(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 102265311 B
(45)授权公告日 2016.03.30

(21)申请号 200980146651.9
(22)申请日 2009.10.07
(30)优先权数据
A1570/2008 2008.10.07 AT
(85)PCT国际申请进入国家阶段日
2011.05.23
(86)PCT国际申请的申请数据
PCT/AT2009/000388 2009.10.07
(87)PCT国际申请的公布数据
WO2010/040162 DE 2010.04.15
(73)专利权人 艾斯麦格控股有限公司
地址 奥地利格吕瑙
(72)发明人 K·施罗德 H·B·常
(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 赵科
(51)Int.Cl.
G07C 9/00(2006.01)
(56)对比文件
CN 101061494 A,2007.10.24,
US 2003234719 A1,2003.12.25,
US 2005132194 A1,2005.06.16,
US 2006136997 A1,2006.06.22,
US 2007204162 A1,2007.08.30,
审查员 崔琳

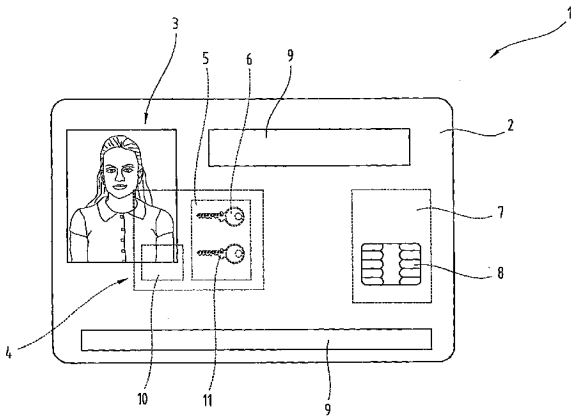
权利要求书2页 说明书11页 附图4页

(54)发明名称

识别标记

(57)摘要

本发明涉及一种用于被授权的人物识别的识别标记(1),包括承载层(2)、具有存储装置(5)的验证装置(4)、与人物相关的标记(3)、具有通信接口(8)的通信装置(7),其中所述存储装置被构造为不易失且可重写的半导体存储器,在所述存储装置(5)中存储和与人物相关的标记(3)关联的第一电子密钥(6)。本发明还涉及一种用于被授权的人物识别的识别标记,包括电子记录,在所述电子记录中存储与人物相关的标记(3)的电子图片和第一电子密钥(6),所述第一电子密钥(6)和与人物相关的标记(3)关联。本发明还涉及一种利用识别标记来识别和认证人物的方法。



CN 102265311 B

1. 一种用于被验证的人物识别的识别标记 (1)，包括承载层 (2)、具有存储装置 (5) 的验证装置 (4)、与人物相关的标记 (3)、具有通信接口 (8) 的通信装置 (7)，其中所述存储装置被构造为非易失性且可重写的半导体存储器，其特征在于，在所述存储装置 (5) 中存储与所述与人物相关的标记 (3) 关联的第一电子密钥 (6)，并且所述第一电子密钥 (6) 由法律权威 (18) 的电子密钥形成，在所述存储装置 (5) 中存储第二电子密钥 (11)，所述第二电子密钥 (11) 与所述第一电子密钥 (6) 关联，所述与人物相关的标记 (3) 的数码图片 (31) 被存储在所述存储装置 (5) 中。

2. 一种用于被验证的人物识别的识别标记 (1)，包括承载层 (2)、电子记录、与人物相关的标记 (3)、具有通信接口 (8) 的通信装置 (7)，其中在所述电子记录中存储与人物相关的标记 (3) 的数码图片 (31) 和第一电子密钥 (6)，其特征在于，所述第一电子密钥 (6) 和所述与人物相关的标记 (3) 关联，并且所述第一电子密钥 (6) 由法律权威 (18) 的电子密钥形成，在所述电子记录中存储第二电子密钥 (11)，所述第二电子密钥 (11) 与所述第一电子密钥 (6) 关联，其中所述电子记录被存储在存储装置中。

3. 如权利要求 1 所述的识别标记，其特征在于，所述承载层 (2) 从包含证明文件、信用卡形的数据卡和移动数据存储器的组中形成。

4. 如权利要求 1 至 3 之一所述的识别标记，其特征在于，由人物的图片形成所述与人物相关的标记 (3)。

5. 如权利要求 4 所述的识别标记，其特征在于，所述数码图片 (31) 符合用于人物成像的国际承认的 ICAO 的标准。

6. 如权利要求 1 至 3 之一所述的识别标记，其特征在于，通过生物识别技术的标记形成所述与人物相关的标记 (3)。

7. 如权利要求 1 或 2 所述的识别标记，其特征在于，通过鉴权或认证机构 (21) 的密钥形成所述第一电子密钥 (6)。

8. 如权利要求 3 所述的识别标记，其特征在于，所述验证装置 (4) 具有数据处理装置或加密模块 (10)。

9. 如权利要求 3 所述的识别标记，其特征在于，所述通信接口 (8) 被构造用于无线通信。

10. 如权利要求 1 所述的识别标记，其特征在于，所述关联通过单向操作构成。

11. 如权利要求 10 所述的识别标记，其特征在于，所述第二电子密钥 (11) 通过法律权威 (18) 的电子密钥形成。

12. 如权利要求 11 所述的识别标记，其特征在于，所述第一电子密钥 (6) 被编码存储在所述数码图片 (31) 中。

13. 如权利要求 2 所述的识别标记，其特征在于，所述电子记录被存储在数据处理装置的存储装置中。

14. 如权利要求 13 所述的识别标记，其特征在于，所述数据处理装置具有构造为使得远程数据站能够实现访问所述电子记录的通信接口。

15. 如权利要求 2 所述的识别标记，其特征在于，所述电子记录被存储在移动存储器中。

16. 一种用于利用根据权利要求 1 至 15 之一所述的识别标记来识别和验证人物的方

法，包括下列步骤：

在存储装置 (5) 或电子记录中存储与人物相关的标记 (3、9)；

通过法律权威 (18) 证明人物 (15) 的合法性；

在存储装置 (5) 或电子记录中存储法律权威 (18) 的第一电子密钥 (6)；

关联 (19) 所述第一电子密钥 (6) 和所述与人物相关的标记 (3)。

17. 如权利要求 16 所述的方法，其特征在于，在所述存储装置 (5) 或所述电子记录中存储鉴权或认证机构 (20) 的第二电子密钥 (11)。

18. 如权利要求 16 或 17 所述的方法，其特征在于，在外部的存储单元中存储与人物相关的数据的参考记录。

19. 如权利要求 17 所述的方法，其特征在于，在识别标记 (1) 处，存储与人物相关的数据的参考记录。

20. 如权利要求 18 所述的方法，其特征在于，将所存储的与人物相关的数据的参考记录和所出示的与人物相关的记录进行比较。

21. 如权利要求 16 所述的方法，其特征在于，为了识别和验证人物，将所存储的与人物相关的标记 (3、9) 和所采集的标记进行比较。

22. 如权利要求 16 所述的方法，其特征在于，所述与人物相关的标记在采集之后马上与所述第一电子密钥 (6) 关联。

23. 如权利要求 22 所述的方法，其特征在于，所述与人物相关的标记实时地在法律权威前或通过法律权威采集。

识别标记

技术领域

[0001] 本发明涉及一种用于被验证的人物识别的个人的识别标记，包括承载层、具有存储装置的验证装置、与人物相关的标记、具有通信接口的通信装置，其中存储装置被构造为非易失性且可重写的半导体存储器。本发明还涉及一种用于被验证的人物身份的识别标记，包括电子记录，其内部存储有第一电子密钥和与人物相关的标记的电子图片。本发明还涉及一种利用识别标记识别和验证人物的方法。

背景技术

[0002] 用于识别人物的识别标记是周知的，大多是基于视觉地检验由人物本身携带的或出示给进行检查的权威人士的人物的标记与存储在识别标记内的个人数据的一致性。这种一致性的检验大都由人执行，当然，识别标记至少可以部分地被自动系统读取和处理也是已知的。在由人实行的目视比较检查中存在已知的信息标记的一个明显缺点，因为这种的标记有可能被潜在的入侵者伪造并且由此操控有效的识别标记，从而识别标记可能被他人以不正当的目的滥用。此外，一致性的评价标准也部分依赖于人的主观判断，尤其是还依赖于个人每天的情绪或状况。因此不能确保客观的检验。

发明内容

[0003] 下述的发明基于的任务是提供一种识别标记，利用该识别标记可以明确地保证人物的识别和真实可靠性。

[0004] 本发明的任务将通过在识别标记的存储装置中存放和与人物相关的标记关联的第一电子密钥来解决。

[0005] 这个构造以特别有益的方式保证了，最大程度地保护与人物相关的标记不被操控，因为为了成功，潜在的入侵者不仅必须操控与人物相关的标记，而且还必须操控该关联并且在可能的情况下必须操控第一个电子密钥。因为第一电子密钥存储在存储装置中并因此存储在验证装置中，所以潜在的入侵者因此必须操控验证装置，这需要非常高的花费并且成功的机会很小。

[0006] 第一电子密钥可例如由伪随机码构成，例如作为字母数字编码。这种密钥可以由算法定义地生成，但是在察看者看来却如同随机排列的符号。尤其地，可以构造独特的电子密钥，其即使受到所谓的强力攻击也不能被规避。尤其地，用于检验这种密钥的所有可能组合所需要的花费将超出入侵者技术和时间上的可能性。

[0007] 通过关联与人物相关的标记和电子密钥而形成标记组合，该标记组合将电子密钥关于防伪的优点同与人物相关的标记结合起来。因此识别标记被如此有益地构造，使得明显提高明确的人物识别和认证的安全性。

[0008] 识别标记的另一构造还通过电子记录解决本发明的任务，其中这里第一电子密钥也和与人物相关的标记关联，这一构造的好处尤其在于，电子记录可以由优选包括数据处理装置的自动采集装置直接来处理。尤其是进行身份检测不需要采集装置来建立与识别标

记的通信联结。这一构造的另一优势还在于，识别标记可以数据技术路径传播并被处理。因此尤其可以使用大量熟悉且推广广泛的装置，以便可以基于所存储的与人物相关的标记来执行识别和 / 或认证人物，

[0009] 由于法律和宪法的原则要求人物携带识别标记，根据改进将承载层构造为证明文件。识别标记可以例如被构造为汽车驾驶执照，也可以被设计为出境旅游的旅行证件。鉴于检查站联网以提高人物识别的安全性，识别标记也可以被如此构造，使得识别标记可以被自动采集设备处理。尤其地，与人物相关的标记符合可以机读的采集的要求。例如可以实现视觉采集与人物相关的标记，可这样构成，标记组件被应用于不同的光谱成分。因此与人物相关的标记的检测例如不仅可以在可见光区域进行，也可以在不可见光区域构造标记组件并为了比较进行采集 - 例如在 IR 或 UV 区域。构造为机器可读的证明文件具有另一优点，即与人物相关的标记的检验总是根据同样的可复制的标准进行，因此排除由鉴定人的个别的评价标准而引起的可能的不安全因素。

[0010] 一个改进的特别的优点在于，根据这个改进将承载层设计为信用卡类的数据卡，其中尤其优选为智能卡。根据权利要求的改进具有特别的优点，即信用卡被构造地尤其紧凑，因此可由人长久携带，不会因大小和 / 或形状而影响行动自由。尤其是构造为信用卡有如下的优点，即可以将其放在人们总可以携带的物体中，比如放在钱包里。

[0011] 承载层也可以通过移动的数据存储器形成，例如业内周知的 U 盘或存储卡。由于科技的进步这种移动数据存储器体积越来越小却能提供越来越大的存储能力。因此这类移动存数据储器已经被大量的使用者携带并且以尤其有益的方式作为根据本发明的识别标记的承载层。

[0012] 根据一个改进，与人物相关的标记通过人物的图片形成。人物的图片 - 尤其是照片，可以非常快速地实现与人物相关的标记和出示识别标记的人之间的一致性的监控。通过根据本发明和第一电子密钥的关联对与人物相关的标记作有益的改进，使得可以更简单快捷地进行视觉比较，但是与人物相关的标记或识别标记却非常难被操控。

[0013] 在承载层上优选放置与人物相关的标记的显示。这样的好处在于，可以很快地进行视觉的监控，其中将所述显示和真人进行比较。

[0014] 鉴于借助图片进行可靠地识别进而可靠地识别和认证人物，一个改进具有特别的优势，根据该改进，图片符合为人物成像的国际认可的标准。优选应用国际民用航空组织 (ICAO) 的要求。尤其地，ICAO 规定了如何成像人物的面貌以及关于人物表情要遵守哪些要求。通过国际认可的标准化例如可以自动处理人物图片。另一个主要的优势在于通过国际标准化确保了通用性，从而在世界范围内应用统一的比较标记。

[0015] 除了人物图片作为与人物相关的标记外，还可以通过生物识别的标记来形成与人物相关的标记，其优势在于，生物识别的标记极难或不能被操控，从而提供非常高的人物识别或认证的安全性。被用作生物识别标记的可以例如是指纹、虹膜图像、皮肤或静脉结构或者声音。此外，生物识别标记为了可以存储在根据本发明的识别标记中被转换为电子的表示。

[0016] 考虑到识别标记的安全性存在一个有利的改进，根据该改进第一密钥由鉴权或认证机构的密钥形成。这种机构大部分是国际认可的组织，其在发配和管理电子密钥方面遵循非常高的标准。然而重要的是这种机构不依赖其他组织进行电子密钥的分配和管理，因

而确保了高度自主性和极小的受影响度。例如第一电子密钥可以是所谓的公共密钥系统一部分，其中密钥的一部分是公开的，而私用的密钥部分只对注册的授权和认证机构的使用者公开。

[0017] 例如第一电子密钥或关联可以如此形成，使得潜在的入侵者通过操控企图(Manipulationsversuch)对第一电子密钥或关联进行无可挽回的损害。

[0018] 因为第一电子密钥和与人物相关的标记存储在认证机构的存储装置中，如果认证机构具有数据处理装置或加密模块是有优势的，因为可以阻止直接地访问所存储的标记。如果外部的检验装置－例如自动的人物识别装置－不能直接地访问存储的密钥、与人物相关的标记或关联，则出于安全的考虑这是非常重要的。利用根据权利要求的改进，可以对存储的标记加密，使得潜在的入侵者从中无法获益。这一构造尤其具有以下优势，即存储的标记可以被最大程度地隐藏，从而阻止滥用的访问可能。例如电子密钥可以用单向加密的算法来加密。在访问识别标记用于检验与人物相关的标记时，认证机构的人物识别装置展示具体的密钥结果(Schlüsselergebnis)，以便获得对识别标记数进行数据技术地访问的许可。在暴力破解法中入侵者试图通过试用可能的密钥结果实现访问的目的。在使用错误的密钥结果多次未成功的访问尝试后，认证机构可以激活保护机制，保护机制例如可以完全禁止访问并要求生成新的第一电子密钥和与人物相关的标记的关联。然而也有可能认证机构将认证标记作废，例如通过销毁第一密钥和/或与人物相关的标记。

[0019] 鉴于尽可能的方便用户使用或应用根据本发明的识别标记，存在一种改进，根据改进构造通接口用于进行无线通信。由此例如可以这样，即携带根据本发明的识别标记的使用者通过采集装置，其中采集装置通过通信装置与认证机构无线通信并且这样例如互换或验证第一密钥和/或可能的其他与人物相关的标记。该构造恰好在增多的人员流通的区域恰好有特别的优势，即人流不会因为出示识别标记而减慢。例如人通过采集装置，该采集装置读取相关的标记并在可能的情况下进行自动的人物识别和认证。

[0020] 在一个改进中，采集装置例如可以和数据处理装置连接，该数据处理装置在读取或检验第一电子密钥后访问中央数据存储装置并读取其中存放的识别标记的参考数据。这些参考标记然后可以显示给控制人员，其将这些标记和当前在场的人的标记进行比较。

[0021] 鉴于可靠的人物认证和识别，如果有存储第二电子密钥，可以使识别标记的安全性的尤其提高。在第一种构造中可以在认证机构的存储装置中存放这个第二电子密钥，或者在第二种构造中存储在电子记录中。这个第二电子密钥不依赖于第一电子密钥并且从而实现通过另外的鉴定或认证机构可以在识别标记处存储附加的安全标记。从而可以使监督机构在检验根据本发明的识别标记时，对两个电子密钥独立地分别检验这样就可以提高的安全性对人物进行识别和认证。通过这一构造也使潜在的入侵者明显更难对根据本发明的识别标记进行操控，因为只有同时并以定义的方式和方法操控两个电子密钥才能伪造身份。

[0022] 如果将第二电子密钥和第一电子密钥关联，则形成一种特别有利的改进，因为这会在两个电子密钥间产生一个唯一的不可动摇的联系，鉴于对人的识别认证的可靠性，这是一个特别的优势。其次由此也可以使可能的操控企图明显变难。可以如此构造关联，使得形成不可逆的密钥产品(Schlüsselprodukt)，从两个密钥关联的结果不能得到子密钥的结论。

[0023] 与人物相关的标记与第一电子密钥的关联可以个通过单向操作建立，其中从关联的结果出发，不可能再反向得出原始的输出产品。在单向关联中尤其只存储关联的结果。在人物识别和认证中，由认证处通过相应的检验算法例如重新建立或产生关联并和已存在的关联进行比较。因此可以对唯一的一致性进行检验，不必对特殊的及与安全相关的主要标记自身进行检验。

[0024] 一种特别有利的改进，其中通过法律权威的电子密钥形成第一和 / 获第二个电子密密钥。法律权威例如是律师或公证人，无论如何是一个人，他的法律身份的势力可以产生关于认证识别标记具有法律效力的陈述。例如一个人将对法律权威出示识别标记，法律权威在对这个人认证后，通过存放专有的电子密钥，确认识别标记可分派给唯一的人。重要的是通过由法律专家唯一的确认，可以确定明确地且可实行地将识别标记分配给一个人并且这一明确的分配可以在之后的人物的识别和认证的过程中是可查询的。由此可实现第三人通过对识别标记的检验来对出示这样识别标记的人进行明确且可靠的识别和认证，尤其是实现了一个具有法律效力的识别和认证。

[0025] 法律权威可是通过每一个、可以符合关于人物身份的在很大程度上被认可的、尤其是具有法律效率的声明的机构产生。例如也可以通过国家和 / 或国际鉴权或认证机构实行。

[0026] 鉴于识别标记的安全性存在特别有利的改进，其中将与人物相关的标记的数码图片存储在存储装置中。潜在入侵者可以例如操控识别标记的承载层，使得使用或设置仿造的与人物相关的标记。如果除了在承载层的与人物相关的标记之外在认证机构的存储装置中存储数码图片，则在之后的访问中总可使用参考图片用于人物认证，当下设置在承载层上的标记可以同参考图片进行比较并由此马上识别出操纵控企图。这一构造尤其具有的优势在于实现所谓的离线认证人物，因为待检验或待比较的参考标记在识别标记上已存在并且因此不需要与中央认证或授权机构进行通信连接。

[0027] 通过相应的认证机构的访问保护例如还可以附加地确保，对参考标记的访问可以只限于读取，尤其是对于写访问通过使用技术的标记和认证机构的安全装置来阻止。在一种改进中可以这样构造认证机构，使得对存储的标记进行写访问将引起对存放的信息、关联的销毁并且可能的话也引起对识别标记的销毁。

[0028] 如果第一电子密密钥编码地存储在数码图片中，则可以得到一个特别有利的改进。例如通过隐写方法进行这种编码，其优势在于第一电子密钥存储在数码图片中，使得在视觉观察所存储的图片时不呈现编码的密钥。另外的优势在于数码图片不被操控，因为每次操控企图自动地使第一电子密钥和与人物相关的标记的关联无效。这一构造的特别的优势在于，这种编码方法大多是不可逆的，即出于操控目的解除编码、改变与人物相关的标记、然后重新进行编码或关联都是不可能的。

[0029] 根据一个改进，将在数据处理装置的存储装置中存储电子记录。为了存储的电子记录的安全性可以将数据处理装置例如安置在安全区域内，只有经选择的人能对其访问。在数据处理装置中在可能的情况下现在也可以存储更多电子记录。例如这样的电子记录可以管理多个人。

[0030] 一种有益的改进，其中数据处理装置具有通信接口，通信接口被构造用于使得远距离数据点能够访问电子记录。例如数据处理装置可以通过服务器构成，服务器存储许多

不同的电子记录作为识别标记并且可以访问全球通信网络。这样许多识别和认证机构可以访问识别标记并进行人物的识别和认证。

[0031] 鉴于应用的简易化和考虑到计算的繁琐，根据本发明的识别标记优选应可携带，存在一种有益的改进，其中将电子记录存储在移动的数据存储器中。如上述的移动的数据存储器多数属于日常使用的装置因而会总携带。

[0032] 本发明的任务也是通过下列识别和认证人物的方法来完成的，该方法具有下述方法步骤。

[0033] 通过在存储装置或电子记录中存放于人物相关的标记，可完成识别标记，它可以由使用者携带或在任意时间可被访问，并且任何时间可以识别人物。

[0034] 为确保人物的身份要通过法律权威证明其合法性。例如可以由此进行，即出示给法律权威证明其身份的有效的法律文件。

[0035] 通过在信息标记的存储装置或电子记录中存储法律权威的第一密钥，以及之后将第一密钥和与人物相关的标记关联，将在物理的识别标记和作为这一标记的载体或占有者的人之间产生有效的联系。

[0036] 人物可以随后通过出示识别标记有效地证实身份。在对第三人展示识别标记是，可以因此假定，尤其具有法律效力的假定，这个人是唯一符合由法律专家指定的特定识别标记的那个人。

[0037] 根据识别标记的第一种构造，出示识别标记意味着承载层将对检验人和 / 或检验机构出示。根据作为电子记录的第二种构造，可以对检验人或检验机构展示记录的存储位置，据此可以通过信息通道访问识别标记。

[0038] 为提高安全性或为提供多级的识别方法存在一个有利的构造，其中存储授权和认证机构的第二电子密钥。这一构造显著提高了人物识别认证的安全性，因为被出示识别标记的第三人通过在发布或设置的鉴权或认证机构检验密钥可以检验出示身份标记的人是否和申请第二电子密钥的人相符。因为这样机构大都具有国家的、优选甚至是国际承认的声誉，通过由法律权威存储的第一电子密钥第一次并通过认证或授权机构的第二电子密钥第二次来确定人物的身分或真实性，这样做鉴于可靠的人物识别和根据本发明的方法大部分的可接受性具有特别有利之处。

[0039] 这一构造实现了不同的安全级别。例如对简单的、安全技术非关键的应用而言，借助于第二电子密钥的检验就够用了。如果要求更高的安全性，则可以再检验第一密钥。

[0040] 为了明显提高根据本发明的方法的安全性，鉴于可靠的人物识别和认证以及尽可能快速地执行方法，存在一个有利的构造，其中在外部存储单元中存储与人物相关的数据的参考记录。这个外置的存储单元例如可以通过中央的数据处理装置形成，该数据处理装置与设备连接，以便可以读取与人物相关的标记或电子密钥及来自识别标记的加密产品。例如参考记录具有识别标记的与人物相关的标记的图像，由此可以在人物认证时随时被访问那些在合法化中通过法律权威和与人物相关的标记关联的原始标记记录。潜在的入侵者可以例如操控识别标记，不能访问存储的参考记录，以致于操控企图在接下来的人物识别中将被马上识别。因此为了识别人物可用一个不能或极难被操控的参考记录，由此对于第三人而言人物识别的安全和可靠性大幅提高。

[0041] 同样鉴于提高根据本发明方法的可靠性和可接受性，存在一个有利的改进，其中

在识别标记－尤其是在存储装置－中存储与人物相关的数据的参考记录。如果采集装置将“离线”运转，也就是说没有直接的通向中心管理装置的通道时，这一构造尤其具有优势

[0042] 在改进中，当然可以对参考记录加密或相应地编码存储－例如通过单向加密，这样给潜在入侵者造成进一步的安全阻碍。

[0043] 根据一个改进，为了识别认证人物将存储的与人物相关的标记和所采集的标记相比较。通过这一构造可以有利的方式确保，根据本发明的识别标记提供充分的标记安全性，以便使得可以根据所采集的标记和将其与所存储的标记比较从而可靠地识别和认证人物。这一比较可以由检验者或自动检验设备来执行，尤其地，如果携带识别标记或出示参考的人对第三方的出示识别标记并希望自身识别和认证，则执行检验。采集装置于是可以采集与人物相关的标记，将该标记传输到数据处理装置或监控人员，其将当前采集的数据和存储的参考数据进行比较。如果一致进而确定，当前的检验对象的实体和通过法律权威为其确定或分配识别标记的人相符。

[0044] 通过一个改进特别提高身份标记的安全性，其中与人物相关的标记在采集后马上和第一电子密钥关联。这样可以明确确保，在采集、存储和关联之间与人物有关的标记不被操控。

[0045] 在采集与人物相关的标记用于存储并和第一电子密钥关联的另一个特别的安全性的提高在于，与人物相关的标记实时地在法律权威前或通过法律权威采集，这样采集的与人物相关标记的真实性被确认。因为与人物相关的标记是识别标记的主要标记，这一构造特别地提高了安全性，因为所采集的标记是在监督下被采集的并且不存在被操制的可能性并且与密钥关联。

附图说明

[0046] 为更好地理解本发明，将结合下列附图对其详细解释。

[0047] 在非常简化的示意图中，

[0048] 图 1 示出了根据本发明的识别标记的构造；

[0049] 图 2 示出了用于形成用于明确地识别和认证人物的身份标记的方法步骤；

[0050] 图 3 示出了在检验人物身份的情况下用于门禁的装置；

[0051] 图 4 示出了用于认证身份标记的装置。

具体实施方式

[0052] 首先应当明确，在不同描述的实施方式中相同的部分使用相同的附图标记或相同的配件名称，其中包含在整个描述中的公开按照意义可以被转移到具有相同的附图标记或相同的配件名称的相同的部分。在描述中所选的位置说明－例如上面、下面、侧面等等－也是关于直接描述以及显示的附图，并且在位置变化时按照意义转移到新的位置。此外，所示和所述的不同的实施例中的单个标记或标记组合也可表示独立的、创新的或根据发明的解决方案。

[0053] 在具体的描述中可以这样理解对数值范围的所有说明，即数值范围的任意的和全部的子范围都包含在内，例如可以这样理解说明 1 到 10，即包含全部的从下限 1 到上限 10 的子范围，即全部的子范围从 1 或大于 1 的下限开始直到 10 或小于 10 的上限为止，例如 1

到 1.7，或 3.2 到 8.1 或 5.5 到 10。

[0054] 图示 1 示出根据本发明的识别标记 1 的构造，其包括承载层 2、与人物相关的标记 3- 尤其是人物的图片、以及具有存储装置 5 的验证装置 4，在存储装置中存储第一电子密钥 6。这个识别标记 1 具有附加的带有通信接口 8 的通信装置 7。在识别装置 1 处还可以安置和 / 或集成其他与个人有关的或机构的标记 9。

[0055] 识别标记 1，尤其是承载层 2 优选被构造为证明文件，以便使识别标记的携带者可以进入一般不能进入的区域或访问一般不能访问的信息。因为根据本发明的识别标记可能必须持续携带，所以承载层优选被构造为信用卡的形式，这样就不会由于人自身的运动而限制识别标记的自由移动或从结构上危害识别标记。尤其地，信用卡形的构造有下列好处，即识别标记也可以放入携带的证件袋或钱包内。智能卡的构造还有其他特别的优点，即这种卡推广尤其广泛且应用成本低廉，尤其地，还具有组件和模块，其对于执行根据本发明的识别标记和认证方法具有重要的意义并且因此不必由用于身份或认证检验的采集装置提供。

[0056] 在熟知的识别标记中大都存在这样的问题，与人物相关的标记 3、9- 尤其是识别标记对应的人物的图片 - 可能出于滥用目的被篡改并且识别标记因此可能被用于伪装虚假身份。尤其地，在高流通的人群区域可能在由检测者进行视觉检测与人物相关的标记时产生错误，由此可能发生对可能敏感的区域的入侵。这时，根据本发明的识别标记的特别的优势在于，电子密钥 6 同与人物相关的标记 3 以及在可能的情况下和另一个标记 9 关联，与人物相关的标记 3 优选由人物的图片形成，其优势是可以附加地将人物标记代表的人和存储的人物的图片 3 进行视觉地比较。电子密钥 6 同与人物相关的标记 3 的关联例如这样形成，即生成与人物相关的标记 3 的电子表示，并且例如和电子密钥 6 加密存储到存储装置 5 中。然而优选的构造是这样的，其中人物的图片 3 的数码表示被存储在存储装置 5 中并且借助于隐写的方法将数码图片和第一电子密钥 6 关连，由此第一电子密钥隐藏在数码图片中。也可以例如从数码图片中算出校验和，该校验和与第一电子密钥加密并随后被隐藏在数码图片中。以上均为将电子密钥和与人物相关的标记关联的示例性的构造。业内人士熟知与此相关的其他可能，以便关联电子密钥和优选以可以电子处理的形式存在的与人物相关的标记，使得明显地增加操控企图的难度。尤其地，根据本发明将电子密钥 6 同与人物相关的标记 3 关接具有的特别优势在于，当对与人物相关的标记 3 有操控企图时，与第一电子密钥 6 的关联将无效并因此明确地识别操控企图。

[0057] 为了识别标记 1 和采集装置进行数据技术的通信，识别标记具有带有通信接口 8 的通信装置 7。根据作为信用卡类的智能卡的优选构造 - 例如根据标准 ISO/IEC 7810，将通信接口 8 安置在承载层 (2) 上以及承载层本身的构造都是确定的。通信接口 8 除了有接触式的构造外还可以被无线地构造并因此可以在不必须在采集设备中安置识别标记的情况下执行认证。例如标准 ISO/IEC14443 确定非接触式的可读智能卡的构造。

[0058] 验证装置 4 可以被构造用于，通过采集设备的通信装置 7 提供在与人物相关的标记 3 和第一电子密钥 6 之间的关联的典型特征。也可以是验证装置比较当下采集的与人物相关的标记和存储的与人物相关的标记并将相符的结果传给采集装置。在这个构造中，以有益的方式关联或第一密钥的特征不会从识别标记向外传播。

[0059] 鉴于所存储的电子密钥或在可能的情况下所存储的与人物相关的标记的人物的

图片的安全性，根据一个改进，验证装置 4 具有数据处理装置或加密模块 10。验证装置 4 可以被构造用于，保护所存储的标记或电子密钥，使得入侵者自己在访问所存储的标记或密钥时不能通过访问得到任何利益。这可以例如同过单向加密实现，单向加密由密码模块执行并且其中从安全的结果不能反向得到原始标记。但是验证装置也可以承担复杂的任务，比如可能要求确定特定于人物的标记的多级标记检验，如果验证装置包括数据处理装置是有利的，因为这样的装置大都可以执行复杂的处理步骤。

[0060] 作为进一步的安全特征可以在验证装置 4 的存储装置 5 内安置第二电子密钥 11。第一和 / 或第二电子密钥的本质在于，它由认证点或安全认证中心发布或提供，其中鉴于生成的电子密钥的可靠性这些验证装置符合国际高标准。尤其地，这类装置满足对于创建和管理用户数据以产生电子密钥的要求。

[0061] 图 2 所示为构造根据本发明的识别标记 1 的方法的原理图，该识别标记使得可以明确识别和认证人物。在第一步骤 12 中将未个人化的识别标记 13 利用与人物相关的标记 3、9 个人化，这就是将标记 3、9 安置在或存储在识别标记 13 上。在第二步骤 14 中使用者 15 将个人化的识别标记 16 连同合法有效文件 17 一起用于确定授权实体 18 的人物 15 的身份。授权实体 18 优选由法律权威形成，例如律师或公证人。通过带来的文件 17 来检验人物 15 的身份然后将特有的第一电子密钥 6 存储在个人化的识别标记 16 中 - 尤其在存储装置中，这样就合法化了。根据本发明的方法地最主要的步骤在于，认证权威 18 将在识别标记 16 中存放的电子密钥 6 和与人物相关的标记 3、9 关联并因此形成不可撤销的连接 19。

[0062] 用于进行个人化 2 或授权识别标记 14 的方法步骤要求将识别标记放置在 - 未示出的 - 访问控制和控制设备中，其中这可以通过数据处理装置和通信地耦合的通信装置形成，该通信装置经由通信接口 8 与验证装置 4 产生数据技术的连接。根据本发明的方法的主要的技术效果是提供识别标记 1，其将与人物相关的标记 3 和第一电子密钥 6 关联 19，使得通过该关联最大程度地阻止对识别标记的操控并因此可以明确而有效地确定人物的身份和可信度。

[0063] 在可能的情况下识别标记 13 的个人化 12 还可以包括一个步骤，其中在验证装置 4 的存储装置 5 中存储第二电子密钥 11。第一电子密钥 6 以及在可能的情况下第二电子密钥 11 优选由外部的认证或授权装置 20、21 提供或管理。如前面已经描述的，在生成或管理电子密钥方面该装置对于安全性接纳显示出很高的程度。这类装置的例子如 RSA 或 VeriSign。这些装置管理唯一地对应于注册用户的电子密钥组。此外根据所谓的公共密钥系统使用密钥组，它是由私钥和公钥组成的。这里省去细节描述，因为业内人士对于公共密钥系统是熟知的。这种密钥系统的优势尤其在于，第三人可以由独立的认证和授权装置随时确定电子密钥的可靠性。

[0064] 图 3 示出了根据本发明的方法的应用，该方法用于借助于根据本发明的识别标记 1 来识别和认证人物 15。例如借助于进入控制装置 22 保卫进入非普通可进入的装置。要激活进入控制装置 22 需要明确的人物 15 的识别和确认。为此人物 15 对采集装置 23 出示识别标记 1，采集装置对识别标记进行分析。例如识别标记 1 被放置在读出装置 24 中，其中通过通信接口 8 与验证装置建立通信连接。采集装置 23 可以例如被构造用于自动识别和认证人物，例如通过采集装置 25- 优选是视觉的图象捕获设备 - 来采集人物的图片并由分析和比较模块 26 将其和在识别标记 1 处存储的与人物相关的标记进行比较。因为与人物

相关的标记 3 优选被构造为根据国际承认的标准 - 尤其是根据 ICAO- 的图片，分析和比较模块 26 大都可以进行全自动的比较当前采集的图片和所存储的与人物相关的标记。为了确保识别标记 1 不被操控，采集装置 23 在外部的认证或授权装置 21 中检验第一电子密钥 6 的有效性和可靠性。同样也可以通过其他的认证或授权装置 20 检验第二电子密钥 11.

[0065] 然而，在一个改进中也可以这样，即在识别标记 1 处存储的与人物相关的标记不由采集装置 23 读出，而是对当前采集的人物的图片 - 例如由采集装置 23 的加密模块 27- 进行准备和处理，然后传给识别标记 1。识别标记 1 的验证装置然后检查所采集的并相应处理过的人物的图象与所存储的与人物相关的标记 3 比较是否一致并在此基础上产生相应的激活信号，激活信号被传回采集装置 23，然后进入控制系统 22 被打开 .

[0066] 图 4 示出了用于构造根据本发明的识别标记 1 的装置，尤其是为了将与人物相关的标记和第一电子密钥关联并存储在识别标记中。此外，用于识别标记的个人化和认证的方法步骤优选通过数据装置 28 被执行，因为这种装置被广泛推广并且尤其是通常构造的用于处理电子或数码信息单元的属性被构造。尤其地，这种装置包含图像处理模块 29，该图像处理模块设备 29 将由图像采集装置 30 采集的人物 15 的图片转换为可以进一步处理的表现形式 31。此外，图像采集装置 30- 例如照相机，通过通信接口和数据处理装置 28 相连。因为图片用于自动图像采集必须优选符合承认的标准 - 尤其符合 ICAO，所以图像处理模块 29 可以这样控制图像采集装置 30，使得实现根据标准要求的图片。图像处理模块优选将采集的图片信息转换为标准化的图片数据形式，该图片数据形式可以由多数数据处理系统处理。

[0067] 根据本发明的识别标记或方法的主要的特征在于满足防伪高要求的电子密钥和与人物相关的标记 - 尤其是图片 - 关联。下面实施更多可能关联的例子，但是要在内行技术人员的专业知识指明哪些方法用于关联电子密钥和以可以数据技术处理的形式存在的与人物相关的标记。例如用隐写 (steganografisch) 方法可以将第一电子密钥 6 放置在数码图片数据中。这样的优势在于与人物相关的标记在被人查看时不会受到消极的影响，将第一电子密钥通过整个的图像数据一体化地拿来。也有可能从处理的图片中确定典型参考值比如散列 (Hash) 值。参考值例如同第一电子密钥一起通过加密模块 32 并由此得出加密结果。这个加密结果可以这样形成，即由此不可以再反向得到原始图像数据或电子密钥。这一构造的优势在于，在权威对于识别标记的认证后，不必再次查询与人物相关的标记，而是在接下来对人物识别和认证时通过第三人采集人物的图片并通过同样的密码的加密方法进行处理，其中此次产生密码结果。这一结果可以和在识别标记内存储的加密结果进行比较，从而对人物的身份进行认证。识别标记 1 的验证装置 4 或验证装置的存储装置可以这样构成，使得只有是作为第一电子密钥占有者的权威，才可以为修改或处理对存储的与人物有关的标记进行访问。根据有益的改进，第一电子密钥 6 可以是密钥系统的一部分，该密钥系统由认证或授权装置来提供和 / 或管理。认证或授权装置可以是数据处理装置 28 的一部分或与可以与其本地连接 33。然而也可以实现远程认证或授装置，其和数据处理装置 28 通过公共的通信介质 - 例如互联网 - 通信地连接。例如这里可使用所谓的公钥系统，其中权威在认证识别标记时将图片同其个人的电子密钥关联，并存储在识别标记出。因为潜在入侵者从不能识别权威的私钥，所以也不可能操控与人物相关的标记，因为由此连与第一电子密钥的关联也会无效。这样第三人可以由此确定对出示识别标记的人物的识别和认

证，即例如将加密的人物图片展示给认证和授权设备，认证和授权设备可以完全自动地证明在识别标记出存储的与人物相关的标记。通过对实际在场的人的典型的标记与在识别标记出存储的参考标记进行比较，可以明确地认证实际在场的人的身份。

[0068] 为访问所存储的参考标记或存储参考标记并进行同第一电子密钥的关联，将识别标记 1 安置在访问设备 34 中，其中该访问设备通过通信装置并且尤其是通过通信接口 8 在数据处理装置 26 和识别标记 1 的验证装置 4 之间建立数据技术的连接。

[0069] 根据本发明的识别标记的另一构造在于，相应的人物自己对其他的标记进行认证。为此人物可以例如借助于数据处理装置的图像捕获装置采集图片，并通过和存储的标记比较来认证自己的身份。此外，不管是对于具有承载层、还是对于具有电子数据组的根据本构造的识别标记是同样有效的。在成功的认证后人物可以建立例如其他的识别标记。被广泛推广的数据处理装置具有大部分的必要的元件，以便可以执行根据本改进的方法步骤。

[0070] 这些实施例展示了识别标记或认证地识别人物的方法的可能的实施变体，其中在这里要指出的是，本发明不局限于特别的描述的实施变体，相反各个实施变体之间的结合也是可能的，并且这种变体的可能性基于关于技术处理的教导结合本发明处于从事这一技术领域的专业人员的能力范围内。因此，通过组合所示或所述的实施变体的各个细节可能得到的全部可设想的实施变体都包含在保护范围之内。

[0071] 最后，由于整齐的原因指出，为了更好地理解识别标记的结构或方法，识别标记或其组成部分有时并没有按照原有尺寸和 / 或放大和 / 或缩小地被显示。

[0072] 作为独立的有创造性的解决方案的基础的任务可以从描述中得出。

[0073] 尤其是在图 1 到 4 中展示的各个实施方式可构成独立的根据本发明的解决方案的对象。根据本发明的相关的任务和解决方案可从图示的细节描述中提取。

[0074] 附图标记列表

[0075] 1. 识别标记

[0076] 2. 承载层

[0077] 3. 与人物相关的标记

[0078] 4. 验证装置

[0079] 5. 存储装置

[0080] 6. 第一电子密钥

[0081] 7. 通信装置

[0082] 8. 通信接口

[0083] 9. 与个人相关的或机构的标记

[0084] 10. 数据处理装置、加密模块

[0085] 11. 第二电子密钥

[0086] 12. 个人化识别模块

[0087] 13. 未个人化的识别模块

[0088] 14. 识别模块认证

[0089] 15. 人物

[0090] 16. 个人化的识别标记

[0091] 17. 文件

[0092] 18. 授权实体

[0093] 19. 关联

[0094] 20. 验证装置、授权装置

[0095] 21. 认证授权机构

[0096] 22. 进入控制设备

[0097] 23. 采集装置

[0098] 24. 读初装置

[0099] 25. 采集装置

[0100] 26. 分析和比较模块

[0101] 27. 加密模块

[0102] 28. 数据处理装置

[0103] 29. 图像处理模块

[0104] 30. 图像采集装置

[0105] 31. 已处理的图片数据、数码图像

[0106] 32. 加密模块

[0107] 33. 本地的验证装置、授权装置

[0108] 34. 访问装置

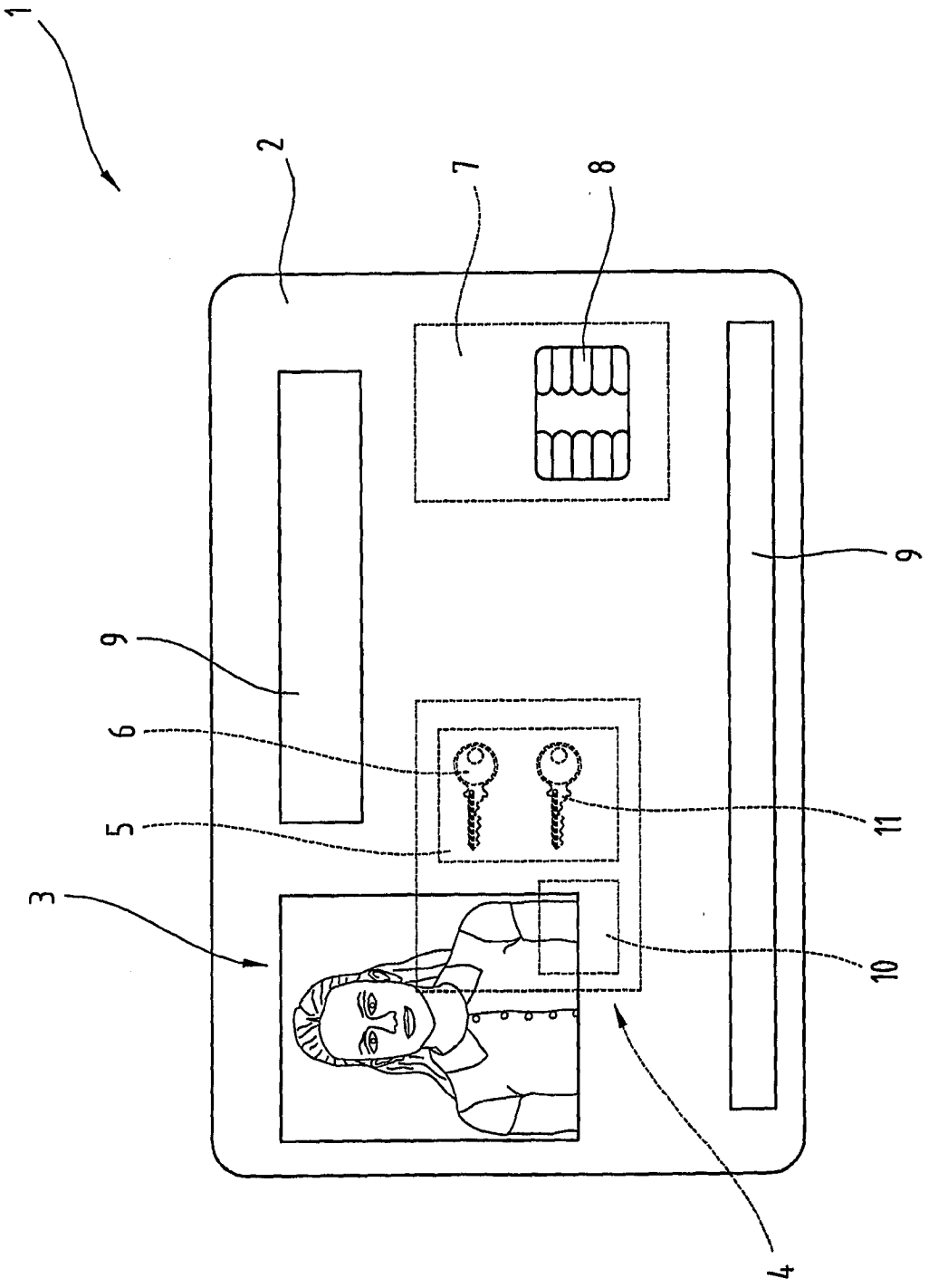


图 1

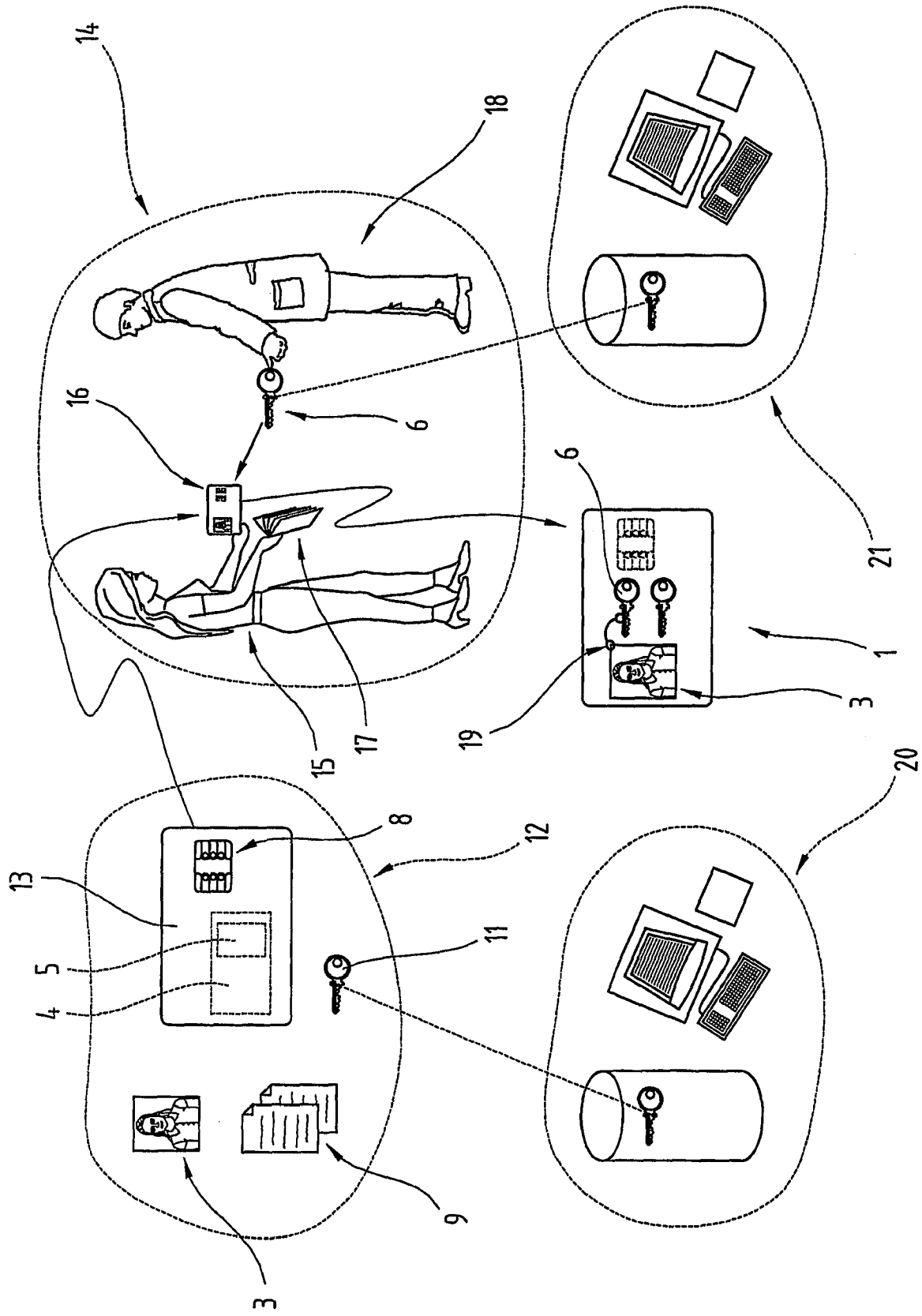


图 2

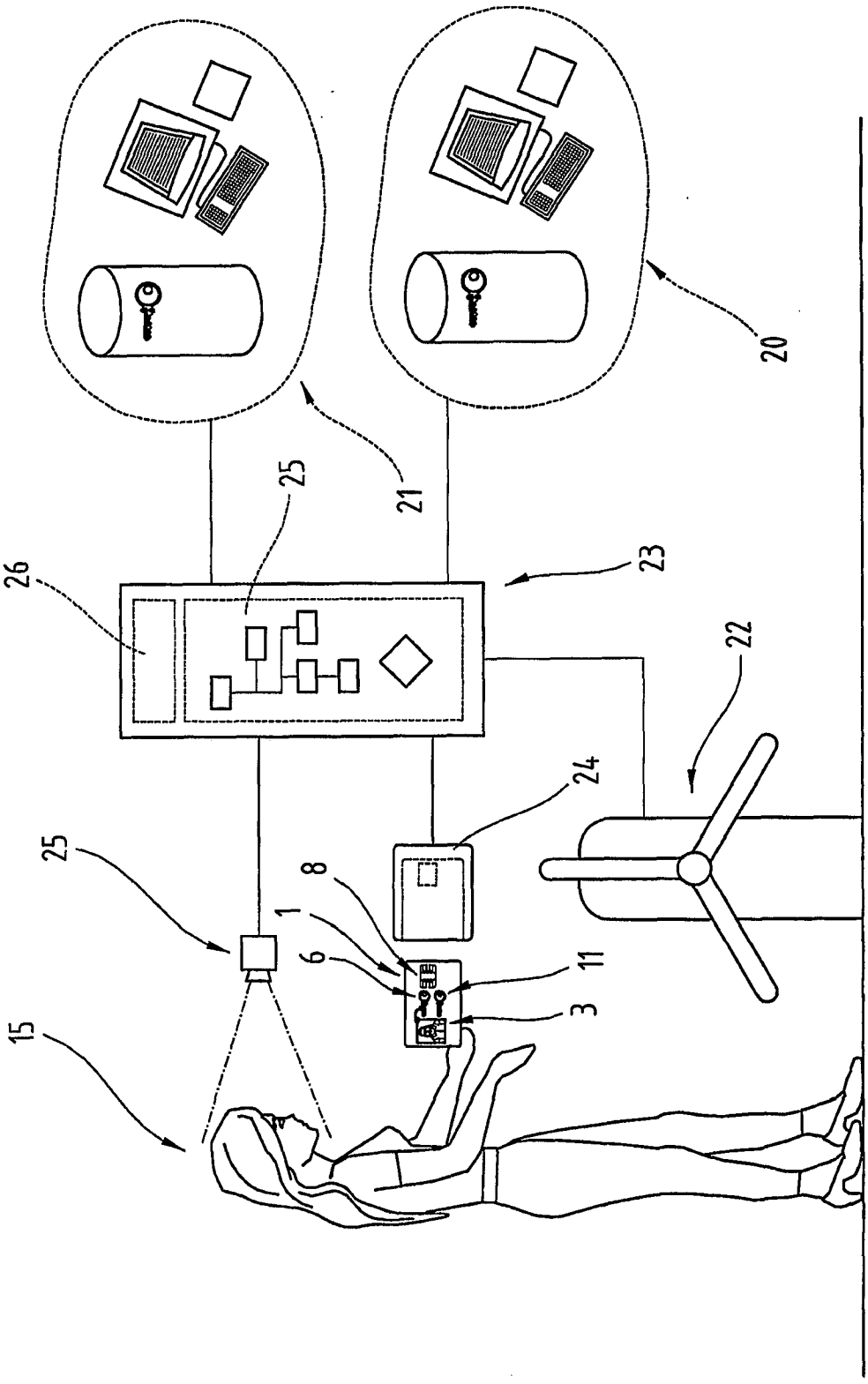


图 3

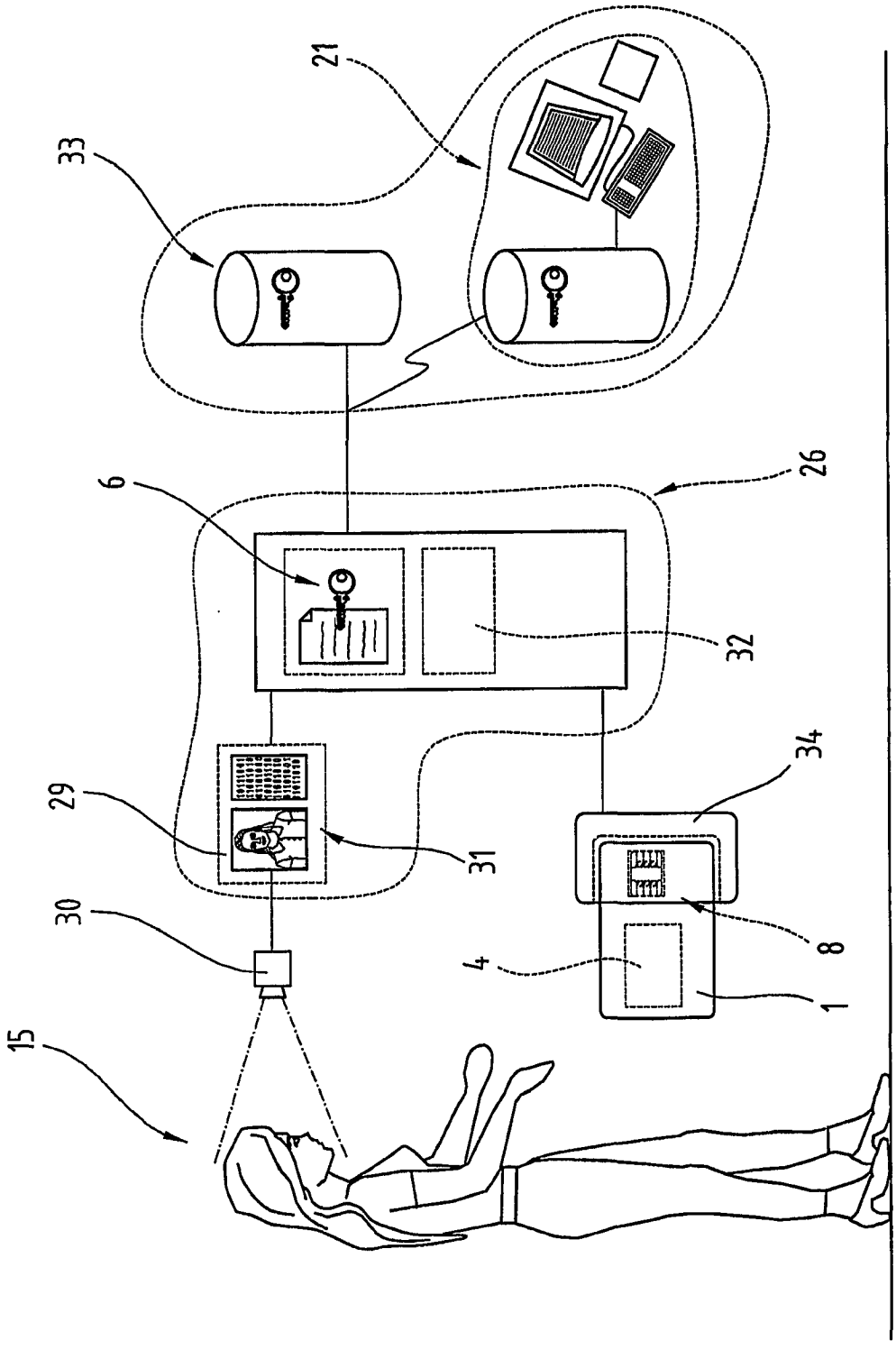


图 4