(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 101918954 B
(45)授权公告日 2014.06.25

(21)申请号 200880125201.7

(22)申请日 2008.11.13

(30)优先权数据
102008000067.1 2008.01.16 DE

(85)PCT国际申请进入国家阶段日
2010.07.16

(86)PCT国际申请的申请数据
PCT/EP2008/065470 2008.11.13

(87)PCT国际申请的公布数据
WO2009/089943 DE 2009.07.23

(73)专利权人 联邦印刷有限公司
地址 德国柏林

(72)发明人 法兰克·迪特里克 法兰克·毕赛奥 曼弗雷德·皮斯达

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 戴建波

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/33(2013.01)
G06F 21/35(2013.01)
G06F 21/43(2013.01)
G06Q 20/34(2012.01)
G06Q 20/40(2012.01)
H04L 9/32(2006.01)

(56)对比文件
US 2001/0045451 A1,2001.11.29,说明书第2页第20段-第5页第41段以及附图1、2、4.
CN 101048790 A,2007.10.03,说明书第11页最后一段-第19页第1段、第22页最后一段-第27页最后一段以及附图1、3、5.
CN 1211330 A,1999.03.17,全文.
CN 1588388 A,2005.03.02,全文.
CN 1744124 A,2006.03.08,全文.
US 2001/0045451 A1,2001.11.29,说明书第2页第20段-第5页第41段以及附图1、2、4.

审查员 杨庆丽

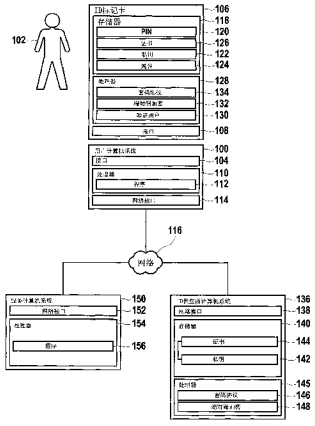
权利要求书2页 说明书13页 附图6页

(54)发明名称

从ID标记卡读取属性的方法

(57)摘要

本发明提供了一种用于读取存储在ID标记卡(106、106′)中至少一个属性的方法,其中,ID标记卡被指派给一用户。该方法包括如下步骤:在ID标记卡上验证用户;在ID标记卡上验证第一计算机系统;在ID标记卡上成功验证了用户与第一计算机系统后,第一计算机系统读取存储在ID标记卡中的至少一个属性,以将该至少一个属性传送至第二计算机系统。



CN 101918954 B

1. 一种用于读取至少一个存储在 ID 标记卡(106,106')中的属性的方法,其中,所述的 ID 标记卡分配给用户(102),其具有如下步骤:

- 在所述的 ID 标记卡上验证用户;

- 通过网络(116)在所述的 ID 标记卡和第一计算机系统(136)之间建立受保护的连接;

- 通过所述受保护的连接在所述的 ID 标记卡上验证所述第一计算机系统(136);

- 随着在所述 ID 标记卡上成功验证了所述的用户与所述的第一计算机系统,所述的第一计算机系统对存储在所述的 ID 标记卡中的至少一个属性进行读取,该读取是通过发送一个或多个读取命令、并通过所述受保护的连接借助端对端加密而将所述 ID 标记卡中的至少一个属性传送到所述第一计算机系统、再通过所述第一计算机系统对所述至少一个属性进行解密而完成的,然后进行如下的步骤:

i. 通过所述的第一计算机系统,对来自所述 ID 标记卡的至少一个属性进行签注;

ii. 将所述的已签注的属性从所述第一计算机系统传送至第二计算机系统;

其中,在所述 ID 标记卡上验证所述第一计算机系统是借助所述第一计算机系统的证书(144)进行的,其中,所述的证书包括对于存储在所述 ID 标记卡中属性的指示,以用于授权所述第一计算机系统进行 读取;

其中,所述的 ID 标记卡借助所述的证书,验证所述第一计算机系统对于所述至少一个属性的读取权限。

2. 如权利要求 1 所述的方法,其进一步包括如下的步骤:

- 从第三计算机系统(100)发送请求(164)至所述的第二计算机系统;

- 通过所述的第二计算机系统指定一个或多个属性;

- 从所述的第二计算机系统将属性清单(166)发送至所述的第一计算机系统;

其中,所述的第一计算机系统进行读取,以从所述 ID 标记卡中读取一个或多个在所述属性清单中指定的属性。

3. 如权利要求 2 所述的方法,其中,所述的请求(164)包括通过所述第二计算机系统识别所述第一计算机系统的识标符,其中,从所述第二计算机系统将所述属性清单传送至所述第一计算机系统时,没有第三计算机系统的参与。

4. 如权利要求 2 所述的方法,其中,所述的第三计算机系统具有多个预定义的配置数据记录(158、160、……),其中,每个配置数据记录指定了一个属性子集,其至少有一个数据源及来自第一计算机系统组(136、136'、……)的一个第一计算机系统;其中,所述的属性清单首先从所述第二计算机系统传送至所述第三计算机系统,使得借助于所述第三计算机系统,选择至少一个配置数据记录,用于指定一属性子集,该属性子集包括所述属性清单中指定的至少一个属性;其中,所述 的第三计算机系统将所述属性清单转发至所述第一计算机系统;其中,在所述第一计算机系统与所述的 ID 标记卡之间的连接由所述的第三计算机系统建立,其中,所述的 ID 标记卡被所选定的配置数据记录中的数据源的指示所指定。

5. 如前述权利要求之一所述的方法,其中,从所述 ID 标记卡中读取的所述至少一个属性,从所述第一计算机系统发送至第三计算机系统,并随着用户的放行,从所述第三计算机系统转发至所述的第二计算机系统。

6. 如权利要求 5 所述的方法,其中,所述的用户在所述属性转发至所述的第二计算机

系统之前，对其进一步补充数据。

7. 如权利要求 2-4 之一所述的方法，其中，所述第一计算机系统具有不同读取权限的多个证书（144.1 ;144.2），其中，所述的第一计算机系统根据接收的所述属性清单，选择至少一个证书，该证书具有用于读取所述属性清单中指定的属性的足够读取权限。

8. 如权利要求 1-4 之一所述的方法，其中，第三计算机系统具有至少一个配置数据记录（161），其通过网络（116），从所述第三计算机系统指定用于请求进一步属性（A）的外部数据源；

其中，所述的进一步属性的请求，是在所述至少一个属性从所述 ID 标记卡读取之后、以及在所述第三计算机系统从所述第一计算机系统接收到已签注的所述至少一个属性之后而进行的，所述的请求包括已签注的所述至少一个属性。

9. 一种用于读取存储在 ID 标记卡中的至少一个属性的计算机系统，该计算机系统具有至少一个第一计算机系统，该第一计算机系统和 ID 标记卡借助受保护的连接经由网络（116）而相互连接，其中，所述的第一计算机系统具有：

- 在 ID 标记卡（106）上进行验证的装置（142、144、146），其中，第一计算机系统在 ID 标记卡上的验证是借助第一计算机系统的证书（144）进行的，所述证书包含存储在所述 ID 标记卡中属性的指示，以用于授权所述第一计算机进行读取；

- 通过受保护的连接从所述 ID 标记卡读取至少一个属性的装置；其中，读取所述至少一个属性的先决条件是，在所述 ID 标记卡上，成功地验证了分配了该 ID 标记卡之用户与所述的计算机系统；

- 用于签注从 ID 标记卡读取的属性的装置；

- 向第二计算机系统传送签注的属性的装置；

其中，所述的 ID 标记卡用于验证分配了该 ID 标记卡之用户（102）和验证第一计算机系统（136），并用于建立与所述第一计算机系统之间的受保护的连接和对所述受保护的连接进行端对端加密，其中，所述第一计算机系统能够使用该连接读取所述的至少一个属性，而且可以通过该连接将所述至少一个属性受保护地传送到所述第一计算机系统；

其中，借助证书验证所述第一计算机系统从所述 ID 标记卡中读取所述至少一个属性的读取权限。

10. 如权利要求 9 所述的计算机系统，其进一步包括从第二计算机系统接收属性清单（166）的装置（138），而且借助该装置（138），将从所述 ID 标记卡中读取的至少一个属性发送至第三计算机系统（100），以转发至所述第二计算机系统。

11. 如权利要求 10 所述的计算机系统，其具有多个不同读取权限的证书（144.1；144.2），其中，所述的计算机系统是如此设计的，其根据接收的所述属性清单，选择至少一个证书，该证书具有足够的读取权限，以读取所述属性清单中指定的属性。

12. 如权利要求 9 或 10 所述的计算机系统，其中，所述的 ID 标记卡是一个电子设备。

13. 如权利要求 12 所述的计算机系统，其中，所述的 ID 标记卡是 USB 记忆棒或文件。

14. 如权利要求 13 所述的计算机系统，其中，所述的 ID 标记卡是有价文件或安全文件。

从 ID 标记卡读取属性的方法

技术领域

[0001] 本发明涉及一种从 ID 标记卡（ID-Token，或称身份标记卡）读取至少一个属性（Attribut）的方法、相关的计算机程序产品、ID 标记卡及计算机系统。

背景技术

[0002] 现有技术已经公开了多种用于管理所谓的用户数字身份的方法。

[0003] 微软的 CardSpace（卡片空间）是一个以客户为基础的数字身份系统，其目的是允许互联网用户将他们的数字身份与在线服务进行交流。除了其它缺点之外，其一个缺点就是，用户能够篡改他的数字身份。

[0004] 与此相反，OPENID 是一个以服务器为基础的系统。所谓的身份服务器存储了一个数据库，其具有注册用户的数字身份。除了其它缺点之外，其一个缺点就是，数据保护不充分，因为用户的数字身份集中存储，并且用户的行为可以被记录。

[0005] 美国专利申请 2007/0294431 A1 公开了一种管理数字身份的方法，其同样需要用户注册。

发明内容

[0006] 与此相反，本发明的目的是提供一种用于读取至少一个属性的改进方法、一种合适的计算机程序产品、一种 ID 标记卡及一种计算机系统。

[0007] 根据本发明，其提供了一种用于读取存储在 ID 标记卡中至少一个属性的方法，其中，ID 标记卡被分配给一用户。该方法包括如下步骤：在 ID 标记卡上验证用户；在 ID 标记卡上验证第一计算机系统；在 ID 标记卡上成功地验证用户与第一计算机系统之后，第一计算机系统对存储在 ID 标记卡中的至少一个属性进行读取，以将该至少一个属性传送至第二计算机系统。这需要提供一个“信任支柱 (Vertrauensanker)”。

[0008] 本发明允许通过第一计算机系统读取存储在 ID 标记卡中的一个或多个属性，其中，ID 标记卡与第一计算机系统之间的连接是可以通过网络建立的，特别是通过互联网。该至少一个属性是与分配了 ID 标记卡的用户的身份标识，特别是用户的数字身份。例如，第一计算机系统读取属性“姓”、“名”、“地址”，以将这些属性转发至第二计算机系统，如在线服务。

[0009] 然而，例如，也可能只读取一个单一属性，其不是用来确认用户身份，而是例如检查用户对于使用一特定在线服务的授权，如用户想要使用的在线服务是提供给特定年龄群的，则需要检查使用者的年龄，或者是另一种属性，该属性表示使用者属于授权使用在线服务的特定组群。

[0010] ID 标记卡可以是一种便携式电子设备，如所谓的 USB 记忆棒，或者可以是一种文件（Document，或称证件），特别是有价文件或安全文件。

[0011] 根据本发明，文件可以理解为纸制和 / 或塑胶制文件，如身份文件，特别是护照、身份证、签证、驾驶证、车辆登记证、车辆登记文件、企业执照、健康卡及其它 ID 文件，还有

芯片卡、支付手段特别是银行卡和信用卡、货运单证或其它权利凭证，其内置了用于存储至少一个属性的数据存储器。

[0012] 因此，本发明的实施方式具有特别的优点，因为该至少一个属性是从一特别值得信赖的文件如官方文件中读取的；其另外的一个优点就是不需要对属性进行集中存储。因此，本发明对于在与数字身份相关的属性的交换中，可以实现一个特别高的信任水平，同时具有极其方便处理的、最佳的数据保护。

[0013] 根据本发明一实施方式，第一计算机系统至少具有一个证书，用于在 ID 标记卡上验证自己。该证书包括如下属性的说明，这些属性指出第一计算机系统具有读取授权。ID 标记卡使用这些证书，在第一计算机系统进行读取之前，验证第一计算机系统对于读取的属性是否具有所必需的授权。

[0014] 根据本发明一实施方式，第一计算机系统将从 ID 标记卡读取的该至少一个属性直接发送至第二计算机系统。例如，第二计算机系统可以是提供在线服务或者其它服务的服务器，如银行服务，或者是订购产品。例如，用户可以在线开一个账户，而包含了用户身份的属性，可以从第一计算机系统传送至银行的第二计算机系统。

[0015] 根据本发明一实施方式，从 ID 标记卡读取的属性首先从第一计算机系统传送至第三计算机系统，即用户的计算机系统。例如，第三计算机系统具有一常规的互联网浏览器，利用互联网浏览器，用户可以打开第二计算机系统的一个网页。用户能够在该网页输入对于产品或服务的订购或请求。

[0016] 然后，第二计算机系统指定一些属性，例如用户或其 ID 标记卡的某些属性，这些属性是提供服务或接纳订购所必需的。然后，包含了这些属性说明的相应的属性清单，被从第二计算机系统发送至第一计算机系统。这个过程可以有，也可以没有第三计算机系统的中间连接。在后者的情况中，用户能够向第二计算机系统指定想要的第一计算机系统，例如，通过第三计算机系统在第二计算机系统的网页中输入第一计算机系统的 URL（网址）。

[0017] 根据本发明一实施方式，用户向第二计算机系统的服务请求包括对于标识符的说明，其中，该标识符识别确定第一计算机系统。例如，该标识符是一个网址，如第一计算机系统的网址。

[0018] 根据本发明一实施方式，属性清单不是直接从第二计算机系统发送至第一计算机系统，而是先从第二计算机系统发送至第三计算机系统。该第三计算机系统具有一系列预定义的配置数据记录（Konfigurations-datensatz），其中第三计算机具有一系列预定义的配置数据记录，每个配置数据记录指定了一个属性的子集、至少一个数据源（Datenquelle）及从一组第一计算机系统中指定一第一计算机系统，其中，属性清单首先从第二计算机系统传送至第三计算机系统，使得借助第三计算机系统来选择至少一个配置数据记录，用于详细说明属性子集，该属性子集包括属性清单中列明的至少一个属性，且第三计算机系统接着将属性清单转发至第一计算机系统，且与 ID 标记卡的连接是通过选定的配置数据记录中的数据源之标识的指定来建立。

[0019] 根据本发明一实施方式，从 ID 标记卡读取的属性，由第一计算机系统标记（signiert，签字），然后传送至第三计算机系统。因此，第三计算机系统的用户能够读取这些属性，但是不能修改它们。只有当用户放行了，这些属性才能够从第三计算机系统转发至第二计算机系统。

[0020] 根据本发明一实施方式，在属性转发之前，用户能够通过进一步的数据来补充该属性。

[0021] 根据本发明一实施方式，第一计算机系统具有一系列不同权限的证书。基于属性清单的接受，第一计算机系统可以选择一个或多个证书，以从 ID 标记卡或一系列不同的 ID 标记卡中读取相关的属性。

[0022] 根据本发明一实施方式，第三计算机系统至少具有一个配置数据记录，其针对通过网络来自第三计算机系统的更多属性的请求，指定外部的数据源。

[0023] 根据本发明一实施方式，在至少一个属性从 ID 标记卡读取后，且第三计算机系统已经接收到来自第一计算机系统的该至少一个属性后，可以请求更多的属性，其中该请求包括该至少一个属性。

[0024] 另一方面，本发明涉及一种计算机程序产品，特别是数字的存储介质，其具有完成本发明方法的可执行的程序指令。

[0025] 再一方面，本发明涉及一种 ID 标记卡，其具有：受保护的存储区域以存储至少一个属性；在 ID 标记卡上验证被分配了 ID 标记卡的用户的手段；在 ID 标记卡上验证第一计算机系统的手段；与第一计算机系统建立受保护的连接的手段，通过该连接第一计算机系统可以读取至少一个属性，其中，第一计算机系统从 ID 标记卡读取至少一个属性的先决条件是，用户及第一计算机系统在 ID 标记卡上验证成功。

[0026] 除了第一计算机系统在 ID 标记卡上验证之外，例如可以是众所周知的机读旅行证件(MRTD)的、由国际民航组织(ICAO)指定的“扩展访问控制(Extended Access Control)”，用户还必须在 ID 标记卡上验证自己。例如，用户在 ID 标记卡上验证成功后，激活了 ID 标记卡，使得可以进行下一步的步骤，也即在 ID 标记卡上验证第一计算机系统，和/或建立用于读取属性的受保护的连接。

[0027] 根据本发明一实施方式，ID 标记卡具有端到端加密(Ende-zu-Ende-Verschluesselung)的手段。这使得可以通过用户的第三计算机系统，在 ID 标记卡与第一计算机系统之间建立连接，因为端到端加密的方式，用户不能对通过该连接传送的数据作出任何修改。

[0028] 又一方面，本发明涉及第一计算机系统，其具有计算机系统，该计算机系统具有：通过网络接收属性清单的手段，其中，该属性清单指定至少一个属性；在 ID 标记卡上进行验证的手段；通过受保护的连接从 ID 标记卡读取至少一个属性的手段，其中读取该至少一个属性的先决条件是，被分配了 ID 标记卡的用户已经在 ID 标记卡上验证了自己。

[0029] 根据本发明一实施方式，第一计算机系统可以包括向用户产生请求的手段。例如，当第一计算机系统接收到来自第二计算机系统的属性清单后，它向用户的第三计算机系统发出一个请求，使得用户被要求在 ID 标记卡上验证自己。当用户在 ID 标记卡上验证成功后，第一计算机系统从第三计算机系统接收到确认。然后，第一计算机系统在 ID 标记卡上验证自己，并借助端到端加密的方式，在 ID 标记卡与第一计算机系统之间建立一个安全的连接。

[0030] 根据本发明一实施方式，第一计算机系统可以具有一系列分别指定不同读取权限的证书。在接受到属性清单后，第一计算机系统从这些证书中选择至少一个，其具有足够的读取权限，以读取指定的属性。

[0031] 根据本发明第一计算机系统的实施方式，其具有特别的优点，因为它们与需要用户在 ID 标记卡上验证相结合，对于用户非伪造的数字身份形成了一个信任支柱。此处的一个独特优势是，用户不需要在计算机系统进行预先注册，也不需要将形成数字身份的用户的属性放入中央存储器重。

[0032] 根据本发明一实施方式，第一计算机系统可以接收与属性清单一起的、第二计算机系统之标识符。借助该标识符，计算机系统可以识别第二计算机系统，其希望利用该识别服务，并为此服务而命令第二计算机系统。

[0033] 根据本发明一实施方式，计算机系统是官方认证的信用中心，特别是与数字签字技术相符合的信用中心。

[0034] 下面借助附图，来详细地描述本发明的优选实施方式。其中：

附图说明

[0035] 图 1 显示了根据本发明之计算机系统的第一实施方式的模块图。

[0036] 图 2 显示了根据本发明之方法的实施方式的流程图。

[0037] 图 3 显示了根据本发明之计算机系统的另一实施方式的模块图。

[0038] 图 4 显示了根据本发明之方法的另一实施方式的 UML 图。

具体实施方式

[0039] 图 1 显示了用户 102 的用户计算机系统 100。该用户计算机系统 100 可以是个人电脑、便携式电脑(如笔记本电脑或掌上电脑)、个人电子记事本、移动通信设备特别是智能手机、或者类似的设备。用户计算机系统 100 具有一接口 104，用于与具有相应接口 108 的 ID 标记卡 106 进行通讯。

[0040] 用户计算机系统 100 至少具有一用于执行程序指令 112 的处理器 110、以及一通过网络 116 进行通讯的网络接口 114。该网络可以是电脑网络，如互联网。

[0041] ID 标记卡 106 具有电子存储器 118，其具有受保护的存储区域 120、122 及 124。受保护的存储区域 120 用于存储一参数值 (Referenzwert)，该参数值是在 ID 标记卡 106 上验证用户 102 所必需的。例如，该参数值是一识别符，特别是所谓的个人识别码(PIN)，或者是能够用于在 ID 标记卡 106 上验证用户的用户 102 之生物特征的基准数据。

[0042] 受保护的区域 122 用于存储私钥，受保护的区域 124 用于存储属性，例如用户 102 的属性，如其名字、居所、出生日期、性别和 / 或关于 ID 标记卡本身的属性，如 ID 标记卡的制作或发行机构、ID 标记卡的有效期或 ID 标记卡的标识符，如护照号码或信用卡号码。

[0043] 电子存储器 118 还可以具有一用于存储证书的存储区域 126。该证书包括一公钥，该公钥分配给存储在受保护存储区域 122 中的私钥。该证书可以是基于公钥基础设施(PKI)标准如 X.509 标准而生成的证书。

[0044] 该证书不是必须要存储在 ID 标记卡 106 的电子存储器 118 中。此外，该证书还可以存储在公共目录服务器中。

[0045] ID 标记卡 106 具有一处理器 128。该处理器 128 用于执行程序指令 130、132 及 134。程序指令 130 用于用户验证，也就是，在 ID 标记卡上验证用户 102。

[0046] 在一使用 PIN (个人识别码)的实施方式中，用户 102 将其 PIN 输入，以在 ID 标记

卡 106 中验证自己，例如通过用户计算机系统 100。然后，执行程序指令，进入受保护区域 120，将输入的 PIN 与存储在此的 PIN 的参数值进行比对。如果输入的 PIN 与 PIN 的参数值匹配，用户 102 就视作通过了验证。

[0047] 另外，可以获得用户 102 的生物特征。例如，ID 标记卡 106 为此目的而具有指纹传感器，或者指纹传感器连接于用户计算机系统 100。在此实施方式中，从用户 102 获得的生物特征数据，将通过执行程序指令 130，而与存储在受保护的存储区域 120 中的生物特征基准数据进行比对。如果在从用户 102 获得的生物特征数据与生物特征基准数据有足够的匹配，则用户 102 就视作已经验证。

[0048] 程序指令 134 用于执行关于 ID 标记卡 106 的密码协议的步骤，以在 ID 标记卡 106 上验证 ID 供应商计算机系统 136。密码协议可以是一个基于对称密钥或非对称密钥对的口令 / 应答协议（Challenge-Response-Protokoll）。

[0049] 例如，密码协议 keyi 实现了一扩展的访问控制方法，如国际民航组织（ICAO）指定的机读旅行证件（MRTD）中那样。通过密码协议的成功执行，可以在 ID 标记卡上验证 ID 供应商计算机系统 136，从而证明其读取存储在受保护存储区域 124 中的属性的读取授权。身份验证还可以是互相的，也就是，ID 标记卡 106 也必需基于相同的或不同的密码协议而在 ID 供应商计算机系统 136 中验证自己。

[0050] 程序指令 132 用于在 ID 标记卡与 ID 供应商计算机系统 136 间传送的数据的端到端加密，至少是通过 ID 供应商计算机系统从受保护的存储区域 124 读取的属性的端到端加密。例如，为了端到端加密，可以使用对称密钥，该对称密钥是在 ID 标记卡 106 与 ID 供应商计算机系统 136 之间执行密码协议时达成的。

[0051] 作为图 1 所显示实施方式的一个选择性方案，用户计算机系统 100 所使用的接口 104 可以不是直接与接口 108 连接，而是通过一个连接于接口 104 的、用于 ID 标记卡 106 的阅读器。通过该阅读器，如被称为 2 级芯片卡终端的阅读器，还能够用于输入 PIN。

[0052] ID 供应商计算机系统 136 具有通过网络 116 进行通讯的网络接口 138。ID 供应商计算机系统 136 还具有存储器 140，其存储了 ID 供应商计算机系统 136 之私钥 142 及相应的证书 144。例如，该证书可以是基于 PKI 标准如 X.509 的证书。

[0053] ID 供应商计算机系统 136 还至少具有一个用于执行程序指令 146 与 148 的处理器 145。通过执行程序指令 146，而可以执行关于 ID 供应商计算机系统 136 的密码协议的步骤。因此，通过由 ID 标记卡 106 的处理器 128 执行程序指令 134，以及通过由 ID 供应商计算机系统 136 的处理器 145 执行程序指令 146，来执行密码协议。

[0054] 程序指令 148 用于在 ID 供应商计算机系统 136 上执行端到端加密，例如基于对称密钥，而该对称密钥是在 ID 标记卡 106 与 ID 供应商计算机系统 136 之间执行密码协议时达成的。原则上，可以使用任何已知的方法，达成端到端加密所使用的对称密钥，如 Diffie-Hellman 密钥交换。

[0055] ID 供应商计算机系统 136 优选处在一个受特别保护的环境中，特别是在所谓的信用中心，使得 ID 供应商计算机系统 136，与用户 102 在 ID 标记卡上所必需的验证相结合，而形成了从 ID 标记卡 106 所读取属性之验证的信任支柱。

[0056] 服务计算机系统 150 设计成能够针对一种服务或者产品进行订购或委托，特别是在线服务。例如，用户 102 能够通过网络 116 在银行开一个账户或者使用其它金融或银行

服务。例如，服务计算机系统 150 还可以是网上商店，使得用户 102 能够购买移动电话或者类似的东西。另外，服务计算机系统 150 还可以设计成提供数字内容，如下载音乐数据和 / 或视频数据。

[0057] 为此，服务计算机系统 150 具有一用于连接至网络 116 的网络接口 152。另外，服务计算机系统 150 具有至少一个用于执行程序指令 156 的处理器 154。例如，通过执行程序指令 156，产生动态的 HTML 页面，用户能够使用这些页面输入其委托或订购。

[0058] 取决于委托或订购的产品或服务的性质，服务计算机系统 150 根据一个或多个预设的标准，来检查用户 102 和 / 或其 ID 标记卡 106 的一个或多个属性。只有通过了检查，来自用户 102 的订购或委托才可以执行。

[0059] 例如，通过相关合同开设一银行账户或购买一移动电话，就要求用户 102 必须向服务计算机系统 150 表明身份，并且需要对该身份进行检查。例如，在现有技术中，用户 102 必须通过提交身份证来这样做。这个过程可以由从用户 ID 标记卡 106 中读取用户 102 的数字身份来替代。

[0060] 然而，根据不同的应用场合，用户 102 不必向服务计算机系统 150 表明身份，而是需要一个能够足以进行交流的属性。例如，用户 102 能够使用属性中的一个，来证明他属于一个特别的组群，该组群已经授权可以访问服务计算机系统 150，下载准备好的数据。例如，这样的标准可以是用户 102 的最小年龄，或者是用户 102 在某一圈子的会员资格，该圈子对于特别的秘密数据具有访问授权。

[0061] 为了使用服务计算机系统 150 所提供的服务，将进行如下的过程 ：

[0062] 1、在 ID 标记卡 106 上验证用户 102。

[0063] 用户 102 在 ID 标记卡 106 上验证自己。在使用 PIN 的执行中，用户 102 通过用户计算机系统 100 或者与之相连的芯片卡终端输入其 PIN 来执行。然后，通过执行程序指令 130，ID 标记卡 106 检查输入的 PIN 的正确性。如果输入的 PIN 与存储在受保护的存储区域 120 中的 PIN 的参数值匹配，用户 102 就视为已经通过验证。如上所述，如果利用用户 102 的生物特征来进行验证，其过程是相似的。

[0064] 2、在 ID 标记卡 106 上验证 ID 供应商计算机系统 136。

[0065] 为此，通过用户计算机系统 100 与网络 116，在 ID 标记卡 106 与 ID 供应商计算机系统 136 之间，建立一个连接。例如，ID 供应商计算机系统 136 通过该连接传送它的证书 144 至 ID 标记卡 106。然后，程序指令 134 产生所谓的口令，也就是一随机号码。该随机号码通过使用证书 144 中的 ID 供应商计算机系统 136 的公钥进行加密。由此产生的密码（Chiffrat）通过该连接，从 ID 标记卡 106 传送至 ID 供应商计算机系统 136。ID 供应商计算机系统 136 使用私钥 142 解密该密码，并以这种方式获得随机号码。ID 供应商计算机系统 136 通过该连接将该随机号码返回至 ID 标记卡 106。通过执行程序指令 134，验证从 ID 供应商计算机系统 136 接收的随机号码与开始生成的随机号码，也就是口令，是否匹配。如果匹配，就视为已经在 ID 标记卡 106 上验证了 ID 供应商计算机系统 136。随机号码可以作为终端对终端加密的对称密钥。

[0066] 3、当用户 102 在 ID 标记卡 106 上成功验证后，而且 ID 供应商计算机系统 136 在 ID 标记卡 106 上也成功验证后，则 ID 供应商计算机系统 136 就拥有了读取存储在受保护的存储区域 124 的一个、多个或所有属性的读取授权。基于 ID 供应商计算机系统 136 通过该

连接向 ID 标记卡 106 所发送的相关的读取命令，所请求的属性就从受保护的存储区域 124 中被读取，并通过运行程序指令 132 进行加密。加密的属性通过该连接传送至 ID 供应商计算机系统 136，在此通过执行程序指令 148 进行解密。这样，ID 供应商计算机系统 136 获得了从 ID 标记卡所读取属性的信息。

[0067] 借助证书 144，这些属性通过 ID 供应商计算机系统而得到签注(签字)，并通过用户计算机系统 100 或者直接传送至服务计算机系统 150。这样，服务计算机系统 150 被告知了从 ID 标记卡 106 所读取的属性，而使得服务计算机系统 150 能够使用预先确定的一个或多个标准来检查这些属性，从而可能为用户 102 提供所请求的服务。

[0068] 必须在 ID 标记卡 106 上验证用户 102，及必须在 ID 标记卡 106 上验证 ID 供应商计算机系统，这提供了必需的信任支柱，使得服务计算机系统 150 能够确定，通过 ID 供应商计算机系统 136 向其传达的用户 102 的属性是正确的，而不是伪造的。

[0069] 根据不同的实施方式，验证的顺序可能不同。例如，可以规定首先是用户 102 在 ID 标记卡 106 上验证自己，然后是 ID 供应商计算机系统 136 的验证。然而，原则上还可以首先是 ID 供应商计算机系统 136 在 ID 标记卡 106 上验证自己，然后是用户 102 的验证。

[0070] 例如，在第一种情况下 ID 标记卡 106 是如此设计的，其通过用户 102 输入正确的 PIN 或正确的生物特征来解锁。只有实现这种解锁，才允许启动程序指令 132 及 134，从而验证 ID 供应商计算机系统 136。

[0071] 在第二种情况下，可以在用户 102 还没有在 ID 标记卡 106 验证自己时，就启动程序指令 132 及 134。在这种情况下，例如，程序指令 134 是如此设置的，直到程序指令 130 已经签注用户 102 成功验证之后，ID 供应商计算机系统 136 才能对受保护的存储区域 124 进行读取，以读取一个或多个属性。

[0072] 在电子商务及电子政务应用方面利用 ID 标记卡 106 有特别的优势，而且由于必须在 ID 标记卡上验证用户 102 与 ID 供应商计算机系统而形成信任支柱，从而没有媒介之干扰，而使权利更安全。还有一个特别的优势是，不需要集中存储不同用户 102 的属性，这意味着现有技术中的数据保护问题在此得到解决。至于方法应用的便捷性，也是一个值得考虑的优点，即为了使用 ID 供应商计算机系统 136，用户 102 不必预先登记。

[0073] 图 2 显示了根据本发明方法的一实施方式。在步骤 200 中，服务请求从用户计算机系统发送至服务计算机系统。例如，用户通过启动用户计算机系统上的浏览器，并输入一 URL 以访问服务计算机系统的一个网页。然后，用户向访问的网页输入其服务请求，例如，针对服务或产品的订购或委托。

[0074] 然后，在步骤 202 中，服务计算机系统 150 指定所必须的一个或多个属性，以检查用户对于服务请求的权利。特别地，服务计算机系统应指定能够确定用户 102 数字身份的属性。这种通过服务计算机系统 150 进行的属性的指定，可以是预先确定的，也可以根据服务请求，通过服务计算机系统 150 按设定的规则来确定。

[0075] 在步骤 204 中，属性清单，也就是在步骤 202 中指定的一个或多个属性，被从服务计算机系统直接或通过用户计算机系统，传送至 ID 供应商计算机系统。

[0076] 在步骤 206 中，为了给 ID 供应商计算机系统提供从 ID 标记卡读取属性的机会，用户要在 ID 标记卡上验证自己。

[0077] 在步骤 208 中，在 ID 标记卡与 ID 供应商计算机系统间建立了一连接。该连接优

选为一个受保护的连接，如基于所谓的安全信息传递方法。

[0078] 在步骤 210 中，ID 供应商计算机系统至少要通过步骤 208 中建立的连接，在 ID 标记卡上进行验证。另外，还可以在 ID 供应商计算机系统上验证 ID 标记卡。

[0079] 当用户与 ID 供应商计算机系统都已经成功地在 ID 标记卡上进行了验证后，就通过 ID 标记卡为 ID 供应商计算机系统提供读取属性的授权。在步骤 212 中，ID 供应商计算机系统发送一个或多个读取命令，以读取来自 ID 标记卡的属性清单中所必需的属性。然后，这些属性通过受保护的连接，借助端到端加密，传送至 ID 供应商计算机系统，并在此解密。

[0080] 在步骤 214 中，这些读取的属性值，通过 ID 供应商计算机系统进行签注。在步骤 216 中，ID 供应商计算机系统通过网络发送已签注的属性值。这些签注的属性值直接或通过用户计算机系统到达服务计算机系统。在后一种情况中，用户有机会识别签注的属性值和 / 或通过进一步的数据进行补充。可以考虑，签注的属性值，也许只有当用户从用户计算机系统中放行后，才能同补充的数据继续传送至服务计算机系统。这在从 ID 供应商计算机系统发送至服务计算机系统的属性方面，给用户提供了最大可能的透明度。

[0081] 图 3 显示了根据本发明另一实施方式的 ID 标记卡与计算机系统。在图 3 的实施方式中，ID 标记卡 106 是一个文件的形式，如带有集成电路的纸制和 / 或塑胶制文件（证件），其形成有接口 108、存储器 118 及处理器 128。例如，集成电路可以是所谓的无线标签，还可以叫做射频标签（RFID- 标签）或 RFID。另外，接口 108 可以设置为接触式接口或者双模接口。

[0082] 特别地，文件 106 可以是一个有价文件或者安全文件，如机读旅行证件、电子护照、电子身份证或者可以是支付手段，如信用卡。

[0083] 在此处所考虑的实施方式中，受保护的存储区域 124 储存了属性 i，其中 $1 \leqslant i \leqslant n$。然后假设，没有任何一般性质的限制，图 3 中所示例的 ID 标记卡 106 是一电子身份证。例如，属性 i=1 是姓、属性 i=2 是名、属性 i=3 是地址及属性 i=4 是出生日期等等。

[0084] 在此处所考虑的实施方式中，用户计算机系统 100 的接口 104 可以是 RFID 阅读器的形式，其可以是用户计算机系统的组成部分，或者也可以是一与其相连的单独元件。

[0085] 用户 102 可以支配一个或多个设计上基本相同的 ID 标记卡，例如 ID 标记卡 106' 是一信用卡。

[0086] 用户计算机系统 100 可以储存一系列配置数据记录 158、160……。每一配置数据记录为一组特定属性指定数据源和 ID 供应商计算机系统，该 ID 供应商计算机系统能够读取指定的数据源。在此实施方式中，用户计算机系统 100 能够使用网络 116，连接不同的 ID 供应商计算机系统 136、136'、……。这些系统可以属于不同的信用中心。例如，ID 供应商计算机系统 136 属于信用中心 A，而结构上基本相同的 ID 供应商计算机系统 136' 属于另外一个信用中心 B。

[0087] 配置数据记录 158，也叫做 ID 容器（ID-Container），定义了用于属性 i=1 至 i=4 的属性组。这些属性分别分配了数据源“身份证”，也就是 ID 标记卡 106，也分别分配了信用中心 A，也就是与他们相连的 ID 供应商计算机系统 136。例如，后者在配置数据记录 158 中可以指定为 URL 的形式。

[0088] 与此相对，配置数据记录 116 中定义了一组属性 I、II 及 III。这些属性的数据源都

指定了相应的信用卡，也就是 ID 标记卡 106’。ID 标记卡 106’具有一受保护区域 124’，其存储了属性 I、II 及III。例如，属性 I 可以是信用卡持有者的名字、属性 II 可以是信用卡号码、属性III可以是信用卡的有效期等等。

[0089] 在配置数据记录 160 中，指定信用中心 B 的 ID 供应商计算机系统 136’作为 ID 用户计算机系统。

[0090] 作为图 3 所示实施方式的替代方式，可以是在这些相同的配置数据记录中，对于不同的属性指定不同的数据源和 / 或不同 ID 供应商计算机系统。

[0091] 在图 3 所示实施方式中，ID 供应商计算机系统 136、136’……中的每个可能具有各自的多个证书。

[0092] 例如，如图 3 所示，ID 供应商计算机系统 136 的存储器 140，储存了多个证书，如分别具有相应私钥 142.1 及 142.2 的证书 144.1 及 144.2。在证书 144.1 中，通过属性 i=1 至 i=4，对 ID 供应商计算机系统 136 的读取权利进行定义，而在证书 144.2 中，通过属性 I 至 III，对读取权利进行定义。

[0093] 为了通过服务计算机系统 150 使用服务，首先用户 102 要向用户计算机系统 100 进行一个输入 162，例如，为了想要的服务，向服务计算机系统 150 上的一网页中输入其请求。该服务请求 164 通过网络 116 由用户计算机系统 100 传送至服务计算机系统 150。然后，该服务计算机系统 150 反映出属性清单 166，也就是指定服务计算机系统 150 要求的那些，用于处理来自用户 102 的服务请求 164 的属性。例如，属性清单能够以属性名称的形式做出，如“姓”、“名”、“地址”、“信用卡号码”。

[0094] 属性清单 166 的回执，通过用户计算机系统 100 显示给用户 102。然后，用户 102 能够选择一个或多个配置数据记录 158、160……，其能够根据属性清单 166 分别定义包含属性的属性组，至少是一个子集。

[0095] 例如，如果属性清单 166 仅仅要求用户 102 姓、名及地址，用户 102 能够选择配置数据记录 158。相反地，如果在属性清单 166 中补充指定了信用卡号码，用户 102 能够补充选择配置数据记录 160。这个过程还能够由用户计算机系统 100 全部自动地进行，例如通过执行程序指令 112。

[0096] 然后，首先假设只有一个配置数据记录，如配置数据记录 158，其是基于属性清单 166 选定的。

[0097] 然后，用户计算机系统 100 向选定的配置数据记录中指示的 ID 供应商计算机系统发送一请求 168，如信用中心 A 的 ID 供应商计算机系统 136。请求 168 根据属性清单 166，包含一个关于属性的报告（Angabe），其需要通过 ID 供应商计算机系统 136，从配置数据记录 158 中指示的数据源读取。

[0098] 然后，ID 供应商计算机系统 136 选择一个或多个具有读取属性所需的读取权利的证书。例如，如果属性 i=1 至 3 是从身份证读取，ID 供应商计算机系统 136 因此选择定义了所需权利的证书 144.1。这种证书的选择是通过程序指令 149 的执行来进行的。

[0099] 然后，开始执行密码协议。例如，ID 供应商计算机系统 136 为此向用户计算机系统 100 发送一个回复。然后用户计算机系统 100 要求用户 102 在指定的数据源上验证自己，也就是，在 ID 标记卡上验证自己。

[0100] 然后，用户 102 把其标记卡，也就是 ID 标记卡 106，放入 RFID 阅读器 104 的范围

内，并输入 PIN，以验证自己。用户 102 在 ID 标记卡 106 上成功验证，解锁了密码协议的执行，也就是程序指令 134 的执行。接着，ID 供应商计算机系统 136 使用选定的证书 144.1 在 ID 标记卡 106 上验证它自己，如使用口令 / 应答的方式。这种验证还可以是相互的。随着 ID 供应商计算机系统 136 在 ID 标记卡 106 上验证成功，ID 供应商计算机系统 136 向用户计算机系统 100 发送一用于读取必要的属性的读取请求，并且后者通过 RFID 阅读器向 ID 标记卡 106 转发该请求。ID 标记卡 106 使用证书 144.1 以检查 ID 供应商计算机系统 136 是否有必要的读取权利。如果有，所需的属性就从受保护的存储区域 124 中读取，并借助端到端加密的方式，通过用户计算机系统 100 传送至 ID 供应商计算机系统。

[0101] 然后，ID 供应商计算机系统 136 通过网络 116 向服务计算机系统 150 发送一回复 170，其包括已经读取的属性。该回复 170 数字签注了证书 144.1。

[0102] 此外，ID 供应商计算机系统 136 向用户计算机系统 100 发送回复 170。然后，提供给用户 102 机会阅读回复 170 中包含的属性，并决定他是否希望向服务计算机系统 150 转发这些属性。仅仅当用户 102 向用户计算机系统 100 输入一个放行命令时，然后回复 170 才会转发至服务计算机系统 150。在此实施方式中，用户 102 还可能向回复 170 增加进一步的数据。

[0103] 如果涉及多个 ID 供应商计算机系统 136、136'……，来自 ID 供应商计算机系统的个别的回复能够通过用户计算机系统 100 结合成一个单独的回复，其包括了所有根据属性清单 166 而来的属性，然后，该回复从用户计算机系统 100 传送至服务计算机系统 150。

[0104] 根据本发明一实施方式，用户 102 在服务请求 164 的情形下，能够向服务计算机系统 150 公开一个或多个其属性，如通过网络 116 向服务计算机系统传送用户的属性，作为服务请求 164 的一部分。特别地，用户 102 能够向服务计算机系统 150 上的网页中输入该属性。然后，通过回复 170 确认这些属性的有效性，也就是，服务计算机系统 150 能够通过 ID 供应商电脑，将从用户 102 接收到的属性与从 ID 标记卡 106 读取的属性进行比对，并检查他们是否匹配。

[0105] 根据本发明进一步的实施方式，还可能在属性清单 166 中至少指示一个更进一步的属性，该属性没有存储在用户 102 的一个 ID 标记卡上，但是可以从一外部信息源那里请求。例如，这种方式是关于用户 102 的信誉的属性。为此，用户计算机系统 100 可以包括另外的配置数据记录 161，其包括对于属性 A 如信誉的数据源与 ID 供应商计算机系统的报告。数据源可以是一网上信用机构，如联邦德国信贷风险保护协会、Dun & Bradstreet 或者类似的机构。例如，ID 供应商计算机系统指示了一个信用中心 C，如图 3 所示。在此情况下，数据源可以定位于信用中心 C 中。

[0106] 为了请求属性 A，用户计算机系统 100 向信用中心 C，也就是 ID 供应商计算机系统 136"，发送相应的请求（图 3 中未示出）。然后，信用中心提交属性 A，其是用户计算机系统 100 转发给服务计算机系统 150 的属性以及从用户 102 的 ID 标记卡中已读取的其它属性。

[0107] 优选地，例如，在关于用户 102 数字身份的属性已经从用户 102 的 ID 标记卡得到请求，并且通过用户计算机系统 100 接收了签注的回复 170 之后，属性 A 才得到请求。通过用户计算机系统 100、而从 ID 供应商计算机系统 136" 请求的属性 A，其请求包括签注的回复 170，使得 ID 供应商计算机系统 136" 关于用户 102 的身份具有可靠的信息。

[0108] 图 4 显示了根据本发明方法的另外实施方式。通过用户 102 向用户系统 100 的用

户输入，用户 102 在服务计算机系统上指定了其需要的服务。例如，这可通过访问服务计算机系统上的网页并选择其提供的一个服务来达到。来自用户 102 的服务请求从用户计算机系统 100 传送至服务计算机系统 150。

[0109] 服务计算机系统 150 通过一个属性清单对服务请求做出回复，也就是，例如属性名称的清单。当该属性清单被接收后，用户计算机系统 100 请求用户 102 在 ID 标记卡 106 上验证他自己，例如通过输入请求的方式。

[0110] 然后，用户 102 在 ID 标记卡 106 上验证他自己，例如通过输入其 PIN。随着验证成功，属性清单从用户计算机系统 100 转发至 ID 供应商计算机系统。然后，后者在 ID 标记卡上验证自己，并根据属性清单向 ID 标记卡发送一用于读取属性的读取请求。

[0111] 假设之前的用户 102 与 ID 供应商计算机系统 136 的验证成功，ID 标记卡以想要的属性对读取请求做出回复。ID 供应商计算机系统 136 签注该属性，并将已签注的属性发送至用户计算机系统 100。随着用户 102 的放行，然后，该已签注的属性传送至服务计算机系统 150，然后，其提供需要的服务。

[0112] 附图标记清单

[0113]

100	用户计算机系统
102	用户
104	接口
106	ID 标识卡
108	接口
110	处理器
112	程序指令
114	网络接口
116	网络
118	电子存储器
120	受保护的存储区域
122	受保护的存储区域
124	受保护的存储区域
126	存储区域
128	处理器
130	程序指令

[0114]

132 程序指令

134 程序指令

136 ID 供应商计算机系统

138 网络接口

140 存储器

142 私钥

144 证书

145 处理器

146 程序指令

148 程序指令

149 程序指令

150 服务计算机系统

152 网络接口

154 处理器

156 程序指令

158 配置数据记录

160 配置数据记录

161 配置数据记录

162 用户输入

164 服务请求

166 属性清单

168 请求

170 回复

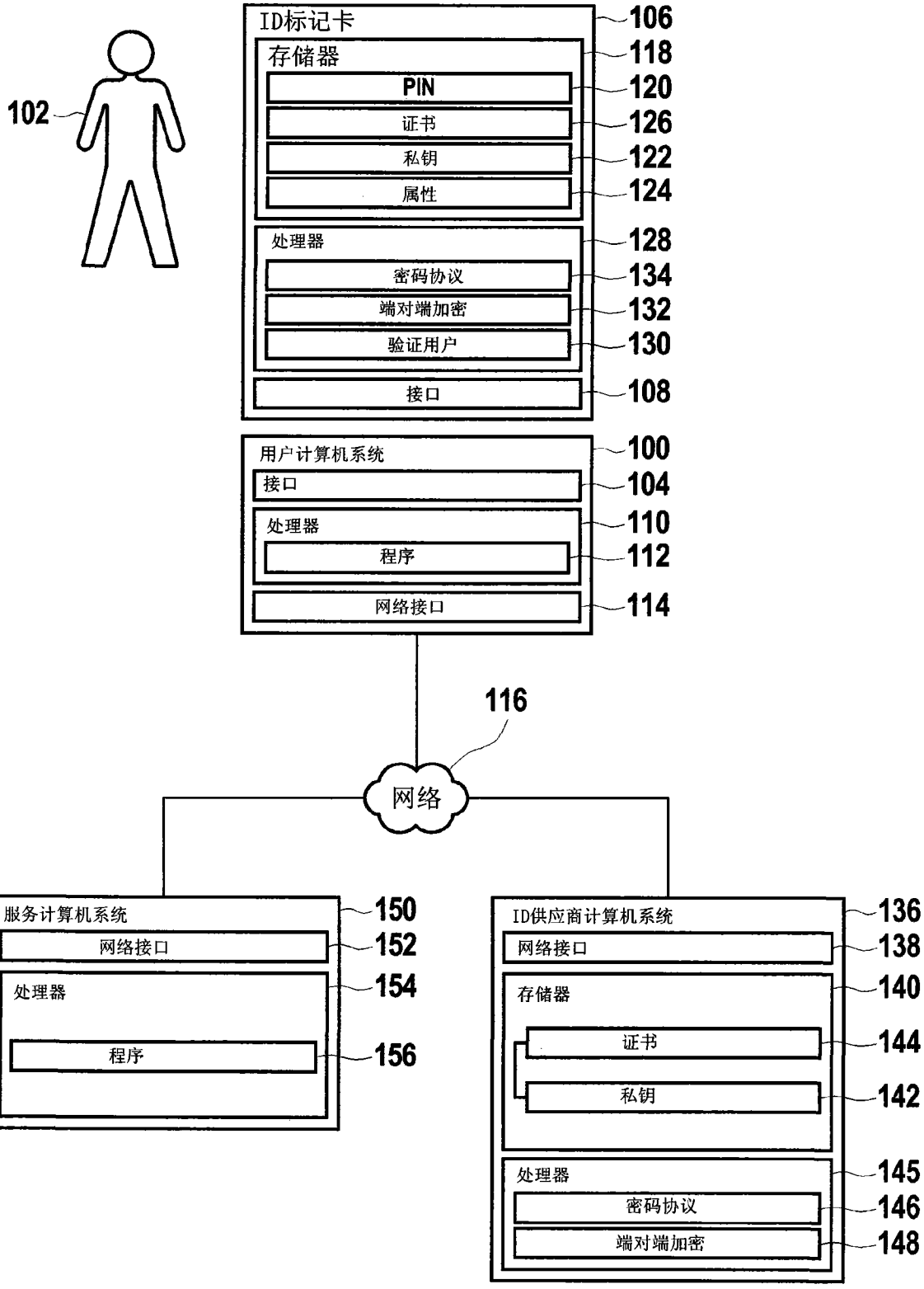

102
ID标记卡
106
存储器
118
PIN
120
证书
126
私钥
122
属性
124
处理器
128
密码协议
134
端对端加密
132
验证用户
130
接口
108
用户计算机系统
100
接口
104
处理器
110
程序
112
网络接口
114
116
网络
服务计算机系统
150
网络接口
152
处理器
154
程序
156
ID供应商计算机系统
136
网络接口
138
存储器
140
证书
144
私钥
142
处理器
145
密码协议
146
端对端加密
148

图 1

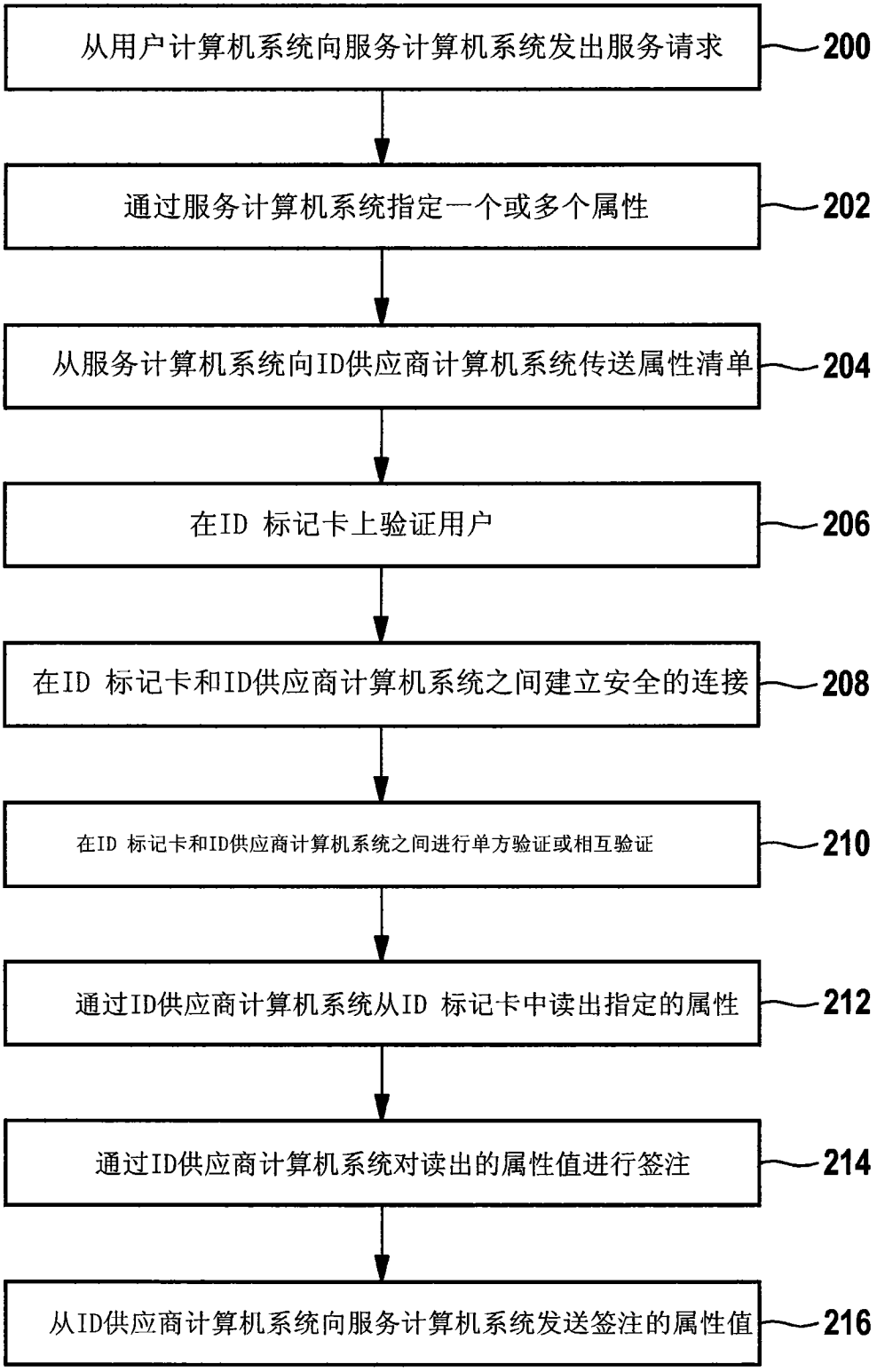

从用户计算机系统向服务计算机系统发出服务请求
200
通过服务计算机系统指定一个或多个属性
202
从服务计算机系统向ID供应商计算机系统传送属性清单
204
在ID 标记卡上验证用户
206
在ID 标记卡和ID供应商计算机系统之间建立安全的连接
208
在ID 标记卡和ID供应商计算机系统之间进行单方验证或相互验证
210
通过ID供应商计算机系统从ID 标记卡中读出指定的属性
212
通过ID供应商计算机系统对读出的属性值进行签注
214
从ID供应商计算机系统向服务计算机系统发送签注的属性值
216

图 2

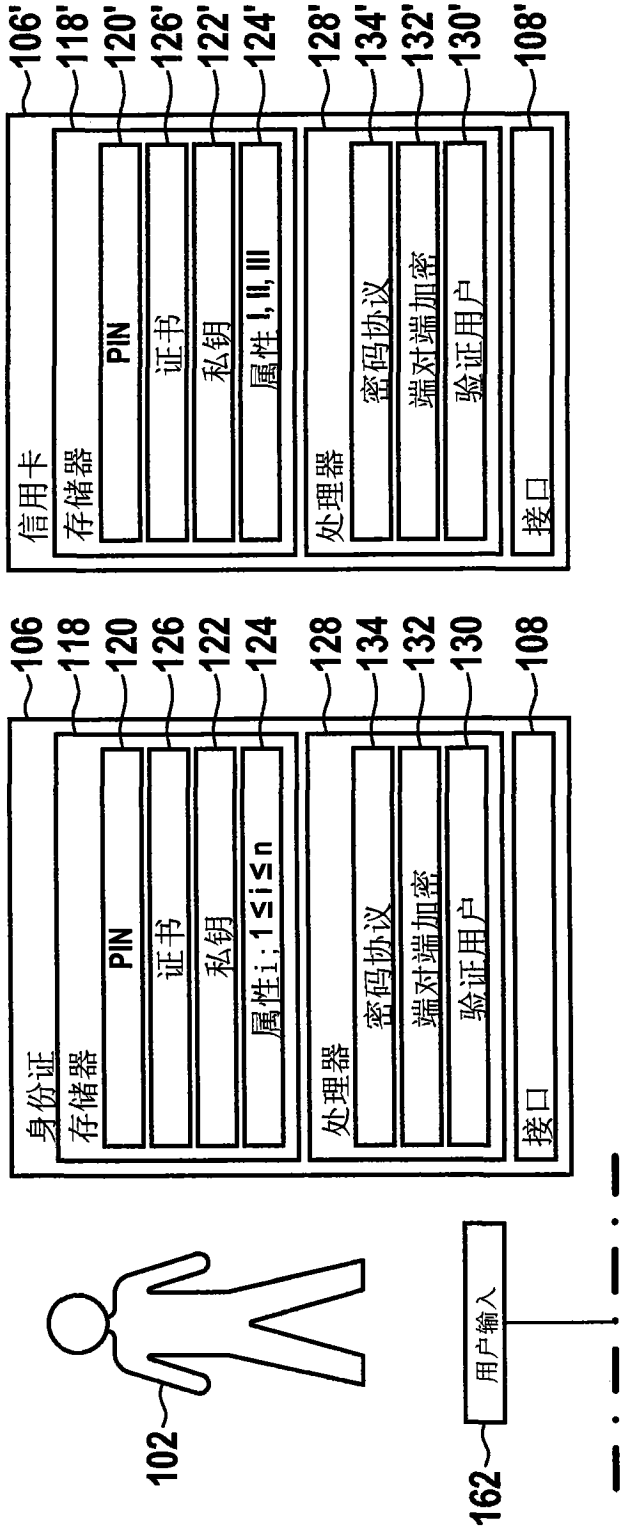

106'
118'
120'
126'
122'
124'
128'
134'
132'
130'
108'
信用卡
存储器
PIN
证书
私钥
属性 I, II, III
处理器
密码协议
端对端加密
验证用户
接口
106
118
120
126
122
124
128
134
132
130
108
身份证
存储器
PIN
证书
私钥
属性 i; 1≤i≤n
处理器
密码协议
端对端加密
验证用户
接口
102
162
用户输入

图 3a

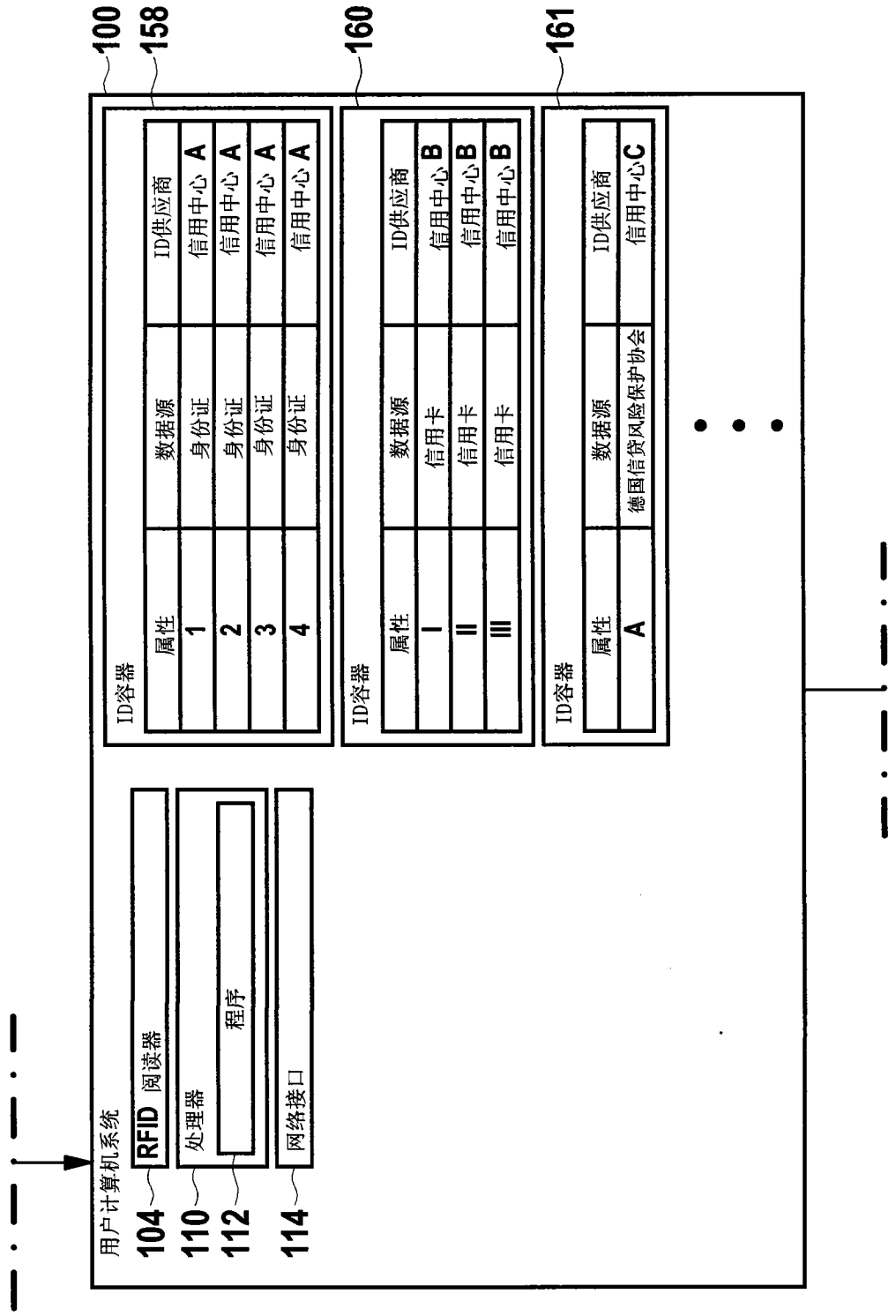

100
158
160
161
ID容器
属性
数据源
ID供应商
1
身份证
信用中心 A
2
身份证
信用中心 A
3
身份证
信用中心 A
4
身份证
信用中心 A
ID容器
属性
数据源
ID供应商
I
信用卡
信用中心 B
II
信用卡
信用中心 B
III
信用卡
信用中心 B
ID容器
属性
数据源
ID供应商
A
德国信贷风险保护协会
信用中心 C
用户计算机系统
RFID 阅读器
处理器
程序
网络接口
104
110
112
114

图 3b

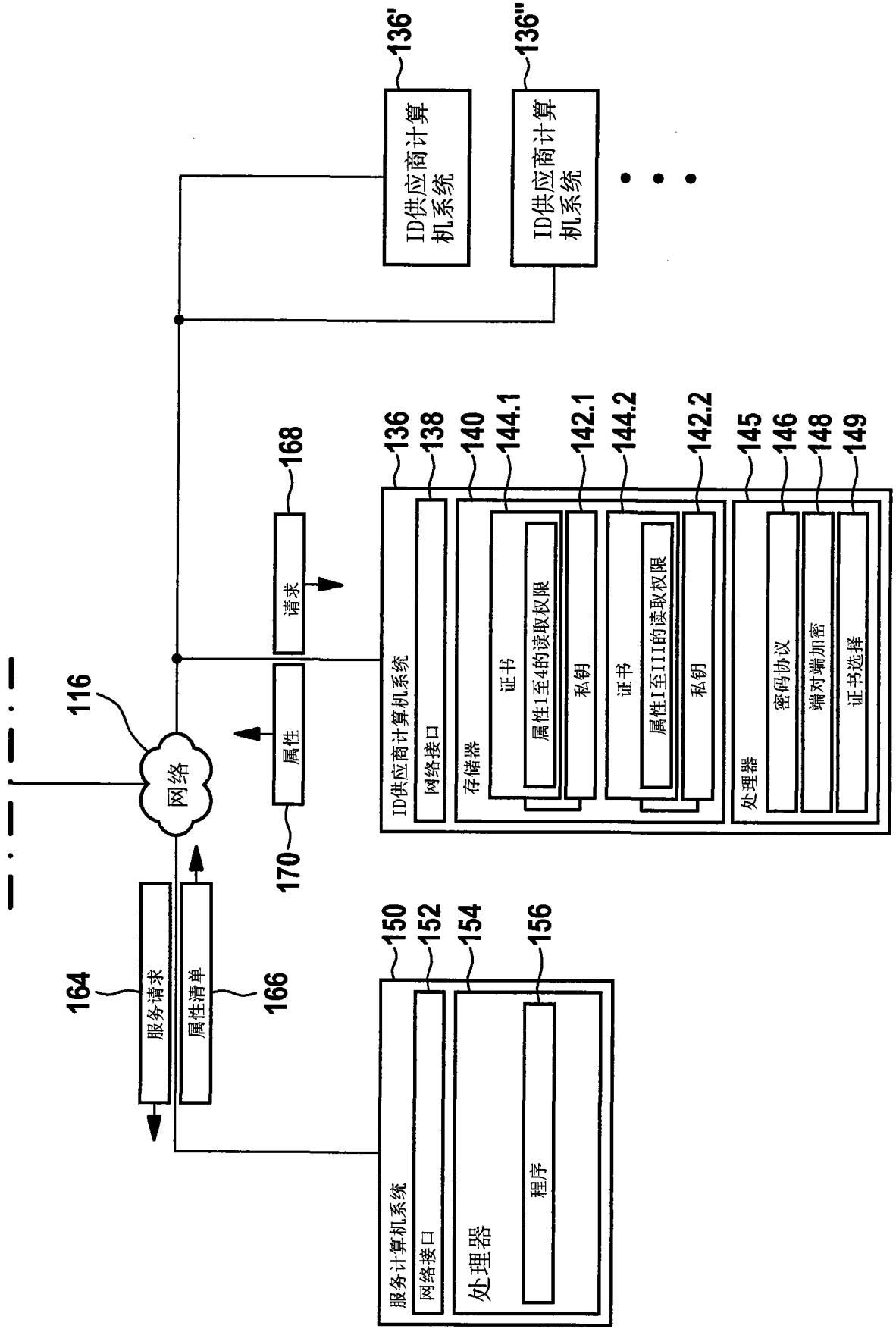

136'
ID供应商计算机系统
136"
ID供应商计算机系统
168
请求
属性
170
116
网络
164
服务请求
属性清单
166
136
138
140
144.1
142.1
144.2
142.2
145
146
148
149
ID供应商计算机系统
网络接口
存储器
证书
属性1至4的读取权限
私钥
证书
属性I至III的读取权限
私钥
处理器
密码协议
端对端加密
证书选择
150
152
154
156
服务计算机系统
网络接口
处理器
程序

图 3c

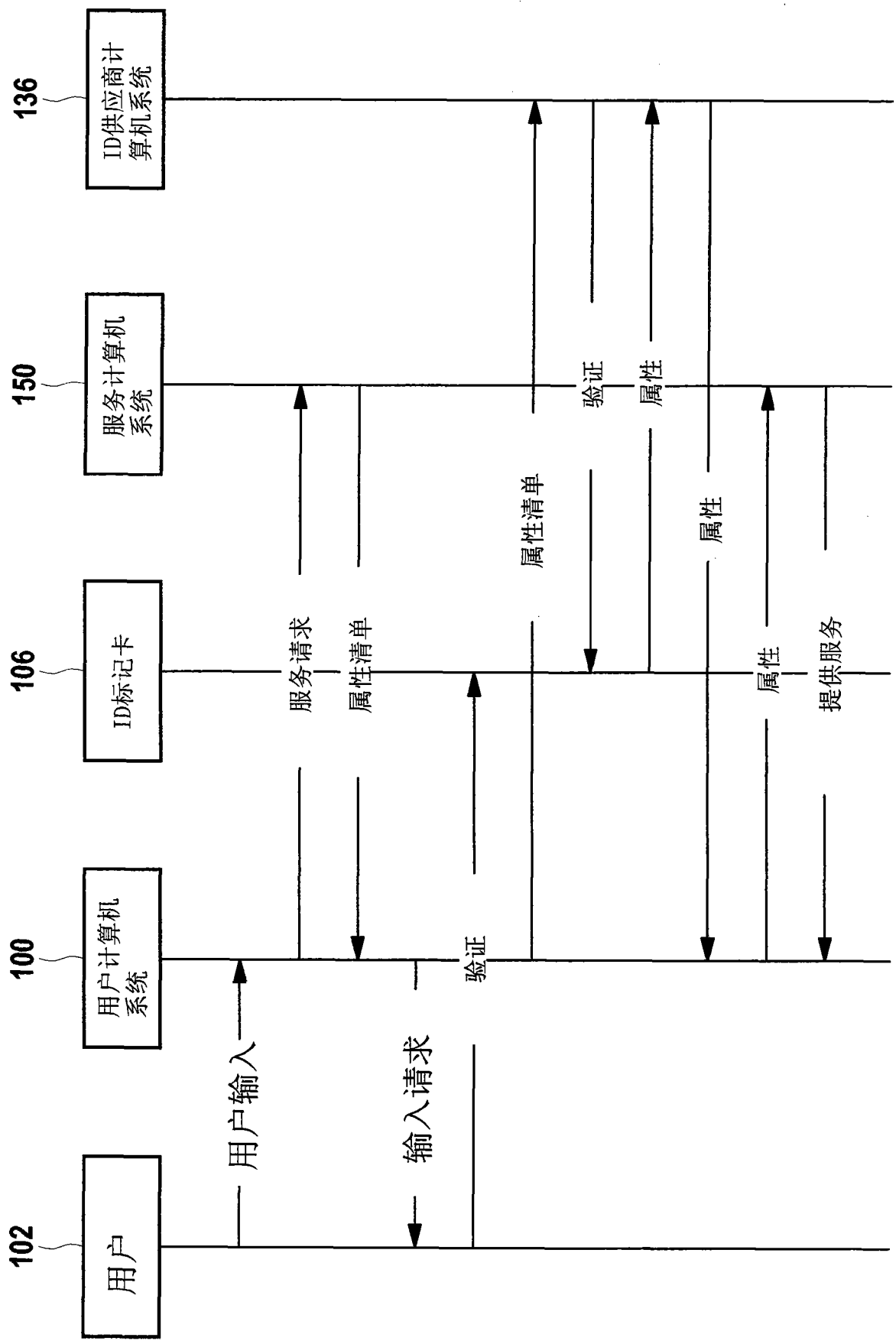

102
用户
100
用户计算机系统
106
ID标记卡
150
服务计算机系统
136
ID供应商计算机系统
用户输入
输入请求
验证
服务请求
属性清单
属性清单
验证
属性
属性
属性
提供服务

图 4