(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 1623167 B
(45)授权公告日 2010.05.26

(21)申请号 02828370.8

(22)申请日 2002.12.20

(30)优先权数据
60/344,658 2001.12.31 US
60/361,458 2002.03.04 US
60/365,068 2002.03.14 US
10/272,464 2002.10.16 US

(85)PCT申请进入国家阶段日
2004.08.27

(86)PCT申请的申请数据
PCT/US2002/041123 2002.12.20

(87)PCT申请的公布数据
WO03/058548 EN 2003.07.17

(73)专利权人 数字数据研究公司
地址 美国佛罗里达州

(72)发明人 小阿瑟·F.·雷吉斯特
弗兰克·J.·坎朋尔

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李德山

(51)Int.Cl.
G06K 19/04(2006.01)
G06K 19/06(2006.01)

(56)对比文件
WO 0163611 A,2001.08.30, 全文.
EP 0956818 A1,1999.11.17, 全文.
FR 28059AA A1,2001.09.07, 全文.
EP 0918301 A3,1999.05.26, 全文.

审查员 李倩

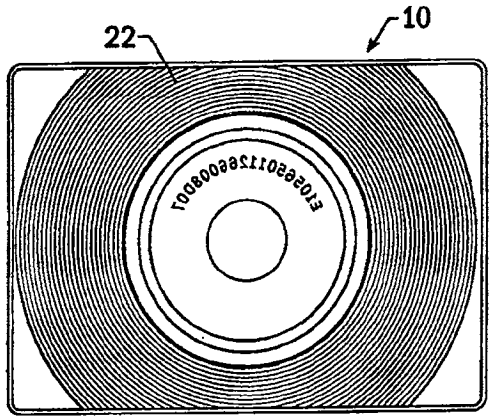
权利要求书 2 页 说明书 21 页 附图 3 页

(54)发明名称

安全许可卡，读取安全许可卡的系统和方法

(57)摘要

本发明的安全许可卡，系统和方法包括存储用于验证卡拥有者的身份的数据的卡。除了其它类型的信息之外，卡存储卡拥有者的生物统计学数据和其它身份数据。数据的不同部分可以利用基于指定给该存储的数据部分的预定安全等级的不同加密技术加密。然后读卡器元件能够读出存储在安全许可卡上的加密数据的至少一部分，并接收来自个人的至少一个生物统计学信息。然后存储在卡中的生物统计学信息和出示安全许可卡的个人的生物统计学信息进行比较，以便验证卡的持有者是否是卡拥有者。



CN 1623167 B

1. 一种安全系统，包括：

安全许可卡 (10)，其具有存储在其上的多个数据部分，其中每个数据部分具有一个和其相关的安全等级值，用于限定数据的安全等级；

至少一个读卡器元件 (16)，其能够从所述安全许可卡读取数据；

至少一个计算系统 (30)，其和所述读卡器元件通信以便从所述安全许可卡访问数据部分，

其中所述至少一个读卡器元件和所述至少一个计算系统具有和其相关的安全许可值，指示所述读卡器元件和所述计算系统可以从所述卡访问哪个安全等级的数据。

2. 根据权利要求 1 所述的安全系统，其中至少一个所述安全许可卡包括存储在其中的卡拥有者的生物统计学识别符，其中所述至少一个读卡器元件能够读取在所述安全许可卡上存储的生物统计学识别符，所述系统还包括：

至少一个生物统计学信息读取器元件，用于读取安全许可卡的持有者的生物统计学信息，

其中所述计算系统和所述读卡器元件以及所述生物统计学信息读卡器元件通信，其中所述计算系统比较由读卡器元件读出的在安全许可卡中存储的生物统计学识别符和由所述生物统计学信息读卡器元件读出的安全许可卡的持有者的生物统计学信息，借以验证持卡者是卡的拥有者。

3. 根据权利要求 1 所述的安全系统，其中当所述安全许可卡被提供给所述读卡器元件时，所述读卡器元件读取在所述卡上存储的所有数据部分，但是只访问具有相关的安全等级的数据部分，所述安全等级被规定为通过和所述读卡器元件相关的安全许可值进行访问。

4. 根据权利要求 3 所述的安全系统，其中所述计算系统接收由所述读卡器元件从所述安全许可卡读出的所有数据部分，并访问具有相关安全等级的那些数据部分，所述安全等级被规定为通过和所述计算系统相关的安全许可值进行访问。

5. 根据权利要求 1 所述的安全系统，还包括：

和所述读卡器元件通信的多个计算系统，其中每个所述计算系统具有和其相关的安全许可值，指示所述计算系统可以从所述卡中访问哪个安全等级的数据，

其中当所述读卡器元件读取在所述安全许可卡上的数据部分时，所述数据部分被提供给每个所述计算系统，并且其中每个所述计算系统只访问对应于和所述计算系统相关的安全许可值的数据部分。

6. 根据权利要求 5 所述的安全系统，

其中所述安全许可卡至少具有第一和第二数据部分，它们分别具有和其相关的第一和第二安全等级值，其中所述读卡器元件具有安全许可值，指示所述读卡器元件可以访问具有第一安全等级的数据，并且至少一个所述计算系统具有安全许可值，指示所述计算系统可以同时访问具有第一安全等级的数据和具有第二安全等级的数据，

其中当所述读卡器元件从所述安全许可卡读出数据时，所述读卡器元件读出第一和第二两个数据部分，并访问具有第一安全等级的数据部分，以及

其中所述计算系统从读卡器元件接收第一和第二数据部分并访问这两个数据部分。

7. 根据权利要求 5 所述的安全系统，其中和至少一个所述计算系统相关的安全许可值

可以被改变，借以改变所述计算系统可以从所述卡访问的数据的安全等级。

8. 根据权利要求 5 所述的安全系统，还包括多个操作者，其能够操作所述计算系统，其中每个所述操作者具有和其相关的安全许可值，指示所述操作者可以访问的数据的安全等级。

9. 根据权利要求 5 所述的安全系统，还包括多个保密位置和与每个所述保密位置相关的读卡器元件，其中每一个所述保密位置具有和其相关的安全等级值。

10. 根据权利要求 9 所述的安全系统，其中所述保密位置是设备、项目的位置和数据文件的位置之一。

11. 根据权利要求 9 所述的安全系统，其中每个安全许可卡具有相关的安全许可值，指示所述安全许可卡的拥有者可以访问的保密位置的安全等级，使得所述卡拥有者只能访问所选择的保密位置。

12. 根据权利要求 11 所述的安全系统，其中和安全许可卡相关的安全许可值可以被改变，从而改变可以由所述安全许可卡的拥有者访问的特定保密位置。

13. 根据权利要求 1 所述的安全系统，还包括多个保密位置，其中每个所述保密位置具有一个和其相关的安全等级值；其中一个读卡器元件和每个所述保密位置相关，并且其中所述计算系统和每个所述读卡器元件通信，其中每个安全许可卡具有和其相关的安全许可值，指示所述安全许可卡的拥有者可以访问的安全等级，以及

其中所述计算系统能够改变保密位置的安全等级值，借以改变哪些安全许可卡拥有者可以访问所述保密位置。

14. 根据权利要求 1 所述的安全系统，还包括多个保密位置，其中每个所述保密位置具有一个数据文件，指示多个个人中的哪一些访问了所述保密位置；其中读卡器元件和每个所述保密位置相关；并且其中所述计算系统和每个所述读卡器元件通信，其中每个安全许可卡具有对应于所述安全许可卡的拥有者的身份值，以及

其中所述计算系统能够改变和保密位置相关的数据文件，借以改变哪些安全许可卡拥有者可以访问所述保密位置。

安全许可卡，读取安全许可卡的系统和方法

技术领域

[0001] 本发明一般涉及安全系统，尤其涉及使用安全许可（securityclearance）卡的安全系统，所述安全许可卡具有增加的存储空间和对于其上存储的信息的增加的安全性，并涉及一种选择性控制由不同的读卡器和操作者访问卡上的数据，以及选择性控制由持卡者对设备的不同部分访问的安全系统。

背景技术

[0002] 大部分公司和政府实体使用安全系统来控制对设备、数据等的访问。访问一般通过使用安全许可卡与／或口令访问进行控制。许多常规的安全系统通过使用读卡器、生物统计学（biometric）扫描仪等用电子方式进行操作。另外，许多常规的安全系统是基于网络的。具体地说，这些系统使用集中的数据服务器，其含有安全访问代码和与允许个人访问设备、数据等相关的数据。例如与个人与／或存储的和个人相关的生物统计学信息相关的数据。一般地说，这些常规的安全系统以集中联网的方式操作，这可能使得访问决策变慢。此外，在这些系统中使用许可卡可能是起码的，它们只包括用于识别和服务器中设置的和用户相关的数据的标记，或者所述的卡可以包括容易被损害的处理器和存储器。常规的安全系统一般也不包括复杂的对设备和位置的关于访问的决策。尤其是，大多数系统只使用标准的进入／非进入决策，并且不允许动态地改变访问准则。最后，许多常规的安全系统没有借助于不同的保密读取器和保密员工对存储在安全许可卡上的不同等级的信息限制访问的能力。下面更详细地讨论这些问题。

[0003] 安全许可卡一般发给已被批准访问特定位置、对象、信息、电子媒体与／或任何其它被限制访问的有形的或无形的对象的个人。例如，包括被限制访问的对象的组织通常对该组织视为有权访问这些对象的个人发放安全许可卡。因此，安全许可卡可以具有某种类型的信息、指示与／或允许具有所述卡的人员一个或几个被限制的对象的装置。例如，一个卡可以包括视觉信息，使得保安或其它人员可以凭视觉检查所述的卡，以便确保所述卡是有效的卡，与／或所述卡可以包括允许自动地访问受限制的对象的信息。

[0004] 通常在发放安全许可卡之前必须对人员进行某种类型的背景检查，例如借助于提供其身份的证明，即出生日期证明，地址证明、驾驶执照、社会保险卡、签证、护照与／或证实个人身份的其它信息。此外，个人必须提供和其背景有关的详详细信息，例如教育程度、职业、社会关系、与／或属于特定类型的背景检查的任何其它和个人历史有关的信息。一旦积累了所需的关于个人的信息，便可以用任何方式证实其对该组织是可接受的，从而这些信息是有效的。

[0005] 一些常规的保密卡包括条形码，磁条与／或其它类似类型的数据存储装置，用于编码与被发给卡的个人相关的数据。所述卡还包括除上述的基本身份数据和访问数据之外的其它类型的数据。

[0006] 在一些安全系统中，使用持卡者的生物统计学信息用于验证。在这些系统中，取持卡者的一个或几个生物统计学信息例如指纹、视网膜扫描、声音抽样、DNA 抽样等，并被存储

在安全系统的集中的数据库内。然后把标记或其它的识别符以条码形式或类似的编码装置被存储在卡上。在操作中，当持卡者把卡呈现给读卡器时，读出和生物统计学信息相关的标记。安全系统使用所述标记轮询网络数据库，检索和持卡者相关的标记。此外，持卡者也具有利用和安全系统相连的生物学统计信息扫描仪扫描的生物统计学信息。安全系统比较取自扫描仪的生物统计学信息和取自卡的存储的生物统计学信息，确定呈现卡的人是否是登记的持卡者。

[0007] 如上所述，生物统计学信息识别符一般不直接存储在保密卡中。而是，把一个标记存储在卡中，并且所述标记提供讯问远方数据库的信息，在所述数据库中存储有和持卡者相关的生物统计学信息识别符。因此，读卡器可以读出存储在卡中的标记，然后根据由所述标记提供的指令讯问合适的远方数据库。在这种情况下，读卡器必须和远方数据库保持连续的或半连续的通信，以便验证持卡者。换句话说，存储的生物统计学信息和扫描的生物统计学信息的比较取决于读卡器和远方数据库通信的能力。此外，存储的生物统计学信息的整体性取决于远方数据库的整体性。生物统计学信息的比较可以容易地遇到危险，因为在读卡器和远方数据库之间的通信可能被阻断，与／或远方数据库可能被有意或无意地破坏。此外，可能具有和从远方数据库中轮询和检索生物统计学信息相关的附加延迟。此外，读卡器的网络连接要求可能是不实际的，例如当安全系统被在位于远方的安全检查点使用时。

[0008] 许多常规的安全卡系统的另一个缺点是存储容量。可以在这些常规的卡中存储的数据的数量受到可被编码而成为被印到卡的表面上的条形码、磁条与／或其它类似类型的数据存储装置的数据的数量的限制。

[0009] 最近研制出了商用卡，其使用 CD-ROM 存储数据。这些商用卡包括 CD-ROM，其形状使得能够装配在卡上。和卡的拥有者相关的商用数据例如姓名、职务、公司、地址、电话号码等位于 CD-ROM 的表面上。这些商用卡的优点是它们允许在 CD-ROM 上存储较多的数据。例如，CD-ROM 卡被用于存储关于和卡拥有者相关的公司的数据。这些数据可以由商用卡的接受者通过常规的 CD-ROM 播放器阅览。

[0010] 虽然 CD-ROM 商用卡增加了可以在卡内存储的数据的数量，但是这些常规的卡不适用于安全环境。特别是，虽然这些常规的商用卡包括在卡的正面上的信息，例如姓名、公司、地址等，以及存储在 CD-ROM 上的关于公司的附加的销售信息，但一般没有印在或存储在卡上的用于使接受者验证该卡属于卡的拥有者的信息。因而，如果一个人出示 CD-ROM 卡，则没有办法保证 CD-ROM 卡属于持卡的人，或者由所述卡记录的数据和持卡的人相关。

[0011] 研制出了用于安全系统的智能卡。所述智能卡包括嵌入的存储器或处理器或者包括嵌入的存储器和处理器。这些卡使得附加的数据信息能够被存储在保密卡上。此外，可以使用处理器处理在存储器内存储的数据。不过，这些卡也可能具有相关的安全问题。特别是，智能卡易于受到窃用。一旦读写智能卡的存储器步骤被确定，在开始的保密数据便可以被容易地访问和改变。因而，这种卡的安全受到威胁，或者可能被改变而被未被授权的人使用。

[0012] 除了和常规的安全许可卡有关的缺点之外，还有和安全系统本身有关的缺点。一个问题是限制的数据访问。特别是，可能需要在保密卡上包括一个宽的数据范围，其中一些数据比数据的其它部分更敏感。例如，除去用于验证持卡者的数据之外，卡还可以包括关

于持卡者的个人数据，例如财政的、金融的和犯罪的记录。在这种情况下，在允许访问用于验证卡拥有者的数据的同时，限制对个人数据的访问是重要的。不幸的是，对于许多常规的保密卡，这是不可能的。一般没有办法保证操作读卡器的人员不能访问在卡上存储的所有数据。因此，一般地说，任何能够读卡的人员都被准许浏览卡上存储的所有数据，这可能限制卡拥有者愿意在卡上存储的数据的类型，除非是卡上存储的数据的唯一的人员是卡拥有者。

[0013] 许多常规的安全系统的另外一个问题是在决定谁可以和谁不可以使用一个设备或数据或需要保密的任何其它的物品时的灵活性。具体地说，许多常规的系统根据“进行 / 不进行”(go/no go) 的决策操作。允许访问某个设备、数据等的人名单在系统中被硬编码，不能被动态地改变。例如，一个人可能最初有权访问设备的一部分，但不能访问设备的另一部分。对于许多常规的安全系统，被提供访问设备的第二部分的人员名单必须利用个人信息被手动地更新，然后提供给读卡器或在设备入口的第二部分的安全门。这可能是费时的，尤其在允许访问一个设备的个人名单被定期地改变的情况下。

[0014] 由现有技术的这些缺点看来，需要一种保密卡，其能够携带大量的数据，同时还提供用于验证卡的拥有者的身份的装置。还需要防止更少的篡改因而提供附加的数据安全的卡。此外，需要一种这样的卡，其根据试图访问信息的个人的安全等级，限制访问存储在卡上的不同等级的数据。

[0015] 还需要一种安全系统，其不需要一直连接到网络上以便验证保密信息，并需要一种允许动态更新关于允许谁访问一个设备的信息的安全系统。

[0016] 法国专利 No.2,805,911 披露了在数字光盘上的预付费卡。所述光盘可以包括条形码、芯片和检索码，以及在盘上的广告。在一种型式中，光盘可以存储和持有者相关的金融信息。

发明内容

[0017] 本发明减轻了现有技术的上述的以及许多其它的有关问题。本发明的安全系统的许多优点在下面进行综述和详细说明。

[0018] 本发明提供一种使用具有大的数据存储容量的安全许可卡的安全系统，同时还提供用于验证卡拥有者的身份的不同特征。此外，本发明的安全许可卡提供一种自含的安全检查系统，使得安全系统的用于验证卡的读卡器不需要一直和网络连接。

[0019] 具体地说，本发明的安全系统提供一种能够存储多个数据部分的安全许可卡。卡拥有者的至少一个生物统计学识别符被存储在至少一个数据部分内。其它的数据部分可以包括关于持卡者的各种信息，例如持卡者的概况、持卡者的银行帐户、犯罪记录等。此外，每个数据部分可以和一个安全等级相关联，使得不同类型的数据可以具有不同的安全等级。

[0020] 数据部分可以根据使用的安全许可卡的类型以不同的方式被存储。例如，可以使用一种包括 CD-ROM 的保密卡，在这种情况下，数据被存储在 CD-ROM 中。卡还可以附加地或者替换地包括位于卡的表面上的数据存储介质，例如存储数据的条形码，全息图等。此外，本发明安全许可卡可以用智能卡来实施，其中把数据存储在卡的存储部分内。

[0021] 如上所述，本发明的安全许可卡包括其中存储的至少一个持卡者的生物统计学信息。这使得和卡相关的安全系统能够独立于网络而操作。具体地说，本发明的安全系统将

包括用于读取所述卡的装置和用于扫描用户的生物统计学信息的装置。在操作中，用户的生物统计学信息被扫描并且预先存储的持卡者的生物统计学信息在 CD-ROM 或智能卡的情况下从卡中存储的数据中或者在条形码或全息图被存储在卡的表面上的情况下从卡的表面上的存储介质上检索。然后使存储的和扫描的生物统计学信息进行比较，以便验证出示卡的个人是卡拥有者。通过在安全许可卡本身设置生物统计学信息数据，安全系统不必询问位于网络上的远方数据库来检索这个数据。

[0022] 这提供了若干优点。首先，所有持卡者的生物统计学信息数据不必都被存储在同一个中心数据库上，在那里所有持卡者的数据可被折中、盗窃和用其它方式被破坏。此外，本发明的安全许可卡不需要通过网络发送保密数据，在那里数据可能被拦截。此外，其允许安全检查点或者完全地或者部分地不需网络连接，使得所述检查点是自含的并且可以位于远方位置。

[0023] 如上所述，本发明的安全许可卡一般包括存储在其上的和持卡者相关的或和持卡者相关联的各种数据。除去用于验证卡拥有者的数据之外，例如生物统计学信息数据，安全许可卡可以包括关于持卡者的信息的数据。这些数据包括关于用户的一般性数据，但是也可以包括更敏感的保密数据，例如金融数据、医疗数据、犯罪记录等。假设各种各样的数据可以位于卡上，重要的是限制访问这些数据。由此看来，存储在本发明的保密卡上的数据被存储在不同的等级下。然后限制这些等级被其他人访问和浏览。在本发明的安全系统中指定操作者与 / 或装置能够访问不同的等级，使得数据只能被指定能够观看某个等级的数据的人员读取。

[0024] 本发明的安全系统还使得从安全许可卡读出的数据能够传递到安全系统中的起其它装置。具体地说，安全许可卡可以包括在按照访问被限制的不同的等级下存储的数据。读卡器可以扫描卡中的所有数据，但是由于限制的安全访问，只能读数据的某些部分。不过数据的其它部分可以传递到安全系统的其它装置，这些装置能够读其它等级的限制数据。用这种方式，可以由读卡器检索卡中的数据，并且虽然不能被读卡器理解，但是可以传递到较高的安全等级的其它装置，这些装置有权读取这些数据。

[0025] 作为一个例子，读卡器只能访问卡上的用于验证持卡者并允许访问一种设备所必须的数据。不过，关于持卡者的政治记录的数据的部分也可以由读卡器读取，虽然读卡器不能解密，但可以传递给和读卡器相连的其它装置，在那里其可以被浏览，以便确定个人具有的安全威胁。

[0026] 在卡中还存储关于卡的事件的记录。例如，对于数据部分的修改或添加、卡的产生与 / 或从持卡者接收生物统计学信息的记录可被存储在卡中。这个审计记录使得保安人员能够跟踪卡的使用以及卡的安全的可能的违反或违反卡的安全的企图。

[0027] 本发明安全许可卡的还能够存储关于开始日期、验证日期等信息。具体地说，卡可以包括可以通过读卡器读出的到期日期。如果卡超过了选择的到期日期，则持卡者将被拒绝访问。这对于防止卡的窃用是重要的。尽管卡已经被盗，但其只能在有限的时间内被使用。此外，卡上可以包括开始日期。开始日期限定一个所述卡变得有效的时间。在开始日期之前卡的使用可以被安全系统拒绝。起点日期也可以被存储在卡上。这个起点日期可用于这样一个方案中，其中用于加密卡上的数据的加密方法被随时改变。具体地说，在日期的一个范围内，在这些日期内产生的卡可以使用一种方法加密，而对于另一个范围内的日期

则使用一种单独的方法。当读卡时，起点日期也被读出。根据起点日期，读卡器将知道使用哪一种加密方法读卡中的数据。

[0028] 为了保证数据的整体性，本发明的安全系统对于卡上存储的数据不总是使用“写一次 / 读多次”的处理。写一次 / 读多次的处理阻止试图再次使用卡进行欺骗访问的某人重写卡上的保密数据。

[0029] 卡上的数据可以利用多种加密技术的至少一种进行加密。具体地说，数据的不同部分可以根据指定给存储的数据的部分的安全等级使用不同的加密技术加密。这些加密技术可以包括多种算法，它们被用于加密卡中存储的数据的至少一部分。例如，所述算法可以是分组密码加密算法。

[0030] 本发明的安全系统还使得能够动态地改变被允许访问设备的某个位置、数据等的人员的表。具体地说，通过网络，允许访问一个特定位置的人员表可以在远方被改变或者被更新，并利用读卡器存储。当卡被读卡器扫描并且持卡者被验证时，读卡器可以访问所述的表，并确定持卡者是否已被指定作为能够访问所述设备的人员。如果持卡者不在表中，则禁止所述访问。

[0031] 作为一种替代方案，保密位置的安全等级可以被改变，借以改变允许访问的卡拥有者的表。例如，如果保密位置具有只允许少数的卡拥有者访问的第一安全等级，则和该保密位置相关的安全等级可被降低，借以允许更多的卡拥有者访问。

附图说明

[0032] 上面说明了本发明的一般原理，现在参照附图进行说明，附图未按比例绘出，其中：

[0033] 图 1 是按照本发明的一个实施例的安全系统的应用的示意图；

[0034] 图 2 是按照本发明一个实施例的安全许可卡的 CD-ROM 的平面图；

[0035] 图 3 是位于按照本发明的一个实施例的安全许可卡的表面上的数据存储介质的平面图；

[0036] 图 4 是按照本发明的一个实施例的能够和控制中心与 / 或远方存储元件通信的多个读卡器的示意图；

[0037] 图 5 是表示按照本发明的一个实施例的读卡器的功能的示意图；以及

[0038] 图 6 表示按照本发明的一个实施例在安全许可卡中存储的数据的等级、数据的用户的可能的分类和子分类、以及哪些子分类允许访问数据的那些等级的图。

具体实施方式

[0039] 现在参照附图详细说明本发明，附图中表示本发明的一些实施例，但不是所有的实施例。的确，本发明可以用许多不同的形式实施，因而不应当的解释为局限于这里提出的实施例；而是提供这些实施例是为了使本说明满足可适用的法律要求。在所有附图中相同的标号表示相同的元件。

[0040] 本发明提供一种安全许可卡，其能够克服和现有技术有关的上述的许多缺点。具体地说，本发明提供一种安全许可卡，其允许大的数据存储容量，同时还提供用于验证卡拥有者的身份的不同的特征。此外，本发明的安全许可卡和读卡器相结合能够关联在卡上存

储的数据的部分和不同的安全等级，并限制读卡器与 / 或读卡器的操作者可以浏览与 / 或访问的数据的数量。

[0041] 本发明一般涉及一种安全系统，其能够验证希望访问受限信息、位置或其它的有形的或无形的项目的个人的身份。本发明的安全系统的一个实施例如图 1 所示，但是可以产生许多所述安全系统的其它的实施例和应用，其中的许多将在下面详细说明。例如，个人 12 可能希望进入门 14。其可以出示安全许可卡 10，所述安全许可卡被读卡器 16 读取。读卡器 16 也能够接收个人 12 的生物统计学信息数据，并和在卡上存储的生物统计学信息数据比较，卡上存储的生物统计学信息数据和卡拥有者相关。通过监视器 18，读卡器的操作者可以看到生物统计学信息的比较和在卡上存储的准许操作者访问的数据的部分。如果个人 12 的生物统计学信息和卡 10 上存储的生物统计学信息匹配，并如果由操作者 20 访问的数据和允许卡拥有者进入门 14 所需的数据匹配，则个人 12 被允许进入门 14。在另一方面，如果个人 12 的生物统计学信息不和卡 10 上存储的生物统计学信息匹配，与 / 或如果由操作者 20 访问的数据和允许卡拥有者进入门 14 所需的数据不匹配，则不允许个人 12 进入门 14。另外，卡拥有者的扫描的生物统计学信息和卡上存储的生物统计学信息的比较可以用电子方式通过计算机或专用处理器进行。

[0042] 卡 10 可以包括身份数据、工作数据 (field data)、以及任何有关的额外数据。身份数据包括可用于证明持卡者确实是卡拥有者的任何类型的数据。例如，身份数据可以包括但不限于 :卡拥有者的姓名、地址和出生日期。身份数据还可以包括卡拥有者的至少一个生物统计学信息。

[0043] 工作数据可以是关于卡拥有者与 / 或卡拥有者所负责的项目的任何类型的更详细的数据。例如，工作数据可以包括但不限于 :驾照号码，驾照限制，投票者信息以及卡拥有者的职业信息，与 / 或这些项目的历史，利用这些项目的信息，或任何其它类型的关于卡拥有者负责的项目的其它类型的信息。工作数据可以具有多个等级，每个等级可以和一个不同的安全等级相关。例如基本雇用信息、例如卡拥有者的老板的姓名和地址，可以位于工作数据的第一级，而卡拥有者的个人记录可以和基本雇用信息相关，但是位于工作数据的一个或几个更高的级，其比第一级更加保密。此外，工作数据可以包括高分类的数据，其具有最高的安全等级。高分类的数据可以包括但不限于 :卡的内部控制和卡拥有者的至少一个生物统计学信息。

[0044] 额外数据可以是卡拥有者的希望在卡中存储的任何其它类型的数据。例如，额外数据可以是文件、文档、表格或其它类型的数据。如果需要，额外数据也可以被指定安全等级。

[0045] 数据一般被分成数据部分或分组，如本领域技术人员熟知的。每个数据部分可以和多个安全等级中的一个相关，并且每个数据部分可以被压缩、编码与 / 或加密，如下所述。为了简明，这里可以把数据部分称为“数据”。

[0046] 卡拥有者是其身份数据被存储在卡中的个人。在卡 10 中存储的工作数据与 / 或额外数据可以和卡拥有者相关联。另外，工作数据与 / 或额外数据可以和卡拥有者负责的某些有形的或无形的项目相关联。例如，在卡上存储的工作数据与 / 或额外数据可以和船、集装箱、组织、概念、电子媒体或其它类型的有形的或无形的物体相关联，卡拥有者可以是负责所述对象的任何个人。此外，在一些用于验证卡 10 的卡拥有者的身份的卡的实施例中，

可以具有一个以上的卡 10 的卡拥有者。在这种情况下，在卡中存储有和每个卡拥有者相关的身份数据。

[0047] 如上所述，在卡 10 中存储的身份数据可以取任何形式，可以是用于识别一个或几个卡拥有者的任何选择的数据。例如，和卡拥有者相关的生物统计学信息数据可被存储在卡中。所述生物统计学信息数据可以是本领域技术人员已知的任何类型的生物统计学识别符。例如，生物统计学识别符可以是指纹、视网膜扫描、语音采样、DNA 抽样中的一个或几个，或者是两个或几个的组合，或者是任何其它类型的生物统计学信息。生物统计学信息数据可被存储在卡中的在呈现所述的卡以便验证卡拥有者的身份时容易访问的位置，使得存储的生物统计学信息能够和出示卡的个人的生物统计学信息比较，如在下面详细说明的。此外，生物统计学信息数据可被存储在卡的高分类的部分，对这个部分的访问具有严格的限制，使得保持生物统计学信息数据的整体性。此外，可容易访问的生物统计学信息数据可以和高分类的生物统计学信息数据比较，以确保容易访问的生物统计学信息数据的精度不会被折中。

[0048] 如果出示卡 10 的个人（也称为持卡者）的生物统计学信息和卡 10 中存储的生物统计学识别符匹配，则出示卡的个人可被允许进行操作、准许访问一个空间或物品，能够利用卡中存储的任何数据，与 / 或由在卡中存储的数据允许的任何其它类型的操作。但是，如果出示卡 10 的个人的生物统计学信息和卡 10 中存储的生物统计学识别符不匹配，则出示卡的个人被拒绝本来可允许卡拥有者进行的任何操作。

[0049] 图 2 和图 3 表示一种按照本发明的一个实施例的安全许可卡 10（下文称为卡）。这个实施例的卡包括用于验证卡拥有者的身份的几个特征。例如，卡 10 被形成在 CD-ROM 22 上。CD-ROM 不仅可以包括一般的工作数据和识别数据，而且可以包括额外数据。如图 3 所示，卡 10 也可以包括位于卡的表面上的数据存储介质 24。数据存储介质 24 可以包括一般的工作数据和识别数据。

[0050] CD-ROM 22 可以是任何类型的本领域技术人员已知的 CD 存储元件。一般地说，CD-ROM 22 呈卡 10 的形状，其中心在卡 10 的中心。这样，卡 10 可被放置在 CD-ROM 读卡器上，在其中可以读卡的 CD-ROM 部分，如下所述。在本发明的优选实施例中，存储在 CD-ROM 中的数据可以只由访问该 CD-ROM 的人员读取，所述数据不能被删除、改变或修改。被写入 CD-ROM 中的数据被永久地存储在 CD-ROM 内。这样，新的数据可被写入 CD-ROM 中，但是旧的数据也保留在 CD-ROM 中。这种类型的 CD-ROM 一般被称为 CDR。CDR 在本发明的安全许可卡 10 中是有利的，因为其确保在卡中存储的所有数据被永久地记录，供将来参考。CDR 有时被称为“写一次 / 读多次”。此外，CD-ROM 也可以包括含有在 CD-ROM 内存储原始数据以及存储随后的数据的操作者的操作者位置和识别信息的审计跟踪。这样，如果在卡中存储的数据曾经具有问题，则原始数据和数据被写入的环境可以容易地从卡中获得。因此，这类数据存储比现有的用于存储数据的技术例如基于微处理器的智能卡安全得多，能够防止篡改，智能卡没有防止其中存储的数据被篡改的能力。

[0051] 必须理解，可以使用其它的数据写入处理。在本发明的其它实施例中，例如不能保证在卡中存储的数据这样高度安全的那些实施例中，可以使用除去被读之外还允许写入的数据被删除、改变或修正的 CD-ROM，这种类型的 CD-ROM 一般被称为 CDRW。

[0052] 关于图 2，数据存储介质 24 可位于卡上的任何位置，只要不妨碍卡的 CD-ROM 部分

即可。例如，数据存储介质 24 一般以编码的格式被印在卡的至少一面上，如图 3 所示。为此目的，编码数据参考一般的电子数据格式存储在卡 10 上。因而，被编码不等于被加密，加密被定义为改变数据使得只有被批准的一方才能对其访问。包括在数据存储介质 24 中的数据使用本领域技术人员已知的任何技术被编码，使得数据可以被能够译码该数据的读取器使用，如下面详细说明的。例如，数据存储介质可以以条形码例如 PDF-417 编码。另外，数据存储介质可以全息图、一系列的编码的点、图形图像、磁条等形式被存储。和上面对 CDR 的讨论类似，条形码或其它类型的不能被容易地改变的标记是一种用于存储数据的有利的技术，因为数据和关于产生数据的环境被永久地存储在卡中供将来参考。

[0053] 除去生物统计学信息数据和在卡中存储的任何其它类型的数据之外，CD-ROM22 与 / 或数据存储介质 24 可以包括卡拥有者的数字照片。该照片可用于将来检查出示卡的人是否是卡拥有者，因为当卡被读卡器读取时，如下面详细说明的，操作者可以访问卡拥有者的照片，凭视觉比较照片和出示卡的人。另外，读卡器可以拍摄出示卡的人的照片，例如利用照相机等，然后比较拍摄的照片和卡拥有者的照片。因而，数字照片一般被存储在 CD-ROM 与 / 或卡的数据存储介质部分中，作为识别数据，但是也可以作为工作数据的一部分被存储。在本发明的卡 10 的其它实施例中，卡拥有者的照片 26 可被包括在卡 10 的表面上，如图 3 所示。照片 26 可被附加在 CD-ROM 与 / 或卡 10 的数据存储介质内，或者作为在其中存储的图像的替代物。

[0054] 除去卡 10 的终止与 / 或有效日期外，卡 10 还可以包括在卡的表面上的任何其它类型的数据，例如卡拥有者的姓名、电话号码与 / 或职务，如图 3 所示的卡的一面的实施例的区域 28 所示。

[0055] 重要的是，如图 2 和图 3 所示，本发明提供一种安全许可卡，其中存储有几种不同类型的识别数据，用于验证卡拥有者。下面和整个安全系统（也称为识别验证处理）的各个方面一道进一步说明卡拥有者的验证处理，所述安全系统用于产生卡并用于通过所述的卡维护安全和访问。

[0056] 图 2 和图 3 说明本发明的安全许可卡，其作为在表面上印有信息的 CD-ROM。必须理解，这仅仅是安全许可卡的一个实施例。具体地说，本发明的安全许可卡可被作为标准的卡来实施，其具有数据存储介质例如被印在其上的条形码。在这个实施例中，识别数据、工作数据以及任何可能有关的额外数据被存储在印在卡的表面上的数据存储介质中。卡的这个实施例的操作非常类似于安全系统中的 CD-ROM 卡，具有 CD-ROM，其优点是比在卡的表面上印的数据存储介质具有更大的数据存储容量。另外，本发明的安全许可卡也可以作为智能卡来实施。数据存储和外观和 CD-ROM 卡类似。简短地说，本发明的各个方面不限于利用基于 CD-ROM 的卡，而是可以利用许多具有不同数据存储装置的不同类型的卡。

[0057] 第一方面是关于卡拥有者的数据的收集和存储，用于产生安全许可卡。具体地说，为了在卡中例如 CD-ROM 与 / 或卡的数据存储介质部分中存储所需的数据，识别验证系统的操作者从未来的卡拥有者接收身份数据，并把该数据存储在数据库中。可以使用本领域技术人员已知的任何类型的数据库，所述数据库可以通过任何合适的协议被访问。在本发明的识别验证系统的一个实施例中，数据库可以是相关的，并且数据库可以通过打开的数据库连接 (ODBC) 标准协议访问。数据库可以位于操作者的位置，或者位于远方，并通过网络例如局域网、广域网、内联网与 / 或互联网和操作者的位置进行常规的或者无线的通信。

[0058] 图 4 表示读卡器 16 的各个实施例，其中之一是常规的计算机 30，操作者可以利用它访问位于计算机 30 或者位于控制中心 56 的数据库。控制中心 56 可以在任何类型的位置，在那里进行可能的卡拥有者的识别验证，如下所述。控制中心 56 还可以是一个位置或者元件，在那里保存着和所有或者至少一部分卡拥有者以及将来的卡拥有者相关的识别数据的中心存储库。如下面详细说明的，读卡器 16 与 / 或读卡器的操作者的数据访问能力可以根据需要通过控制中心被控制和改变。

[0059] 可以用本领域技术人员已知的任何方式从未来的卡拥有者获得数据。例如，未来的卡拥有者可以向操作者提交文件，例如出生证、地址证明、驾驶执照、护照、签证、或其它官方文件。一旦操作者通过任何可接受的确定方式确定由未来的卡拥有者提供的信息属实，操作者便可以在数据库中产生一个记录，例如文档，其包括和未来的卡拥有者相关的被证实的身份数据。记录还可以包括和卡相关的终止日期，使得在终止日期之后使卡失效，与 / 或和卡相关的有效日期，指定使卡成为有效的某个将来的日期。永久的或长期的安全许可卡没有终止日期，或者对卡拥有者产生为数年的终止日期，这种卡存储各种类型的长期的识别和工作数据。例如，在本发明的安全许可卡的某个实施例中，驾驶执照信息、选举注册信息、雇用信息和其它类型的长期信息可被包括在卡具有的工作数据中。这样，一旦在卡中要包括的所有信息被验证，便可以发给卡拥有者一个永久的或长期的卡。此外，对于短期的应用，例如对于办公大楼的短期的访问者，对于一个国家的短期访问者与 / 或在对于时间信息正在被检验期间的永久的或长期的卡，可以发给临时的安全许可卡，其可以只包括为卡的短期应用所需的识别与 / 或工作数据。

[0060] 为了在数据库中产生一个记录，操作者通过接口向数据库输入识别数据，所述接口可以是任何类型的计算机 30、处理元件与 / 或和数据库通信的数据输入元件与 / 或网络 32 或和数据库通信的类似物，例如位于控制中心 56 的数据库，如图 4 所示。例如，在本发明的识别验证系统的一个实施例中，操作者接口可以是利用任何现代操作系统例如 Windows 或 Unix 操作系统的计算机。其它的信息也可以包括在记录中，根据卡的将来应用、特定识别验证系统的要求或任何其它理由而定。如果操作者不能确定由未来的卡拥有者提供的信息属实，则可以拒绝发给其安全许可卡，而发给一个临时卡，该卡直到完成验证时才有效，与 / 或要求个人进一步提供信息。

[0061] 未来的卡拥有者还至少提交一个生物统计学信息，用于在数据库记录中存储。例如，在本发明的身份验证系统的一个实施例中，未来的卡拥有者可以通过和操作者的接口通信的指纹扫描仪向数据库提供至少一个指纹。所述指纹扫描仪可以是本领域技术人员已知的任何类型的。在本发明的身份验证系统的一个实施例中，指纹扫描仪是安全触摸 PC 扫描仪，可以在市场上从生物统计学信息访问公司 (BAC) 得到。生物统计学信息例如个人指纹的图像然后可被从扫描仪传递给操作者的接口。生物统计学信息可被分析与 / 或制备以便通过操作者的接口以本领域技术人员熟知的任何方式被存储。例如，如果生物统计学信息是指纹的图像，可以从图像中利用 BAC 软件或本领域技术人员已知的任何其它类型的软件提取特征模板。特征模板从图像中消除无关的数据，以便有助于生物统计学信息图像的比较。

[0062] 可以使用和指纹不同的或者除指纹之外另外的生物统计学信息。例如，可以取卡拥有者的视网膜或面部扫描，DNA 或语音抽样，心跳特征等并被记录。然后或者独立地或者

组合地使用这些不同的生物统计学信息验证安全许可卡的卡拥有者。

[0063] 还可以记录未来的卡拥有者的一个或几个图像，以便被包括在数据库记录中。所述图像可以是数字的或任何其它类型的照片。如果图像是数字的，则可以直接传递给操作者的接口和数据库。如果图像不是数字的，则可以被扫描而成为数字格式的，如本领域技术人员熟知的那样，或者被转换成能够被传递给操作者的接口和数据库的格式。为了记录未来的卡拥有者的图像，操作者的接口可以和本领域技术人员已知的任何类型的图像记录装置通信。

[0064] 在本发明的身份验证系统的一个实施例中，未来的卡拥有者的图像可以使用任何的 TWAIN 适应图像记录装置被记录。TWAIN 是一种计算机硬件和软件，它们用于规定标准的协议和应用程序接口 (API)，用于在软件应用程序和图像应用装置之间通信，并且可以在市场上从 Twain Working Group 得到。一旦记录了未来的卡拥有者的图像，该图像便通过 TWAIN 或本领域技术人员任何已知的其它技术被传递给操作者的接口。该图像然后可以本领域技术人员已知的方式被分析与 / 或制备，以便通过操作者的接口被存储在卡中。例如操作者可以修剪图像或用其它方法准备要被存储在数据库与 / 或卡中的图像。

[0065] 此外，从个人取得的生物统计学信息、图像与 / 或其它的识别数据可以被制备成能够和存储的生物统计学信息、图像和其它的识别数据的现有的法律强制数据库兼容的格式。

[0066] 这样，可以使捕获的生物统计学信息，图像与 / 或其它识别数据和合适的法律强制数据库比较，从而获得关于个人的法律强制信息，如果有的话。此外，从个人获取的生物统计学信息，图像与 / 或其它识别数据可被传递给合适的法律强制数据库，用于增加或更新所述法律强制数据库，如果需要的话。在本发明的这些身份验证系统的实施例中，操作者接口与 / 或数据库通过网络，常规的或无线的，和法律强制数据库通信。

[0067] 例如，在本发明的身份验证系统的一个实施例中，操作者接口与 / 或数据库和属于不同的州的与 / 或联邦法律强制机构的自动指纹识别系统 (AFIS) 通信。这样，当从试图获得安全许可卡的个人获得一个或几个指纹时，所述指纹可被传递给 AFIS，一边合记录上的指纹进行比较。这个处理也允许另一种技术用于验证未来的卡拥有者的身份，其中通过匹配传递的生物统计学信息与 / 或图像和法律强制数据库中现有的生物统计学信息与 / 或图像，并确定和任何匹配相关的个人的现有的生物统计学信息与 / 或图像是否和向操作者提交生物统计学信息与 / 或图像的个人相同。

[0068] 本发明的安全许可卡的另一个重要的方面是在卡本身存储和卡拥有者的身份相关的数据的能力。具体地说，一旦操作者把记录输入到数据库，或者在操作者把记录输入到数据库的同时，在所述记录中包含的数据的全部或至少一部分可被存储在卡例如卡的存储介质中，(例如 CD-ROM，智能卡存储器等)，与 / 或安全许可卡 10 的数据存储介质部分中。

[0069] 重要的是，在一些实施例中，为了使卡成为一个自含系统，至少包括生物统计学信息的记录的部分可被存储在卡中或卡上。这使得安全系统不必从网络数据库中检索数据便能验证卡拥有者。

[0070] 除去接收、验证和存储识别数据之外，如上所述，操作者也可以接收、检验并在安全许可卡中存储工作数据和额外数据。如上所述，工作数据可以包括卡的各种应用可能需要的任何类型的信息。此外，工作数据还可以根据分配给工作数据中包括的每种类型的数

据的安全等级被分开。本发明的安全许可卡的各个实施例可以包括各种类型的工作数据的各种组合。例如，和个人有关的工作数据可以包括驾驶执照信息，语音记录信息，雇用信息，账号信息以及所需的任何其它类型的信息。在本发明的安全许可卡 10 的其它实施例中，工作数据可以和一个对象（有形的或无形的）相关。例如，如果工作数据和车辆相关，则工作数据可以包括关于车辆正在装运的物品或人员、车辆的形式历史的信息，以及和车辆或其操作有关的任何其它信息。

[0071] 每个类型的工作数据可被分配给不同的安全等级，在每个类型的工作数据内的数据也可以具有对其分配的不同的安全等级。如下面详细说明的，由于分配给每个类型的工作数据和每个类型的工作数据内的数据的安全等级，能够读卡的每个人将只能够访问可以直接应用于特定应用的数据。例如，数据的较低的等级可以包括卡拥有者的姓名和可能的数字照片。较高等级的保密数据可以包括卡拥有者的个人信息，例如地址、账号等。更高等级的保密数据可以包括更敏感的信息。常规系统的限制在于，所有这些数据一般可以被扫描卡的任何人访问，而不管数据的灵敏度。然而，本发明通过确保特定的读卡器与 / 或读卡器的操作者只能读取某个或某些等级的数据减轻了这个问题，如下面详细说明的。

[0072] 在卡 10 中不仅存储身份、工作数据与 / 或其它数据，而且能够在卡中存储数据产生和数据存储的环境（下文称为“产生数据”）。例如，当操作者在卡中存储数据时，可以在卡中存储操作者的识别信息。用于在卡中存储卡拥有者的数据并用于所述卡的设备的识别信息也可以被存储在卡中。此外，从中获得、处理或存储卡拥有者的任何数据的服务器或数据库的识别信息可被存储在卡中。产生数据和关于卡的产生和在卡中存储数据的任何其它类型的信息也可以被包括在卡中存储的数据中。因而，所有用于跟踪卡的产生和卡上的数据的存储所需的信息都可被直接存储在卡中，使得如果发生和卡有关的任何问题，都可以直接地访问所述卡。通过把包括产生数据在内的所有的数据直接存储在卡上，使得不必访问任何数据的单独的数据库，和常规的对于系统利用的许多数据依赖单独的数据库的系统相比，本发明的安全系统的速度和安全性被大大增加。

[0073] 此外，因为本发明的安全许可卡 10 不仅可以包括 CD-ROM 部分 22，而且包括数据存储介质部分 24，如上所述，根据数据的位置、读卡器的类型与 / 或读卡器的操作者的识别信息，使得对某类数据的访问受到进一步限制。例如，在本发明的一个实施例中，较低安全等级的数据可位于印在卡的正面上的数据存储介质部分 24 中，而较高安全等级的数据可位于 CD-ROM 部分 22 中。一个特定的读卡器可以只包括用于数据存储介质例如条形码的读卡器，磁条读卡器或其类似物，使得只有该读卡器可以访问的数据是被存储在位于卡的表面上的数据存储介质中的数据。此外，在上述的例子中，可以批准一个特定的操作者只访问较低安全等级的数据，因而，操作者可以只能操作用于卡的数据存储介质部分的读卡器。因而，卡中包括不同类型的存储介质对卡提供了常规的安全许可卡不能处理的进一步的安全特征。

[0074] 此外，本发明的安全许可卡 10 能够存储大量的不同类型的数据，并且用于身份验证所需的所有信息和任何其它可应用的数据被包括在本发明的安全许可卡中。对于用于和出示卡的人的生物统计学信息比较的生物统计学信息数据，或者卡的读卡器所需的任何其它数据，不需要访问集中的数据库。这样，和常规技术相比，卡和读卡器一道，如下面详细说明的，是一种用于验证安全许可卡拥有者的身份的低成本的、高效和更可靠的技术。

[0075] 除去提供具有各种特征的用于验证卡拥有者的身份的安全许可卡之外，安全验证系统提供了用于确保在卡中存储的数据的安全性的各种特征。这些特征在下面在单独的标题下进行讨论。

[0076] A. 压缩

[0077] 存储在卡中例如 CD-ROM22 与 / 或数据存储介质 24 中的包括生物统计学信息数据和选择地包括光学数据的数据可以用本领域技术人员已知的任何方式被压缩。例如，数据可以利用依据句法的压缩、基于字典的压缩例如在市场上可以通过数字数据研究公司得到的 TextComp 压缩、与 / 或任何类型的算术压缩以数字方式被压缩。借助于利用压缩方法压缩在卡中存储的数据，可以使卡存储最多的数据。

[0078] 如上所述，在卡 10 中存储的数据一般按部分或分组存储，以便有助于在卡中存储的数据的压缩。数据部分可以用本领域技术人员已知的任何方式设置。例如，数据部分可被设置在固定的字段位置，其提供高效的存储和处理方式，但是当对数据部分发生改变时则难于产生。在本发明的其它实施例中，数据可以通过包括语言的人造物例如字段识别符、记录标记的结尾与 / 或句法的和语义的人造物来设置。这种技术是需要的，因为其提供了对数据部分修改的灵活性。根据卡 10 的特定应用的要求，可以使用任何其它合适的设置技术。

[0079] B. 加密

[0080] 存储在卡中例如 CD-ROM22 与 / 或数据存储介质 24 中的包括生物统计学信息数据和选择地包括光学数据的数据可以用本领域技术人员已知的任何方式加密。在本发明的卡 10 的一个实施例中，数据在被加密之前可被压缩，如上所述。在本发明的卡的另外的实施例中，数据可以不经压缩被加密。

[0081] 可以使用本领域技术人员已知的任何类型的加密技术对卡中存储的数据加密。例如，可以使用任何类型的加密算法加密数据，所述的加密可以包括密钥。如果加密包括密钥，则密钥内容和尺寸可以定期地改变。因而，根据使用的加密算法的类型和数量、算法是否利用密钥、如果利用密钥，则还根据密钥的内容和尺寸，可以产生多种类型的加密技术。加密算法可以是动态地产生的分组密码加密算法。

[0082] 由一个卡或一组卡利用的加密技术可被称为加密鸡尾酒。因而，可以产生多种类型的加密鸡尾酒，使得每个卡或每组卡具有不同的加密鸡尾酒。因此不同的加密鸡尾酒对于所述的卡或一组卡是唯一的加密结构。例如，用于访问一个公司的大楼的一个卡或一组卡将利用和用于访问另一个公司大楼的一个卡或一组卡不同的加密鸡尾酒。这种类型的加密分配产生一个非常安全的环境，因为即使一个卡或一组卡的加密结构被确定，其它的卡或其它的卡组的加密结构仍然被保持，这和现有技术的安全系统不同，尤其是利用微处理器卡的安全系统。

[0083] 此外，可以利用一种以上的加密技术加密卡上存储的数据的不同部分。因而，不同的加密技术可被分配给卡中存储的不同类型的数据，例如根据分配给数据的安全等级与 / 或数据的敏感性而定。例如，分配给在卡中存储的身份、工作数据与 / 或额外数据的每个不同的安全等级，如上所述，可被分配给一种不同的加密技术。这种配置和对卡中存储的数据的可能的读卡器分配的只读某个类型的加密或几种加密相结合，确保读卡的人员被允许只读与 / 或访问在卡中存储的数据的部分，所述的卡适合于和所述读卡器相关的应用。

[0084] 如上所述，安全许可卡可以包括多种等级的数据。例如，较低等级的数据可以包括卡拥有者的姓名和可能的数字照片。较高等级的保密数据可以包括卡拥有者的个人信息，例如地址、账号等。还有更高安全等级的数据可以包括更敏感的信息。常规系统的限制在于，所有这些数据一般由扫描卡的任何人访问，而不管数据的敏感性。然而，本发明减轻了这个问题。具体地说，本发明的系统把和卡拥有者相关的数据分类为不同的安全等级，并且只允许有权访问和数据相关的特定安全等级的读卡器的操作者访问所述数据。

[0085] 例如某个读卡器和操作者或者读卡器的一组操作者可以只能访问卡中存储的数据的某些部分。读卡器可以只能解密某个或某些类型的加密，这限制了读卡器对于利用其它类型的加密加密的数据的可访问性。此外，每个操作者或每组操作者可以和只读每个操作者或操作者组被允许访问的所述数据的所述加密类型的能力相关。不管读卡器与/或操作者是否被批准读取某个类型的加密，被加密的数据可以通过加密读卡器 58 读取，如图 5 所示。

[0086] 存储在卡中的身份数据、工作数据、与/或额外数据可以根据分配给特定类型的数据的安全等级利用不同的加密技术加密。例如，在图 1 所示的例子中，操作者 20 可以和只读第一级加密的数据的能力相关，例如存储在卡中的身份数据部分，而操作者的管理者可以不仅和只读第一级加密数据的能力相关，而且和读取被分配给一个较高级的加密的数据的至少一部分的能力相关，这可以帮助管理者评价由卡拥有者对组织带来的危险。在本发明的安全系统的其它实施例中，卡拥有者的基本身份数据例如姓名、地址和生物统计学信息可以不加密，而所有其它的身份、工作与/或额外数据被加密。因而，一些读卡器与/或操作者可以不与只读任何类型的加密的能力相关，使得只有基本的身份数据可以不需访问任何加密数据的能力便能够被访问。

[0087] 此外，加密技术可以和卡拥有者的生物统计学信息关联。这样，如果出示卡的人员的生物统计学信息和存储在卡 22 的至少 CD-ROM 部分中的卡拥有者的生物统计学信息匹配，由卡存储的数据可以是只对一个读卡器为非加密的，如下面详细说明的。此外，借助于使用于卡中存储的数据的加密技术和卡拥有者的生物统计学信息关联，每个卡使用的每个加密技术是不同的，这有助于由卡携带的数据的安全性。

[0088] 在本发明的其它实施例中，加密技术可以和卡中存储的产生数据相关联。这样，在每个卡中存储的数据的加密基于和每个卡相关的不同的产生环境而不同。

[0089] 上述的各种加密技术提供非常安全的环境，用于存储敏感的安全卡数据。此外，即使用于一个卡的加密鸡尾酒以未准许的方式被发现，也只有一个卡被危及，常规的安全许可卡，其中所有的卡在卡上或在数据库中都具有相同的保密结构，例如微处理器卡、智能卡等，则具有非常不同的情况，因为如果这些卡与/或数据库的保密结构被发现，则将危及所有的或者大部分的卡。

[0090] 因为每个卡可能利用不同的数据排列（如三“压缩”标题下所述）和不同的加密技术，在每个卡中利用的数据排列和加密必须以某个方式和读卡器通信，使得读卡器能够发现和读出在卡中存储的数据的合适的部分。在本发明的安全系统的一个实施例中，数据库与/或管道方法可被用于记录和数据部分相关的排列、加密以及任何其它信息。数据库与/或表可被存储在卡 10 中。此外，在卡中存储的每个数据部分可被分配给一个 ID 数，其可用于查看和数据库与/或表中的数据部分有关的信息。

[0091] 当读卡器扫描在卡中存储的数据部分时，从数据部分提取 ID 数。然后读卡器访问数据库与 / 或表，并利用 ID 数查看关于数据部分的排列、数据部分的加密和关于数据部分的任何其它信息。如果读卡器与 / 或在读卡器上操作的操作者被批准解密分配给数据部分的加密类型，则读卡器可以读出所述数据部分。不管读卡器是否读出数据部分，其可以把数据部分传递给另一个下游应用，如下所述。

[0092] C. 读卡器

[0093] 本发明的安全验证系统还可以包括读卡器 16，其能够读按照本发明的安全许可卡 10，以便验证卡拥有者的身份，并在某种情况下，至少访问在卡上存储的身份数据、工作数据与 / 或额外数据的一部分。图 5 示出了读卡器 16 的一个实施例，其中示出了读卡器的一些功能。读卡器可以包括 CD-ROM 读取器 34，其能够读取在卡 22 的 CD-ROM 存储的数据的至少一部分。具体地说，CD-ROM 读取器 34 能够读取在卡 22 的 CD-ROM 部分中存储的卡拥有者的生物统计学信息数据。此外，读卡器 16 可以包括读取器 36，其能够读取在卡 24 的数据存储介质部分存储的至少一些数据。因而，读取器 36 能够解码在数据存储介质上存储的至少一部分数据。例如，如果出现在卡上的数据存储介质是条形码，则本发明的读卡器 16 将包括条形码扫描仪作为读取器。

[0094] 本发明的读卡器 16 还可以包括至少一个生物统计学信息检测器 40，用于访问持卡者的生物统计学信息。生物统计学信息检测器的性质取决于被选择进行扫描的生物统计学信息的类型。例如，一个或几个生物统计学信息检测器可以是指纹扫描仪、视网膜扫描仪、语音识别装置等。

[0095] 读卡器 16 还包括处理元件 38，其接收来自 CD-ROM 读取器 34、读取器 36、生物统计学信息检测器 40 与 / 或任何其它能够接收来自卡 10 与 / 或提交卡的个人的数据的元件的数据。处理元件 38 能够比较被存储在卡中的卡拥有者的生物统计学信息和由读卡器通过合适类型的生物统计学信息检测器 40 接收的出示卡的个人的生物统计学信息。如果比较得到的在两个生物统计学信息之间的差在一个给定的允差内，则出示卡的个人被安全系统视为卡拥有者。允差值可被设置为任何所需的值。例如，允差值可被设置为这样一个值，其可以阻止除去完全匹配的任何结果表示出示卡的人员被视为卡拥有者。另外，允差值可被设置为这样一个值，其允许在两个生物统计学信息之间具有某个数量的误差。

[0096] 如果出示卡 10 的人员被视为卡拥有者，则匹配指示器 42 可以通过发送器 44 向位于读卡器 16 的外部上的合适的指示器发送一个匹配指示。例如，所述指示器可以是发光二极管 (LED)，其点亮一种特定的颜色表示匹配，或者可以是在显示器上的一个指示。

[0097] 读卡器 16 还能够通过记录由试图获得访问的人员呈现的生物统计学信息保持所有访问试图的记录，成功的和未成功的。存储元件或记录 46 可以被存储在对于读卡器是当地的数据库中，可以被定期地下载到一个永久的或暂时的存储元件中，或者可以被清除，视读卡器的特定应用而定。因而，读卡器可以是单独的，或者是和至少一个远方存储元件 48 例如数据库通过任何类型的网络 32，常规的或无线的，例如局域网、广域网、内联网与 / 或互联网，组合的，如图 4 所示。在本发明的其它实施例中，读卡器可以不能存储本地的访问企图的记录，即使是暂时的，但是可以通过上述的网络和远方存储元件 48 通信，例如数据库。这样，访问尝试的数据在尝试的当时可被直接地传递给远方存储元件 48。记录数据 46，其包括提交的生物统计学信息，可以被分析，以便识别试图利用不属于其本人的安全许

可卡的任何人员。然后采取合适的操作来对付这些人员，如果需要的话。

[0098] 读卡器 16 可以是有人操纵的或无人操纵的，根据读卡器的位置而定。例如，读卡器的实施例可以是一种常规的计算机，或者是其它类型的装置，如图 4 的装置 30，50，52 和 54 所示。所述装置可以是静止的或移动的，视读卡器 16 的特定应用而定。

[0099] 对于有人操纵的读卡器 16，读卡器的操作者可被要求记录在读卡器上，其记录操作者的识别信息。为了登录，读卡器的可能的操作者被要求提交至少一个生物统计学信息，其可以和被读卡器存储与 / 或被访问的可能的操作者的生物统计学信息匹配。例如，可能的操作者的生物统计学信息可被存储在和读卡器分开的但是和读卡器通信的存储元件 48 中。在读卡器 16 的其它实施例中，可能的操作者的生物统计学信息被存储在读卡器包括的存储元件中，使得读卡器 16 是一个独立的装置而不必访问任何类型的远方元件。每当操作者登录读卡器，可以要求操作者提交至少一个生物统计学信息，其可以和由读卡器存储与 / 或访问的生物统计学信息比较。如果操作者提交的生物统计学信息和由读卡器存储与 / 或访问的生物统计学信息匹配，则允许操作者操纵读卡器。如果操作者提交的生物统计学信息和由读卡器存储与 / 或访问的生物统计学信息不匹配，则操作者可以被拒绝访问读卡器，并要求提交另一个生物统计学信息，与 / 或任何其它的功能，根据读卡器的特定应用与 / 或位置而定。同样，读卡器可以存储由系统的试图使用者扫描的生物统计学信息的记录，用于以后进行分析并确定谁在试图进入系统。

[0100] 如上所述，安全许可卡可以包括不同安全等级的数据。例如，较低级的数据可以包括卡拥有者的姓名和卡拥有者的可能的数字照片。较高级的保密数据可以包括卡拥有者的个人的信息，例如地址、账号等。更高级的保密数据可以包括更敏感的信息。常规系统的限制在于，所有这些数据都能被扫描卡的任何人访问，而不管数据的敏感性。然而，本发明减轻了这个问题。具体地说，本发明的系统把关于卡拥有者的信息分成不同的安全等级，并只允许有权访问和信息相关的特定安全等级的读卡器与 / 或读卡器操作者访问所述信息。

[0101] 因而，除去存储读卡器的可能的操作者的生物统计学信息之外，也可以在读卡器本地存储和读卡器的可能的操作者或操作者组有关的其它数据，或者在通过任何类型的网络 32 或其类似物和读卡器通信的远方存储元件上存储所述数据。例如，在本发明的一个实施例中，关于访问卡上存储的数据即上述的身份数据、工作数据、与 / 或额外数据的等级的信息，其被分配给特定读卡器的每个可能的操作者或操作者组，也可以被存储在可以由读卡器访问的位置。因而，根据记录在读卡器上的操作者的识别信息与 / 或类型，并根据分配给操作者的访问等级，读卡器可以只读由卡存储的数据的某个部分。

[0102] 例如，在位于飞机场的本发明的身份验证系统的一个实施例中，在机场入口的读卡器的一个操作者或操作者组，例如一个或几个保安人员，可被允许一个访问等级，其允许操作者只检查卡中存储的数据的身份数据的部分，即生物统计学信息，姓名、地址、出生日期与 / 或有效和到期日期。这样，保安人员可以只查看生物统计学信息比较的结果，如上所述，并查看关于卡拥有者的其它识别数据的至少一部分。在这个实施例中，读卡器的另一个操作者或操作者组，例如一个或几个机场管理者可被允许一个访问等级，其允许管理者查看在卡上存储的身份数据、工作数据与 / 或额外数据的其它部分。例如，在本发明的身份验证系统的实施例中，身份数据可以和已被识别为对机场 / 飞机安全具有可能的威胁的人员的身份数据的表比较。如果出示卡的人员和表匹配，则机场管理者便可以登录读卡器，其将

识别机场管理者的生物统计学信息，以便允许访问卡中存储的其它数据，并允许机场管理者访问可以帮助其评价特定的个人对飞机／机场构成的危险的数据部分。

[0103] 在本发明的身份验证系统的实施例中，通过使每个操作者或操作者组和只读所述每个操作者或操作者组被允许通过加密读取器 58 访问的数据的加密类型的能力相关联，读卡器的某些操作者或操作者组可以只访问在卡中存储的数据的某些部分，如图 5 所示。如上所述，存储在卡中的身份数据、工作数据与／或额外数据，根据分配给特定类型的数据的安全等级，可以利用不同的加密技术加密。例如，在上述的例子中，可以使保安人员和只读由卡携带的身份数据的身份数据或身份数据的一部分的加密的能力相关联，同时使机场管理者和不仅读由卡携带的部分或所有的身份数据的加密的能力相关联，而且还能读在卡中存储的工作数据与／或额外数据的至少一部分的加密的能力相关联，以便帮助机场管理者评价由卡拥有者对机场／飞机存在的危险。

[0104] 在本发明的身份验证系统的另一个实施例中，读卡器的某些操作者可以具有修改例如改变、添加与／或删除在安全许可卡 10 中存储的数据的功能。例如，卡 10 可以包括 CD-ROM 22 例如 CDRW，用于存储身份数据、工作数据与／或额外数据，操作者不仅能够读取 CD-ROM 中存储的数据，而且还能改变、删除与／或添加修改数据。在本发明的其它实施例中，卡可以包括 CD-ROM22 例如 CDR，用于存储身份数据、工作数据与／或额外数据，操作者只能够读取这些数据。如果允许操作者修改 CDR 中存储的数据，唯一的修改涉及增加在卡中存储的数据而不改变或删除在卡中存储的现有的数据。必须理解，可以使用其它的数据写处理。

[0105] 在本发明的其它实施例中，例如不保证在卡中存储的数据的这样严格的保密的那些实施例，可以使用允许删除、改变或修正写入的数据的 CD-ROM。这种类型的 CD-ROM 一般被称为 CDRW。

[0106] 因此这些操作者利用的读卡器 16 也具有数据输入装置，例如键盘 60，或其它类型的用于接收信息的插孔，并具有例如通过发送器 44 在卡的合适的部分存储修改的数据的能力。对在卡中存储的数据进行修改的能力可以和特定的操作者的生物统计学信息相关，使得当操作者登录读卡器时，操作者至少提交一个和存储的可能的操作者的生物统计学信息匹配的生物统计学信息，如上所述，并且读卡器识别操作者能够对在卡中存储的数据进行修改。在本发明的身份验证系统的一个实施例中，不允许操作者改变其自身的安全许可卡，这样任何对安全许可卡进行的改变必须在存储在卡中之前由第三人改变。此外，在本发明的身份验证系统的实施例中，可以跟踪对卡中存储的数据进行的所有修改，使得所进行的精确的修改和进行所述修改的操作者被识别并被存储在卡中与／或远方存储元件中，以备后用。如上所述，关于其中把数据存储在 CDR 中的卡，为了将来跟踪在卡中存储的数据的改变，所述的修改可以不完全重写在卡中以前存储的数据，使得所作修改可以在先前的数据上产生一个数据的附加层，并且不删除以前的任何数据。这样，可以在后来访问以前的数据，万一需要以前的数据的话。

[0107] 作为另一种保密处理，读卡器还可以能够在允许个人访问一个位置或对象之前和在各种应用中依赖于卡中存储的数据之前，检查安全许可卡，以便验证卡的完整性。这样，卡可以包含可以被读卡器检验的高度可靠的内部控制。此外，读卡器可以能够检查修改的数据，以便确保在卡中存储的数据的修改已经按照上述的过程进行。如果在卡的数据或内

部控制中存在任何不一致，则读卡器可以拒绝个人访问所需的位置，并且对于有人操纵的读卡器，向操作者显示所述的不一致。例如，如果读卡器删除卡的数据或内部控制中的不一致，则读卡器可以显示特定的颜色与/或符号，用于表示不一致的位置与/或性质。这种不一致也可以触发读卡器，有人操纵的或无人操纵的，启动一个或几个操作，如下面详细说明的。

[0108] 一般地说，无人操纵的读卡器只能读取卡中存储的数据的身份数据的至少一部分，使得无人操纵的读卡器可以根据在卡中存储的生物统计学信息和由读卡器从出示卡的人员接收的生物统计学信息之间的比较允许访问或拒绝访问一个位置或对象（有形的或无形的）。不过，在本发明的身份验证系统的其它实施例中，有人操纵与/或无人操纵的读卡器根据其特定的应用也可以能够读取卡中存储的所有的身份数据、工作数据的至少一部分、与/或额外数据。以和上述相同的方式，借助于关联读卡器和每个读卡器的只能读取允许其访问的数据的加密类型的能力，每个读卡器可以只访问在卡中存储的身份数据、工作数据与/或额外数据的某个部分。

[0109] 读卡器可以访问的数据的类型与/或数量可被改变，使得某个卡拥有者可以访问的项目可被改变。在本发明的身份验证系统的一个实施例中，中心节点，例如控制中心 56，可以和安全系统这的一个或几个读卡器 16 通信。因而可以在控制中心改变允许一个特定的持卡者访问的类型，并把所述改变发送给有关的读卡器，例如，持卡者 A 起初可能被允许访问一个特定组织的所有项目。由于项目的改变或持卡者的状况的改变，持卡者 A 访问允许可能改变，使得持卡者 A 不再被允许访问该组织的门 5。持卡者 A 的允许的改变可以在中心节点进行，并且中心节点把所述改变发送给有关的读卡器，对于这个例子，即和门 5 有关的读卡器。门 5 的读卡器现在将拒绝持卡者 A 访问门 5。类似地，读卡器的操作者可以访问的数据的类型和数量也可以被改变。因而，这种安全系统能够有效地对持卡者的访问进行改变，同时还确保在读卡器级作出访问决定，而不要求读卡器当必须作出决定时询问远方数据库，如常规的安全系统那样。

[0110] 因此，安全许可卡 10 和本发明的读卡器 16 一道，不仅提供了一种安全、可靠和高效的技术，应用于确定出示安全许可卡的人员是否真正是卡拥有者，而且还确保读卡器与/或操作读卡器的任何个人能够只访问所需的数据。这样，和卡拥有者有关的个人信息保持私密，只有被授权访问这些私人信息的那些读卡器与/或人员才能够访问。此外，通过中心节点可以改变读卡器与/或读卡器操作者可以访问的数据和类型与/或数量，并把所述改变发送给有关的读卡器，使得可以在读卡器级继续进行访问决定的同时高效地进行所述改变。

[0111] 有人操纵与/或无人操纵的读卡器 16 还可以包括显示器 62，例如图 1 所示的监视器 18，用于向操作者与/或出示卡的人员显示信息。例如，在包括有人操纵与/或无人操纵的读卡器 16 的本发明的身份验证系统的实施例中，操作者与/或出示卡的个人可以观看显示器，其至少指示在卡中存储的生物统计学信息是否和出示卡的人员提交的生物统计学信息匹配。这个指示可以至少由显示屏的一部分构成，其根据生物统计学信息比较的结果接通一种特定的颜色，例如当生物统计学信息匹配时为绿色，而不匹配时为红色。或者，或除去通过显示屏呈现给操作者的颜色之外，也可以对操作者提供文字、符号与/或对象，用于进一步表示生物统计学信息比较的结果。例如，当生物统计学信息匹配时，“yes”，“ok”，竖

起拇指的符号等都可以在屏幕上显示，而当不匹配时则显示“no”，“stop”，停止符号等。在包括有人操纵与/或无人操纵的读卡器16的本发明的身份验证系统的其它实施例中，卡拥有者的身份数据即生物统计学信息、姓名、地址与/或出生日期的至少一部分与/或卡的有效期和期满目当读卡器读取身份数据时被显示。出于安全/私密的原因，无人操纵与/或有人操纵的读卡器16可以限制被显示的身份数据的数量。当登录到一个有人操纵的读卡器的操作者能够读取由卡携带的工作数据与/或额外数据的至少一部分时，则这些数据也可以通过显示器62向操作者显示。

[0112] 根据生物统计学信息的比较结果，读卡器可以启动某个动作。在本发明的身份验证系统的一个实施例中，当生物统计学信息不匹配与/或当在卡中存储的身份数据和由于某种原因曾经识别过的个人相关的身份数据匹配时，无人操纵与/或有人操纵的读卡器16可以通过动作启动器64启动一些动作，例如有声的或无声的报警。例如，读卡器可以能够存储或访问和已经识别过的个人相关的身份数据，例如由于和个人有关的特殊问题或者其它原因。此时读卡器可以在生物统计学信息比较的前后比较在卡中存储的身份数据和在读卡器中存储的身份数据，但是要在允许出示卡的个人访问所需的位置或对象之前并在依赖于卡中存储的数据之前进行所述比较。因此，有声的或无声的报警向读卡器的操作者指示，出示卡的个人应当被进行进一步的检查，根据读卡器的应用与/或位置而定。在本发明的身份验证系统的其它实施例中，可以由读卡器通过动作启动器64启动其它的动作，例如当生物统计学信息不匹配与/或当卡中存储的身份数据和由于某种原因被识别过的个人相关的身份数据匹配时，立即和管理者与/或法律强制部门即下游的应用接触。这类动作可以用或者不用上述的报警动作启动，与/或用任何其它类型的动作启动。

[0113] 读卡器还可以能够读取在读卡器、个人的安全许可卡、与/或读卡器能够访问的任何其它位置中存储的指令。这些指令可以包括根据生物统计学信息的比较结果、身份数据分析、与/或出示卡的人员提供的信息而启动的动作的类型。例如，读卡器可以根据由卡拥有者提交的生物统计学信息的类型读出命令其启动不同动作的指令。例如，在本发明的身份验证系统的一个实施例中，读卡器被命令执行正常操作，即，当出示卡的个人向读卡器提供右手的食指指纹时，根据生物统计学信息比较允许或拒绝出示卡的个人访问。不过，如果所述个人出示一个不同手指的指纹，则读卡器可以立即命令通知可以帮助处理这种情况的人员或组织，例如管理者与/或法律强制机构。读卡器16的实施例的这个功能在读卡器16能够允许访问价值高的敏感的信息与/或位置的情况下是有利的。例如，在读卡器16允许卡拥有者访问一个银行帐户的情况下，卡拥有者在正常情况下可以提供右手食指指纹，但是如果卡拥有者处于危险之中，例如如果另一个人强迫卡拥有者访问该银行帐户，使得其他人可以访问，则卡拥有者可能提供不同手指的指纹，这将触发读卡器立即接触法律强制机构，即下游应用。

[0114] 如图6所示，按照本发明的任何给定的安全系统可以被这样配置，使得只有某个读卡器、每个读卡器操作者、某个持卡者与/或某个下游应用可以访问在卡10中存储的数据的某些级与/或子级。图6表示一种安全系统，其中每个卡具有至少10级的存储数据，并且每个级可以具有一个以上的子级，被表示为级1和7。在安全系统的卡中存储的数据的可能的用户或子类用户列于图的上部。例如，具有3个读卡器的子类(CR1，CR2，CR3)，3个读卡器操作者的子类(OP1，OP2，OP3)，3个卡拥有者的子类(CO1，CO2，CO3)，和3个下游应

用的子类(AP1,1P2,AP3)作为在图6所示的安全系统的卡上存储的数据的可能的用户。本发明的身份验证系统的其它的实施例可以包括不同数量的级、子级与/或用户的子类。在其它的实施例中,用户的类可以不被划分成子类,而是,每个用户可以被单独地列表。

[0115] 在用户的可能的子类正下方的方块中的X表示该子类可以读和X所在的该行相关的数据的级与/或子级。例如,如图6所示,CR1可以读在卡10的1-4级中存储的任何数据,而OP3只可以读在级8中存储的数据。因而,借助于在某些级与/或子级中只存储某些类型的数据,并借助于在战略上指定用户的哪些可能的子级可以读那些级与/或子级,本发明的安全系统可以提供常规系统不能提供的灵活性、高效性以及数据保护。此外,虽然本发明的安全系统不必访问任何类型的远方数据库或存储元件便能工作,但是其也能传递卡中存储的数据给其它用户,例如安全系统的任何下游应用,它们可以位于远方。例如,如图6所示,CR1不能读在卡的级10中存储的数据,但是CR1可以从级10向AP2发送数据,在那里可以读级10的数据。

[0116] 此外,本发明的安全系统能够允许对在卡中存储的数据的某些级与/或子级的有条件的访问。例如,操作者或卡拥有者可被指定为一个或几个数据级与/或子级的拥有者。在读卡器开始对卡进行扫描并借助于按照上述匹配生物统计学信息对操作者与/或卡拥有者进行识别验证之后,读卡器可以提示数据的级与/或子级的拥有者批准或拒绝访问数据。本发明的安全系统的一个实施例中,可以同时拥有者提交另一个生物统计学信息抽样,以表示拥有者的批准。例如,在图6所示的例子中,CO3可以是卡拥有者的子类,它们已经请求根据逐案审查批准另一个用户或用户的子类是否能够读卡拥有者的社会安全号。假定级19含有卡拥有者的社会安全号,则在允许在OP2子类与/或AP2子类中的一个下游应用访问级9中的数据之前,CO3子类中的卡拥有者必须批准。

[0117] 因此,读卡器16能够确保只能由安全系统的任何可能的用户读、浏览与/或访问合适类型的数据。此外,对于读卡器的命令,其包括处理元件,可以位于读卡器内,使得读卡器不需要为获得指令或数据而访问远方装置。此外,读卡器能够借助于存储提交给读卡器的生物统计学信息记录利用安全许可卡的企图,使得任何欺骗性的使用这种卡的企图可以通过分析存储的生物统计学信息被容易地识别。因而,读卡器和本发明的安全许可卡一道提供了一种安全的、灵活的、低成本的技术,其不仅用于验证个人的身份,而且用于确保只有被批准的个人才能浏览与/或访问卡拥有者的数据。

[0118] D. 应用的例子

[0119] 下面说明本发明的身份验证系统的一些有利的实施例。本发明的身份验证系统的可能的应用具有宽的范围,因而提供这些特定的实施例只用于说明的目的。例如,这种身份验证系统可用于海口、空港、外国人注册(学生和劳动力),用于政府和私人的大楼中、电厂、水厂和监狱中,只略举几个。在这些实施例的说明中,身份验证系统的说明,包括身份验证系统的说明,其包括说明提供的本发明的安全许可卡。

[0120] 本发明的身份验证系统的实施例可用于其中雇员或其它的个人在访问“受限制”的区域之前必须经历背景检查的任何应用中。在这种情况下,一旦进行了背景检查,并且执行了正确的可应用的处理,雇员和其它的个人便可以被发给按照本发明的安全许可卡。这样,因为安全许可卡存储卡拥有者的生物统计学信息,并因为出示卡的个人必须提供匹配的生物统计学信息,才能访问受限区域,使得未按正确的程序进行背景检查的个人可以访

问受限区域的危险极小。这种类型的应用可用于海口、电厂、水厂、政府和私人大楼、监狱以及任何含有只有选择的人员才能访问的某些区域与/或项目的任何其它位置中。

[0121] 在其它实施例中，个人当其离开受限区域时也可以被要求通过读卡器利用其安全许可卡进行检查。在这个实施例中，身份验证系统能够跟踪特定的个人访问某些区域的时间与/或次数。这类数据可用于其它的下游应用中，例如对应用进行计数与/或对在某些区域的停留时间具有强制限制的应用中，例如对个人可以暴露于辐射的时间量的限制。在后一个例子中，一旦个人达到所述限制，读卡器便不再一些个人访问所述受限区域，即使个人的生物统计学信息和卡上携带的生物统计学信息匹配。一旦个人可以再次暴露于辐射，读卡器将再次允许其进入受限区域。此外，在某些应用中，可能需要允许个人进入一个特定区域，但是至少在一个预定的时间间隔内不允许其离开该区域。因而，本发明的安全系统也能实现这种应用。

[0122] 在本发明的身份验证系统的另一个实施例中，安全许可卡可以和一个对象相关，或者是有形的或者是无形的，而不和个人相关。例如，安全许可卡可以和货运相关，使得卡存储和货运相关的数据，例如内容、原发地、目的地、货主以及关于货运的任何其它数据。此外，卡存储有负责货运的个人的身份数据，使得个人的生物统计学信息被存储在卡中，并且个人必须提交匹配的生物统计学信息，以便证明货运的有效性。

[0123] 本发明的身份验证系统也可以用于选举人的验证和注册。例如，个人的选举人的注册可被存储在卡中，并且投票位置可以具有读卡器。这样，选举工作者可被视为读卡器的操作者，具有只读在安全许可卡中存储的数据的选民注册部分的能力。因此，个人可以向操作读卡器的选举工作者出示它们的卡，所述读卡器比较在卡上存储的生物统计学信息和由个人提交的至少一个生物统计学信息。如果所述生物统计学信息匹配，并且个人的选民注册信息被确认，则允许其在这个位置投票。因此，借助于保证投票人员是注册的选举人员，本发明的身份验证系统大大减少了选民作弊的危险。

[0124] 本发明的身份验证系统的实施例也可以用于外国人的注册和跟踪中，包括学生和劳动力。在这种应用中，本发明的安全许可卡可以发给每个外国人，并且所述的卡包括关于特定外国人的身份数据，至少包括一个生物统计学信息。可以要求外国人根据某个时间间隔向合适的官方机构报告，使得政府可以获得关于外国人的状态的信息，使得确保其继续在学校学习与/或在该国家工作。当一个外国人向合适的机构报告并出示卡时，在该机构的工作人员可以操作读卡器，以便读出由卡携带的身份数据的至少一部分，并检验由个人提交的至少一个生物统计学信息是否和卡中存储的生物统计学信息匹配。然后工作人员可以根据外国人的活动确定它们的状况。产生一个外国人的报告的记录，以便用文件证明外国人应当遵守的义务。如果外国人不报告，或者如果其状况已经改变，则本发明的身份验证系统可以自动地向合适的机构报告这个信息，使得它们可以采取合适的措施。在这个实施例中，读卡器可以和管理外国人的信息的中心控制设备与/或下游应用通信，使得读卡器可以自动地把有关外国人的数据发送到合适的地点。

[0125] 如上述的各种例子和整个说明可见，本发明的安全许可卡和身份验证系统可应用于多种可能的应用中。不仅是安全许可卡，连同读卡器，能够验证个人的身份而不必访问远方数据库，但是该系统也能确保读卡器的操作者可以只浏览与/或访问它们有权访问的卡携带的数据的一部分。此外，通过记录在个人试图利用卡时提交的生物统计学信息，本发明

跟踪卡的使用，使得容易发现任何作弊的使用，并识别责任人。因此，本发明的安全许可卡和身份验证系统提供了一种高效的、安全的和精确的技术，用于确保只有合适的个人才能访问某些位置、信息、对象与/或任何需要保护的项目。

[0126] 本发明所属领域技术人员应当记住这里提出的本发明的许多改型和其它实施例，从前面的说明和相关的附图中都能得到教导。因此，应当理解，本发明不限于所披露的特定的实施例，并且还有许多改型和其它的实施例都应当包括在所附的权利要求的范围内。虽然本说明使用了许多特定的术语，但是它们只具有一般的和描述的意义，而没有限制的目的。

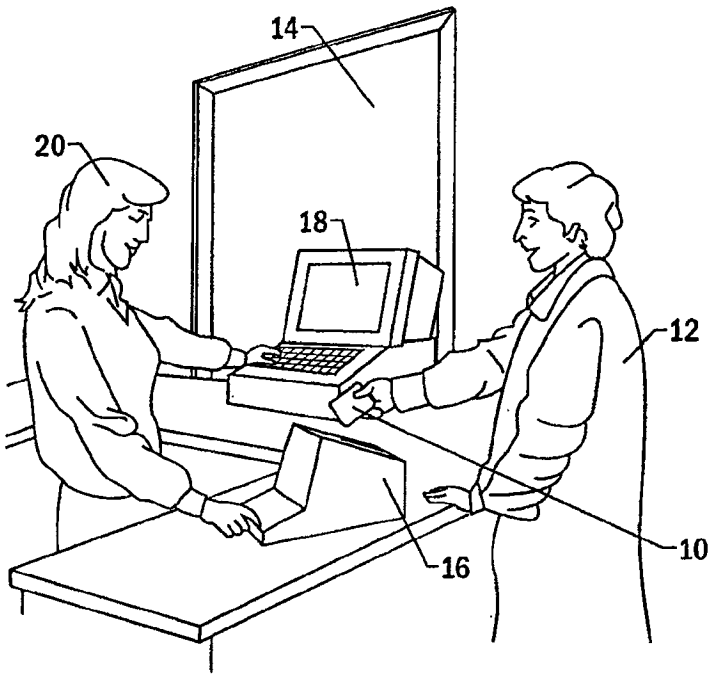

14
20
18
12
10
16

图 1

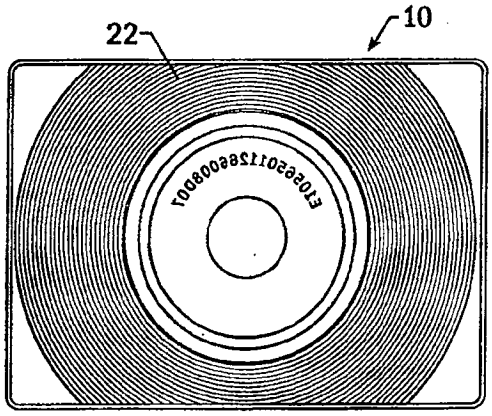

22
10

图 2

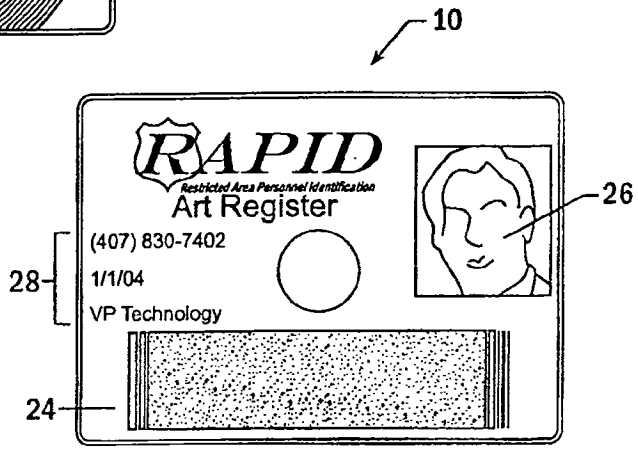

10
RAPID
Restricted Area Personnel Identification
Art Register
(407) 830-7402
1/1/04
VP Technology
26
28
24

图 3

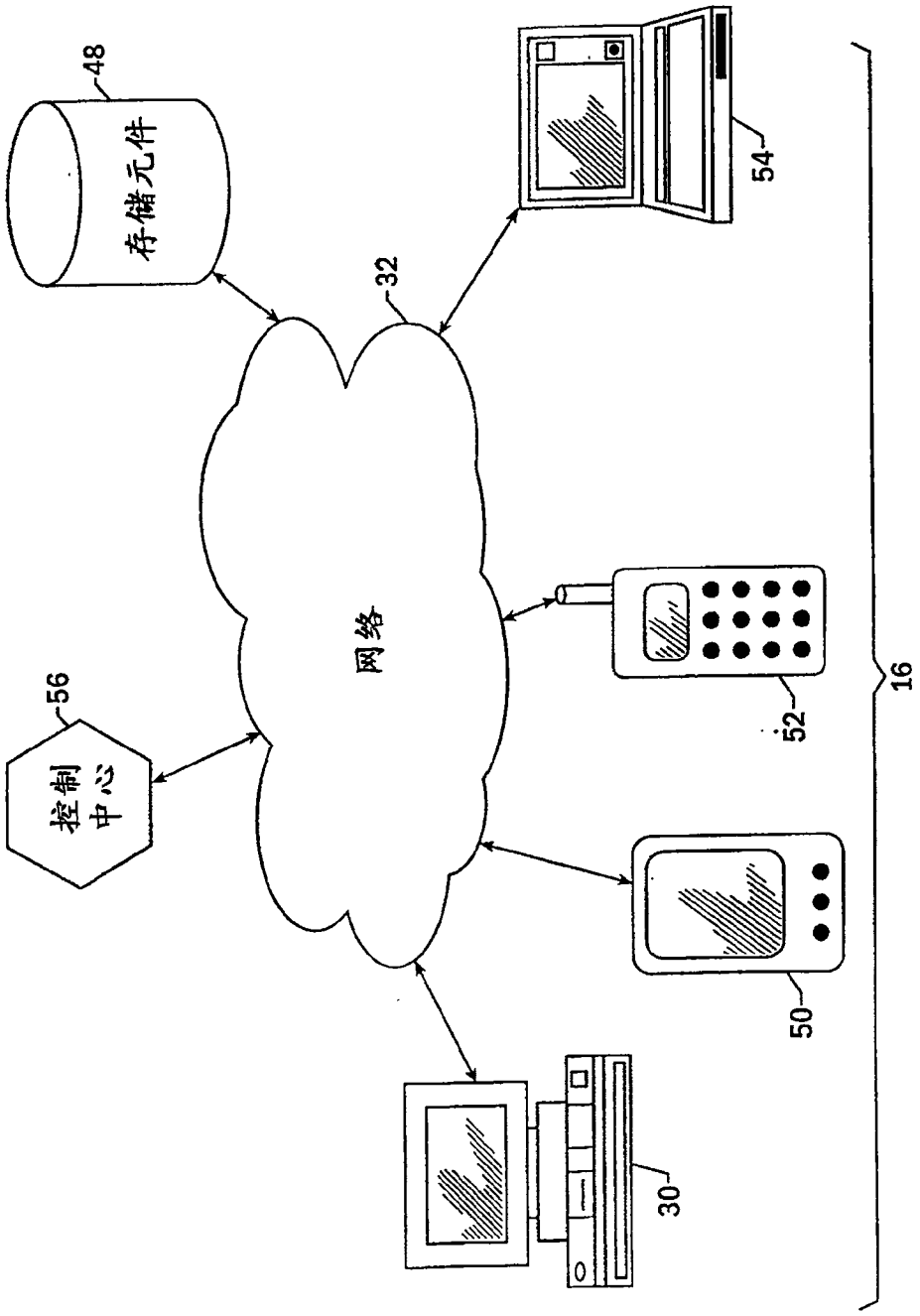


图 4

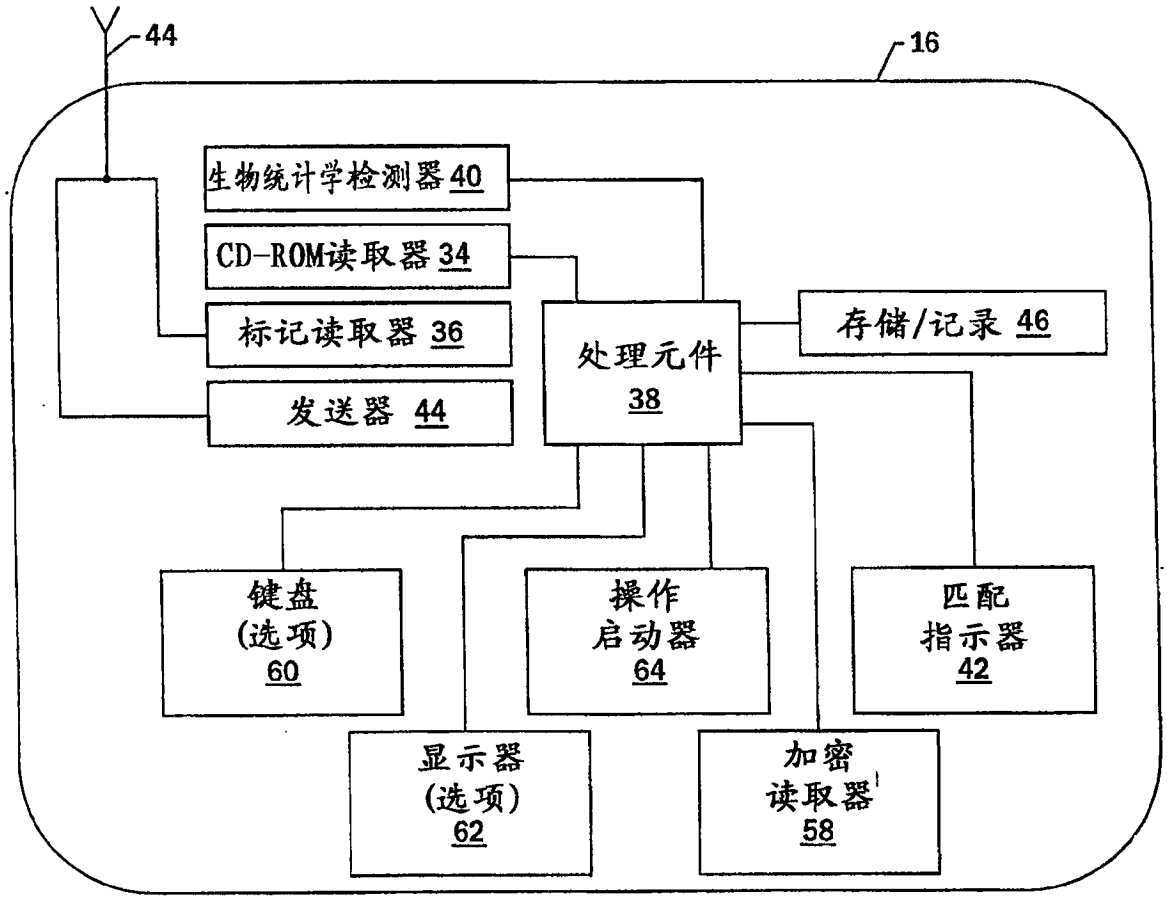


图 5

		用户											
		类	读卡器			操作者			卡拥有者			下游应用	
		子类	CR1	CR2	CR3	OP1	OP2	OP3	CO1	CO2	CO3	AP1	AP2	AP3
数据														
级	子级													
	1		X			X	X		X	X	X	X	X	
1	2		X			X	X		X	X	X	X	X	
2	3		X				X		X		X			X
3	4		X		X				X			X		
4	5		X		X					X				
5	6			X	X	X					X			
6	7			X			X		X				X	
	8			X	X		X			X	X		X	
7	9			X	X		X			X	X		X	
8	10				X			X	X				X	
9	11						X				X		X	
10	12												X	

图 6