发明名称
安全令牌、控制系统及控制方法

摘要
本发明的一个方面，提供了一种安全令牌，具体地是智能卡，包括触觉感测用户接口，其中所述触觉感测用户接口适用于捕获认证数据流，所述认证数据流与所述触觉感测用户接口结合的手指的一系列位置相对应并且表示用于访问可控对象的至少一个功能的用户特定凭证，所述安全令牌适用于向可控对象发送所述认证数据流以访问所述功能。
1. 一种安全令牌，具体是智能卡，包括触觉感应用户接口，其中所述触觉感应用户接口适于捕获认证数据流，所述认证数据流与所述触觉感应用户接口接合的手指的一系列位置相对应并且表示用于对可控对象的至少一个功能进行访问的用户特定凭证，所述安全令牌适用于向可控对象发送所述认证数据流以访问所述功能。

2. 根据权利要求1所述的安全令牌，还适用于支持多因素用户认证。

3. 根据权利要求1或2所述的安全令牌，其中触觉感应用户接口还适用于捕获控制数据流，所述控制数据流与所述触觉感应用户接口接合的手指的一系列位置相对应并且表示用于控制所述功能的输入数据，所述安全令牌适用于向可控对象发送所述控制数据流以控制所述功能。

4. 根据权利要求3所述的安全令牌，所述安全令牌还包括存储单元，其中所述存储单元适用于存储用于访问所述功能的访问权和/或用于控制所述功能的控制权。

5. 根据权利要求4所述的安全令牌，其中由支持NFC的移动设备向安全令牌写入访问权和/或控制权。

6. 根据权利要求4所述的安全令牌，其中由非接触的读取器或结合接触的读取器向安全令牌写入访问权和/或控制权。

7. 根据权利要求1到6中的任何一个所述的安全令牌，其中用户特定凭证是个人标识号。

8. 根据权利要求1到7中的任何一个所述的安全令牌，所述安全令牌包括：基于接触的接口，用于向可控对象发送数据。

9. 根据权利要求1到7中的任何一个所述的安全令牌，所述安全令牌包括：非接触的接口，用于向可控对象发送数据。

10. 根据任何一个前述权利要求所述的安全令牌，还适用于产生用户反馈，具体是与所述功能执行的控制操作相关的用户反馈。

11. 根据任何一个前述权利要求所述的安全令牌，安全令牌还适用于向外部显示设备发送显示数据，具体是对于所述功能执行的控制操作的日志加以表示的显示数据。

12. 根据任何一个前述权利要求所述的安全令牌，还适用于方便在多个可控对象之间的流行数据传输。

13. 一种控制系统，包括任何一个前述权利要求所述的安全令牌和可控对象，其中可控对象适用于接收认证数据流，验证由所述认证数据流表示的用户特定凭证，并在成功验证用户特定凭证之后向安全令牌访问所述功能。

14. 根据权利要求13所述的控制系统，其中可控对象还适用于在成功验证用户特定凭证之后向安全令牌发送配置数据，其中安全令牌还适用于使用所述配置数据来配置触觉感应用户接口。

15. 根据权利要求13或14所述的控制系统，其中可控对象还适用于向安全令牌发送所述功能执行的控制操作的日志。

16. 根据权利要求13、14或15所述的控制系统，其中可控对象是以下之一：房间入口、建筑物入口、机器、设备、交通工具、船、软件应用。

17. 一种控制方法，其中具体是智能卡的安全令牌中包括的触觉感应用户接口捕获认证数据流，所述认证数据流与所述触觉感应用户接口接合的手指的一系列位置相对应并
且表示用于对可控对象的至少一个功能进行访问的用户特定凭证，其中安全令牌向可控对象发送所述认证数据流以访问所述功能。
安全令牌、控制系统及控制方法

技术领域
[0001] 本发明涉及安全令牌。此外，本发明涉及控制系统。此外，本发明涉及控制方法。

背景技术
[0002] 出于多方面原因，需要保护例如机器和设备等可控对象以免被未授权的第三方非故意使用。这些可控对象可以是工厂控制、敏感生产线控制或医院中的安全相关设备。存在需要保护以免被非故意访问的许多可控对象。现有技术的保护方案典型地基于单因素认证（例如，使用密钥或口令）或双因素认证（例如，使用卡和口令）。已报道的事件是：向可控制对象认证了授权用户，随后该授权用户在没有退出的情况下离开可控制对象。在这种情况，可控制对象容易受到未经授权操作。此外，在恶劣环境（例如，有爆炸危险的区域）中，通常需要昂贵的键盘或触摸屏来提供用于数据录入的用户访问。

发明内容
[0003] 本发明的目的是方便对上述类型的可控对象的安全控制，具体地，对所述可控对象的功能的安全控制。通过如权利要求1所述的安全令牌、通过如权利要求12所述的控制系统，以及通过如权利要求16所述的控制方法来实现该目的。
[0004] 根据本发明的一个方面，构思了一种安全令牌，具体地是智能卡，包括触觉感应用户的接口，其中所述触觉感应用户接口适用于获取认证数据流。所述认证数据流与跟所述触觉感应用户接口接合（engage）的手指的一系列位置相对应并且表示用于对可控对象的至少一个功能进行访问的用户特定凭证（user-specific credential），所述安全令牌适用于向可控对象发送所述认证数据流以访问所述功能。
[0005] 根据示例实施例，安全令牌还适用于支持多因素用户认证。
[0006] 根据另一示例实施例，触觉感应用户接口还适用于获取控制数据流，所述控制数据流与跟所述触觉感应用户接口接合的手指的一系列位置相对应并且表示用于控制所述功能的输入数据，所述安全令牌适用于向可控对象发送所述控制数据流以控制所述功能。
[0007] 根据另一示例实施例，安全令牌还包括存储单元，其中所述存储单元适用于存储用于访问所述功能的访问权和/或用于控制所述功能的控制权。
[0008] 根据另一示例实施例，由支持NFC的移动设备向安全令牌写入访问权和/或控制权。
[0009] 根据另一示例实施例，由非接触的读取器或结合接触的（contact-bound）读取器向安全令牌写入访问权和/或控制权。
[0010] 根据另一示例实施例，用户特定凭证是个人标识码。
[0011] 根据另一示例实施例，所述安全令牌包括：基于接触的接口，用于向可控对象发送数据。
[0012] 根据另一示例实施例，所述安全令牌包括：非接触的接口，用于向可控对象发送数据。
[0013] 根据另一示例实施例，安全令牌还适用于产生用户反馈，具体地，与对所述功能执行的控制操作有关的用户反馈。

[0014] 根据另一示例实施例，安全令牌还适用于向外部显示设备发送显示数据，具体地，对于对所述功能执行的控制操作的日志 (log) 加以表示的显示数据。

[0015] 根据另一示例实施例，安全令牌还适用于方便在多个可控对象之间的流行 (epidemic) 数据传输。

[0016] 根据本发明的另一方面，构思了一种控制系统，包括上述类型的安全令牌和可控对象，其中可控对象适用于接收认证数据流，验证由所述认证数据流表示的用户特定凭证，并在成功验证用户特定凭证时或成功验证用户特定凭证之后授权 (grant) 安全令牌访问所述功能。

[0017] 根据另一示例实施例，可控对象还适用于在成功验证用户特定凭证时或成功验证用户特定凭证之后向安全令牌发送配置数据，其中安全令牌还适用于使用所述配置数据来配置触觉感应用户接口。

[0018] 根据另一示例实施例，可控对象还适用于向安全令牌发送对所述功能执行的控制操作的日志。

[0019] 根据另一示例实施例，可控对象是以下之一：房间入口、建筑物入口、机器、设备、交通工具、船、软件应用。

[0020] 根据本发明的另一方面，构思了一种控制方法，其中安全令牌（具体地，智能卡）中包括的触觉感应用户接口捕获认证数据流，所述认证数据流与所述触觉感应用户接口接合的手指的一系列位置相对应并且表示用于对可控对象的至少一个功能进行访问的用户特定凭证，其中安全令牌向可控对象发送所述认证数据流以访问所述功能。

附图说明

[0021] 将参考附图更详细地描述本发明，其中：
[0022] 图 1 显示了非接触智能卡的示例实施例；
[0023] 图 2 显示了双接口智能卡的示例实施例；
[0024] 图 3 显示了智能卡系统架构的第一示例；
[0025] 图 4 显示了智能卡系统架构的第二示例；
[0026] 图 5 显示了智能卡系统架构的第三示例；
[0027] 图 6 显示了如何根据若干组件制造智能卡；
[0028] 图 7 显示了智能卡中触觉参考图案的登记；
[0029] 图 8 显示了智能卡中触觉参考图案的识别；
[0030] 图 9 显示了智能卡的多种元件；
[0031] 图 10 显示了通过智能卡控制机器人；
[0032] 图 11 显示了通过智能卡向制造过程进行认证；
[0033] 图 12 显示了通过智能卡控制制造过程；
[0034] 图 13 显示了通过 NFC 向移动电话传送显示数据；
[0035] 图 14 显示了通过非接触读取器设备向 PC 传送显示数据；
[0036] 图 15 显示了通过基于触摸的读取器设备向 PC 传送显示数据。
具体实施方式

[0037] 根据本公开，可以利用支持多因素认证的智能卡来保护对安全相关可控对象的控制。更具体地，认证可以基于用户具有的（例如，智能卡、访问权）、基于用户知道的（例如，PIN）和基于用户本身的（即，个人特性，例如，手写特性）。智能卡可以是非接触的、基于接触的或双接口的智能卡，适用于作为对可控对象的访问接口和控制接口二者。可控对象可以配备有读取器设备，以便与智能卡通信。

[0038] 此外，可以将用户特定访问权存储在智能卡上。这些用户特定访问权规定用户可以访问可控对象的哪个（哪些）功能。例如，用户特定访问权可以由支持NFC的移动电话从可控对象接收，并通过NFC从支持NFC的移动电话传送至智能卡。备选地，用户特定访问权可以由非接触的或基于接触的读取器从可控设备接收，并从非接触的或基于接触的读取器经由相应的非接触或基于接触的通信信道传送至智能卡。此外，可以将用户特定或应用特定的控制权存储在智能卡上。用户特定或应用特定的控制权规定了用户可以如何控制可控对象的访问功能。此外，可以将控制事件（即，控制功能执行的控制操作）的日志存储在智能卡上以便之后检索。

[0039] 嵌入智能卡中的触觉检测用户接口（简称“触觉传感器”）可以有效地用于作二指触控设备。所述二指触控设备能够类似于其它手指设备（例如，鼠标）控制可控对象的至少一个功能。因此，智能卡可以对于所述功能的使用作访问接口也用作控制接口。仅在将智能卡连接到或附着到功能要被控制的可控功能块相连的读取器的情况下，才有可能控制所述功能。

[0040] 相较于现有技术的访问/控制接口，实现对可控对象的功能访问/控制接口是相对低成本的。此外，这避免了例如显示器和机械按钮的冗余组件，从而能够实现承重机械压力或其他机械结构。因此，可以将其用于控制环境的可控对象或有爆炸危险的环境中的可控对象。此外，这种访问/控制接口使用无电池操作，这使得增加了可靠性，延长了操作寿命、减少了成本和减少了回收问题。触觉传感器提供便于用户友好且直观的触觉接口。例如，这种触觉接口也允许由视觉受损用户或老用户来操作。可以针对特定应用和用户特定定义来控制触觉传感器。

[0041] 如上所述，在成功验证由触觉传感器捕获的用户特定凭证时或成功验证由触觉传感器捕获的用户特定凭证之后，可以授权对可控对象的至少一个功能的访问。此后，通过使用触觉传感器捕获控制数据，可以通过智能卡来控制该功能。因此，智能卡可以用作用于可控对象的交互控制的安全二指触控设备。例如，智能卡可以用作用于交互用户菜单控制的安全二指触控设备、用于进入数字的安全键盘、用于进入数字的安全键盘或用于预定用户接口功能（菜单功能）的安全控制接口。

[0042] 此外，智能卡可以产生视觉的或听觉的用户反馈，以便指示例如控制序列的开始和设备控制的成功/失败。为此，智能卡可以配备有光学反馈指示器（例如发光二极管（LED））或语音反馈单元。用户反馈也可以是显示数据的形式，以便通过例如移动设备或PC/膝上型电脑等外部设备呈现给用户。例如，可以通过NFC从智能卡向支持NFC的移动设备发送显示数据，或者通过结合触控的或非触控的读取器向PC/膝上型电脑发送显示数据。智能卡可以提供具有多语种支持（西文、中文、日文、泰语、韩语等）的可训练参考代
码空间（trainable reference code space）。此外，智能卡可以使用注册（enrollment）用户相关手写特性。此外，例如，智能卡可以启用固件和算法更新（类别签名更新），以使能现场维护。

[0043] 智能卡可以用于控制多种可控对象。例如，可控对象可以是如下之一：房间入口、建筑物入口、机器、设备、交通工具、船、软件应用。技术人员将认识到，也可以通过所述智能卡来控制其他可控对象。

[0044] 图 1 示出了非接触智能卡的示例实施例。根据本公开，如上所述，非接触智能卡 100 包括：二维触觉传感器，适用于定位与该触觉传感器接合的手指的位置。

[0045] 图 2 示出了双接口智能卡的示例实施例。根据本公开，如上所述，双接口智能卡 200 包括：二维触觉传感器，适用于定位与该触觉传感器接合的手指的位置。

[0046] 图 3 示出了智能卡系统结构的第一示例。在该示例中，智能卡 300 包括：存储单元 302、312；中央处理单元 304、314；密码设备 306；RFID 接口单元 308；天线 310；基于接触的接口 316；电力单元 318；输入结构 320 和输出结构 322；状态指示器 324；以及输入 / 输出端口 326。

[0047] 智能卡 300 包括：第一 CPU304 和第二 CPU314，可以通过软件进行配置以便进行所需数据处理。可以从电力单元 318 以非接触操作获得智能卡系统所需的电力，电力单元 318 整流来自天线 310 的天线信号，并将其调节到所需电压电平。在接触模式下，可以通过电力单元 318 调整由接触接口 316 提供的供给电压。在非接触模式下，RFID 接口单元 308 可以解调该天线信号，以便从可控制对象获得有效载荷信息。RFID 接口单元 308 也可以调制由智能卡系统产生的有效载荷信息，并且可以通过天线 310 向可控对象提供调制后的信号。接触模式下，可以通过由接触接口 316 表达的 ISO7816 接口来实现可控对象和第一 CPU304 之间的信息交换。第二 CPU314 可以处理由输入结构 320 提供的触觉信息，可以将所述信息转发到输出结构 322 或状态指示器 324 以用于用户反馈，或可以改变一般输入 / 输出（GPIO）设备的电学状态。可以将限制第一 CPU304 的功能所需的固件和数据存储在附着到该 CPU304 的存储单元 302 中。类似地，可以将限制第二 CPU314 的功能所需的固件和数据存储在附着到该 CPU314 的存储单元 312 中。

[0048] 图 4 示出了智能卡系统结构的第二示例。在该示例中，将 RFID 接口单元 308 连接到第二 CPU314，而不是第一 CPU304。在该实施中，第二 CPU314 执行 ISO14443 解码的一部分。

[0049] 图 5 示出了智能卡系统结构的第三示例。在该示例中，使用第一 CPU304 的功能，从而将 RFID 接口单元 308 连接到第二 CPU314。在该实施中，第二 CPU314 可以执行 ISO14443 解码的一部分。

[0050] 图 6 示出了如何根据若干组件制造智能卡。具体地，所述类型的智能卡可以包括：底箔（bottom foil）600，系统镶嵌（system inlay）602，触觉接口 604，具有切口（cut-out）608 的补偿层 606，顶箔（top foil）610，和接触接口模块 612。在图 6 的右侧显示了装配的智能卡 614。

[0051] 为了节约成本，可以将智能卡系统装配在单个基底或系统镶嵌 602 上，所述单个基底或系统镶嵌 602 由与嵌入卡相同的材料制成。在层压之后，可以将其与其它卡层一同形成固体材料块。可以使用直接芯片附着来装配芯片组件，因此避免昂贵的芯片封装。可以
通过低温焊料来焊接或使用各项同性导电胶 (ICP) 来粘合无源组件。可以将在芯片和组件位置处有切口 608 的补偿层 606 放置在基底 602 的顶部。顶层层 610 和底层层 600 可以完成卡组装。可以直接层压卡层，或可以使用薄胶层来联结各种卡层。

在层压而不用胶层的情况下，除了防化温度之外，基底材料可以与嵌入材料相同，其中基底材料比嵌入材料具有更高的防化温度。因此，可以在层压期间保持基底上的 PCB 结构。可以将聚氨酯箔 (TPU) 用作胶层。在卡层压之后，可以向卡表面中研磨开口，开口可以向下到达基底连接层。可以通过 ACA 胶、ACF、NCA 胶、NFC，通过焊接或用于固定接触模块的其它方法，将接触模块装配到研磨的切口中。接触模块可以配置为在接触模块表面和智能卡基底之间提供接触，以便将接触点口与相关智能卡组件相连接。

图 7 示出了智能卡中触觉参考图案的登记。图 8 示出了智能卡中触觉参考图案的识别。在用户认证期间，智能卡可以使用手写格式的数据条码，例如，如由申请人 NXP B.V. 在 2012 年 2 月 14 日申请的申请号为 EPI2153351.5，名之为“Security Token and Authentication System”的欧洲专利申请所述，其中该申请通过引用合并与此。手写用户输入数据的解码可以基于触觉图案识别，触觉图案识别包括：触觉传感器接口 700，配置为捕获触觉图案 702；触觉图案调节器 704，配置为令触觉图案机器可读；以及模式选择器 706，在参考图案捕获或登记模式（如图 7 所示）和识别模式（如图 8 所示）之间进行切换。在参考图案捕获或登记模式下，智能卡有效地处于“训练模式”；在“训练模式”下智能卡为实际使用做准备。

在所述登记模式下，可以将表示代码字母表（code alphabet）的触觉参考图案的集合与机器可读格式存储在智能卡上。可以使用附加的代码转换表来增加代码表。在所述识别模式中，可以将输入的触觉图案转换为机器可读格式，然后相对于以机器可读格式存储在智能卡上的训练代码字母表的字符进行相关（correlate）。基于相关器的分类器可以确定已录入的代码字母表成员。多个字符条目可以形成个人识别号 (PIN) 码。

根据本公开，可以定义智能卡的附加模式。例如，在指向模式下，可以将从触觉传感器获得的触觉数据转换为机器可读位置数据，可以通过所选通信接口向可控对象发送该机器可读的位置数据以便控制所述可控对象。可控对象可以配置为根据预定动作的位置数据来动作。出于安全原因，指向模式可以涉及失败主控功能 (fail-home function)，从而将可控对象控制到安全可操作条件下，其中失败主控功能基于与跟触觉传感器中心接合的手指相对应的位置数据。例如，在交通工具或船舶的情况下，安全可操作条件意味着速度为零且转向角为零。此外，在键区模式下，可以将从触觉传感器获得的触觉数据用作键区条目，其中从 0 到 9 的每个数字可以对应于专用按钮区域。激活这些按钮区域可以导致产生机器可读格式的控制数据并向可控设备提供所述控制数据。

图 9 示出了智能卡的多种元件。根据本公开，例如非接触智能卡或双接口智能卡。902 上的系统 900 可以包括以下元件：触碰接口 904，光学反馈指示器 906 和附加反馈单元 908。

可以将所述类型的智能卡用于多种应用领域。例如，根据本公开，如果将智能卡配置为访问卡，则在成功进行多因素认证之后，可以授权访问建筑物或房间。例如，在可控制对象是机器、设备、交通工具或船舶的情况下，也可以在成功多因素认证之后授权访问，以便控制可控对象的功能。此外，可以将用户特定和/或对象特定的访问权和控制权存储在智
能卡上。用户特定访问权和控制权允许对可控对象的定制操作。用户特定和 / 或对象特定的访问权和控制权可以是可修改的或可配置的。此外，所述类型的智能卡使能向其他可控对象流行传输 (epidemic transport) 这些用户特定和 / 或对象特定的访问权和控制权，这可以使能减少维护成本。此外，可以创建反映了所执行的控制操作的控制事件的目志并在智能卡上存储所述目志。

[0058] 如上所述，智能卡提供多因素认证，用于授权对例如建筑物和房间以及机器、设备、交通工具和船舶的访问。一旦授权了访问，就可以通过由可控对象或与可控对象连接的 PC 或膝上型电脑执行的控制应用来配置该智能卡，以使产生控制数据并使用加密通信信道向可控对象提供该控制数据。只要将授权用户的智能卡附着在与前述可控对象连接的或包括在前述可控对象中的读取设备上，就可以进行对可控对象的控制。在智能卡和可控对象之间的适合接口设备是例如符合标准 ISO/IEC 14443 的非接触的读取器和符合标准 ISO/IEC 18092 的基于接口的读取器。

[0059] 例如，智能卡可以支持以下多因素 PIN 码认证处理。首先，用户通过智能卡的触觉感测用户接口手写录入所请求的 PIN 码。接着，智能卡在识别模式下识别录入的 PIN 码。接着，可以将该 PIN 码发送给可控对象并通过前述可控对象进行认证。如果 PIN 码是有效的，则智能卡可以与可控对象接收配置数据。这些配置数据规定了应如何配置触觉感测用户接口以便使能对可控对象进行专门控制。

[0060] 图 10 显示了通过智能卡控制机器人。在该示例中，可控对象是应是二维平面上移动的机器人。通过无线通信连接（例如，蓝牙或 WLAN）将机器人与 PC 或膝上型电脑（未示出）相连接。将非接触的读取器连接到所述 PC / 膝上型电脑。认证应用请求用户录入该用户的认证数据（PIN）。在成功录入并验证了该认证数据时，启用智能卡与 PC / 膝上型电脑之间的链接。此外，将智能卡上的触觉感测用户接口配置为与膝上型电脑接口。只要用户用手指触摸该触觉感测用户接口，就产生位置数据，其中可以将该位置数据加密并发送给 PC / 膝上型电脑。可由 PC / 膝上型电脑执行的控制应用可以对从触觉感测用户接口获得的位置数据进行加密，并将其转化为机器人可读格式，以便控制机器人，使得机器人在所请求的方向上移动。应注意，也可以对在 PC / 膝上型电脑和机器人之间通信的数据进行加密。在用户将智能卡从非接触读取器产生的 RF 场移开时，断开与机器人的数据链接，机器人进入安全模式（例如，速度 = 0，方向 = 0 度）。可以将触觉感测用户接口上的短指指尖 (short fingertip) 转化为不具有或关闭机器人的视频摄像机。通过 WLAN 连接，可以将视频流发送给 PC / 膝上型电脑上的控制应用。

[0061] 图 11 显示了通过智能卡向制造过程认证。更具体地，将所述类型的智能卡用于对制造过程控制器接口 1100 认证用户。图 12 显示了通过智能卡控制制造过程。更具体地，将所述类型的智能卡用于向制造过程控制器接口 1100 提供控制数据。

[0062] 在更具体的应用中，可控对象是制造过程控制器接口 1100。可以将基于接触的读取器连接到制造过程控制器接口 1100。在制造过程控制器接口 1100 上运行的认证应用可以请求用户录入他的访问信息（例如，PIN）。在成功录入和验证该访问信息时，可以启用对制造过程控制器接口的控制，使可以向制造过程控制器接口 1100 提供键盘和 / 或鼠标信息。

[0063] 也可以通过非接触读取器将智能卡连接到制造过程控制器接口 1100。只要用户向嵌入智能卡中的触觉传感器提供输入，就可以将位置数据发送给制造过程控制器接口 1100，制
造过程控制接口 1100 可以将所述位置数据库转化为键盘或鼠标数据形式的控制数据，用于控制该制造过程。只要用户从非接触读取器移除智能卡，就可以终止控制会话并且用户可以退出。此外，可能需要读取所执行的控制操作的日志。在这种情况下，通过可用的外部显示器（例如，通过基于接触的或非接触的接口连接的支持 NFC 的移动设备或 PC / 膝上型电脑的显示器）提供所记录的控制信息是可行的。

[0064] 图 13 表示出了通过 NFC 向移动电话发送显示数据。具体地，可以将支持 NFC 的移动设备用于从非接触的或非接触的智能卡读出信息。可以执行以下步骤以向显示反馈数据，反馈数据例如反映了对可控制对象的控制动作的状态：开始移动设备应用；将非接触或非接触的卡附着到移动设备；移动设备请求反馈数据（询问）；移动设备通过 NFC 读取反馈数据；移动设备应用显示反馈数据；用户检查反馈数据；用户拆卸卡；当移除智能卡时终止移动设备应用。

[0065] 图 14 表示了通过非接触读取器设备向 PC 传送显示数据。具体地，可以将结合了非接触读取器的 PC / 膝上型电脑用于从非接触或非接触的智能卡读出信息。可以执行以下步骤以便向显示反馈数据反映了对可控制对象的控制动作的状态：开始 PC 应用；将非接触的或非接触的卡附着到读取器；PC 请求反馈数据（询问）；PC 通过读取器读取反馈数据；PC 应用显示反馈数据；用户检查反馈数据；用户拆卸卡；当移除智能卡时终止了 PC 应用。

[0066] 图 15 表示了通过接触的读取器设备向 PC 传送显示数据。具体地，可以将结合了基于接触的读取器的 PC / 膝上型电脑用于从接触的或非接触的智能卡读出信息。可以执行以下步骤以便向显示反馈数据反映了对可控制对象的控制动作的状态：开始 PC 应用；将接触的或非接触的卡附着到读取器；PC 请求反馈数据（询问）；PC 通过读取器读取反馈数据；PC 应用显示反馈数据；用户检查反馈数据；用户拆卸卡；当移除智能卡时终止了 PC 应用。

[0067] 最后，应注意图是示意性的。在不同附图中，相同的附图标记用于表示相似或相同部件。此外，应注意在提供这些示例性实施例的简明描述中，可能并未描述落入本领域技术人员常规实践中的实现细节。应该意识到，在任何这些实现的开发中，如在任何工程或设计项目中一样，许多特定于实现方式的决定必须实现开者的具体目的，比如与系统相关和商业相关约束兼容，这些约束可能根据实现方式的不同而不同。此外，应该意识到，这种开发可能是复杂和耗时的，然而对于本领域技术人员而言可能是设计、加工和制造的例行程序。

[0068] 上述实施例示出而非限制发明，本领域技术人员将能够在不背离所附权利要求的范围的情况下设计许多备选实施例。在权利要求中，圆括号之间放置的任何参考标记不应该解释为限制权利要求。单词“包括”或“包含”不排除与权利要求中列出的元件或步骤之外的其他元件或步骤的存在。元件之前的单词“一”或“一个”不排除多个这种元件的存在。可以以包括若干不同元件的硬件和 / 或以适当编程的处理器来实现发明。例如可以基于若干装置的设备权利要求中，这些装置中的若干可以通过同一硬件来实现。在互不相同的从属权利要求中记载特定措施的事实并非表示不可以有利地使用这些措施的组合。

[0069] 附图标记列表

[0070] 100 非接触智能卡
[0071] 200 双接口智能卡
[0072] 300 智能卡架构
[0073] 302 存储单元
[0074] 304 中央处理单元
[0075] 306 密码设备
[0076] 308 RFID 接口
[0077] 310 天线
[0078] 312 存储单元
[0079] 314 中央处理单元
[0080] 316 接触接口
[0081] 318 电力单元
[0082] 320 输入结构
[0083] 322 输出结构
[0084] 324 状态指示器
[0085] 326 输入 / 输出端口
[0086] 400 智能卡架构
[0087] 500 智能卡架构
[0088] 600 底箱
[0089] 602 系统镶嵌
[0090] 604 触觉接口
[0091] 606 补偿层
[0092] 608 切口
[0093] 610 顶箱
[0094] 612 接触接口模块
[0095] 614 装配的智能卡
[0096] 700 触觉传感器接口
[0097] 702 触觉图案
[0098] 704 触觉图案调节器
[0099] 706 模块选择器
[0100] 900 智能卡上的系统
[0101] 902 双接口智能卡
[0102] 904 触觉接口
[0103] 906 光学反馈指示器
[0104] 908 附加反馈单元
[0105] 1100 制造过程控制接口
图 1

图 2
图 2
图 4
图 9
图 15