度服务器为身份证读卡终端提供认证安全控制模块调度服务，认证安全控制模块根据身份证读卡终端身份标识信息获得认证解密密钥密文，获得认证解密密钥后获得身份证读卡终端首次发送信息，即只有拥有认证加密密钥的身份证读卡终端才能与云认证平台进行数据传输，而只有拥有认证解密密钥的设备才能获得身份证读卡终端发送的数据，保障了身份证读卡终端与云认证平台的信息交互安全。在获得身份证读卡终端首次发送信息之后，云认证平台和身份证读卡终端分别生成第一会话密钥和第二会话密钥，并使用第一会话密钥和第二会话密钥对身份证读卡终端与云认证平台后续传输的数据进行加密，减少使用认证加密密钥和认证解密密钥的使用，提高认证加密密钥和认证解密密钥的安全性。

[0111] 实施例4

[0112] 本实施例提供了一种身份证读卡终端与云认证平台数据传输系统，本实施例的系统与实施例1属于同一发明构思，与该方法一一对应，因此，与实施例1相同之处在此不再赘述，仅针对不同之处进行如下说明。

[0113] 图2为本实施例提供的身份证读卡终端与云认证平台数据传输系统的架构示意图，如图2所示，该系统主要包括：身份证读卡终端401和云认证平台402。

[0114] 身份证读卡终端401，用于获得身份证读卡终端首次发送信息和认证加密密钥，使用认证加密密钥加密身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文；对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信

息密文摘要，并调用身份证读卡终端401的身份证读卡终端私钥加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名；读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台402，身份证读卡终端传输信息至少包括身份证读卡终端身份标识信息、身份证读卡终端首次发送信息密文、身份证读卡终端首次发送信息密文签名、和身份证读卡终端证书；获得第二会话密钥，使用第二会话密钥解密从云认证平台402接收的信息，使用第二会话密钥加密向云认证平台402发送的信息；

[0115] 云认证平台402，用于接收身份证读卡终端传输信息，验证身份证读卡终端证书是否正常；若身份证读卡终端证书正常，云认证平台402根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文；如果得到认证解密密钥密文，从第二预设存储区域内获得第二密钥，使用第二密钥解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，获得身份证读卡终端首次发送信息；获得第一会话密钥，使用第一会话密钥加密向身份证读卡终端401发送的信息，使用第一会话密钥解密从身份证读卡终端401接收的信息。

[0116] 在本实施例的一个可选实施方式中，系统还包括身份证；身份证读卡终端首次发送信息至少包括寻卡请求；身份证读卡终端401，还用于在身份证读卡终端401获得身份证读卡终端首次发送信息之前，发送寻卡指令至身份证；终端接收身份证发送的确认寻卡指令，身份证读卡终端401生成寻卡请求；身份证，用于接收到寻卡指令后发送确认寻卡指令信息至身份证读卡终端401。在本可选实施方式中，身份证读卡终端首次发送信息包括寻卡请求，在发送寻卡请求前获取确认寻卡指令信息，保障身份证读卡终端401在后续操作中顺利读取身份证信息。

[0117] 在本实施例的一个可选实施方式中，云认证平台402，具体用于接收对身份证读卡终端证书或身份证读卡终端证书编号进行查询的查询结果，查询结果为数字证书在线查询服务器对身份证读卡终端证书或身份证读卡终端证书编号进行在线查询是否有效得到的；如果查询结果为无效，云认证平台402获得身份证读卡终端证书异常提示，根据身份证读卡终端证书异常提示对身份证读卡终端401发送的信息进行处理；如果查询结果为有效，云认证平台402获得身份证读卡终端证书有效提示，云认证平台402使用根证书验证身份证读卡终端证书是否合法，如果身份证读卡终端证书合法，则云认证平台402获得身份证读卡终端证书正常提示，如果身份证读卡终端证书不合法，则云认证平台402获得身份证读卡终端证书异常提示。本实施方式中，对身份证读卡终端证书的有效性和合法性进行认证，保障了没有证书、证书失效或虚假身份证读卡终端401不能访问云认证平台402。

[0118] 在本实施例的一个可选实施方式中，云认证平台402，还用于对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，调用身份证读卡终端证书中的身份证读卡终端公钥解密身份证读卡终端首次发送信息密文签名，得到身份证读卡终端首次发送信息密文签名的明文，通过判断身份证读卡终端首次发送信息密文签名的明文与身份证读卡终端首次发送信息密文摘要是否相同，判断验签是否通过；若不相同，云认证平台402判断验签没有通过，云认证平台402获得身份证读卡终端签名异常提示；若相同，云认证平台402判断验签通过，云认证平台402根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。即云认证平台402进一步验证身份证

读卡终端首次发送信息密文签名，若没有通过验签，云认证平台402可以根据身份证读卡终端签名异常提示，根据该身份证读卡终端签名异常提示进行处理，若验签通过，则可进一步确认身份证读卡终端401的身份，进一步保障云认证平台402的安全。

[0119] 在本实施例的一个可选实施方式中，如果云认证平台402从第一预设存储区域无法得到认证解密密钥密文，云认证平台402获取身份证读卡终端解密密钥异常提示。在本实施方式中，若云认证平台402无法得到认证解密密钥，说明身份证读卡终端401存在异常，云认证平台402可进一步根据异常提示处理身份证读卡终端401传输的信息。

[0120] 在本实施例的一个可选实施方式中，身份证读卡终端首次发送信息包括安全控制信息；云认证平台402，还用于根据安全控制信息进行调度服务。可选地，安全控制信息可以是计数器信息，还可以是时间戳信息，身份证读卡终端401根据向云认证平台402发送信息的次数获得计数器信息，自身生成时间戳信息或从与身份证读卡终端401连接的设备中读取时间戳信息。云认证平台402接收到安全控制信息后，根据安全控制进行调度服务可以为，若相同身份证读卡终端401针对读取不同身份证发送的计数器信息无变化，可以判定该身份证读卡终端401可能被破解，将该身份证读卡终端401列入黑名单中，不再处理该身份证读卡终端401发送的信息，还可以为，若相同身份证读卡终端401针对读取不同身份证发送的时间戳信息无变化，可以判定该身份证读卡终端401可能被破解，将该身份证读卡终端401列入黑名单中，不再处理该身份证读卡终端401发送的信息，本实施例不做具体限制。

[0121] 在本实施例的一个可选实施方式中，云认证平台402，具体用于生成会话随机因子，将会话随机因子作为第一会话密钥，使用身份证读卡终端公钥加密第一会话密钥，得到第一会话密钥密文，将云认证平台第一传输信息发送至身份证读卡终端401，第一传输信息至少包括第一会话密钥密文；身份证读卡终端401，具体用于接收云认证平台第一传输信息，调用身份证读卡终端私钥解密第一会话密钥密文，得到第二会话密钥。在本实施方式中，第一会话密钥由云认证平台402生成，使用身份证读卡终端公钥加密后发送至身份证读卡终端401，由于解密第一会话密钥密文的解密密钥为身份证读卡终端私钥，而身份证读卡终端私钥是存储在身份证读卡终端401的安全芯片之中的，身份证读卡终端私钥是无法被导出的，也就是说，只有该身份证读卡终端401可以解密第一会话密钥密文，其他身份证读卡终端401或设备是无法解密第一会话密钥密文，无法得到第二会话密钥的，保障了第一会话密钥和第二会话密钥的安全性，保障了身份证读卡终端401与云认证平台402的通信安全。

[0122] 在本实施例的一个可选实施方式中，云认证平台402，具体用于将云认证平台402第二传输信息发送至身份证读卡终端401，云认证平台402第二传输信息中至少包括认证证书、认证验签信息和对认证验签信息进行签名得到的认证签名；使用认证证书私钥解密第二会话密钥密文，得到第一会话密钥。身份证读卡终端401，具体用于接收云认证平台第二传输信息，根据根证书判断认证证书是否合法，如果合法，使用认证证书公钥和认证验签信息对认证签名进行验签计算，如果验签通过，则生成第二随机因子，将第二随机因子作为第二会话密钥，使用认证证书公钥加密第二会话密钥，得到第二会话密钥密文；将第二会话密钥密文发送至云认证平台402。在本可选实施方式中，身份证读卡终端401首先验证云认证平台402的身份，可避免其他设备仿冒云认证平台402，验证通过后再生成第二会话密钥密文，并使用认证证书公钥加密，得到第一会话密钥，使得只有云认证平台402拥有认证证书

私钥时才可解密第二会话密钥密文，保障了第二会话密钥的安全。

[0123] 本实施例提供的身份证读卡终端401与云认证平台402的数据传输系统中，身份证读卡终端首次发送信息使用认证加密密钥进行加密，云认证平台402接收到身份证读卡终端首次发送信息密文后，根据身份证读卡终端身份标识信息获得认证解密密钥，获得身份证读卡终端首次发送信息，即只有拥有认证加密密钥的身份证读卡终端401才能与云认证平台402进行数据传输，而只有拥有认证解密密钥的设备才能获得身份证读卡终端401发送的数据，保障了身份证读卡终端401与云认证平台402的信息交互安全。在获得身份证读卡终端首次发送信息之后，云认证平台402和身份证读卡终端401分别生成第一会话密钥和第二会话密钥，并使用第一会话密钥和第二会话密钥对身份证读卡终端401与云认证平台402后续传输的数据进行加密，减少使用认证加密密钥和认证解密密钥的使用，提高认证加密密钥和认证解密密钥的安全性。

[0124] 实施例5

[0125] 本实施例提供的一种身份证读卡终端与云认证平台数据传输系统，与方法实施例2属于同一构思并一一对应，与实施例2相同之处不再赘述，以下仅针对本实施例与实施例2不同之处进行说明：

[0126] 图3为本实施例提供的身份证读卡终端与云认证平台数据传输系统的架构示意图，如图3所示，该系统主要包括：身份证读卡终端501、云认证平台502；云认证平台502包括：调度服务器5021、认证安全控制模块5022。

[0127] 身份证读卡终端501，用于获得身份证读卡终端首次发送信息和认证加密密钥，使用认证加密密钥加密身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文。对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，并调用身份证读卡终端501的身份证读卡终端私钥加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名。读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台502的调度服务器5021，身份证读卡终端传输信息至少包括身份证读卡终端身份标识信息、身份证读卡终端首次发送信息密文、身份证读卡终端首次发送信息密文签名和身份证读卡终端证书。获得第二会话密钥；使用第二会话密钥解密从认证安全控制模块5022接收的信息；身份证读卡终端501使用第二会话密钥加密向认证安全控制模块5022发送的信息。

[0128] 调度服务器5021，用于接收身份证读卡终端传输信息，验证身份证读卡终端证书是否正常。若身份证读卡终端证书正常，根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。如果得到认证解密密钥密文，则从第二预设存储区域内获得第二密钥。将认证解密密钥密文、第二密钥和身份证读卡终端首次发送信息密文发送至符合预设条件的认证安全控制模块5022。

[0129] 认证安全控制模块5022，用于使用第二密钥解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，获得身份证读卡终端首次发送信息，获得第一会话密钥，使用第一会话密钥加密向身份证读卡终端501发送的信息，使用第一会话密钥解密从身份证读卡终端501接收的信息。

[0130] 在本实施例中，还可以有如下可选实施方式：调度服务器5021，用于获得针对身份证读卡终端证书是否有效的查询结果，如果查询结果为有效，获得身份证读卡终端证书有

效提示;认证安全控制模块5022,用于至少接收身份证读卡终端证书,使用预存的根证书的公钥对身份证读卡终端证书签名信息进行解密,得到身份证读卡终端证书内容信息第一摘要,对身份证读卡终端证书内容信息进行散列计算,得到身份证读卡终端证书内容信息第二摘要,判断身份证读卡终端证书内容信息第一摘要与身份证读卡终端证书内容信息第二摘要是否相同,如果相同,则判断身份证读卡终端证书合法,身份证读卡终端证书正常;认证安全控制模块5022将身份证读卡终端证书正常提示发送至调度服务器5021。

[0131] 在本实施例中,还可以有如下可选实施方式:若身份证读卡终端证书正常,认证安全控制模块5022用于根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

[0132] 在本实施例中,还可以有如下可选实施方式:如果得到认证解密密钥密文,则认证安全控制模块5022用于从第二预设存储区域内获得第二密钥。

[0133] 在本实施例中,还可以有如下可选实施方式:认证安全控制模块5022,用于至少使用身份证读卡终端证书对身份证读卡终端签名信息进行验签操作;如果验签不通过,则生成身份证读卡终端签名异常提示,并发送至调度服务器5021;调度服务器5021,还用于根据身份证读卡终端签名异常提示对身份证读卡终端501发送的信息进行处理。

[0134] 需要说明的是,以上内容之间并不具有对应关系,也就是说,身份证读卡终端证书的有效性的结果由调度服务器5021接收的情况下,对该证书的合法性验证还可以由认证安全控制模块5022进行;在合法性验证由认证安全控制模块5022进行的情况下,对身份证读卡终端签名信息的验签操作可以由调度服务器5021进行,也可以由认证安全控制模块5022进行,获得认证解密密钥密文的操作可以由调度服务器5021进行,也可以由认证安全控制模块5022进行,获得第二密钥的操作可以由调度服务器5021进行,也可以由认证安全控制模块5022进行。本实施例并不做限制。在认证安全控制模块5022可以是安全芯片的情况下,使用根证书验证身份证读卡终端证书的合法性或验证身份证读卡终端签名信息更具有安全性更高。

[0135] 本实施例提供的身份证读卡终端501与云认证平台502的数据传输方法,云认证平台502至少包括至少一个调度服务器5021和至少一个认证安全控制模块5022,由调度服务器5021完成身份证读卡终端501的证书认证,并为身份证读卡终端501提供认证安全控制模块5022调度服务,调度服务器5021根据身份证读卡终端身份标识信息获得认证解密密钥密文,认证安全控制模块5022获得认证解密密钥后获得身份证读卡终端首次发送信息,即只有拥有认证加密密钥的身份证读卡终端501才能与云认证平台502进行数据传输,而只有拥有认证解密密钥的设备才能获得身份证读卡终端501发送的数据,保障了身份证读卡终端501与云认证平台502的信息交互安全。在获得身份证读卡终端首次发送信息之后,云认证平台502和身份证读卡终端501分别生成第一会话密钥和第二会话密钥,并使用第一会话密钥和第二会话密钥对身份证读卡终端501与云认证平台502后续传输的数据进行加密,减少使用认证加密密钥和认证解密密钥的使用,提高认证加密密钥和认证解密密钥的安全性。

[0136] 实施例6

[0137] 本实施例提供的一种身份证读卡终端与云认证平台数据传输系统,与实施例3属于同一构思并一一对应,与实施例3相同之处不再赘述,以下仅针对本实施例与实施例3不同之处进行说明:

[0138] 图3为本实施例提供的身份证读卡终端与云认证平台认证数据传输系统的架构示意图，如图3所示，该系统主要包括：身份证读卡终端501、云认证平台502；云认证平台502包括：调度服务器5021、认证安全控制模块5022。

[0139] 身份证读卡终端601，用于获得身份证读卡终端首次发送信息和认证加密密钥，使用认证加密密钥加密身份证读卡终端首次发送信息，得到身份证读卡终端首次发送信息密文。对身份证读卡终端首次发送信息密文进行散列计算，得到身份证读卡终端首次发送信息密文摘要，并调用身份证读卡终端601的身份证读卡终端私钥加密身份证读卡终端首次发送信息密文的摘要，得到身份证读卡终端首次发送信息密文签名。读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台602的调度服务器6021，身份证读卡终端传输信息至少包括身份证读卡终端身份标识信息、身份证读卡终端首次发送信息密文、身份证读卡终端首次发送信息密文签名和身份证读卡终端证书；获得第二会话密钥；使用第二会话密钥解密从认证安全控制模块6022接收的信息；使用第二会话密钥加密向认证安全控制模块6022发送的信息；

[0140] 调度服务器6021，用于接收身份证读卡终端传输信息，将身份证读卡终端传输信息发送至符合预设条件的认证安全控制模块6022；

[0141] 认证安全控制模块6022，用于验证身份证读卡终端证书是否正常，若身份证读卡终端证书正常，根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。如果得到认证解密密钥密文，则从第二预设存储区域内获得第二密钥。使用第二密钥解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，获得身份证读卡终端首次发送信息，获得第一会话密钥，使用第一会话密钥加密向身份证读卡终端601发送的信息，使用第一会话密钥解密从身份证读卡终端601接收的信息。

[0142] 在本实施例中，还可以有如下可选实施方式：认证安全控制模块6022获得针对身份证读卡终端证书是否有效的查询结果，如果查询结果为有效，认证安全控制模块6022获得身份证读卡终端证书有效提示；调度服务器6021至少接收身份证读卡终端证书，使用预存的根证书的公钥对身份证读卡终端证书签名信息进行解密，得到身份证读卡终端证书内容信息第一摘要，对身份证读卡终端证书内容信息进行散列计算，得到身份证读卡终端证书内容信息第二摘要，判断身份证读卡终端证书内容信息第一摘要与身份证读卡终端证书内容信息第二摘要是否相同，如果相同，则判断身份证读卡终端证书合法，身份证读卡终端证书正常；调度服务器6021获得身份证读卡终端证书正常提示。

[0143] 在本实施例的一个可选实施方式中，身份证读卡终端传输信息还包括身份证读卡终端601签名信息；认证安全控制模块6022，还用于至少使用身份证读卡终端证书对身份证读卡终端签名信息进行验签操作；如果验签不通过，则生成身份证读卡终端签名异常提示并发送至调度服务器6021；调度服务器6021还根据身份证读卡终端签名异常提示对身份证读卡终端601发送的信息进行处理。

[0144] 在本实施例中，还可以有如下可选实施方式：若身份证读卡终端证书正常，调度服务器6021根据身份证读卡终端身份标识信息从第一预设存储区域内读取认证解密密钥密文。

[0145] 在本实施例中，还可以有如下可选实施方式：如果得到认证解密密钥密文，则调度

服务器6021从第二预设存储区域内获得第二密钥。

[0146] 在本实施例中，还可以有如下可选实施方式：调度服务器6021至少使用身份证读卡终端证书对身份证读卡终端签名信息进行验签操作；如果验签不通过，则获得身份证读卡终端签名异常提示；调度服务器6021还根据身份证读卡终端签名异常提示对身份证读卡终端601发送的信息进行处理。

[0147] 需要说明的是，以上内容之间并不具有对应关系，也就是说，身份证读卡终端证书的有效性的结果由认证安全控制模块6022接收的情况下，对该证书的合法性验证还可以由调度服务器6021进行；在合法性验证由调度服务器6021进行的情况下，对身份证读卡终端601签名信息的验签操作可以由调度服务器6021进行，也可以由认证安全控制模块6022进行，获得认证解密密钥密文的操作可以由调度服务器6021进行，也可以由认证安全控制模块6022进行，获得第二密钥的操作可以由调度服务器6021进行，也可以由认证安全控制模块6022进行。本实施例并不做限制。

[0148] 本实施例提供的身份证读卡终端601与云认证平台602的数据传输系统，云认证平台602至少包括至少一个调度服务器6021和至少一个认证安全控制模块6022，由认证安全控制模块6022完成身份证读卡终端证书认证，由调度服务器6021为身份证读卡终端601提供认证安全控制模块6022调度服务，认证安全控制模块6022根据身份证读卡终端身份标识信息获得认证解密密钥密文，获得认证解密密钥后获得身份证读卡终端首次发送信息，即只有拥有认证加密密钥的身份证读卡终端601才能与云认证平台602进行数据传输，而只有拥有认证解密密钥的设备才能获得身份证读卡终端601发送的数据，保障了身份证读卡终端601与云认证平台602的信息交互安全。在获得身份证读卡终端首次发送信息之后，云认证平台602和身份证读卡终端601分别生成第一会话密钥和第二会话密钥，并使用第一会话密钥和第二会话密钥对身份证读卡终端601与云认证平台602后续传输的数据进行加密，减少使用认证加密密钥和认证解密密钥的使用，提高认证加密密钥和认证解密密钥的安全性。

[0149] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0150] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0151] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0152] 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以

是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

[0153] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0154] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0155] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。本发明的范围由所附权利要求及其等同限定。

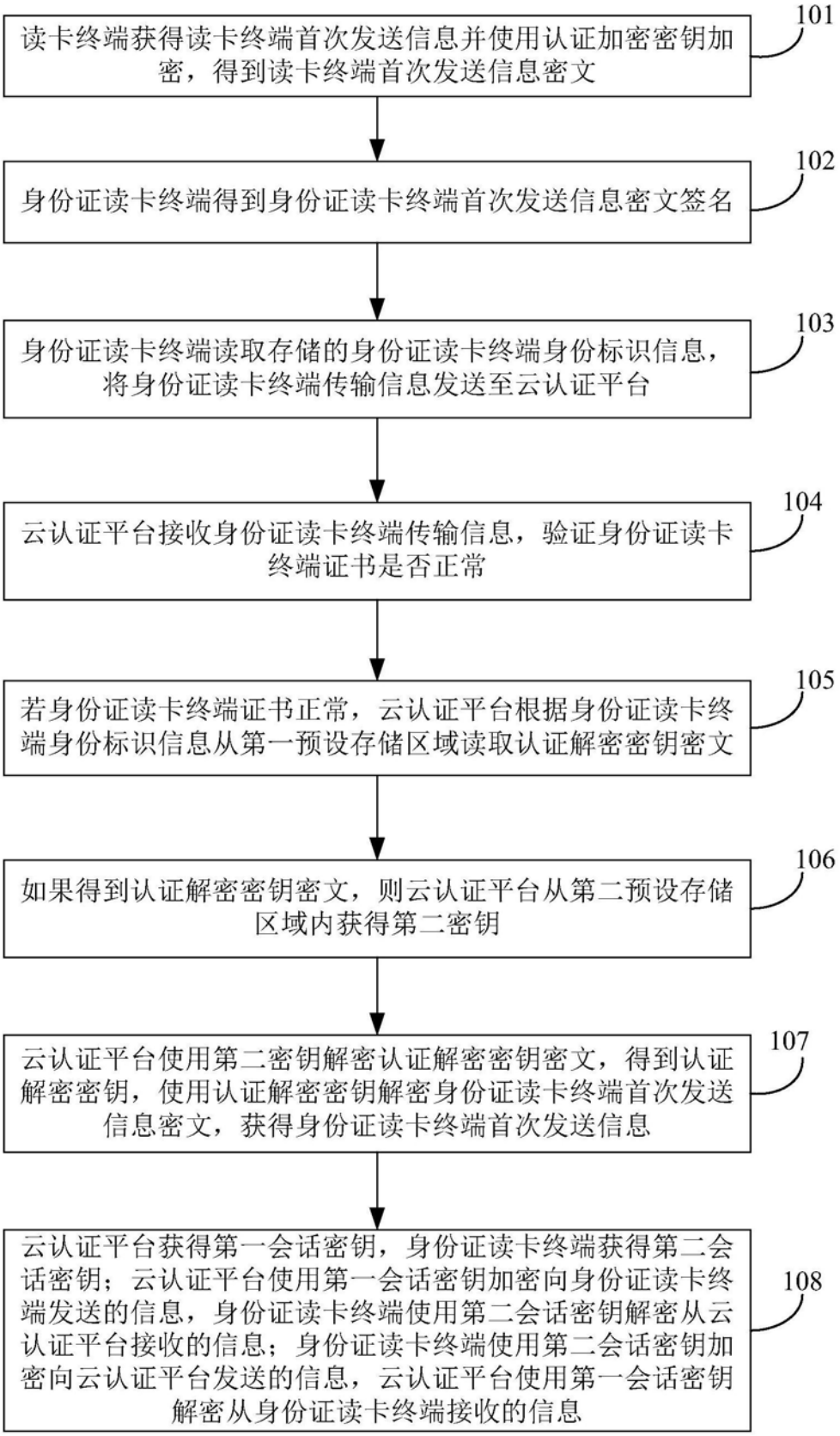

读卡终端获得读卡终端首次发送信息并使用认证加密密钥加密，得到读卡终端首次发送信息密文
101
身份证读卡终端得到身份证读卡终端首次发送信息密文签名
102
身份证读卡终端读取存储的身份证读卡终端身份标识信息，将身份证读卡终端传输信息发送至云认证平台
103
云认证平台接收身份证读卡终端传输信息，验证身份证读卡终端证书是否正常
104
若身份证读卡终端证书正常，云认证平台根据身份证读卡终端身份标识信息从第一预设存储区域读取认证解密密钥密文
105
如果得到认证解密密钥密文，则云认证平台从第二预设存储区域内获得第二密钥
106
云认证平台使用第二密钥解密认证解密密钥密文，得到认证解密密钥，使用认证解密密钥解密身份证读卡终端首次发送信息密文，获得身份证读卡终端首次发送信息
107
云认证平台获得第一会话密钥，身份证读卡终端获得第二会话密钥；云认证平台使用第一会话密钥加密向身份证读卡终端发送的信息，身份证读卡终端使用第二会话密钥解密从云认证平台接收的信息；身份证读卡终端使用第二会话密钥加密向云认证平台发送的信息，云认证平台使用第一会话密钥解密从身份证读卡终端接收的信息
108

图1

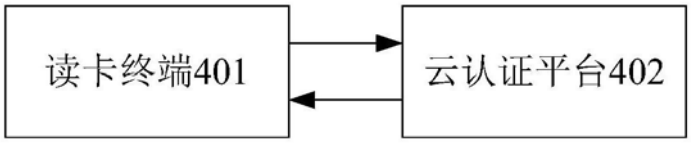

读卡终端401
云认证平台402

图2

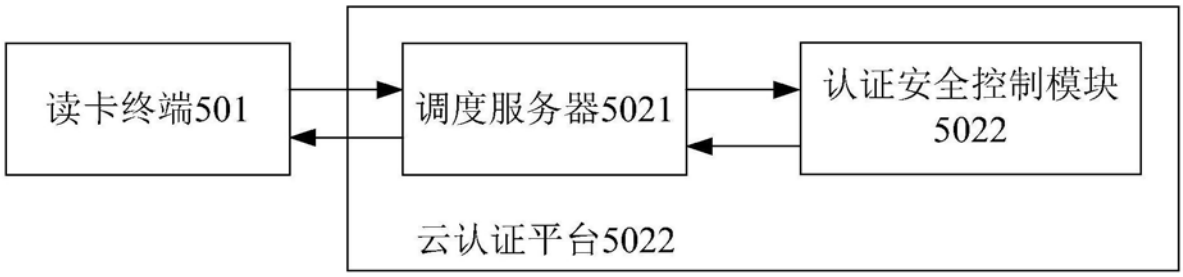

读卡终端501
调度服务器5021
认证安全控制模块5022
云认证平台5022

图3

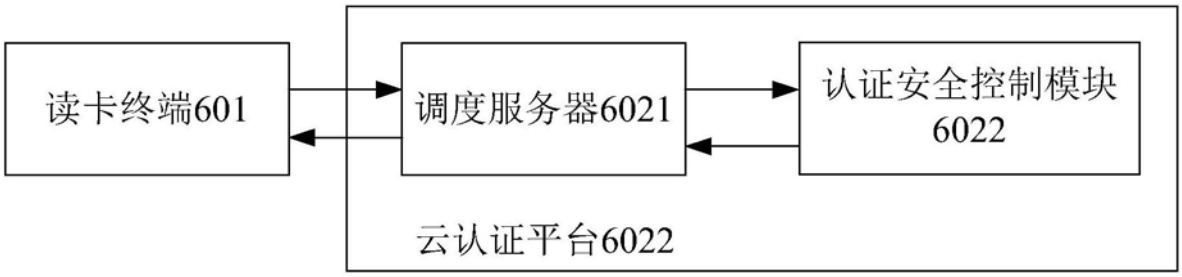

读卡终端601
调度服务器6021
认证安全控制模块6022
云认证平台6022

图4