(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 106537403 B
(45)授权公告日 2022.03.04

(21)申请号 201480053687.3
(22)申请日 2014.08.29
(65)同一申请的已公布的文献号
申请公布号 CN 106537403 A
(43)申请公布日 2017.03.22
(30)优先权数据
1315420.8 2013.08.29 GB
(85)PCT国际申请进入国家阶段日
2016.03.29
(86)PCT国际申请的申请数据
PCT/GB2014/052640 2014.08.29
(87)PCT国际申请的公布数据
WO2015/028824 EN 2015.03.05
(73)专利权人 利伯蒂沃特斯有限公司
地址 英国伦敦
(72)发明人 克里斯托弗·伊恩·约翰斯通
米歇尔·莱杜克
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 戚传江 金洁
(51)Int.Cl.
G06F 21/32(2006.01)
G06F 21/34(2006.01)
G06F 21/40(2006.01)
G06F 21/73(2006.01)
(56)对比文件
US 2007066288 A1,2007.03.22
US 2008104393 A1,2008.05.01
US 2005278775 A1,2005.12.15
US 2010323664 A1,2010.12.23
US 2010323664 A1,2010.12.23
审查员 周燕

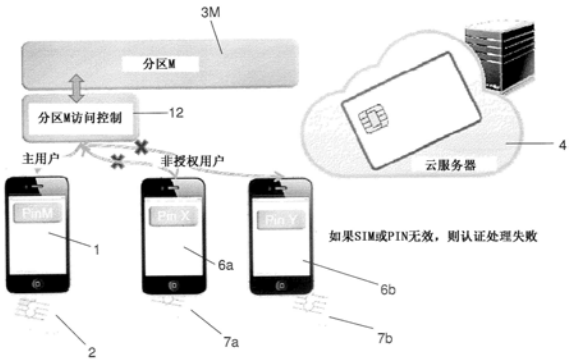
权利要求书8页 说明书22页 附图11页

(54)发明名称

用于从多个装置访问数据的系统

(57)摘要

一种在装置上访问数据的方法,其中数据远离装置存储或者存储在可移动存储设备中,所述方法包括以下步骤:(i)从装置发送访问数据的请求,请求包括与装置相关联的安全元件或存储卡的识别码;(ii)至少部分地基于识别码,验证是将允许还是将拒绝对数据的访问;以及(iii)因此允许或拒绝装置对数据的访问。



CN 106537403 B

1.一种在装置上访问数据的方法,其中所述装置包括安全元件,其中所述数据存储在所述装置中、或者远离所述装置存储在远程存储设备中、或者存储在可移动存储设备中,所述方法包括以下步骤:

(i) 在所述装置上输入密码或PIN;

(ii) 在所述装置的所述安全元件中进行所述密码或PIN的验证;

(iii) 如果所述验证成功,从所述装置向远离所述装置的数据访问控制器发送访问所述数据的请求,所述请求包括所述验证的结果以及所述安全元件的识别码;

(iv) 至少部分地基于所述识别码,验证是将允许还是将拒绝对所述数据的访问;以及

(v) 因此允许或拒绝所述装置对所述数据的访问,

其中,所述方法进一步包括,在步骤(i)-(v)之前,将所述安全元件的所述识别码登记到所述数据,并且能够将一个以上的安全元件的识别码登记到所述数据。

2.根据权利要求1所述的方法,其中所述数据存储在云中。

3.根据权利要求1所述的方法,其中所述请求包括表示所述装置的用户固有的事物的数据,并且步骤(iv)还包括基于表示所述装置的用户固有的事物的数据,验证是将允许还是将拒绝对所述数据的访问,和/或

其中所述请求包括包含位置的数据,并且步骤(iv)还包括基于所述位置验证是将允许还是将拒绝对所述数据的访问;和/或

其中所述请求包括包含时间的数据,并且步骤(iv)还包括基于所述时间验证是将允许还是将拒绝对所述数据的访问;和/或

其中所述请求包括指示所述用户是群组一部分的数据,并且步骤(iv)包括基于所述群组的另一个成员是否正在访问所述数据,验证是将允许还是将拒绝对所述数据的访问。

4.根据权利要求3所述的方法,其中表示所述装置的用户固有的事物的数据包括表示关于所述用户的遗传学和/或生物统计学信息的数据。

5.根据权利要求1所述的方法,其中所述安全元件是与所述装置相关联的SIM、虚拟SIM、SIM软件、TPM、SE、TEE、微型SD、USB密钥或智能卡。

6.根据权利要求1所述的方法,其中所述数据存储在与所述装置相关联的分区中,并且所述请求包括指定所述分区的数据。

7.根据权利要求1所述的方法,其中所述数据帮助连接到第三方服务。

8.根据权利要求6所述的方法,其中指定所述分区的所述数据包括:

表示所述装置的用户固有的事物的数据。

9.根据权利要求8所述的方法,其中表示所述装置的用户固有的事物的数据包括表示关于所述用户的遗传学和/或生物统计学信息的数据。

10.根据权利要求1所述的方法,其中所述装置是电话、平板电脑、笔记本电脑、台式电脑、TV、机顶盒、相机、汽车、游戏机、眼镜、手表、Chromecast、智能计量仪或者能够向远程装置发送和接收数据的任何其他装置。

11.一种控制从装置访问数据的方法,所述方法由远离所述装置的数据访问控制器来执行,其中所述装置包括安全元件,其中所述数据存储在所述装置中、或者远离所述装置存储、或者存储在可移动存储设备中,所述方法包括以下步骤:

(i) 从所述装置接收访问所述数据的请求,所述请求包括在所述装置输入的密码或

PIN的验证的结果以及所述安全元件的识别码，所述验证由所述安全元件执行；

(ii) 至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问；以及

(iii) 因此允许或拒绝所述装置对所述数据的访问，

其中，所述方法进一步包括，在步骤(i)-(iii)之前，将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

12.一种用于由装置控制访问数据的数据访问控制器，其中所述装置包括安全元件，并且其中所述数据存储在所述装置中、或者远离所述装置存储、或者存储在可移动存储设备中，所述数据访问控制器被布置为执行以下步骤：

(i) 从所述装置接收访问所述数据的请求，所述请求包括在所述装置输入的密码或PIN的验证的结果以及所述安全元件的识别码，所述验证由所述安全元件执行；

(ii) 至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问；以及

(iii) 因此允许或拒绝所述装置对所述数据的访问，

其中，所述数据访问控制器远离希望访问所述数据的装置，

并且其中，所述数据访问控制器被布置为，在步骤(i)-(iii)之前，将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

13.一种包括装置和数据访问控制器的系统，所述数据访问控制器用于控制从所述装置访问数据，其中所述装置包括安全元件，并且其中所述数据存储在所述装置中、或者远离所述装置存储、或者存储在可移动存储设备中，其中所述装置被布置为：

接收在所述装置上输入的密码或PIN；

在所述安全元件中进行所述密码或PIN的验证；

如果所述验证成功，向所述数据访问控制器发送访问所述数据的请求，所述请求包括所述验证的结果以及所述安全元件的识别码；

以及所述数据访问控制器被布置为至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问，以及因此允许或拒绝所述装置对所述数据的访问，

其中，所述数据访问控制器远离希望访问所述数据的装置，

并且其中，所述数据访问控制器被布置为将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

14.一种存储计算机程序的计算机可读介质，所述计算机程序用于控制从装置访问数据，其中所述装置包括安全元件，并且其中所述数据存储在所述装置中、或者远离所述装置存储、或者存储在可移动存储设备中，所述程序被配置为在其由远离所述装置的数据访问控制器的处理器执行时执行以下步骤：(i) 从所述装置接收访问所述数据的请求，所述请求包括在所述装置输入的密码或PIN的验证的结果以及所述安全元件的识别码，所述验证由所述安全元件执行；(ii) 至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问；以及(iii) 因此允许或拒绝所述装置对所述数据的访问，

其中，所述程序进一步被配置为在步骤(i)-(iii)之前执行以下步骤：将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

15.一种将装置登记到访问控制器使得所述装置可经由所述访问控制器访问数据的方法，其中所述装置包括安全元件，所述数据存储在所述装置中、或者远离装置存储、或者存

储在可移动存储设备中，其中所述方法包括：

在所述装置上输入密码或PIN；

在所述装置的所述安全元件中进行所述密码或PIN的验证；

如果所述验证成功，发送为了访问数据而登记装置的请求，所述请求包括所述验证的结果以及所述安全元件的识别码；

检查是否将允许对所述数据的访问；以及

如果将允许访问，则针对待访问的所述数据登记所述识别码，

其中，所述数据访问控制器远离希望访问所述数据的装置，

并且其中，所述数据访问控制器被布置为将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

16.根据权利要求15所述的方法，其中所述请求的形式为电子邮件或SMS。

17.根据权利要求15所述的方法，进一步包括向管理者装置发送与所述请求有关的信息。

18.根据权利要求17所述的方法，其中所述管理者装置决定是否将许可对所述数据的访问。

19.一种将装置登记到访问控制器，使得所述装置可经由所述访问控制器访问数据的方法，其中所述装置包括安全元件，所述数据存储在所述装置中、或者远离装置存储或者存储在可移动存储设备中，其中所述方法包括：

接收为了访问数据而登记装置的请求，所述请求包括在所述装置输入的密码或PIN的验证的结果以及所述安全元件的识别码，所述验证由所述安全元件执行；

检查是否将允许对所述数据的访问；以及

如果将允许访问，则针对待访问的所述数据登记所述识别码，

其中，所述访问控制器远离希望访问所述数据的装置，

并且其中，所述访问控制器被布置为将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

20.一种用于控制将装置登记到对数据的访问的数据访问控制器，所述控制器被布置为执行以下步骤：

接收为了访问数据而登记装置的请求，其中所述装置包括安全元件，所述请求包括在所述装置输入的密码或PIN的验证的结果以及所述安全元件的识别码，所述验证由所述安全元件执行；

检查是否将允许对所述数据的访问；以及

如果将允许访问，则针对待访问的所述数据登记所述识别码，

其中，所述数据访问控制器远离希望访问所述数据的装置，

并且其中，所述数据访问控制器被布置为将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

21.一种包括装置和数据访问控制器的系统，所述数据访问控制器用于控制将装置登记到对数据的访问，其中所述装置包括安全元件，所述数据访问控制器被布置为执行以下步骤：

从所述装置接收为了访问数据而登记装置的请求，所述请求包括在所述装置输入的密

码或PIN的验证的结果以及所述安全元件的识别码，所述验证由所述安全元件执行；

检查是否将允许对所述数据的访问；以及

如果将允许访问，则针对待访问的所述数据登记所述识别码，

其中，所述数据访问控制器远离希望访问所述数据的装置，

并且其中，所述数据访问控制器被布置为将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

22.一种存储计算机程序的计算机可读介质，所述计算机程序用于控制将装置登记到对数据的访问，所述程序被配置为在其由数据访问控制器的处理器执行时执行以下步骤：

从具有安全元件的装置接收为了访问数据而登记装置的请求，所述请求包括在所述装置输入的密码或PIN的验证的结果以及所述安全元件的识别码，所述验证由所述安全元件执行；

检查是否将允许对所述数据的访问；以及

如果将允许访问，则针对待访问的所述数据登记所述识别码，

其中，所述数据访问控制器远离希望访问所述数据的装置，

并且其中，所述数据访问控制器被布置为将所述安全元件的所述识别码登记到所述数据，并且能够将一个以上的安全元件的识别码登记到所述数据。

23.一种第一装置允许第二装置访问数据的方法，其中所述数据远离所述第一和第二装置存储，所述方法包括：

从所述第一装置向所述第二装置发送邀请以访问所述数据；

在所述第二装置上接收访问所述数据的邀请，所述邀请包括口令、代码或PIN；

从所述第二装置发送访问所述数据的请求，所述请求包括所述口令、代码或PIN；

至少部分地基于所述口令、代码或PIN，验证是将允许还是将拒绝由所述第二装置对所述数据的访问；以及

因此允许或拒绝所述第二装置对所述数据的访问，

其中所述口令、代码或PIN在所述第一装置中生成，并且所述方法进一步包括：验证允许所述第一装置邀请进一步的装置访问所述数据，并且然后将所生成的口令、代码或PIN登记到待访问的所述数据，

或者其中所述口令、代码或PIN通过控制对所述数据的访问的装置远离所述第一装置和第二装置两者生成，并且所述方法进一步包括：从所述第一装置发送对于待生成的所述口令、代码或PIN的请求，其中待生成的所述口令、代码或PIN仅在已经验证允许所述第一装置邀请进一步的装置访问所述数据之后生成，其中验证允许所述第一装置邀请进一步的装置访问所述数据的步骤包括验证与所述装置相关联的安全元件的识别码。

24.根据权利要求23所述的方法，其中所述口令、代码或PIN通过随机数生成器生成。

25.根据权利要求23的方法，其中所述口令、代码或PIN是一次性口令。

26.根据权利要求23所述的方法，其中所述口令、代码或PIN仅在指定的时间段内有效。

27.根据权利要求23所述的方法，其中验证允许所述第一装置邀请进一步的装置访问所述数据的步骤进一步包括验证从所述第一装置发送的指定分区的数据。

28.根据权利要求27所述的方法，其中指定所述分区的数据包括以下的一个或多个：

-PIN或密码；以及

-表示对所述装置的用户是固有事物的数据。

29.根据权利要求28所述的方法，其中所述固有事物的数据是遗传学和/或生物统计学信息。

30.一种包括第一装置、第二装置和数据访问控制器的系统，所述第一装置被布置为邀请所述第二装置访问数据，其中所述数据远离所述第二装置存储或者存储在可移动存储设备中，

其中所述第一装置被布置为向所述第二装置发送访问所述数据的邀请，所述邀请包括口令、代码或PIN；

所述第二装置被布置为发送访问所述数据的请求，所述请求包括所述口令、代码或PIN；以及

所述数据访问控制器被布置为至少部分地基于所述口令、代码或PIN，验证是将允许还是将拒绝对所述数据的访问，以及因此允许或拒绝所述第二装置对所述数据的访问，

其中所述口令、代码或PIN在所述第一装置中生成，并且其中所述系统被配置为验证允许所述第一装置邀请进一步的装置访问所述数据，并且然后将所生成的口令、代码或PIN登记到待访问的所述数据，

或者其中所述口令、代码或PIN通过所述数据访问控制器远离所述第一装置和第二装置两者生成，并且其中所述系统被配置为从所述第一装置发送对于待生成的所述口令、代码或PIN的请求，其中待生成的所述口令、代码或PIN仅在已经验证允许所述第一装置邀请进一步的装置访问所述数据之后生成，其中验证允许所述第一装置邀请进一步的装置访问所述数据的步骤包括验证与所述装置相关联的安全元件的识别码。

31.根据权利要求1所述的方法，包括：仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

32.根据权利要求31所述的方法，其中所述进一步的装置是登记到所述数据的管理者装置。

33.根据权利要求31所述的方法，在步骤 (v)之前进一步包括：检查是否至少一个进一步的装置正在访问所述数据。

34.根据权利要求11所述的方法，包括：仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

35.根据权利要求12所述的数据访问控制器，被配置为：仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

36.根据权利要求35所述的数据访问控制器，其中所述数据访问控制器被布置为在执行步骤(iii)之前检查是否至少一个进一步的装置正在访问所述数据。

37.根据权利要求13所述的系统，所述数据访问控制器被布置为：仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

38.根据权利要求37所述的系统，其中所述装置被布置为将访问所述数据的请求发送给所述数据访问控制器。

39.根据权利要求37所述的系统，其中所述数据访问控制器被布置为在执行步骤(v)之前检查是否至少一个进一步的装置正在访问所述数据。

40.根据权利要求14所述的存储计算机程序的计算机可读介质，所述程序被配置为：仅

当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

41.根据权利要求40所述的存储计算机程序的计算机可读介质，其中所述程序被进一步配置为在进行步骤(v)之前检查是否至少一个进一步的装置正在访问所述数据。

42.一种从装置访问基于云或基于网络的第三方服务的方法，所述方法包括以下步骤：

(i) 从所述装置向与所述装置相关联的基于云的分区发送请求，所述分区包括用于帮助连接到所述第三方服务的数据，所述请求包括与所述装置相关联的安全元件的识别码；

(ii) 至少部分地基于所述识别码，验证是将允许还是将拒绝对所述分区的访问；以及

(iii) 因此允许或拒绝所述装置对所述分区的访问；以及在允许对所述分区的访问之后：

(iv) 将凭证传输给所述第三方服务。

43.根据权利要求42所述的方法，其中所述请求包括在所述装置上输入的密码或PIN，并且步骤(ii)还包括基于所述密码或PIN验证是将允许还是将拒绝对所述数据的访问。

44.根据权利要求42或43所述的方法，其中所述请求包括表示所述装置的用户固有的事物的数据，并且步骤(ii)还包括基于表示所述装置的用户固有的事物的数据验证是将允许还是将拒绝对所述数据的访问。

45.根据权利要求44所述的方法，其中表示所述装置的用户固有的事物的数据包括表示关于所述用户的遗传学和/或生物统计学信息的数据。

46.根据权利要求42所述的方法，其中传输所述凭证的步骤包括以下步骤：

在所述装置的安全元件与关联于所述分区的安全元件之间执行相互认证处理；

在所述装置的安全元件与关联于所述分区的安全元件之间创建安全通道。

47.根据权利要求46所述的方法，其中传输所述凭证的步骤包括通过所述安全通道从所述装置的安全元件向所述分区传输所述凭证的步骤。

48.根据权利要求47所述的方法，其中在通过所述安全通道传输之前将所述凭证加密。

49.根据权利要求46或47所述的方法，其中传输所述凭证的步骤包括以下步骤：

在所述装置的安全元件与关联于所述第三方服务的安全元件之间执行相互认证处理；

在所述装置的安全元件与关联于所述第三方服务的安全元件之间创建安全通道；

将所述凭证加密；以及

通过所述安全通 道从所述装置的安全元件向关联于所述第三方服务的安全元件传输所加密的凭证。

50.根据权利要求49所述的方法，其中所述第三方服务请求访问第三方服务的特定PIN码，并且所述PIN码通过在所述安全元件与关联于所述第三方服务的安全元件之间创建的安全通道来传输。

51.根据权利要求46所述的方法，其中在顺利完成所述认证处理之后自动提供访问第三方服务的凭证和/或第三方服务所请求的形式填充数据。

52.根据权利要求46所述的方法，其中在顺利完成所述认证处理之后在第三方服务中自动启动应用。

53.根据权利要求42所述的方法，其中所述安全元件是与所述装置相关联的SIM、虚拟SIM、SIM软件、TPM、SE、TEE、微型SD、存储卡、USB密钥或智能卡。

54.根据权利要求42所述的方法，其中所述凭证被安全地存储在所述分区中。

55.根据权利要求42所述的方法，其中所述凭证被安全地存储在所述装置的安全元件中。

56.根据权利要求42所述的方法，其中所述凭证从所述安全元件提供给所述分区。

57.根据权利要求42所述的方法，包括用户注册处理，由此用户为使用所述第三方服务进行注册，所述用户注册处理包括以下步骤：

收集用于访问所述第三方服务的凭证和/或形式填充数据；以及

安全地存储所述凭证和/或形式填充数据。

58.根据权利要求42所述的方法，包括用户注册处理，由此用户为使用所述第三方服务进行注册，所述用户注册处理包括以下步骤：

初始化相互认证处理；以及

选择所述第三方服务。

59.根据权利要求58所述的方法，其中在允许对所述分区的访问之后通过所述分区自动生成所述凭证。

60.根据权利要求59所述的方法，其中所述自动产生的凭证被周期性地或者按需更新。

61.根据权利要求59或60所述的方法，其中所自动生成的凭证不同于通过其他器件访问所述服务时使用的凭证。

62.根据权利要求59或60所述的方法，其中根据用户安全策略或第三方服务安全策略来调整所自动生成的凭证的复杂性和复杂度。

63.根据权利要求42所述的方法，其中在所述安全元件上存储多个小程序，以及在生成所述凭证之前每个小程序执行分离的认证处理，以访问与给定小程序有关的服务。

64.根据权利要求42所述的方法，其中所述凭证包括用户ID和/或口令。

65.根据权利要求42所述的方法，其中所述装置是用于创建新凭证或者更新凭证以访问所述第三方服务的主装置。

66.根据权利要求42所述的方法，其中所述装置充当允许进一步的装置也访问所述第三方服务的主装置，其中在所述装置上生成并显示访问代码，或者通过SMS或电子邮件将所述访问代码发送给用户，以及所述用户使用所述进一步的装置将所述访问代码输入至与所述第三方服务相关联的网站。

67.根据权利要求66所述的方法，其中由在所述装置上运行的应用生成所述访问代码，和/或其中所述访问代码是时间敏感的。

68.根据权利要求42所述的方法，包括以下步骤：将进一步的装置连接到所述分区。

69.根据权利要求42所述的方法，包括以下步骤：同步分区内容和/或用于所连接的装置的凭证。

70.根据权利要求42所述的方法，其中要求识别和/或访问所述分区的信息是从NFC标签或信号发射装置读取的。

71.根据权利要求70所述的方法，其中所述信号发射装置是蓝牙、BLE、wifi、zigbee、NFC、GPS、或ISO 14443装置，或者利用任何其他形式的无接触通信的装置。

72.根据权利要求42所述的方法，其中所述分区存储用于电话或消息服务的唯一标识符。

73.根据权利要求72所述的方法，其中所述电话或消息服务是移动电话的电话服务、

VOIP服务、或者即时消息服务。

74.根据权利要求72或73所述的方法，其中将所述唯一标识符链接到电话或消息服务标识符。

75.根据权利要求74所述的方法，其中所述电话或消息服务标识符是用户名和关联口令或者国家或国际电话号码。

76.根据权利要求74所述的方法，其中所述唯一标识符与电话和所述消息服务标识符之间的映射可以存储在所述装置的安全元件中，或者可以存储在所述分区中，或者可以通过移动网络运营商来存储。

77.根据权利要求72所述的方法，其中根据用户的位置来激活与特定服务相关联的唯一标识符。

78.根据权利要求1所述的方法，进一步包括以下步骤：

(iv) 在所述装置与所述远程或可移动存储设备之间执行相互认证处理；

(v) 在所述装置与所述远程或可移动存储设备之间创建安全通道；以及

(vi) 在两个所述装置之间传输数据。

79.根据权利要求78所述的方法，其中所述认证包括两个或更多的因素，所述因素选自以下列表：

-与所述装置相关联的智能对象的识别码；

-密码或PIN；

-遗传学或生物统计学识别数据；

-位置；

-时间；或

-另一个成员或者用户所属的群组是否正在访问数据。

80.根据权利要求79所述的方法，其中所述另一个成员是管理者。

81.根据权利要求78所述的方法，其中所述认证包括两个因素，所述因素是：

与所述装置相关联的智能对象的识别码；以及

密码或PIN。

82.根据权利要求79或81所述的方法，其中所述智能对象包括安全元件。

83.一种控制通过装置访问基于云或基于网络的第三方服务的方法，所述方法包括以下步骤：

(i) 从所述装置接收对与所述装置相关联的基于云的分区的请求，所述分区包括用于帮助连接到所述第三方服务的数据，所述请求包括安全元件的识别码；

(ii) 至少部分地基于所述识别码，验证是将允许还是将拒绝对所述分区的访问；

(iii) 因此允许或拒绝所述装置对所述分区的访问；以及，在允许对所述分区的访问时：

(iv) 将凭证传输给所述第三方服务。

84.一种存储计算机程序的计算机可读介质，所述计算机程序用于控制通过装置访问基于云或基于网络的第三方服务，所述程序被配置为在其由处理器执行时执行权利要求83的方法。

用于从多个装置访问数据的系统

技术领域

[0001] 本发明涉及数据访问领域。更具体地，本发明涉及用于从多个装置访问数据的系统。

背景技术

[0002] 本领域公知向用户提供基于云的数据存储设备。可以从多个装置访问这种基于云的存储设备。

[0003] 例如，Dropbox™是一种向用户提供用于他们数据的基于云的远程存储设备的系统。数据可包括例如用移动电话拍摄的照片。，一旦将数据从移动电话上传到例如远程存储设备中，就可以从诸如笔记本电脑或台式电脑的连接到互联网的其他装置()访问该数据。用256位AES加密算法加密所存储的数据，并且在许可访问他们的数据之前，用户必须经由网站来输入他们登记的电子邮件地址和口令。

[0004] 但是，这种系统的一个问题是，如果第三方发现了用户的电子邮件地址和口令，那么第三方也可从任何装置访问所存储的数据。因此，需要一种可以从一个或多个装置访问的更安全的远程存储设备系统。

发明内容

[0005] 根据本发明的第一方面，提供一种在装置上访问数据的方法，其中所述数据远离所述装置存储或者存储在可移动存储设备中，所述方法包括以下步骤：(i)从所述装置发送访问所述数据的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；(ii)至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此允许或拒绝所述装置对所述数据的访问。

[0006] 仅当提供与装置相关联的正确的识别码才因此允许对数据的访问。因此可以防止未授权装置访问数据，因为它们不能提供正确的识别码。

[0007] 如上所述，请求包括与装置相关联的安全元件或存储卡的识别码。但是，可以按照修改的形式将识别码包括在请求中，例如，按照加密的形式和/或与一个或多个进一步的代码、数据或信息组合。

[0008] 待访问的数据包括能够存储在存储器中的任何形式数据。例如，它可包括一个或多个文件数据、数据库、应用、软件、和/或服务。下面讨论服务的一些示例。

[0009] 优选地，经由安全通道发送识别码。替代或附加地，可将识别码加密。这能够使得处理更安全，并帮助防止识别码被拦截和/或被第三方发现。

[0010] 进一步的(附近或替代的)可能性将是基于安全元件或存储卡的识别码以及来自装置的一个或多个其他元件或代码，在装置上生成代码。然后可以发送这个生成的代码，并且例如这个生成的代码仅对于特定会话有效。因此即使它被拦截，也将对第三方没有用处。

[0011] 可将数据存储在可移动存储设备装置、云、或远程数据存储设备的其他形式中。例如，可将数据存储在USB密钥、笔记本电脑、计算机服务器(个人或公司)、计算机网络(个人

或公司)、平板电脑或电话中。

[0012] 请求还可包括在装置上输入的密码或PIN并且步骤(ii)还可包括基于密码或PIN验证是将允许还是将拒绝对数据的访问。因此,为了访问数据可以要求双因素认证。

[0013] 可通过与装置相关联的安全元件或存储卡(例如SIM或虚拟SIM)(首先)验证密码或PIN。

[0014] 替代或附加地,可以远离装置验证密码或PIN,例如在被布置为控制对数据的访问的访问控制器上。

[0015] 在通过安全元件或存储卡验证密码或PIN的情况下,优选地按照安全和/或受保护的方式将该验证的结果传送给例如访问控制器,例如经由安全通道。例如,可按照证书、加密代码、会话代码或加密会话代码的形式传送结果。优选地,仅在验证成功时,即,在输入正确的密码或PIN时,传送验证的结果。

[0016] 在远离装置验证密码或PIN的情况下,例如在访问控制器上,优选按照安全和/或受保护的方式将密码或PIN传送给例如访问控制器。例如,可经由安全通道和/或在传送之前将密码或PIN加密来传送密码或PIN。

[0017] 替代或附加地,请求可包括表示装置的用户固有的事物的数据,并且步骤(ii)还可包括基于表示装置的用户固有的事物的数据验证是将允许还是将拒绝对数据的访问。因此,为了访问数据可以要求双因素认证或三因素认证,并且仅许可授权用户对数据的访问。

[0018] 例如,表示装置的用户固有的事物的数据可包括表示关于用户的遗传学和/或生物统计学信息的数据,诸如指纹或虹膜数据。

[0019] 替代或附加地,对于使用PIN和/或表示装置的用户固有的事物的数据的认证(使用识别码的双因素认证或三因素认证),以下形式的认证是可能的。

[0020] 请求可包括包含位置的数据(即,用户尝试由其访问数据的地方),并且步骤(ii)还可包括基于位置验证是将允许还是将拒绝对数据的访问。

[0021] 请求可包括包含时间的数据(即,用户尝试访问数据的时间),并且步骤(ii)还包括基于时间验证是将允许还是将拒绝对数据的访问。

[0022] 请求可包括指示用户是群组一部分的数据,并且步骤(ii)还包括基于群组的另一个成员(例如管理者)是否正在访问数据,验证是将允许还是将拒绝对数据的访问。

[0023] 安全元件或存储卡例如是“智能对象”或者具有唯一识别码的安全或防篡改硬件装置,识别码本身理论上也是安全和防篡改的。安全元件或存储卡例如可以是SIM、虚拟SIM、SIM软件、TPM(可信平台模块)、SE(安全元件)、TEE(可信执行环境)、微型SD、存储卡、USB密钥或智能卡。

[0024] 如上所述,安全元件的一个普通示例是SIM卡。在所有GSM移动装置以及在智能电话中都提供SIM卡。但是,SIM卡是由电话网络提供,因此不易访问(其含义是不易将小程序下载至SIM,或修改SIM)。此外,装置的操作系统可能没有与SIM交互的软件工具包。为了克服上述缺点,可以下载虚拟SIM(软件SIM),虚拟SIM能够作为应用被载入至装置上。虚拟SIM表现得像实体SIM,意思是它能够接收和处理小程序,并安全地存储小程序、凭证、密钥和算法等等。

[0025] 安全元件或存储卡可以是本地形式、远程形式或可移动形式的存储器的任何一种。

[0026] 优选将安全元件或存储卡的识别码妥善保护，并存储在例如安全元件或存储卡的保险箱中。

[0027] 在本发明的优选实施例中，安全元件或存储卡用于创建安全通道，和/或加密识别码和/或PIN或密码。

[0028] 可将数据存储在与装置相关联的分区中，例如存储器分区，并且请求可包括指定例如待访问的分区的分区的数据。

[0029] 在安全元件或存储卡与分区之间可创建安全通道，然后安全通道能够用于在装置与分区之间传送数据、文件、凭证或其他形式填充数据。

[0030] 因此，所述方法可包括步骤：(iv)在装置与远程或可移动存储设备之间执行相互认证处理；(v)在装置与远程或可移动存储设备之间创建安全通道。

[0031] 认证可包括两个或更多因素，因素选自以下列表：

[0032] 与所述装置相关联的智能对象(存储卡或安全元件)的识别码；

[0033] 密码或PIN；

[0034] 遗传学或生物统计学识别数据；

[0035] 位置；

[0036] 时间；或

[0037] 另一个成员(例如管理者)或者用户所属的群组是否正在访问数据。

[0038] 装置可以从NFC(近场通信)标签、生物统计学传感器/读卡器或信号发射装置读取代码，以识别并访问分区。NFC标签、生物统计学传感器/读卡器或信号发射装置可以向装置提供选择分区(否则将需要由用户输入分区)并最终打开它所必须的信息。

[0039] 信号发射装置可以是蓝牙、BLE(蓝牙低功耗)、wifi、zigbee、NFC、GPS、或ISO 14443装置，或者使用任何其他形式的无接触通信的装置。

[0040] 分区可存储用于帮助连接到基于网络或基于云的第三方服务(例如银行提供的网上银行或物流公司提供的包裹跟踪)的数据。

[0041] 指定分区的数据可包括以下的一个或多个：PIN或密码；以及表示装置的用户固有的事物的数据。表示装置的用户固有的事物的数据例如可包括表示关于用户的遗传学和/或生物统计学信息的数据。

[0042] 装置可以是或包括电话(移动或固定)、智能电话、平板电脑、笔记本电脑、台式电脑、TV、机顶盒、相机、汽车、游戏机、眼镜、手表、Chromecast、智能计量仪(例如，用于测量电力、建筑物的煤气和水消耗)、珠宝首饰、旅游卡、银行卡、ATM机、服装、运动装备、电子阅读器、望远镜、MP3播放器、手持游戏机、诸如飞机、火车、自行车、船或公交车的交通工具、EPO、厨房用品、镜子、手袋、钱包、帽子、婴儿车、高保真或其它音乐播放器或收音机、或者是能够向远程或可移动装置发送和接收数据的任何其他装置或具有与其相关联的器件的任何其他装置。

[0043] 装置，或者优选地，安全元件或存储卡，优选具有安装在其上用于访问数据的数据访问软件代码。优选地，为了安装数据访问软件代码，装置必须登记到系统，例如通过提交至少与安全元件或存储卡的识别码有关的信息。

[0044] 在步骤(i)-(iii)之前方法优选包括：向数据登记安全元件或存储卡的识别码、或者基于此的代码或证书。

[0045] 可将一个以上的安全元件或存储卡的识别码与数据相关联。因此，可以将一个以上的装置登记到数据并且一个以上的装置可以安全地访问数据。

[0046] 主装置例如可以登记或请求与进一步的装置相关联的识别码的登记。

[0047] 如上所述，识别码优选是与装置的智能对象相关联的识别码。智能对象例如可以是与装置相关联的SIM、虚拟SIM、SIM软件、TPM(可信平台模块)、SE(安全元件)、TEE(可信执行环境)、微型SD、存储卡、USB密钥或智能卡。可以使用不同的智能对象为不同的装置提供识别码。智能对象可以是本地形式、远程形式或可移动形式的存储器的任何一种。

[0048] 在某些情况下，如果至少一个进一步的装置也正在访问数据，那么只允许装置访问数据。在某些情况下，至少一个进一步的装置可以是特别指定的装置，诸如管理者装置。

[0049] 根据进一步的方面，提供一种控制从装置访问数据的方法，其中所述数据远离所述装置存储或者存储在可移动存储设备中，所述方法包括以下步骤：(i)从所述装置接收访问所述数据的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；(ii)至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此允许或拒绝所述装置对所述数据的访问。

[0050] 该方面可包括上述第一方面的附加或可选特征的任何一个。

[0051] 优选地，通过数据访问控制器执行该方面的方法。数据访问控制器可以远离希望访问数据的装置。例如，数据访问控制器可以在云中。

[0052] 根据进一步的方面，提供一种用于控制访问数据的数据访问控制器，所述数据远离装置存储或者存储在可移动存储设备中，所述数据访问控制器被布置为进行以下步骤：(i)从所述装置接收访问所述数据的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；(ii)至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此允许或拒绝所述装置对所述数据的访问。

[0053] 数据访问控制器可以远离希望访问数据的装置。例如，数据访问控制器可以在云中。

[0054] 待访问的数据可以是用于帮助对基于云或基于网络的第三方服务的访问的数据。本发明的全部以下方面(连同其优选或可选特征)也可包括这个可选特征。

[0055] 可通过基于云的分区接收访问数据的请求。在可应用的地方，本发明的以下方面(连同其优选或可选特征)也可包括这个可选特征。

[0056] 根据进一步的方面，提供一种包括装置和数据访问控制器的系统，所述数据访问控制器用于控制从所述装置访问数据，所述数据远离所述装置存储或者存储在可移动存储设备中，其中所述装置被布置为向所述数据访问控制器发送访问所述数据的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；以及所述数据访问控制器被布置为至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问，以及因此允许或拒绝所述装置对所述数据的访问。

[0057] 根据进一步的方面，提供一种用于控制访问数据的计算机程序，所述数据远离装置存储或者存储在可移动存储设备中，所述程序被配置为在其由处理器执行时执行以下步骤：(i)从所述装置接收访问所述数据的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；(ii)至少部分地基于所述识别码，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此允许或拒绝所述装置对所述数据的访问。

[0058] 根据进一步的方面，提供一种将装置登记到访问控制器，使得所述装置可经由所述访问控制器访问数据的方法，所述数据远离装置存储或者存储在可移动存储设备中，其中所述方法包括：发送为了访问数据而登记装置的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；检查是否将允许对所述数据的访问；以及如果将允许访问，则针对待访问的所述数据登记所述识别码。

[0059] 请求优选包括基于例如与所述装置相关联的安全元件或存储卡的识别码和一个或多个PIN或密码，以及表示所述用户固有的事物的数据的双因素代码或三因素代码。这允许装置请求对分区的访问的可审查轨迹。

[0060] 请求的形式可以是电子邮件或SMS。

[0061] 优选地，所述方法进一步包括向管理者装置发送与请求有关的信息，其中管理者装置优选决定是否将许可对数据的访问。例如可以从访问控制器或者寻求登记的装置发送与请求有关的信息。可以使用管理者装置为请求访问的装置设置访问权限，诸如只能读取，或者向数据编辑/删除/添加附加内容的能力。

[0062] 例如，在登记儿童装置(例如电话或平板电脑)的安全元件或存储卡使其能够访问父母数据的情况下，可将父母装置(例如电话或平板电脑)的安全元件或存储卡登记为该数据的管理者，使其能够监测和控制儿童对数据的访问。数据本身实际上可以存储在父母的管理者装置中。因此，例如，装置(或多个装置)可以(各自)允许一个或多个进一步的装置访问该装置中存储的数据，但是以有限或指定的读取/写入权限。

[0063] 优选地，如果管理者决定允许装置有权访问数据，则从管理者向访问控制器发送信号以指出这一点。

[0064] 根据进一步的方面，提供一种将装置登记到访问控制器，使得所述装置可经由所述访问控制器访问数据的方法，所述数据远离装置存储或者存储在可移动存储设备中，其中所述方法包括：接收为了访问数据而登记装置的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；检查是否将允许对所述数据的访问；以及如果将允许访问，则针对待访问的所述数据登记所述识别码。

[0065] 根据进一步的方面，提供一种用于控制将装置登记到对数据的访问的数据访问控制器，所述控制器被布置为执行以下步骤：接收为了访问数据而登记装置的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；检查是否将允许对所述数据的访问；以及如果将允许访问，则针对待访问的所述数据登记所述识别码。

[0066] 根据进一步的方面，提供一种包括装置和数据访问控制器的系统，所述数据访问控制器用于控制将装置登记到对数据的访问，所述控制器被布置为执行以下步骤：从所述装置接收为了访问数据而登记装置的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；检查是否将允许对所述数据的访问；以及如果将允许访问，则针对待访问的所述数据登记所述识别码。

[0067] 优选地，所述系统还包括管理者装置。

[0068] 优选地，所述数据访问控制器被布置为向管理者装置发送信号，以检查对于待登记的装置，是否将允许对数据的访问。

[0069] 优选地，所述管理者装置被布置为发送信号，以确认对于待登记的装置，是否将允许对数据的访问和/或对请求访问的装置设置访问权限，诸如只能读取，或者向数据编辑/

删除/添加附加内容的能力。

[0070] 根据进一步的方面，提供一种用于控制将装置登记到对数据的访问的计算机程序，所述程序被配置为在其由处理器执行时执行以下步骤：从所述装置接收为了访问数据而登记装置的请求，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；检查是否将允许对所述数据的访问；以及如果将允许访问，则针对待访问的所述数据登记所述识别码。

[0071] 根据进一步的方面，提供一种在装置上访问数据的方法，其中所述数据远离所述装置存储或者存储在可移动存储设备中，所述方法包括：在装置上接收访问所述数据的邀请，所述邀请包括口令、代码或PIN；从所述装置发送访问所述数据的请求，所述请求包括所述口令、代码或PIN；至少部分地基于所述口令、代码或PIN，验证是将允许还是将拒绝对所述数据的访问；以及因此允许或拒绝所述装置对所述数据的访问。

[0072] 因此，对于用户而言可以向进一步的装置(他自己的或另一个用户的)发送邀请，使得进一步的装置也可以访问数据。为了被许可访问，不需要一定将这些装置(或者与其相关联的识别码)登记到数据。

[0073] 根据该方面，可以向装置许可无限时间或者预定时间长度的访问。在任一情况下，在已经许可访问之后的某个点，例如可由另一个用户阻止访问。

[0074] 口令、代码或PIN例如可通过随机数生成器生成。

[0075] 优选地，口令、代码或PIN是一次性口令。这能够向进一步的用户提供许可访问的安全方法。

[0076] 优选地，口令、代码或PIN仅在指定的时间段内有效。因此，如果在指定时间段内没有使用口令、代码或PIN，则将不基于该口令、代码或PIN来许可访问。时间段例如可以多达1、2、3、4、5、6、7、8、9、10、15、20、25、30、45、60、90或120分钟。优选地，时间段为24小时或更少时间。另一方面，在某些实施例中，口令、代码或PIN不一定有特定的过期时间。

[0077] 优选地，经由安全通道至少向装置和/或从装置发送口令、代码或PIN(优选地，向装置和从装置发送口令、代码或PIN)。

[0078] 在某些实施例中，通过控制对数据的访问的装置，例如主装置，来生成口令、代码或PIN。替代地，主装置可以向非主装置许可该相同功能。

[0079] 该方法可以是第一装置允许第二装置访问数据的方法，其中数据远离第一装置和第二装置存储，邀请从第一装置发送给第二装置，访问数据的请求从第二装置发出，以及向第二装置允许或拒绝对数据的访问。

[0080] 在这种情况下，在第一装置中生成口令、代码或PIN。

[0081] 替代地，可以远离第一装置和第二装置两者生成口令、代码或PIN，例如在控制对数据的访问的处理器中。

[0082] 在任一情况下，该方法优选进一步包括将所生成的口令、代码或PIN登记到待访问的数据。

[0083] 将所生成的口令、代码或PIN登记到待访问的数据的步骤可包括验证，在登记所生成的口令、代码或PIN之前允许所述第一装置邀请进一步的装置访问所述数据。

[0084] 该方法可进一步包括从所述第一装置发送对于待生成的口令、代码或PIN的请求，其中待生成的口令、代码或PIN仅在已经验证允许所述第一装置邀请进一步的装置访问所

述数据之后生成。

[0085] 因此在任一情况下,仅授权装置可以邀请进一步的装置访问数据。

[0086] 优选地,验证允许所述第一装置邀请进一步的装置访问所述数据的步骤包括验证与所述装置相关联的识别码,诸如如上所述的与所述装置相关联的安全元件或存储卡的识别码。

[0087] 验证允许所述第一装置邀请进一步的装置访问所述数据的步骤可进一步包括验证从所述第一装置发送的指定所述分区的数据。

[0088] 优选地,指定所述分区的数据包括以下的一个或多个:PIN或密码;以及表示所述装置的用户固有的事物的数据,诸如遗传学和/或生物统计学信息。

[0089] 根据进一步的方面,提供一种允许在装置上访问数据的方法,其中所述数据远离所述装置存储或者存储在可移动存储设备中,所述方法包括:向所述装置发送访问所述数据的邀请,所述邀请包括口令、代码或PIN;从所述装置发送访问所述数据的请求,所述请求包括所述口令、代码或PIN;至少部分地基于所述口令、代码或PIN,验证是将允许还是将拒绝对所述数据的访问;以及因此允许或拒绝所述装置对所述数据的访问。

[0090] 可以优选经由访问控制器从管理者装置发送邀请。邀请的形式可以是消息,诸如电子邮件或SMS消息,和/或消息可以经由数据访问应用中的消息系统来发送并且可见。当受邀用户打开或登录该应用时,他们可以看见,已经接收邀请来访问特定数据。然后用户可以访问数据。

[0091] 邀请可包括OTP(一次性口令),例如,为了经由网络浏览器访问数据,用户可将OTP输入至网络浏览器中(例如,与经由数据访问应用相对)。

[0092] 根据进一步的方面,提供一种包括第一装置、第二装置和数据访问控制器的系统,所述第一装置被布置为允许在所述第二装置上访问数据,其中所述数据远离所述第二装置存储或者存储在可移动存储设备中,其中所述第一装置被布置为向所述第二装置发送访问所述数据的邀请,所述邀请包括口令、代码或PIN;所述第二装置被布置为发送访问所述数据的请求,所述请求包括口令、代码或PIN;以及所述数据访问控制器被布置为至少部分地基于所述口令、代码或PIN,验证是将允许还是将拒绝对所述数据的访问,以及因此允许或拒绝所述第二装置对所述数据的访问。

[0093] 根据进一步的方面,提供一种在装置上访问数据的方法,其中所述数据远离所述装置存储或者存储在可移动存储设备中,所述方法包括以下步骤:(i)从所述装置发送访问所述数据的请求,所述请求包括与所述请求有关的数据;(ii)至少部分地基于所述数据,验证是将允许还是将拒绝对所述数据的访问;以及(iii)因此并且仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

[0094] 这种方法能够提供安全环境,其中仅当出现进一步的装置时才可执行特定动作,诸如金融交易、发消息和/或查看(例如秘密的)数据。然后进一步的装置(例如管理者装置)可以监测由装置执行的任何动作。如果适当的话,则可以采取快速动作,例如阻止或防止对数据的进一步访问。

[0095] 优选地,该方法在步骤(iii)之前包括:检查是否至少一个进一步的装置正在访问所述数据。例如,至少一个进一步的装置可以是特别指定的装置,诸如“主”装置。

[0096] 根据进一步的方面,提供一种控制在装置上访问数据的方法,其中所述数据远离

所述装置存储或者存储在可移动存储设备中，所述方法包括以下步骤：(i)从所述装置接收访问所述数据的请求，所述请求包括与所述请求有关的数据；(ii)至少部分地基于所述数据，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此并且仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

[0097] 根据进一步的方面，提供一种用于控制在装置上访问数据的数据访问控制器，其中所述数据远离所述装置存储或者存储在可移动存储设备中，所述数据访问控制器被布置为执行以下步骤：(i)从所述装置接收访问所述数据的请求，所述请求包括与所述请求有关的数据；(ii)至少部分地基于所述数据，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此并且仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

[0098] 优选地，所述数据访问控制器还被布置为在进行步骤(iii)之前检查是否至少一个进一步的装置正在访问所述数据。

[0099] 根据进一步的方面，提供一种包括装置和数据访问控制器的系统，所述数据访问控制器用于控制在装置上访问数据，其中所述数据远离所述装置存储或者存储在可移动存储设备中，所述数据访问控制器被布置为执行以下步骤：(i)从所述装置接收访问所述数据的请求，所述请求包括与所述请求有关的数据；(ii)至少部分地基于所述数据，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此并且仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

[0100] 优选地，所述装置被布置为将访问所述数据的请求发送给所述数据访问控制器。

[0101] 优选地，所述数据访问控制器还被布置为在执行步骤(iii)之前检查是否至少一个进一步的装置正在访问所述数据。

[0102] 根据进一步的方面，提供一种用于控制访问数据的计算机程序，所述数据远离装置存储或者存储在可移动存储设备中，所述程序被配置为在其由处理器执行时执行以下步骤：(i)从所述装置接收访问所述数据的请求，所述请求包括与所述请求有关的数据；(ii)至少部分地基于所述数据，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此并且仅当至少存在一个进一步的装置正在访问所述数据时允许所述装置对所述数据的访问。

[0103] 优选地，所述程序还被进一步配置为在执行步骤(iii)之前检查是否至少一个进一步的装置正在访问所述数据。

[0104] 本发明的进一步的方面涉及一种在装置上访问数据的方法，其中所述数据远离所述装置存储、存储在可移动存储设备中或者存储在所述装置自身中，所述方法包括以下步骤：(i)发送访问所述数据的请求，所述请求包括与所述装置相关联的识别码以及以下的一个或多个：PIN或密码；以及表示所述装置的用户固有的事物的数据，诸如遗传学和/或生物统计学信息；(ii)基于所述识别码、以及所述PIN或密码、和/或表示所述用户固有的事物的数据，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此允许或拒绝所述装置对所述数据的访问。

[0105] 数据优选存储在分区中。在这种情况下，PIN或密码和/或表示所述装置的用户固有的事物的数据，诸如遗传学和/或生物统计学信息，与用户正在寻求访问的分区相关联。例如，PIN或密码和/或表示所述装置的用户固有的事物的数据，诸如遗传学和/或生物统计学信息，可以识别数据或者存储数据的分区。

[0106] 在遗传学和/或生物统计学信息的情况下，一个选项可以是将来自不同手指的指纹与不同的数据或分区相关联，从而根据输入和发送哪个指纹来访问对应的数据或分区。

[0107] 本发明的进一步的方面涉及一种控制在装置上访问数据的方法，其中所述数据远离所述装置存储、存储在可移动存储设备中或者存储在所述装置自身中，所述方法包括以下步骤：(i)接收访问所述数据的请求，所述请求包括与所述装置相关联的识别码以及以下的一个或多个：PIN或密码；以及表示所述装置的用户固有的事物的数据，诸如遗传学和/或生物统计学信息；(ii)基于所述识别码、以及所述PIN或密码和/或表示所述用户固有的事物的数据，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此允许或拒绝所述装置对所述数据的访问。

[0108] 本发明的进一步的方面涉及一种用于控制在装置上访问数据的数据访问控制器，其中所述数据远离所述装置存储、存储在可移动存储设备中或者存储在所述装置自身中，所述数据访问控制器被布置为执行以下步骤：(i)接收访问所述数据的请求，所述请求包括与所述装置相关联的识别码以及以下的一个或多个：PIN或密码；以及表示所述装置的用户固有的事物的数据，诸如遗传学和/或生物统计学信息；(ii)基于所述识别码、以及所述PIN或密码和/或表示所述用户固有的事物的数据，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此允许或拒绝所述装置对所述数据的访问。

[0109] 本发明的进一步方面涉及一种用于控制在装置上访问数据的计算机程序，其中所述数据远离所述装置存储、存储在可移动存储设备中或者存储在所述装置自身中，所述程序被配置为在其由处理器执行时执行以下步骤：(i)接收访问所述数据的请求，所述请求包括与所述装置相关联的识别码以及以下的一个或多个：PIN或密码；以及表示所述装置的用户固有的事物的数据，诸如遗传学和/或生物统计学信息；(ii)基于所述识别码、以及所述PIN或密码和/或表示所述用户固有的事物的数据，验证是将允许还是将拒绝对所述数据的访问；以及(iii)因此允许或拒绝所述装置对所述数据的访问。

[0110] 本发明的方面可包括任何特征，包括本发明任何其他方面的优选特征或可选特征。

[0111] 在任何方面中，优选将数据加密。优选地，由访问数据的装置将数据解密。在这种情况下，装置优选具有将数据解密的密钥。密钥优选存储在安全元件或存储卡中，但是也可以远程存储。优选地，将密钥自身加密。优选地，以安全的方式将密钥传送给装置，例如通过TSM(可信访问管理器)。

[0112] 如上所述，可以理解本发明的实施例可以提供方法和系统，其中：

[0113] 多个装置能够具有分区访问

[0114] 用户能够在保持控制和审查轨迹的同时与其他用户(装置)进行安全地共享。

[0115] 能够安全地执行交易。

[0116] 多个装置可以访问相同的远程分区。

[0117] 在访问数据或分区(多个分区)时，装置可能能够访问以下服务的一个或多个：消息、媒体、TV、电影、收音机、杂志、社交媒体、电子商务、智能设备(例如，公共设施和家庭控制)、企业服务、图片、照片和视频共享、政府服务、金融服务、医疗服务、旅游服务、音乐和游戏。当然，也可以存在本文未提及的进一步的服务，它们也可以或者替代地被访问。

[0118] 为了访问分区，装置可能能够提供双因素或三因素认证。可通过认证的一个因素

以及进一步的因素或多个因素来保护装置，其中认证的一个因素是智能对象(存储卡或安全元件)的识别码，进一步的因素或多个因素是密码或PIN、或者某些形式的遗传学或生物统计学识别数据、或者位置、或者时间，或者另一个用户(例如管理者)或用户所属的群组是否正在访问数据。

[0119] 下表列出用户可能希望由其访问分区的示例性装置以及它们可能的对应“智能对象”(即，安全元件或存储卡)。智能对象是装置的对象，装置的对象的识别码与分区相关联，并且为了允许访问分区必须验证装置的对象。

[0120]

装置	智能对象
电话	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、NFC 智能对象（用于 NFC 智能电话）
平板电脑	SIM、SE、TEE、微型 SD、存储卡
笔记本电脑	SIM、虚拟 SIM、SIM 软件、SE、TEE、TPM、存储 SD、存储卡、USB 密钥、智能卡
台式电脑	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡
TV	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡
机顶盒	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡
相机	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡

[0121]

汽车	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡
游戏机	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡
眼镜	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡
手表	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡
Chromecast	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡
智能计量仪（家庭公共设施）	SIM、虚拟 SIM、SIM 软件、SE、TEE、微型 SD、存储卡、USB 密钥、智能卡

[0122] 可以提供不同类型的分区，例如：

[0123] -仅该用户有权对其访问的封闭分区

[0124] -仅能够通过邀请与其他用户共享的封闭分区

[0125] -具有审查历史轨迹的开放分区

[0126] -没有用户的历史或审查轨迹的开放和匿名分区

[0127] 基于诸如时隙的标准，可将任何类型的分区切换为开放或封闭的。例如，可将分区设置为在特别的预定时间开放，以及在特别的预定时间封闭。

[0128] 用户可以针对分区登记多个装置，并且可以针对他们登记的附加装置进行切换、编辑和上传功能。例如，用户可能希望他们的相机具有向分区上传图片、并且在分区中查看图片的能力，但是没有删除或编辑分区中任何内容的能力。

[0129] 用户可以挑选，使得一个或多个装置作为分区的管理者装置(多个管理者装置)。这可以允许管理者控制对分区的访问，并且如果他们认为必要，就停止访问。在管理者能力范围内，用户还能够有权访问已经对是管理者的用户许可访问分区的所有其他用户的装置。这可以允许用户实时编辑或消除对分区的访问权限。如果用户丢失装置或者不再拥有装置，还可以允许该用户禁止对装置的访问。

[0130] 管理者装置可以具有创建更好的时间敏感代码的能力，该代码可以是用户切换的，并且可以给予他访问以登录并未连接到登记的智能对象的机器。该代码可以是任何长度和/或可以输入至与访问控制器相连接的接口，并且可以在诸如台式电脑或笔记本电脑的未登记装置上允许对分区的访问。用户可从管理者装置具有在任何点上中止该会话的能力，例如通过启动管理者装置上的中止按钮。所创建的代码优选为使用管理者装置的双因素或三因素认证的结果。

[0131] 智能对象可以管理多个分区，多个分区可以具有隶属于它们的相同或不同的密码/认证符。在分区中系统可以允许用户对很多不同的第三方服务报名或者自动报名。在分

区中系统可将由用户设置的用户ID以及口令转化为用于口令和用户ID两者的字母数字串。这可以传递给第三方服务提供者。可以基于用于服务的最佳实践指南将这些代码更新。例如，依照NHS信息管理要求，如果用户正访问UK中的医疗记录，可以每60天将它们更新。

[0132] 因此，根据本发明的进一步的方面，提供一种使用装置访问基于云或基于网络的第三方服务的方法，所述方法包括以下步骤：(i)从所述装置向与所述装置相关联的基于云的分区发送请求，所述分区包括用于帮助连接到所述第三方服务的数据，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；(ii)至少部分地基于所述识别码，验证是将允许还是将拒绝对所述分区的访问；以及(iii)因此允许或拒绝所述装置对所述分区的访问；以及在允许对所述分区的访问之后：(iv)将凭证传输给所述第三方服务。

[0133] 根据本发明的进一步的方面，提供一种控制由装置访问基于云或基于网络的第三方服务的方法，所述方法包括以下步骤：(i)接收从所述装置到与所述装置相关联的基于云的分区的请求，所述分区包括用于帮助连接到所述第三方服务的数据，所述请求包括与所述装置相关联的安全元件或存储卡的识别码；(ii)至少部分地基于所述识别码，验证是将允许还是将拒绝对所述分区的访问；以及(iii)因此允许或拒绝所述装置对所述分区的访问；以及在允许对所述分区的访问之后：(iv)将凭证传输给所述第三方服务。

[0134] 因此，仅当提供与装置相关联的正确的识别码时才允许对第三方服务的访问。因此，可以防止未授权装置访问第三方服务，因为它们不能提供正确的识别码。

[0135] 下面的优选特征同样适用于本发明的前面两个方面。

[0136] 为了装置能够访问特定分区，装置可以在其上安装用于访问分区的适当的软件(例如应用)。例如将其存储在与装置相关联的安全元件或存储卡中。

[0137] 替代地，可以只将应用部分地存储在安全元件或存储卡中；例如，应用可由标准移动应用组成以及由安全元件内部的小程序组成。

[0138] 分区可与多个不同的网络服务相关联。

[0139] 如果至少部分地基于识别码验证将允许对分区的访问，就可以在装置的安全元件或存储卡与云分区之间启动相互认证证处理。该处理允许在装置的安全元件或存储卡与云分区之间创建安全通道。然后可在装置的安全元件或存储卡与云分区之间传送数据。数据可被加密。

[0140] 因此，传输凭证的步骤(iv)包括以下步骤：在装置的安全元件或存储卡与分区之间执行相互认证处理；以及在安全元件或存储卡与分区之间创建安全通道。该步骤还可包括通过安全通道将凭证传输给分区。凭证可被加密，在这种情况下在通过安全通道传输之前将凭证加密。然后通过分区将凭证提供给第三方服务。

[0141] 替代地，可将凭证存储在分区的安全元件中。在这种情况下，不需要从安全元件或存储卡向分区传输凭证。反而，当向装置许可对分区的访问时，可以直接从分区向第三方服务传输凭证。

[0142] 可以按照加密形式将凭证传输给第三方服务。在这种情况下，在网络服务的等级上实施兼容安全元件，以允许将所传输的加密凭证的解密。

[0143] 安全元件或存储卡例如是“智能对象”或者具有唯一识别码的安全或防篡改硬件装置，识别码本身理论上也是安全和防篡改的。安全元件或存储卡例如可以是SIM、虚拟SIM、SIM软件、TPM(可信平台模块)、SE(安全元件)、TEE(可信执行环境)、微型SD、存储卡、

USB密钥或智能卡。

[0144] 因此，安全元件是用于各种类型的能够安全地存储和/或处理数据(例如，密钥、算法、小程序、凭证)的安全芯片、装置或软件方案的通用术语。

[0145] 安全元件或存储卡可以是本地形式、远程形式或可移动形式的存储器的任何一种。

[0146] 优选将安全元件或存储卡的识别码妥善保护，并存储在例如安全元件或存储卡的保险箱中。优选地，经由安全通道发送识别码。替代或附加地，可将识别码加密。这能够使得处理更安全，并帮助防止识别码被拦截和/或被第三方发现。

[0147] 如上所述，请求包括与装置相关联的安全元件或存储的的识别码。但是，可以按照修改的形式将识别码包括在请求中，例如，按照加密的形式和/或与一个或多个其他代码、数据或信息组合。

[0148] 请求还可包括在装置上输入的密码或PIN并且步骤(ii)还可包括基于密码或PIN验证是将允许还是将拒绝对数据的访问。因此，为了访问数据可以要求双因素认证。

[0149] 可通过与装置相关联的安全元件或存储卡(例如SIM或虚拟SIM)(首先)验证密码或PIN。

[0150] 替代或附加地，请求可包括表示装置的用户固有的事物的数据，并且步骤(ii)还可包括基于表示装置的用户固有的事物的数据验证是将允许还是将拒绝对数据的访问。因此，为了访问数据可以要求双因素验证或三因素认证，并且仅许可授权用户对数据的访问。

[0151] 例如，表示装置的用户固有的事物的数据可包括表示关于用户的遗传学和/或生物统计学信息的数据，诸如指纹或虹膜数据。

[0152] 替代或附加地，对于使用用PIN和/或表示装置的用户固有的事物的数据的认证(使用识别码的双因素认证或三因素认证)，以下形式的认证是可能的。

[0153] 请求可包括包含位置的数据(即，用户尝试由其访问数据的地方)，并且步骤(ii)还可包括基于位置验证是将允许还是将拒绝对数据的访问。

[0154] 请求可包括包含时间的数据(即，用户尝试访问数据的时间)，并且步骤(ii)还包括基于时间验证是将允许还是将拒绝对数据的访问。

[0155] 请求可包括指示用户是群组一部分的数据，并且步骤(ii)还包括基于群组的另一个成员(例如管理者)是否正在访问数据，验证是将允许还是将拒绝对数据的访问。

[0156] 在本发明的优选实施例中，将安全元件或存储卡用于执行相互认证处理，和/或创建安全通道，和/或加密识别码和/或PIN或密码。

[0157] 该方法可包括用户注册处理，由此用户为使用第三方服务进行注册。这种用户注册处理可包括以下步骤：收集用于访问第三方服务的凭证和/或第三方服务所请求的形式填充数据；以及安全地存储所述凭证和/或形式填充数据。凭证可包括用户ID和/或口令。附加地，凭证可包括注册第三方服务所必须的关于用户的任何信息(例如包括支付细节)。例如，凭证可包括以下信息片段的一个或多个：名、姓、职务、地址、年龄、出生日期、性别、会员状态、会员卡号、支付卡号、卡的类型、到期日期、CVV码、身份证或护照号码。这些信息片段也可以称为形式填充数据。

[0158] 取代在用户注册处理中收集凭证，在允许对分区的访问之后可通过分区自动生成凭证。也就是说，通过装置与第三方服务组合来管理注册处理，而不需要用户的主动干预。

在这种情况下，用户注册处理可包括以下步骤：启动相互认证处理；以及选择第三方服务。也就是说，用户不一定需要提供他们的凭证以访问第三方服务；为了访问分区，提供正确的识别码(以及，在还要求密码/PIN的实施例中优选地提供密码/PIN)就可能足够了。

[0159] 可将凭证和/或形式填充数据安全地存储在分区中。替代地，可将凭证和/或形式填充数据安全地存储在安全元件或存储卡中。在后一种情况下，在必要时可将凭证从安全元件或存储卡提供给分区。

[0160] 在自动生成凭证(诸如用户ID和/或口令)的实施例中，可以周期性地或按需更新自动生成的凭证。可根据用户安全策略或第三方服务安全策略来调整更新凭证之间的周期。自动生成的凭证可以不同于通过其他器件访问服务时所使用的凭证(例如，使用网络浏览器从PC、平板电脑、或智能电话等等的标准网络访问，即，不使用特殊应用)。可根据用户安全策略或第三方服务安全策略来调整自动生成的凭证的复杂性和/或复杂度。例如，可根据用户安全策略或第三方服务安全策略来设置口令的最小长度。也可要求用户ID和/或口令包括以下两个或更多的混合：小写字母、大写字母、标点符号或符号、以及数字。

[0161] 可将单个小程序安装在装置的安全元件或存储卡中，单个小程序被配置为驱动对所有认证处理和服务的访问。但是，某些类型的服务可能要求管理其自身安全的能力，从而控制认证处理以及对它们的服务的访问，而与安全元件或存储卡中安装的任何其他小程序无关。银行服务是一个示例。因此，替代地，可将多个小程序存储在装置的安全元件或存储卡中。在生成凭证之前，每个小程序可以进行分离的认证处理，以访问与给定小程序有关的第三方服务。

[0162] 除了在装置的安全元件或存储卡与分区之间的认证步骤之外，该方法还可包括实施在装置的安全元件或存储卡与第三方服务的安全元件之间的第二认证处理的步骤。这可以是第三方服务要求附加安全性以使得第三方服务要求对认证处理的控制的情况。第三方服务例如可以是银行。

[0163] 因此，传输凭证的步骤(iv)可包括以下步骤：在装置的安全元件或存储卡与第三方服务的安全元件之间执行相互认证处理；在装置的安全元件或存储卡与第三方服务的安全元件之间创建安全通道；将凭证加密；以及通过安全通道向第三方服务的安全元件传输加密凭证。

[0164] 第三方服务可以请求访问第三方服务的密码/PIN，且优选通过在安全元件或存储卡与第三方服务的安全元件之间创建的安全通道来传输密码/PIN。

[0165] 优选地，通过安全通道从安全元件或存储卡向第三方分区自动提供访问第三方服务的凭证和/或第三方服务所请求的形式填充数据，然后当请求接下来的顺利完成第二认证处理时将其提供给第三方服务。

[0166] 在顺利完成第二认证处理之后，可以自动启动第三方服务。

[0167] 装置可充当主装置，允许进一步的装置(例如，PC或平板电脑)也访问第三方服务。在这种情况下，可生成访问代码并在装置上显示访问代码(或者，例如可通过SMS或电子邮件发送给用户)，以及用户可使用进一步的装置将访问代码输入至与第三方服务相关联的网站。优选地，可由装置上运行的应用生成访问代码。

[0168] 替代地，主装置可以向非主装置许可相同的功能(生成用于另一个装置的访问代码)。

[0169] 访问代码可以是时间敏感的，即，仅在特定时间段内有效。该时间段例如可以多达1、5、10、15、20、25、30、45、60、90或120分钟。

[0170] 主装置可用于创建新的凭证或者更新凭证以访问第三方服务。当进一步的装置连接到分区(并且因此也连接到与分区相关联的网络服务)时，在所连接的装置(即，装置和进一步的装置)之间可同步凭证。替代或附加地，在所连接的装置之间可同步分区内容。例如，在从装置可以得到新的凭证、新的服务、或者新的内容时，只要进一步的装置被连接至该装置并且已经顺利通过了认证处理，新的凭证、新的服务、或者新的内容就变得立刻可用于进一步的装置。

[0171] 装置可以从NFC(近场通信)标签读取代码，以访问分区并从分区启动第三方服务。NFC标签可以向装置提供选择分区(否则将需要由用户输入分区)并最终打开它所必须的信息。

[0172] 替代性地，装置可以从生物统计学传感器/读卡器读取代码，以访问分区并从分区启动第三方服务。生物统计学传感器/读卡器可以向装置提供选择分区(否则将需要由用户输入分区)并最终打开它所必须的信息。

[0173] 在另一个实施例中，装置可以从信号发射装置接收代码。信号发射装置可以向装置提供选择分区(否则将需要由用户输入分区)并最终打开它所必须的信息。信号发射装置可以是蓝牙、BLE(蓝牙低功耗)、wifi、zigbee、NFC、GPS、或ISO 14443装置，或者使用任何其他形式的无接触通信的装置。

[0174] 每个分区可以存储用于电话或消息服务的唯一标识符。电话或消息服务例如可以是移动电话的电话服务、VOIP服务、或者即时消息服务。可将唯一标识符链接到电话或消息服务标识符，诸如用户名和口令或者电话号码(国家或国际)。

[0175] 可以有多个分区，每个分区一个具有唯一标识符。作为示例，一个用户可以有10个分区，每个分区与唯一标识符相关联，每个标识符链接到不同的电话号码。

[0176] 可将唯一标识符与电话或消息服务标识符之间的映射存储在装置的安全元件或存储卡中。替代地，可将映射存储在云中。替代地，移动网络运营商可以帮助唯一标识符至电话或消息服务标识符的映射。

[0177] 当标识符存储在分区上时，只要用户能够从装置访问分区，用户就能够访问电话或消息服务(不管他们使用哪个装置访问分区)。因此用户将具有发送或接收与该电话或消息服务相关联的任何语音、文本或数据消息的能力，而与使用的装置无关。

[0178] 根据用户的位置，可以激活特定的电话或消息服务标识符以及关联的电话或消息服务。这可以是用户的位置是双因素或三因素认证处理的一部分的情况。例如，在通过家庭wifi网络连接到分区时，可以在装置上激活家庭电话号码。类似地，如果经由另一个地区的GPS或4G基站进行连接，那么可以在装置上激活该区域中的本地电话号码。例如，如果用户旅行到法国，就可以生成法国电话号码以让他们使用。在离开法国时，可以给予用户保留号码，或者解除号码以让另一个用户使用的选择。

[0179] 另一个可能的应用是雇主给予雇员用于工作使用的移动电话。雇员可能不希望同时带着其个人电话和工作电话。作为替代，雇员可以创建具有链接到他们个人电话号码的唯一标识符的分区(与工作电话相关联)。然后雇员可以使用工作移动电话打电话和接电话，而不需要使用雇主的电话合同。

[0180] 本发明还延伸到用于控制通过装置来访问基于云或基于网络的第三方服务的计算机程序，程序被配置为执行以上方面的方法(和/或如上所述，方法的优选特征)。

[0181] 本发明的每个方面可包括任何特征，包括本发明任何其他方面的优选特征或可选特征。

[0182] 因此，如同本发明的全部前述方面(及其优选特征)中所定义的，本发明还延伸到数据访问控制器、将装置登记到数据访问控制器的方法、包括装置和访问控制器的系统、用于控制装置登记的计算机程序、在装置上访问数据的方法、允许在装置是对数据的访问的方法、包括第一装置、第二装置和数据访问控制器的系统，其中待访问的数据是基于云或基于网络的第三方服务和/或通过基于云的分区发送和/或接收访问数据的请求。

[0183] 与访问基于云或基于网络的第三方服务有关的后两个方面的优选特征还可以结合如同本发明的全部前述方面(及其优选特征)中所定义的数据访问控制器、包括装置和访问控制器的系统、用于控制装置登记的计算机程序、在装置上访问数据的方法、允许在装置上对数据的访问的方法、包括第一装置、第二装置和数据访问控制器的系统。

[0184] 分区还可以经受多个智能对象锁。例如，仅当两个或更多的不同用户登录分区时分区是开放的。在涉及公司前景或者承担秘密会议中的文档共享时这特别有意义。在允许诸如与第三方供应商的交易的服务，或者诸如对等交易的较不正式的交易需要安全环境时，使用多个智能对象来开放分区也能够用于保护第三方的身份。

[0185] 很多前述方面参照基于与装置相关联的安全元件或存储卡的识别码验证是将允许还是将拒绝对数据的访问(或类似步骤)。

[0186] 为了访问分区(其中访问包括创建、编辑或删除分区)，这些方面可以能够提供双(或者更多)因素认证。认证的一个因素可以是与装置相关联的智能对象(存储卡或安全元件)的识别码，进一步的因素或多个因素可以是密码或PIN、或者某些形式的遗传学或生物统计学识别数据、或者位置、或者时间、或者另一个成员(例如管理者)或用户所属的群组是否正在访问数据。

[0187] 在与上面所讨论的那些相对应的方面中，因素之一不必是与装置相关联的存储卡或安全元件的识别码。

[0188] 因此，在本发明的进一步的方面中，提供一种从装置访问分区的方法，该方法包括步骤：在所述分区与所述装置之间进行相互认证；以及在所述分区与所述装置之间创建安全通道，其中所述认证证包括两个或更多因素，所述因素选自以下列表：与所述装置相关联的智能对象(存储卡或安全元件)的识别码；密码或PIN；某些形式的遗传学或生物统计学识别数据；位置；时间；或者另一个成员(例如管理者)或者所述用户所属的群组是否正在访问数据。优选地，术语“访问”包括创建、编辑、或删除分区。

[0189] 参照本发明的较早方面，在上面的描述中更详细地讨论了该列表中包括的因素。

附图说明

[0190] 限制仅通过示例的方法并参照附图来描述本发明的优选实施例，其中：

[0191] 图1是包括移动电话及其对应的基于云的远程存储设备的系统的示意图；

[0192] 图2是包括移动电话和平板电脑装置及其对应的基于云的远程存储设备的系统的示意图；

[0193] 图3是示出从移动电话对远程存储数据的授权和非授权访问尝试的示意图；

[0194] 图4是示出从移动电话对远程存储数据的授权、受邀和非授权访问尝试的示意图；

[0195] 图5是示出有访问监测的情况下从移动电话对远程存储数据的授权、受邀和非授权访问尝试的示意图；

[0196] 图6是示出没有访问监测的情况下从移动电话对远程存储数据的授权、受邀和非授权访问尝试的示意图；

[0197] 图7是示出登记装置使其能够访问分区的处理的流程图；

[0198] 图8是示出认证处理的流程图；

[0199] 图9是示出访问代码加密处理的流程图；

[0200] 图10是包括移动装置、云和第三方网络服务的系统的示意图；以及

[0201] 图11是包括移动装置、云和要求高安全性的第三方网络服务的系统的示意图。

具体实施方式

[0202] 如图1所示，移动电话1包括SIM 2且有权访问云服务器4中的数据存储设备分区3a、3b、3c。SIM 2包含用于访问远程数据分区的软件。

[0203] 移动电话1在输入用于分区3a、3b或3c的正确密码或PIN时只能够访问该分区3a、3b或3c。每个分区具有它自己的由用户设置的密码或者PIN。

[0204] 除了正确密码或PIN之外，还可提供用于对分区3a、3b或3c中数据的待许可访问的来自正确SIM 2的识别码。

[0205] 当用户希望访问特定分区3a、3b或3c时，他们通过敲击移动电话1的键盘或触摸屏来输入用于该分区3a、3b或3c的密码或PIN。然后输入的密码或PIN被传递给SIM 2，在SIM2中密码或PIN经过将其与SIM识别码相结合的加密算法以创建哈希码。

[0206] 然后，哈希码被传递给云服务器4中的处理器，在云服务器4中的处理器中将它解密，以提取密码或PIN并识别用户正寻求访问分区3a、3b或3c中的哪个。然后，如果哈希码对应于云服务器4的存储器中已经存储的用于该分区3a、3b或3c的哈希码，那么允许对请求的分区3a、3b或3c的访问，并且能够经由移动电话1访问该分区3a、3b或3c中存储的数据。

[0207] 在某些实施例中，为了对分区3a、3b或3c的待许可访问，还要求认证的第三形式，诸如用户“拥有”的事物，例如遗传学或生物统计学ID(例如指纹或虹膜扫描)的形式。在其他实施例中，要求这些而不是用于分区3a、3b或3c的密码或PIN。

[0208] 每个分区3a、3b和3c中存储的内容或数据被加密，因此在允许对特定分区3a、3b或3c的访问时，使用用于分区3a、3b或3c的密码或PIN和SIM识别码、或者在SIM 2中存储的密钥，将该分区3a、3b或3c的内容解密。

[0209] 当许可对分区3a、3b或3c的访问并且其内容被解密时，能够在移动电话1的屏幕上查看该内容。

[0210] 移动电话1是控制分区3a、3b和3c的管理者装置。但是，用户(或其他用户)可以具有他们想要从其访问分区3a、3b和3c的进一步的装置。例如，如图2所示，用户具有带SIM 5a的平板电脑装置，用户想要从该平板电脑装置访问分区3a、3b和3c。平板电脑装置5的SIM 5a也被登记到分区3a、3b或3c，因此在平板电脑装置5上输入正确的PIN或密码和/或正确的遗传学或生物统计学信息时，就许可平板装置5对分区3a、3b或3c的访问。按照与上文所述

的用于移动装置1的方法相同的方法来控制许可对分区3a、3b或3c的访问的方法。

[0211] 图3示出非授权用户寻求访问云服务器4中存储的分区3M的情况。非授权用户具有移动电话6a或6b，移动电话6a或移动电话6b分别具有SIM 7a或SIM 7b。对分区的访问由访问控制器12控制。访问控制器12位于云中。在某些实施例中，访问控制器12是移动电话提供者系统的一部分。

[0212] 非授权用户在他们的移动电话6a或6b中输入PIN或密码，但是对因为PIN或密码不正确和/或SIM识别码不正确，所以分区3M的访问不被许可。访问控制器12不允许移动电话6a或6b访问分区3M。但是，它允许主移动电话1访问分区3M。

[0213] 图4示出非授权用户和受邀用户寻求访问云服务器4中存储的分区3M的情况。

[0214] 在这种情况下，如同图3的情况，访问控制器12向非授权用户的移动电话6a拒绝对分区3M的访问。

[0215] 为了对受邀用户许可访问，主用户从他们的移动电话1向云服务器4发送对与对分区3M的访问相关的一次性口令(OTP)的请求。云服务器4验证移动电话1的SIM 2的识别码被登记到分区3M，并且与SIM 2相关联的用户被允许邀请其他用户访问分区3M，并且如果情况如此，则将OTP发回移动电话1。然后主用户将此OTP发送给受邀用户的移动电话8。然后受邀用户向访问控制器12发送请求，以访问分区M并输入OTP。访问控制器12验证OTP，并且如果OTP正确，则许可受邀用户对分区3M的访问。

[0216] 在替代实施例(未示出)中，主用户在他们的移动电话1中生成OTP，然后将此OTP发送给云服务器4，以用于针对分区3M的登记。OTP还从移动电话1将此OTP发送给受邀用户的移动电话8。一旦针对分区3M登记OTP，受邀用户就能够通过输入如上所述的OTP来访问分区3M。

[0217] 在某些实施例中，OTP仅在特定时间段内有效，例如5分钟。

[0218] 在某些实施例中，仅向受邀用户许可在例如1-24小时的特定时间段内对分区3M的访问。

[0219] 在某些实施例中，OTP仅对于对分区3M的单个访问尝试有效。一旦已经使用了一次OTP，它就不再可用于访问3M。对于对分区3M的后续访问，必须由主用户请求进一步的OTP。

[0220] 在某些实施例中，如果需要的话，主用户能够对受邀用户监测和/或阻止对分区3M的访问。

[0221] 当分区建立在云服务器4中时，可以将其设置为“开放”分区，使得任何人都可以访问存储在那里的数据。图5示出这种开放分区30A的示例。在某些实施例中，某些用户对分区30A中存储的数据只具有“读取”访问，而诸如受邀用户和/或主用户的其他用户对存储在那里的数据具有“读取”和“写入”这两种访问。

[0222] 在图5所示情况下，因为分区30A是从主移动电话1、受邀用户的移动电话8以及另一个(非受邀)用户的移动电话10访问的开放分区，所以在存储器30A-h中监测和记录对分区30A的访问。所记录的数据例如由与访问分区30A的装置相关联的识别码和/或访问尝试的时间所组成。也可以记录其他数据。这能够允许主用户监测对分区30A的访问，并且如果需要的话，基于所记录的数据，对特定用户阻止对分区30A的访问。

[0223] 图6除了没有对分区30A的访问的监测之外，与图5相似。

[0224] 为了登记装置，使其能够访问特定分区，必须在装置上安装用于访问分区的适当

软件(例如应用)。例如,将其安装在与装置相关联的安全元件或存储卡中。

[0225] 为了登记装置,使其能够访问特定分区,然后执行如图7所示的以下处理。

[0226] 待登记的装置的用户从装置向管理者装置发送经由分区访问控制器获取对分区或多个分区的访问的请求——S1。请求的形式例如是电子邮件或SMS。请求包括双因素认证码。该代码从与装置相关联的安全元件或存储卡的识别码、以及或者密码或PIN、或者表示用户固有的事物的数据中创建。这允许装置已经请求对分区的访问的可审查轨迹。

[0227] 当分区管理者在管理者装置上接收请求时,管理者决定是将许可对分区(多个分区)的访问还是将拒绝访问——S2。管理者还可以为用户设置访问权限,诸如只能读取,或者向分区编辑/删除/添加附加内容的能力。

[0228] 如果所有者决定向用户允许对分区的访问,那么他们将从管理者装置向访问控制器发送信号,确认他们对于要针对分区登记的装置的协定,使得装置能够访问分区(具有由管理者指定的访问分区)——S3。

[0229] 然后访问控制器针对具有指定的访问分区的分区(多个分区)登记装置(即,与其存储卡或安全元件相关联的识别码)——S4。

[0230] 当用户打开或登录用于访问分区的应用时,他们能够通过输入与该分区相对应的PIN或密码或表示用户固有的事物的数据来访问分区(多个分区)。为了访问给定分区,不同装置能够具有不同的PIN或密码或表示用户固有的事物的数据。

[0231] 待登记的装置的用户能够是与管理者相同的人员,也能够是不同的人员。

[0232] 分区的管理者还能够邀请某人访问分区并向他们发出邀请来这么做。如同以上情况,受邀用户必须在他们的装置上安装用于访问分区的适当软件(例如应用)。邀请经由访问控制器发送。邀请的形式能够是消息,例如电子邮件或SMS消息,和/或消息可以经由分区访问应用中的消息系统来发送并且可见。当用户打开或登录该应用时,他们能够看见,已经接收邀请来访问特定分区。然后用户能够访问分区。

[0233] 邀请能够包括OTP(一次性口令),为了经由网络浏览器(与经由分区访问应用相对)访问分区,用户可将OTP输入至网络浏览器中)。

[0234] 为了任何用户打开或登录分区访问应用,他们必须输入用于应用的他们的PIN或者密码、或生物统计学信息,并且连同用于与他们的装置相关联的安全元件或存储卡的识别码一起对其进行检查。

[0235] 图8是示出装置的认证或验证处理的实施例的流程图。装置的用户打开他们装置上的分区访问应用并登录。这自动导致信号被发送给分区访问控制器,以表明应用已经被打开。然后执行机器间握手,机器间握手包括访问控制器检查SIM(或其他安全元件或存储卡的识别码)被登记,以及装置检查访问控制器的ID证书。这是通过从访问控制器向装置发送的“盘问”,然后装置回答“答案”来执行的。如果该检查被确认为正确的,则在装置与访问控制器之间打开安全通道——S5。

[0236] 然后访问控制器经由安全通道向装置发送请求,以便用户输入用于他们希望访问的分区的他们的PIN或密码——S6。

[0237] 用户输入PIN或密码并且SIM(或者与装置相关联的其他安全元件或存储卡)检查这是正确的。如果情况如此,则SIM(或其他安全元件或存储卡)基于输入的PIN或密码生成证书——S7。

[0238] 在替代实施例中，代替PIN或密码或者除了PIN或密码之外，用户可以请求并且之后输入表示他们固有的事物的数据，诸如生物统计学数据。然后证书将基于该数据。

[0239] 然后经由安全通道将生成的证书从装置发送给访问控制器——S8。

[0240] 访问控制器检查证书，并且如果针对请求的分区该证书被登记，则许可装置访问所请求的分区的权限，并且装置访问所请求分区——S9。

[0241] 图9是示出能够怎样将用于受邀用户访问分区的访问代码加密的流程图。

[0242] 当管理者希望提供用于分区的访问代码，使得另一个用户能够从未登记装置访问分区(或者使得管理者能够访问分区)时，从访问控制器向管理者装置发送PIN请求——S10。

[0243] 管理者将用于他们想要对其许可访问的分区的PIN输入至管理者装置，然后管理者装置(或者与装置相关联的其他安全元件或存储卡)的SIM创建加密代码——S11。

[0244] 然后经由安全通道将加密代码从管理者装置发送给访问控制器——S12。

[0245] 然后访问控制器针对分区登记加密代码，使得如果在随后输入该代码，就能够许可对该分区的访问(S13)。

[0246] 访问控制器还经由安全通道将加密代码发送给受邀装置，使得受邀装置能够访问分区。

[0247] 在某些实施例中，加密代码仅对于单个访问有效和/或在有限的时间段内有效。在其他实施例中，加密代码可以无限期有效或者不会过期。

[0248] 在某些实施例中，分区访问应用是作为Apache Cordova Javascript桥访问的API。它存储在安全元件或存储卡中，并保存在板上(即，在安全元件或存储卡中)生成的以下密钥和PIN：

[0249] ●用于应用的一个RSA 2048公有/私有密钥对

[0250] ●每个分区一个可变大小的PIN，以认证用户

[0251] ●每个分区一个3DES-2密钥，以用于加密文件

[0252] 服务器或访问控制器保存能够逐个装置不同的两个3DES-2主密钥。这两个密钥在其创建后被发送给应用，通过应用安全域的安全通道来保护：

[0253] ●用于为了验证应用的可靠性将安全元件应用返回的公有密钥数据加密的初始化密钥

[0254] ●用于在生成用于分区的远程访问代码时提供安全时间源的时间密钥

[0255] 安全时间是后面跟有UNIX时间戳由目标装置给出的随机数、通过时间密钥加密的3DES-2CBC。

[0256] 根据目标文件的大小，能够将分区密钥直接用于加密文件数据，或者将通过手机处-理的密钥用于加密文件数据。

[0257] 下面描述当用户Sarah需要与另一个人Robert共享她的分区数据时随后的处理。

[0258] 前提：

[0259] ●Robert的装置公有密钥被登记到认证服务器(访问控制器)，该公有密钥通过公共标识符(例如Robert的电子邮件)来识别

[0260] ●Sarah登录分区以共享

[0261] ●Sarah请求与Robert共享该分区

[0262] ○服务器获得用于Sarah的应用的安全时间随机数

[0263] ○服务器发送Robert的公有密钥和当前安全时间,它们都被加密以用于Sarah的应用

[0264] ○手机应用获得共享团块,并向Sarah显示共享代码

[0265] ○将共享团块发送给服务器并将其与Robert的公共标示相关联

[0266] ○Sarah将共享代码提供给Robert(通过电子邮件、SMS、电话、语音…)

[0267] ●Robert通过连接到服务器看见新分区被向他共享,并输入由Sarah提供的共享代码

[0268] ○服务器获得用于Robert的应用的安全时间随机数

[0269] ○服务器发送共享团块以及用于Sarah的应用的加密的当前安全时间

[0270] ○通过Robert的安全元件或者Robert的应用恢复分区访问密钥

[0271] 定义以下低级别管理API:

[0272] isSecureElementPresent()

[0273] 如果出现安全元件则返回真

[0274] getSecureElementID()

[0275] 返回安全元件的唯一ID(从CPLC提取)作为HexStringgetCCSEApplicationVersion()

[0276] 返回CC分区应用的版本作为字符串,或者如果没有安装应用,则“不定义”

[0277] 定义以下应用更新和初始化API:

[0278] getKeysetCounter(aid,keysetVersion)(HexString,Number)

[0279] 返回用于给定安全域AID和密钥集版本的计数器

[0280] executeAPDUScript(apdus)(Array of HexString)

[0281] 执行安全元件上的APDU脚本,期望用于每个APDU的9000个状态字

[0282] 定义以下高级别管理API:

[0283] getPublicKey()

[0284] 返回应用的公有密钥、使用初始化密钥加密的3DES-2CBC

[0285] createPartition(shortName,pin)(String,HexString)

[0286] 创建给出短名称和PIN的分区,返回一个字节的分区ID

[0287] listPartitions()

[0288] 返回[id,shortName]的阵列,识别在安全元件上创建的分区

[0289] deletePartition(id)(Number)

[0290] 删除分区。用户必须登录分区来进行删除,或者必须阻止分区的PIN

[0291] 限定以下用途API:

[0292] loginPartition(id,pin)(Number,HexString)

[0293] 登录给定分区

[0294] logoutPartition()

[0295] 从当前登录的分区退出

[0296] encryptData(data,iv)(HexString,HexString)

[0297] 使用具有给定IV的3DES-2CBC加密算法以及当前选择的分区密钥将数据加密

[0298] decryptData(data,iv)(HexString,HexString)

[0299] 使用具有给定IV的3DES-2CBC加密算法以及当前选择的分区密钥将数据解密

[0300] getSecureTimeNonce()

[0301] 返回将要传递给服务器的8字节随机数返回,以提供下一个安全时间

[0302] getSharingCode(secureTime,encryptedPublicKey,validityMinutes)(HexString,HexString,Number)

[0303] 得到用于另一个装置的共享代码。例如将两个元件的阵列、要传递给远程装置的团块以及所生成的8位数代码返回。团块包含共享代码的有效期的终止的时间戳,共享代码与分区密钥相级联并使用PKCS#1填充通过远程装置的公有密钥来加密。在其他实施例中,代码能够具有任何长度和/或能够是字母数字。

[0304] useSharingCode(secureTime,blob,accessCode)(HexString,HexString,String)

[0305] 使用从远程装置获得的共享代码。如果团块、访问代码和时间有效性被应用认可,就能够使用利用分区Id 0xff所提取的分区密钥将文件加密和解密,直到用户退出或者安全元件断电。

[0306] 图10是包括移动装置1、云4和第三方网络服务14的系统的示意图。移动装置1被配置为运行可操作于允许经由云分区3d访问网络服务14的应用。当应用启动时,提示用户输入PIN码。如果提供正确的PIN码,则云分区3d被打开。一旦分区被打开,就从分区3d传送访问网络服务14的凭证C,以允许访问网络服务14。

[0307] 图11是与图10相似的系统的示意图,但是示出了在装置与第三方分区3e之间执行第二认证的情况。如同图10,移动装置1被配置为运行可操作于允许经由云分区3d访问网络服务14的应用。当应用启动时,提示用户输入PIN码。如果提供正确的PIN码,则云分区3d和第三方分区3e被打开。第三方分区启动包括以下步骤的新处理:从装置请求新PIN码,如果收到正确的PIN,就在装置的安全元件与第三方云安全元件之间启动相互认证处理。从装置的安全元件向第三方分区3e传送访问网络服务14的凭证C,从而允许访问网络服务14。

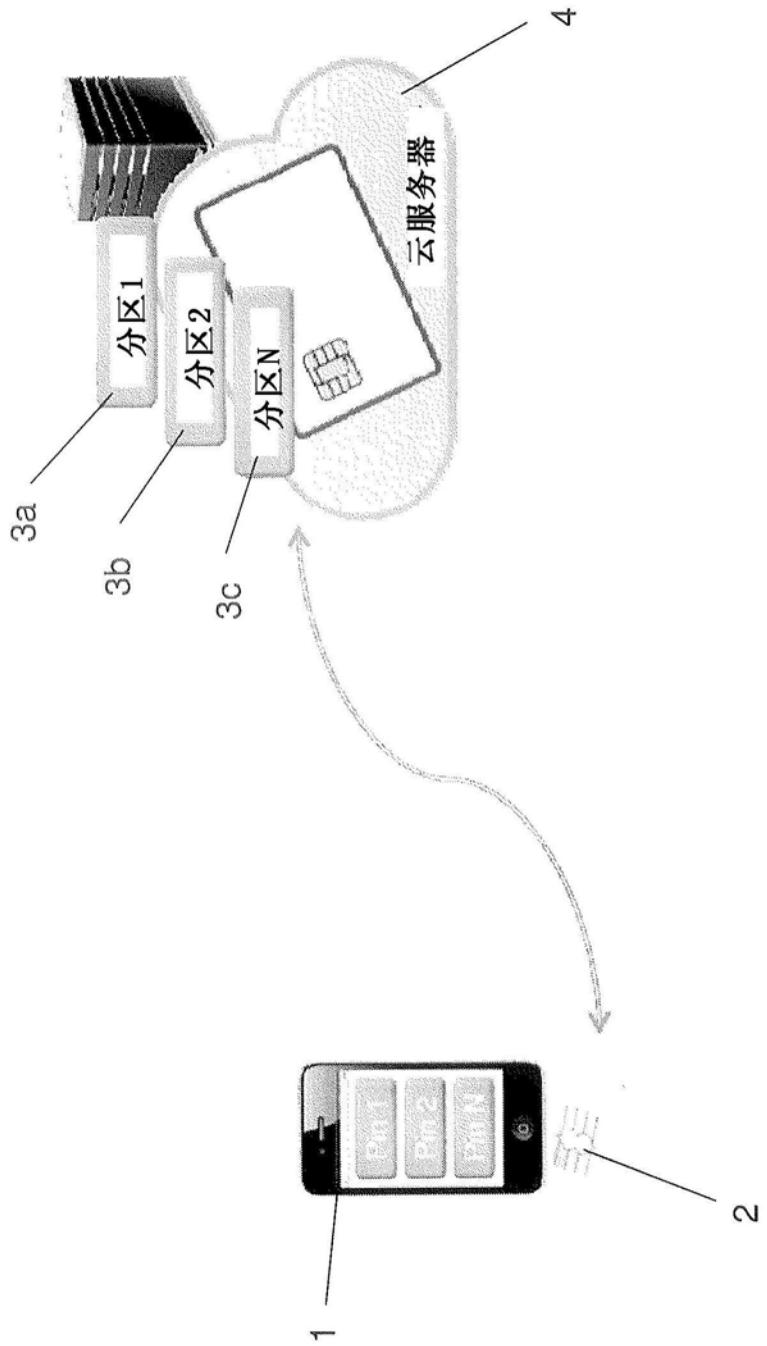


图1

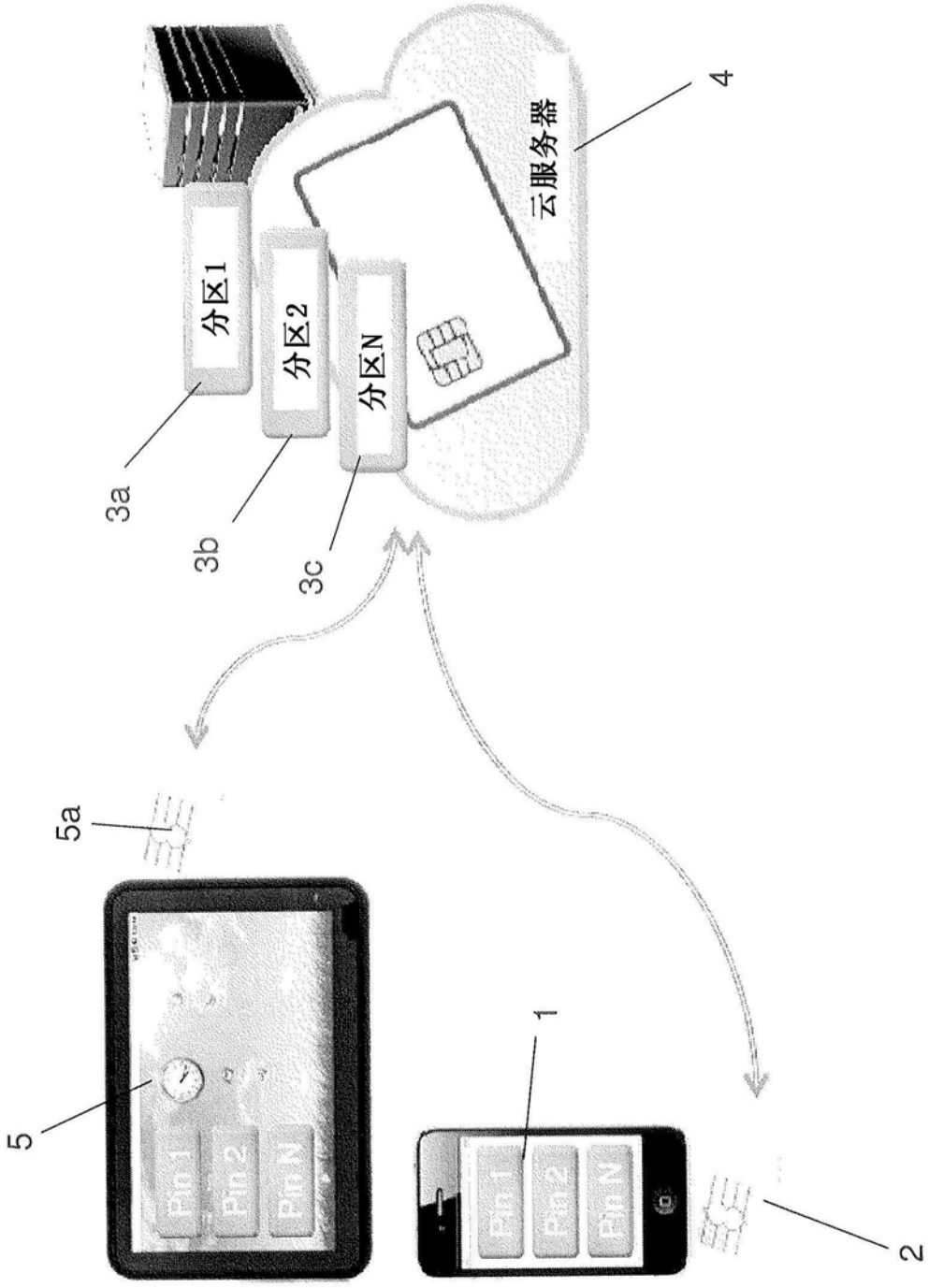


图2

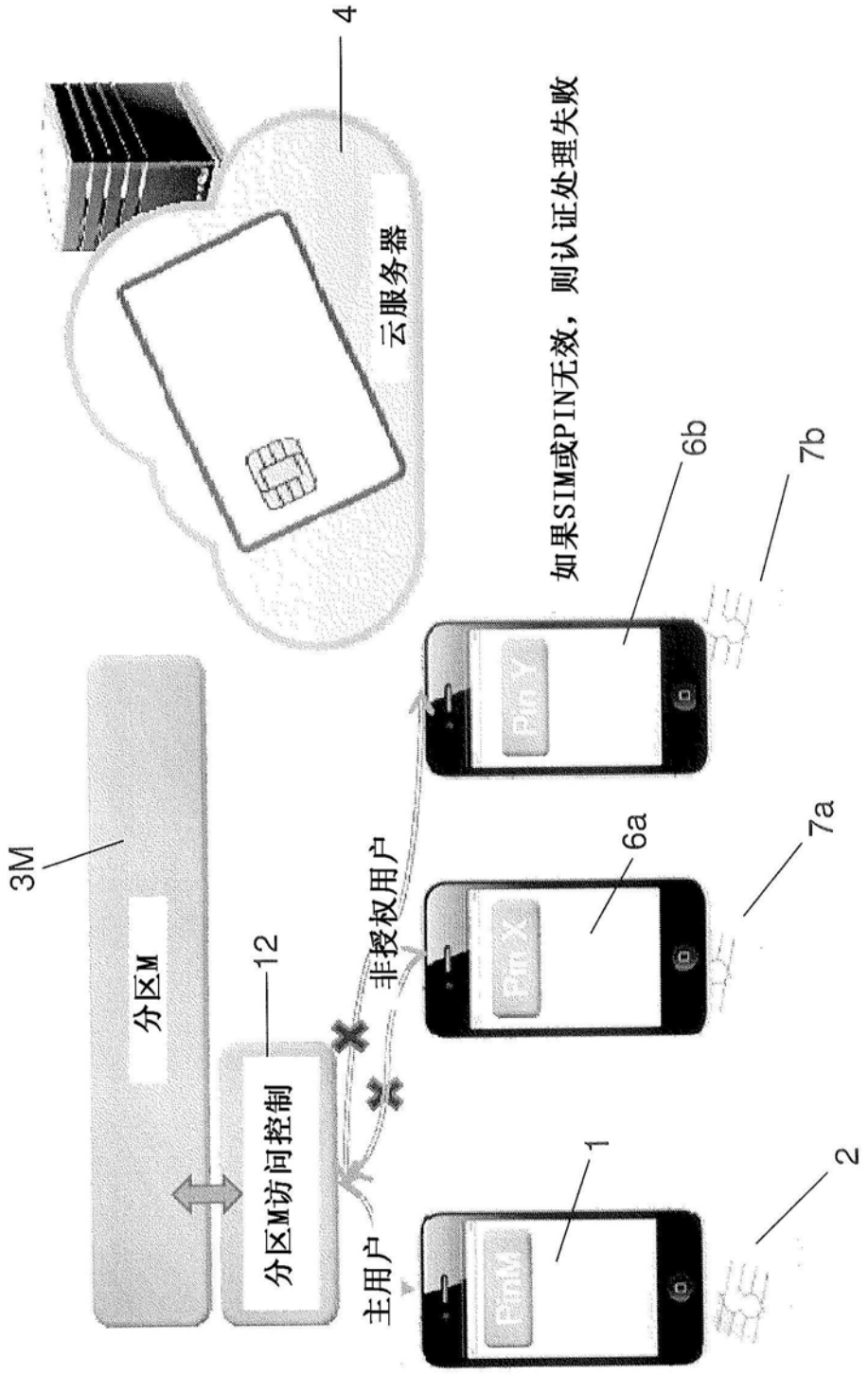

4
云服务器
如果SIM或PIN无效，则认证处理失败
6b
7b
3M
分区M
12
非授权用户
6a
7a
分区M访问控制
主用户
1
2
Pin M
Pin X
Pin Y

图3

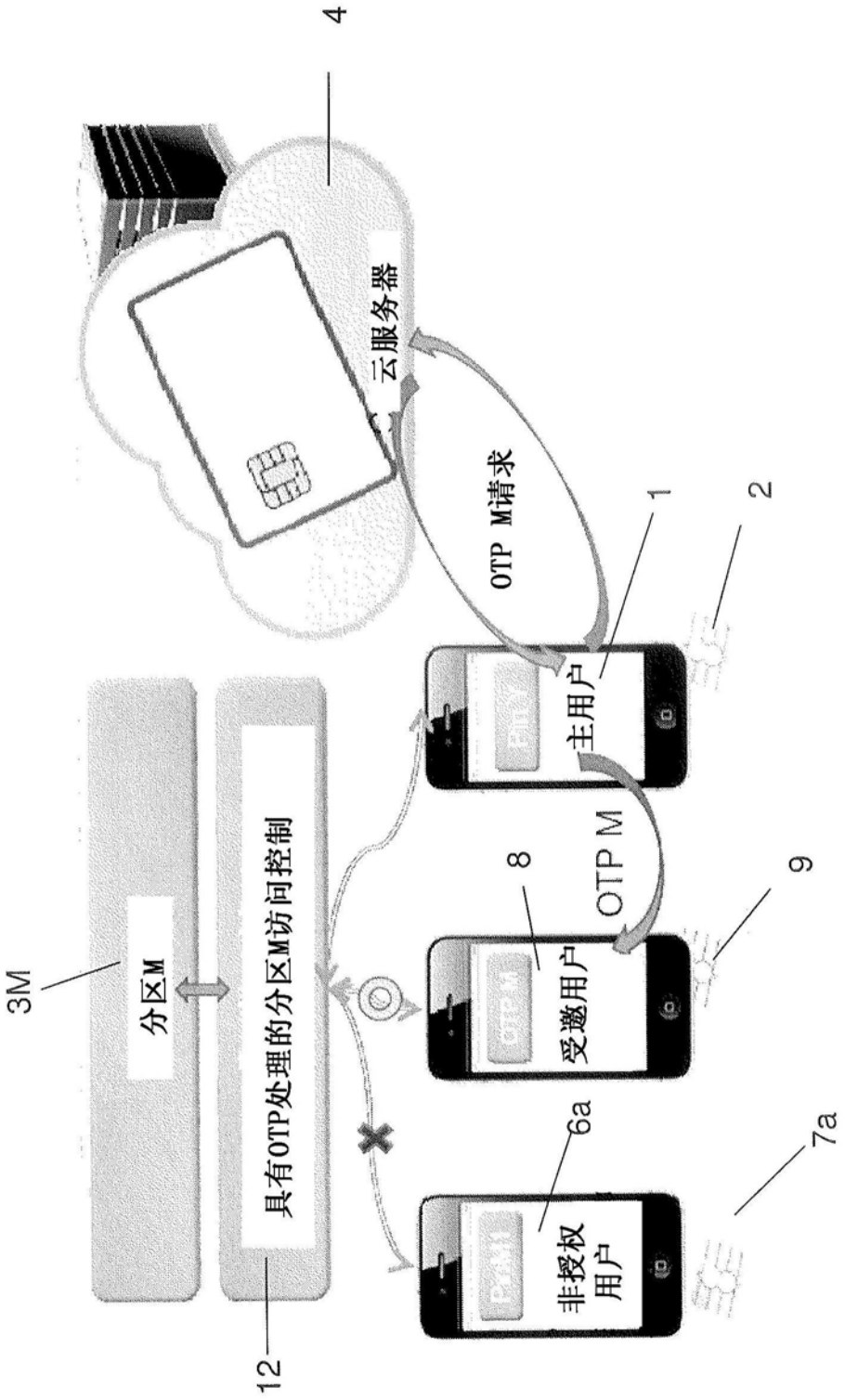

4
云服务器
OTP M请求
1
2
主用户
OTP M
8
9
受邀用户
6a
7a
非授权用户
3M
分区M
具有OTP处理的分区M访问控制
12

图4

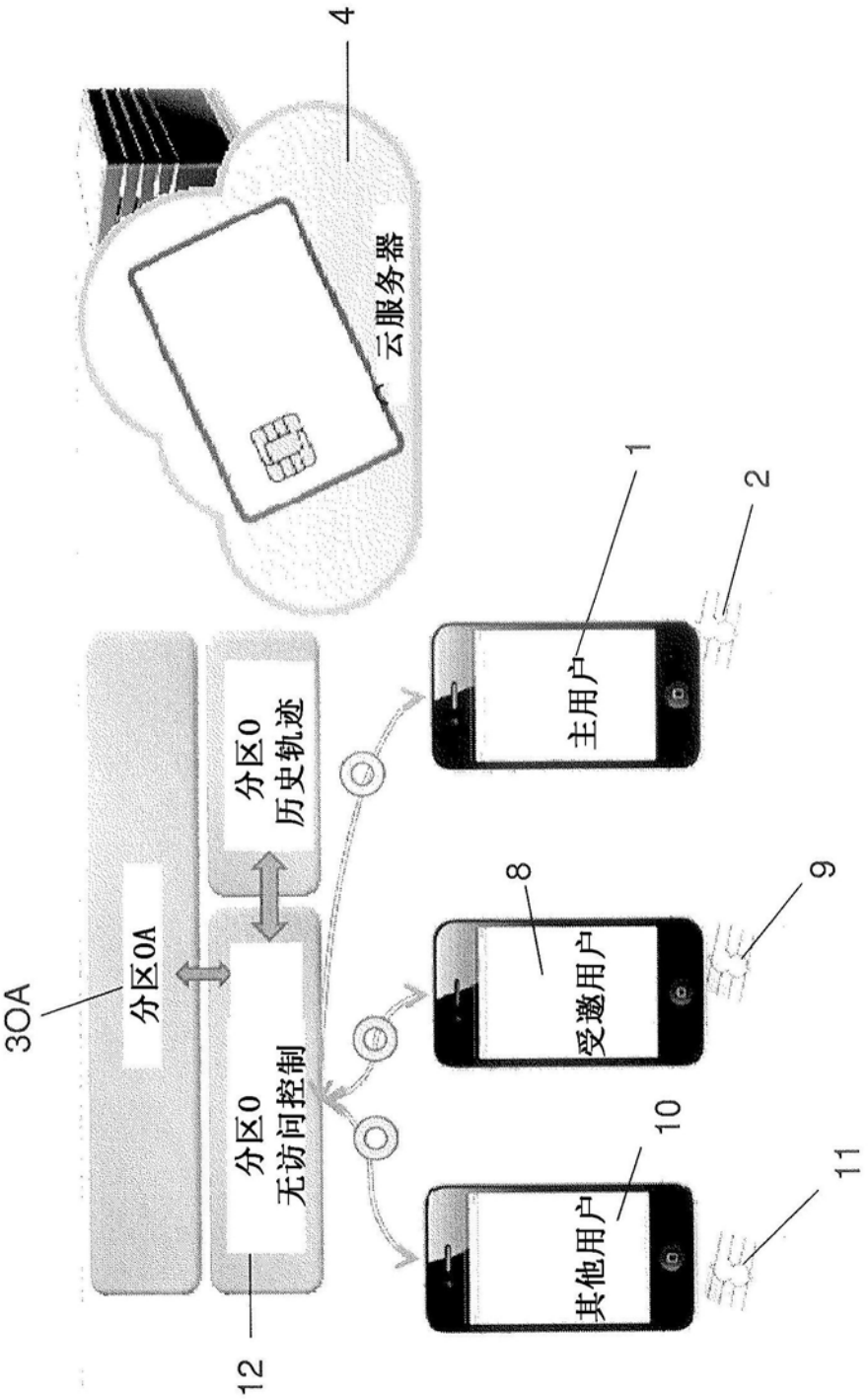


图5

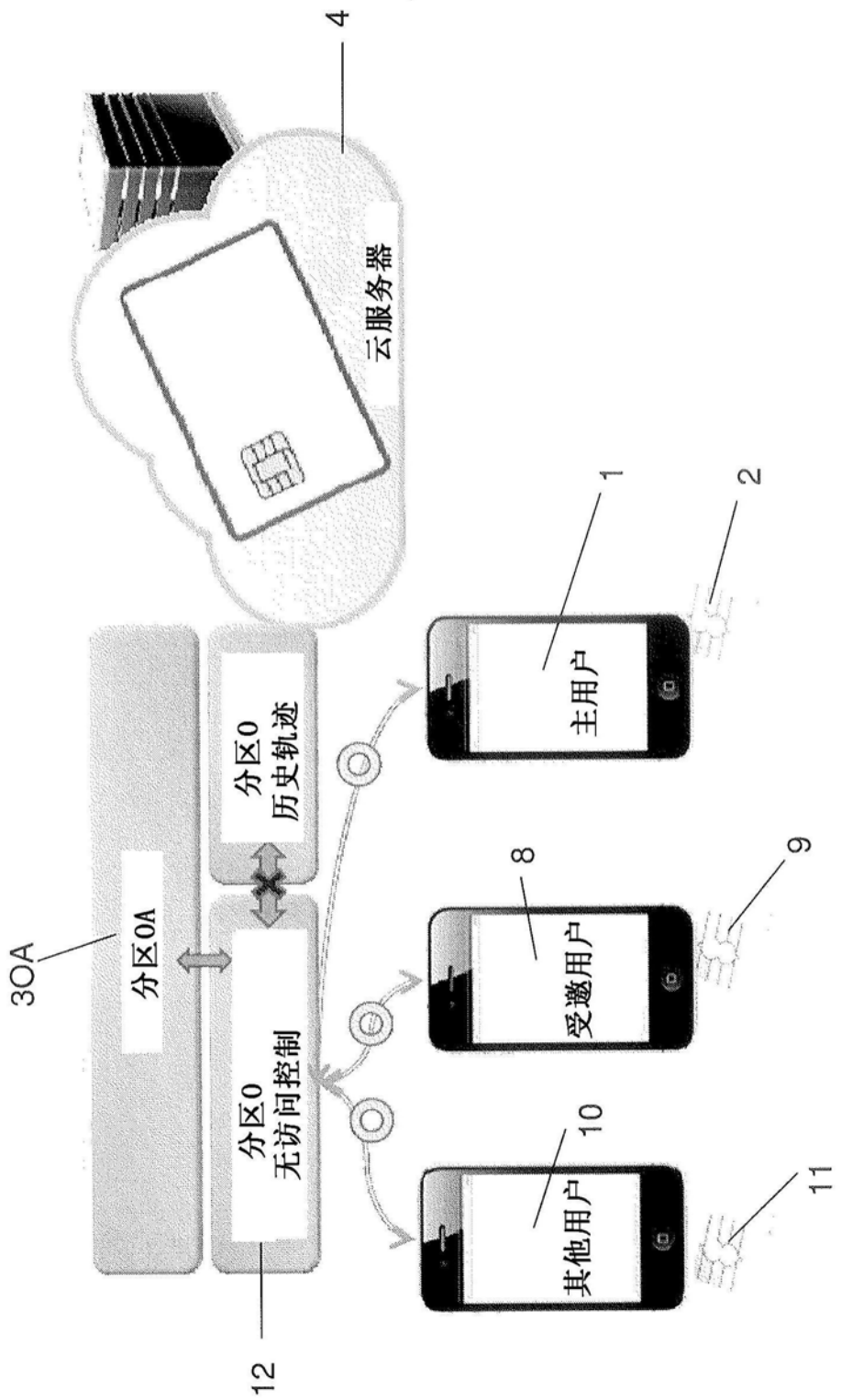


图6

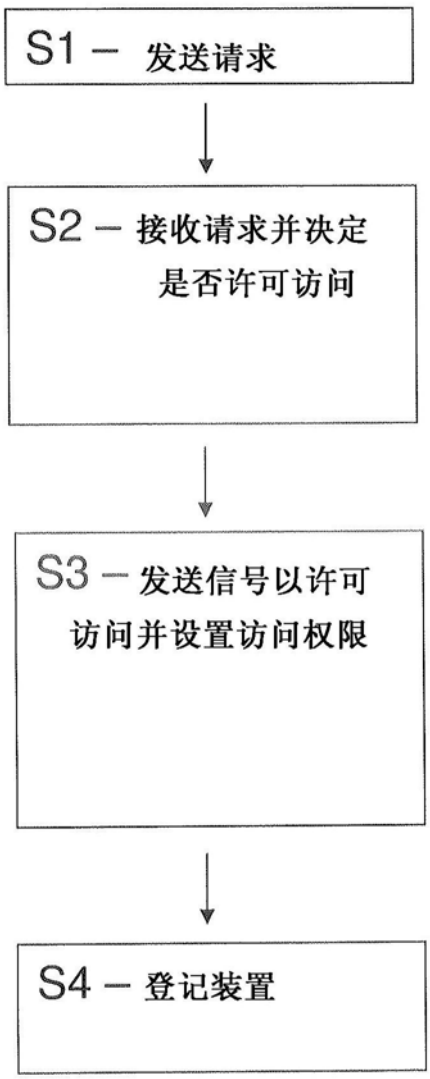


图7

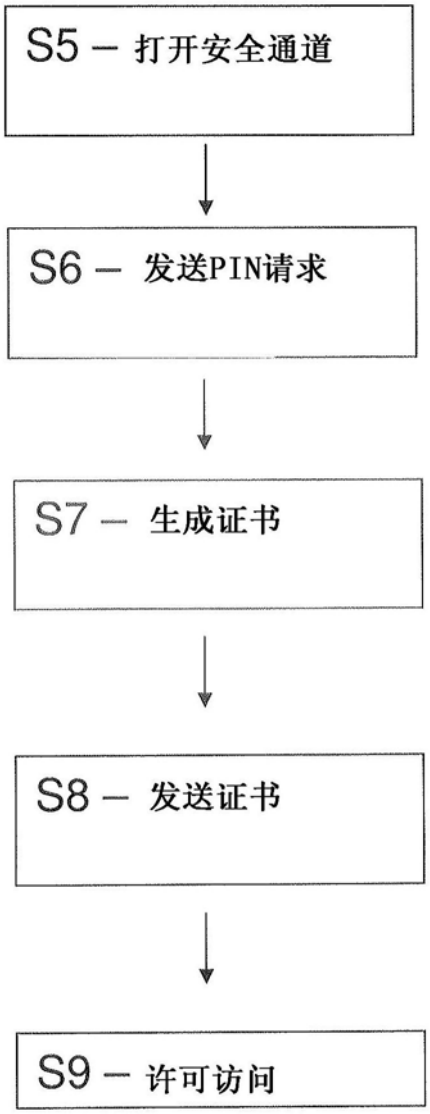


图8

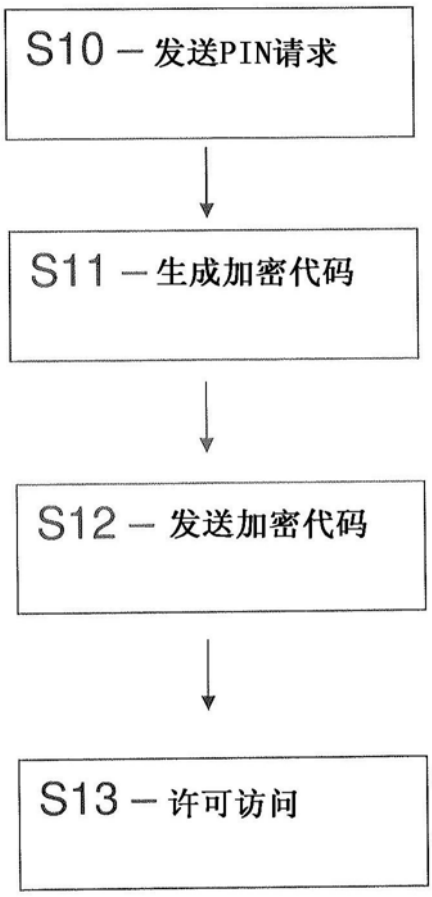


图9

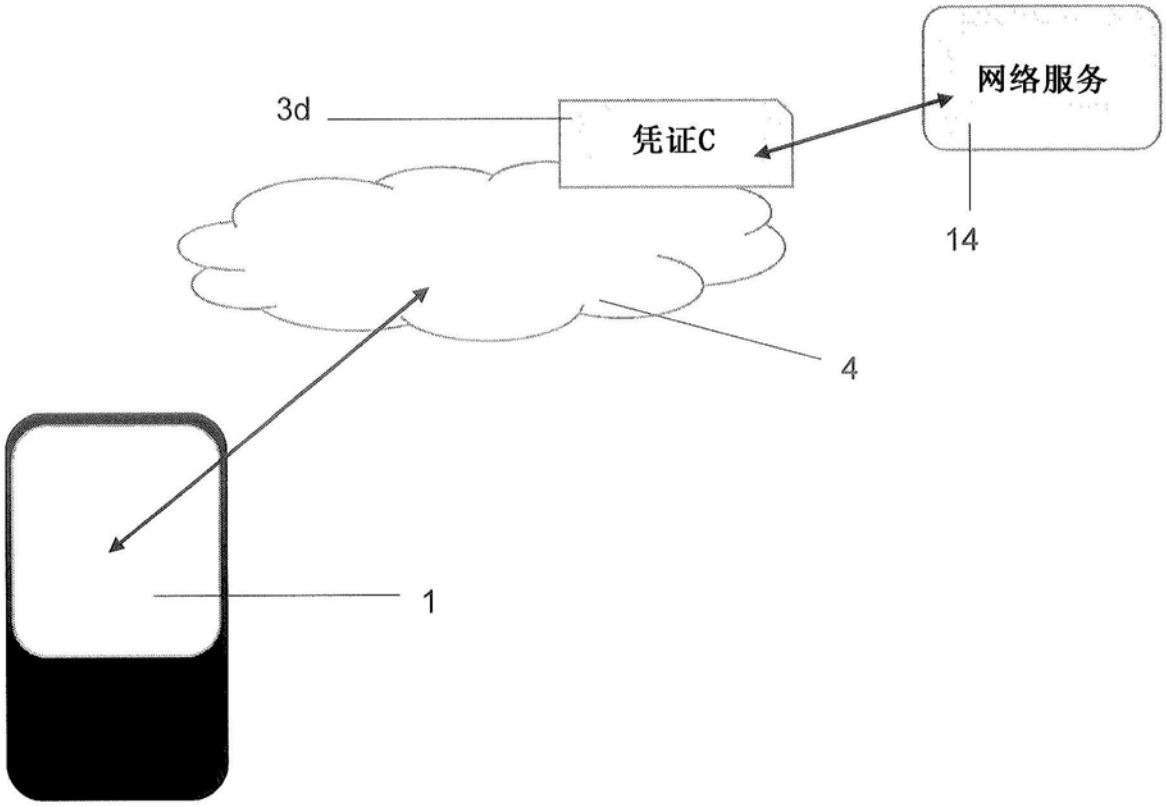


图10

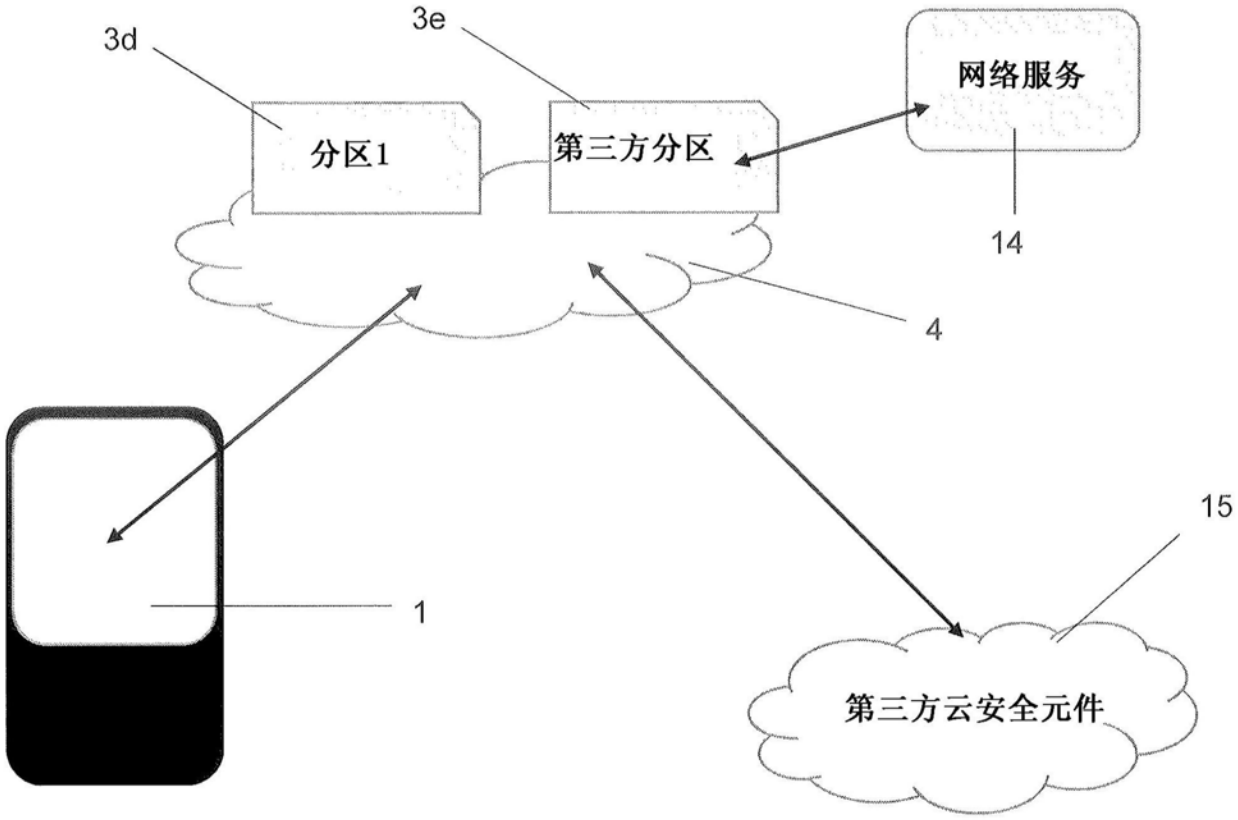


图11