(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102713927 A
(43)申请公布日 2012.10.03

(21)申请号 201080046324.9
(22)申请日 2010.08.13
(30)优先权数据
61/274,139 2009.08.13 US
(85)PCT申请进入国家阶段日
2012.04.13
(86)PCT申请的申请数据
PCT/US2010/045443 2010.08.13
(87)PCT申请的公布数据
WO2011/019996 EN 2011.02.17
(71)申请人 托马斯·索克
地址 美国佛罗里达州
申请人 丹尼尔·福扎提
安德拉什·瓦戈
(72)发明人 托马斯·索克 丹尼尔·福扎提
安德拉什·瓦戈
(74)专利代理机构 北京信慧永光知识产权代理有限责任公司 11290
代理人 武玉琴 陈桂香
(51)Int.Cl.
G06K 5/00(2006.01)

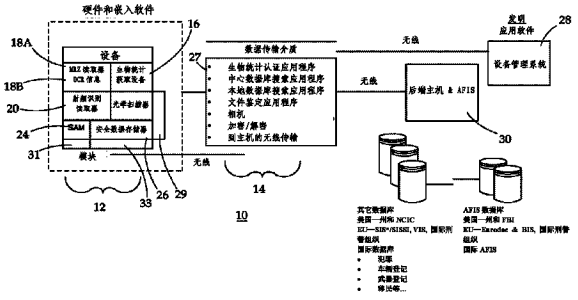
权利要求书 5 页 说明书 18 页 附图 22 页

(54)发明名称

通过具有数据存储功能的安全多功能鉴定服务对个人和/或文件进行鉴定和验证的智能外围设备和系统

(57)摘要

本发明涉及智能外围设备，该智能外围设备具有包括数据存储功能的安全多功能鉴定服务，其中，该设备包含多功能的智能外围设备或者辅助设备，当实施到系统中时，所述多功能的智能外围设备或者辅助设备用于与受到所述设备控制的数据传输介质协同地对该设备指示系统执行的一组处理进行控制。



CN 102713927 A

1. 一种智能外围设备，其包括：

生物统计鉴定模块；

光学字符识别读取器；

射频识别读取器，所述射频识别读取器还包括天线；

光学文件扫描器；

安全访问模块；

机器可读区域读取器；

无线通信模块；和

多个数据存储模块，其中所述生物统计鉴定模块；

光学字符识别读取器；

射频识别读取器，其中，所述射频识别读取器、所述生物统计鉴定模块、所述光学字符识别读取器、所述光学文件扫描器、所述安全访问模块、所述机器可读区域读取器、所述无线通信模块和所述多个数据存储模块进行电子通信；并且

所述设备在实施到系统中时用于与受到所述设备控制的数据传输介质协同地对所述设备指示所述系统执行的一组事务进行控制。

2. 如权利要求 1 所述的设备，其中，所述生物统计鉴定模块用于获取个人的多个指纹。

3. 如权利要求 1 所述的设备，其中，所述光学字符识别读取器用于将多个扫描图像转译成多个机器编码文本。

4. 如权利要求 1 所述的设备，其中，所述射频识别读取器用于读取位于电子护照内的多个非接触式芯片。

5. 如权利要求 1 所述的设备，其中，所述光学文件扫描器用于获取个人持有的多个文件内所包含的多个数据。

6. 如权利要求 1 所述的设备，其中，所述安全访问模块与数据传输介质连接，以向多个远程数据库安全地传输信息。

7. 如权利要求 1 所述的设备，其中，所述无线通信模块通过数据传输介质与多个远程数据库进行数据通信。

8. 如权利要求 6 的所述设备，其中，所述设备与多个数据库进行数据通信。

9. 如权利要求 1 所述的设备，其中，所述设备具有多个生物统计搜索功能、非生物统计搜索功能和匹配功能，以用于识别和验证多个个人。

10. 如权利要求 6 所述的设备，其中，所述设备用于远程识别和验证多个个人。

11. 如权利要求 1 所述的设备，其中，所述设备通过保存在所述设备上的所述多个数据存储模块对多个个人和文件进行识别和验证。

12. 如权利要求 9 所述的设备，其中，用于识别和验证的所述非生物统计功能是从由下列项组成的群组中选出的：姓名、车辆登记、武器登记、驾驶执照、车辆 VIN 和签证。

13. 如权利要求 12 所述的设备，其中，所述设备用于对位于文件内安全证书进行鉴定。

14. 如权利要求 13 所述的设备，其中，所述安全证书所位于的所述文件是从由下列项组成的群组中选出的：电子护照、标准护照、国民身份证明、驾驶执照和政府颁发的任何其它证件。

15. 如权利要求 1 所述的设备，其中，所述多个数据存储模块用于保存从由下列项组成

的群组中选出的数据库信息：被拒绝人员名单、观察名单和指纹名单。

16. 如权利要求 1 所述的设备，其中，所述多个数据存储模块与多个远程数据库进行数据通信，以用于更新所述设备上保存的数据库。

17. 如权利要求 1 所述的设备，其中，所述设备是唯一识别的，以确认哪个设备获得哪些数据库信息。

18. 如权利要求 1 所述的设备，其中，所述数据存储模块被加密，并且在被不具有正确授权的个人篡改时被删除。

19. 如权利要求 7 所述的设备，其中，所述计算设备还包括边界控制移动应用程序，所述边界控制移动应用程序用于控制对多个个人和文件的识别和验证。

20. 如权利要求 19 所述的设备，其中，所述边界控制移动应用程序与所述设备进行数据通信。

21. 如权利要求 19 所述的设备，其中，所述边界控制移动应用程序与多个国家主机进行数据通信。

22. 如权利要求 1 所述的设备，其中，所述设备上保存有多个本地数据库。

23. 如权利要求 22 所述的设备，其中，所述多个本地数据库还包括多个数据库子集和多个日志数据。

24. 如权利要求 1 所述的设备，其中，所述设备与数据传输介质配对，以在所述设备和多个远程数据库之间安全传输多个信息。

25. 如权利要求 24 所述的设备，其中，所述设备包括安全信息交互设备，所述安全信息交互设备用于在所述设备和数据传输介质之间创建安全信任环境。

26. 如权利要求 25 所述的设备，其中，所述安全信息交互设备用于为所述设备和多个远程数据库之间的信息交互创建安全加密环境。

27. 一种用于通过安全多功能鉴定服务对多个个人和文件进行鉴定和验证的系统，其包括：

智能外围设备，所述设备在实施到所述系统中时用于与数据传输介质协同地对所述设备指示所述系统执行的一组事务进行控制；

数据传输介质，所述数据传输介质与所述设备进行数据通信，并且受到所述设备的控制；并且

安全信息交互设备，所述安全信息交互设备位于所述设备上，并且用于在所述设备和数据传输介质之间创建安全环境。

28. 如权利要求 27 所述的系统，其中，所述设备还包括一系列相互通信的组件，所述组件包括：

生物统计鉴定模块；

光学字符识别读取器；

射频识别读取器，所述射频识别读取器还包括天线；

光学文件扫描器；

安全访问模块；

机器可读区域读取器；

无线通信模块；和

多个数据存储模块，

其中，所述数据存储模块、所述生物统计鉴定模块、所述光学字符识别读取器、所述射频识别读取器、所述光学文件扫描器、所述安全访问模块、所述机器可读区域读取器、所述无线通信模块和所述多个数据存储模块进行电子通信。

29. 如权利要求 27 所述的系统，其中，所述设备与多个远程数据库通过所述数据传输介质进行数据通信。

30. 如权利要求 27 所述的系统，其中，所述安全信息交互设备用于鉴定所述设备和所述数据传输介质。

31. 一种利用如权利要求 27 所述的系统在设备和数据传输介质之间进行安全配对的方法，所述方法包括如下步骤：

向所述设备发送配对请求；

向所述数据传输介质发送配对请求；

获取所述系统的操作员的指纹，以用于鉴定查询；

向所述设备发送来自所述安全信息交互设备的数字证书；

向所述数据传输介质发送来自所述安全信息交互设备的数字证书；

通过所述设备鉴定所述安全信息交互设备的所述数字证书；

通过所述数据传输介质鉴定所述安全信息交互设备的所述数字证书；

所述设备产生包括公共密钥和私有密钥的密钥对；

所述数据传输介质产生包括公共密钥和私有密钥的密钥对；

向所述安全信息交互设备发送所述设备的所述公共密钥和所述数据传输介质的所述公共密钥；

向所述安全信息交互设备发送来自所述设备的数据通信地址和来自所述数据传输介质的数据通信地址；

通过所述安全信息交互设备向外部证书颁发机构设备发送所述设备的公共密钥和所述数据传输介质的公共密钥；

通过所述安全信息交互设备从所述外部证书颁发机构接收签名证书；

所述安全信息交互设备通过所述设备的私有密钥和所述数据传输介质的私有密钥对各个证书进行签名；

通过所述安全信息交互设备产生随机字符串；并且

上传所述设备与所述数据传输介质的配对信息。

32. 如权利要求 31 所述的方法，其中，所述配对信息是从由下列项组成的群组中选出的：数字证书、数据通信地址、密码和操作员的指纹。

33. 一种利用如权利要求 27 所述的系统进行个人识别的方法，所述方法包括如下步骤：

使用所述设备的所述机器可读区域读取器来扫描对象的多个证件；

通过所述设备对所述多个证件进行解码；

通过所述设备选择搜索查询；

通过所述设备发送搜索请求；以及

通过所述设备接收所述搜索请求的响应。

34. 如权利要求 33 所述的方法，其还包括如下步骤：

所述系统的操作员确定所述对象的所述证件上是否存在芯片；并且

当存在芯片时，通过所述设备上的所述射频识别读取器读取所述芯片。

35. 如权利要求 33 所述的方法，其还包括如下步骤：

使用所述生物统计鉴定模块获取对象的多个指纹。

36. 如权利要求 33 所述的方法，其还包括如下步骤：

将对象的信息打包成文件；并且

将所述文件发送到多个远程数据库。

37. 如权利要求 33 所述的方法，其中，所述搜索查询是从由下列项组成的群组中选出的：姓名、本地指纹数据库、远程指纹数据库和其它类似的人口统计资料。

38. 如权利要求 33 所述的方法，其中，所述搜索请求被发送到从由下列项组成的群组中选出的远程数据库：国家主机、中心数据库和自动指纹识别系统。

39. 如权利要求 33 所述的方法，其还包括如下步骤：

所述系统的操作员选择本地数据库搜索；

通过所述设备发送搜索请求；以及

向所述设备发送所述搜索请求的响应。

40. 如权利要求 33 所述的方法，其中，所述搜索查询是从由下列项组成的群组中选出的：人员、车辆、财产、船只和枪支。

41. 如权利要求 40 所述的方法，其中，人员的所述搜索查询包括多个搜索参数，所述多个搜索参数是从由下列项组成的群组中选出的：名字、姓氏、州、性别、种族、生日和城市。

42. 如权利要求 40 所述的方法，其中，用于车辆的所述搜索查询包括多个搜索参数，所述多个搜索参数是从由下列项组成的群组中选出的：汽车牌照、州、类型、年份、车辆识别号码和制造商。

43. 如权利要求 40 所述的方法，其中，用于财产的所述搜索查询包括多个搜索参数，所述多个搜索参数是从由下列项组成的群组中选出的：序列号和类型。

44. 如权利要求 40 所述的方法，其中，用于枪支的所述搜索查询包括多个搜索参数，所述多个搜索参数是从由下列项组成的群组中选出的：序列号、口径和制造商。

45. 如权利要求 40 所述的方法，其中，用于船只的所述搜索查询包括多个搜索参数，所述多个搜索参数是从由下列项组成的群组中选出的：船只号码、登记号码和州。

46. 如权利要求 33 所述的方法，其中，所述搜索查询通过证实多个文件来识别个人，所述方法还包括如下步骤：

选择所述设备上的文件选项；

通过所述设备扫描所述文件上的机器可读区域；

通过所述设备向所述多个远程数据库发送所述机器可读区域中包含的信息。

47. 如权利要求 46 所述的方法，其中，所述文件是从由下列项组成的群组中选出的：护照、电子护照、个人身份证明和驾驶执照。

48. 如权利要求 46 所述的方法，所述方法还包括如下步骤：

扫描所述文件内包含的非接触式芯片；以及

将所述非接触式芯片内的信息发送到所述设备。

49. 如权利要求 46 所述的方法，所述方法还包括如下步骤：

获取对象的多个指纹；

确定所述文件是否包括多个指纹数据；以及

用所述文件中包含的所述指纹数据来验证对象的所述指纹。

50. 如权利要求 1 所述的设备，其中，所述设备还包括：

相机；

键盘，所述键盘允许操作员输入多个信息；

磁条读取器；以及

接触式读卡器。

通过具有数据存储功能的安全多功能鉴定服务对个人和/或文件进行鉴定和验证的智能外围设备和系统

[0001] 相关申请的交叉参考

[0002] 本申请要求于2009年8月13日提交的美国临时申请第61/274,139的优先权，在此通过引用的方式将其全部内容合并入本文。

技术领域

[0003] 本发明一般涉及用于个人和/或文件的识别、验证和鉴定的设备和方法，更具体地，本发明涉及具有包括数据存储功能的安全多功能鉴定服务的设备，其中所述设备包括多功能的智能外围设备或者辅助设备，当实施到系统中时，所述多功能的智能外围设备或者辅助设备用于与受到所述设备控制的数据传输介质协同地对所述设备指示所述系统执行的一组事务进行控制。

背景技术

[0004] 在1987年，MITRE公司编制了国家犯罪情报中心(NCIC)2000的技术报告。该报告用作建立NCIC 2000程序的参照标准(framework)。报告的重点部分指出执法巡警需要具有发送和接收指纹和照片信息的能力。该报告建议，“美国联邦调查局负责获取、保存和发送通缉人员文件或者失踪人员文件中对象的两个拇指印的二进制或者灰度级的数字格式的指纹图像”。该报告还进一步建议，“美国联邦调查局开展研究以确定用于照片、指纹、文字和其它美国联邦调查局服务的最经济有效的传输系统，来满足用户对使用NCIC 2000系统进行快速反应的要求”。

[0005] 虽然目前已完成NCIC 2000项目，并且系统的升级也已完成，但指纹传输的领域和其它支助性建议尚未顺利实施。基于当时进行的调查，这些功能在实施中处于最高优先级。于1989年在三个地点进行了概念验证，但是不具备用于顺利启动该项目所需要的技术。

[0006] 对执法需求的增加使得更加迫切地要求警察无论身在何处都能够访问关键的识别信息，这些识别信息包括明确的指纹识别。随着无线基础设施的出现，不再需要依赖于陆基电话线进行可靠通信。无线系统使警察在任何地点都能够通过手持设备访问关键信息。警察能够通过利用了现代的查询软件的简化界面来访问和获取数据。这样，警察不仅能够即时访问最接近机构的数据库，而且还能够即时访问诸如NCIC-2000或者州机动车局等其它数据库。

[0007] 对于进行1:N搜索以确定嫌疑犯的身份并且将该身份与嫌疑犯的其它已确定的信息相关联的执法人员来说，移动/无线指纹功能主要的目的在于实时的明确识别。国际事件的变化使得更加需要验证个人的身份，并将这些个人与用于建立他们的身份的文件相关联。在这些情形下，需要进行1:1比较来验证所要求的身份。安全、防止诈骗以及边界控制对验证身份的要求会有所不同。能够应用移动/无线指纹的领域存在有诸如公共援助、海关、移民、护照和医疗ID验证等民事申请以及商业机构(银行和信用卡)。

[0008] 美国之外的其它政府正在开发新的电子边界控制方案，特别是，在欧盟（“EU”），从2012年开始使用EU电子护照，将能够采用无人关卡以供其公民进出申根区域(Schengen zone)。EU还允许使非EU国民使用电子签证、电子护照、电子身份证进出。这些场所是有人值守的；然而，这些人员将需要特殊设备来处理这些事务。在如机场等固定场所，需要带有生物统计和安全证件读取辅助设备的标准计算技术，然而，在陆地边界口岸和海港需要手持设备。因而，需要处理如下问题：边界哨兵需要检查火车、公交车或者船上的人员。

[0009] 当今，已使用移动无线技术实现了一些系统，然而除了洛杉矶警察局(LAPD)之外，其它所有警察局都使用专门的个人数字助理(PDA)设备。LAPD使用Cogent BlueCheck设备，该设备是智能手机或者PDA的辅助设备。该设备的功能限于获取指纹，而智能手机或者PDA仅把信息转发到中心的自动指纹识别系统(AFIS)。因此，随着对边界控制的关注和安全电子证件的使用的增加，要求这些移动手持设备不仅仅具有生物统计功能。

[0010] 此外，要求警方能够从安全证件获取同时以纸件和电子保存的信息，然后使用该信息来验证证件的真实性以查明持有者的真实身份，并最后确定被识别的持有者是否在本国国民数据库或者甚至国际数据库中。

发明内容

[0011] 如本文所述，本发明显然是无法预见和非显而易见的，并且不存在于任何现有设计中。

[0012] 本发明提供了一种智能外围设备，该智能外围设备具有包括数据存储功能的安全多功能鉴定服务，其中该设备包括多功能的智能外围设备或者辅助设备，当实施到系统中时，所述多功能的智能外围设备或者辅助设备与受到所述设备控制的数据传输介质协同地对所述设备指示系统执行的一组处理进行控制。

[0013] 本发明提供了一种设备，该设备通过具有数据存储功能的安全多功能鉴定服务对个人和/或文件进行鉴定和验证，其中所述设备通过数据传输介质与多个远程数据库进行数据通信。在一个实施例中，数据传输介质可被定义为用于从所述设备发送多条信息到远程数据库的介质。此外，所述设备包括安全信息交互设备，以实现该设备和数据传输介质之间的安全的配对和操作，其中安全信息交互设备(SIED)能够在所述设备和数据传输介质之间形成信任的和加密的环境，以更好地用于个人和/或文件的识别、验证和鉴定。

[0014] 本发明提供了1:N和1:1两种生物统计操作的要求，以及使用人口统计数据进行搜索，并且通过使用在新建立的扩展访问控制(EAC)协议的电子证件中保存的生物统计信息来核实人员的身份。

[0015] 本发明能够进行多个生物统计功能，这取决于具体情况和/或本发明的操作员的要求，其中，所述功能包括但不限于：

[0016] • 1:N本地识别

[0017] • 1:N远程识别

[0018] • 1:1本地验证

[0019] • 1:1远程验证

[0020] 此外，专门的证件鉴定功能使本发明的操作员能够获得存在问题的对象有关的安全证件的真实性的信息；这些证件包括但不限于：

[0021] • 电子护照

[0022] • 标准护照

[0023] • 国民身份证

[0024] • 驾驶执照

[0025] 本发明的操作员可选择这些功能的任意组合或者全部来满足他们的需要。在这种情况下，设备允许主功能及其子功能的任意组合。

[0026] 用有限设备的数据库进行识别

[0027] (1:N(少量)和本地搜索)

[0028] 本发明提供多个数据库的存储，所述数据库包括但不限于：观察名单、指纹和/或被拒绝人员名单(DPL)或者其它类型的子集数据库。本实施例允许本发明的操作员在通信受限制的情况下更好地识别对象，这些情况包括但不限于远程区域或者通信信号不可靠的建筑物。此外，本实施例能够用于搜索一组具体人员的情况，而非搜索单个人员。

[0029] 该方案提供了供操作员通过数据传输介质对设备中保存的多个数据库进行更新的方法。此外，每个设备是唯一识别的，从而能够分辨出访问数据库信息的设备的身份。而且，数据库在保存到设备上时被加密，如果该设备在没有正确授权的情况下被篡改和/或使用，该设备就删除所有的数据库信息。

[0030] 操作员能够使用该功能进行下列操作：

[0031] 1. 仅搜索指纹(FP)-在辅助设备上获取并且搜索FP；

[0032] 2. 仅搜索人口统计资料-在能够进行光学字符识别(OCR)时，通过设备中的机器可读区域(MRZ)读取器获取人口统计数据；当有非接触式芯片时，通过设备中的射频识别(RFID)读取器获取人口统计数据；或者能够由本发明的操作员通过位于设备12上的键盘29手动输入数据；以及，

[0033] 3.FP和人口统计搜索。

[0034] 识别(1:N远程，中心数据库搜索)

[0035] 本方案提供了通过使用从设备发送的记录对数据库的指定片段进行搜索的能力，该设备通过数据传输介质与远程数据库进行通信。1:N FP方案使系统的操作员能够在室外获取未知对象。一旦获取指纹，本发明就向中心AFIS网站发送指纹，以用于搜索。在发送之后，将命中/未命中的响应返回到该设备；如果命中，就会同时返回该对象的照片。

[0036] 中心数据库搜索允许本发明的操作员在室外获取来自对象的人口统计数据(其能够通过对人员证件的肉眼观察来得到，或者通过对位于设备内部的OCR或者RFID芯片进行读取得到)。

[0037] 操作员能够使用本功能执行多个搜索，搜索包括但不限于：

[0038] 1. 仅FP搜索

[0039] a)根据国家法律，执行1:N FP搜索以确定要求被识别的人员是否在数据库中。根据进行识别的理由以及国家法律，可以对国家的或者州(US)的AFIS进行1:N搜索，或者也可以向诸如BIS、国际刑警组织(Interpol)或者Eurodac等EU中心AFIS提交1:N搜索，或者向美国联邦调查局(FBI)提交1:N搜索。

[0040] b)系统的操作员应当具有从他们被授权访问的AFIS数据库选择性地开展搜索的能力；他们应当能够选择AFIS数据库的搜索顺序。

[0041] 2. 仅人口统计搜索

[0042] a) 可以在一个或多个不同的数据库中进行该搜索，这取决于操作员启动的数据库以及从有关人员得到的信息类型。这种搜索的一些示例包括但不限于：

[0043] i. 被拒绝人员名单

[0044] ii. 被通缉和逮捕的人员 (US)

[0045] iii. 观察名单

[0046] iv. 驾驶执照

[0047] v. 车辆登记

[0048] vi. 武器登记等

[0049] b) 操作员具有从他们被授权访问的数据库选择性地进行搜索的能力；他们还应当能够选择数据库的搜索顺序。

[0050] 3. 人口统计和 FP 搜索 - 该搜索能够结合前述两种功能。操作员将能够选择先执行哪种类型的搜索。

[0051] 验证和 / 或鉴定 (1:1 本地和文件鉴定)

[0052] 该方案允许优选通过生物统计验证和 / 或证件鉴定进行人员的身份确认。本实施例需要使用智能卡 / 电子护照或者其它机器可读的嵌入式生物统计手段。当对象具有这种形式的身份证明时，操作员将能够使用对象提供的证件来验证该对象的身份，同时验证该证件的真实性。在这种情况下，负责这项工作的操作员将能够从该对象的证件获得参考指纹以及任何其它合适的识别信息和 / 或照片图像信息。设备也能够从对象获取指纹，以便比较这两个指纹图像。在设备中处理新获取的指纹图像，指纹细节被抽取并且与参考指纹进行比较。如果这两个指纹匹配，就核实了这名人员的身份。

[0053] 当根据其它政府颁发的有效文件的数据库进行鉴定并且该数据库被定期更新时，设备也能够从数据传输介质获得更新。当使用保存在设备上的其它数据库，该设备本身是唯一标识的，就能够确切地知道哪个设备获得哪个版本的数据库信息。此外，当数据库保存到设备上时该数据库被加密，并且未经正确授权不能访问该数据库。

[0054] 远程的验证和鉴定 (1:1 远程和文件鉴定)

[0055] 本实施例提供一种用于当操作员正在验证新的申根签证或者其它政府 / 机构发布的证件时的情形的解决方案，然而，生物统计数据没有保存在证件本身中，而保存在中心数据库中。

[0056] 在这种情况下，优选地，操作员应当能够将所获得的人员的指纹提交给中心 AFIS，在中心 AFIS 中将该指纹与被保存的和申根签证号码或者其它政府 / 机构颁发的证件号码相关联的指纹进行比较。

[0057] 操作员使用该功能能够进行如下操作，这些操作包括但不限于：

[0058] 1. 使用设备上的 MRZ 读取器读取签证或者其它证件号码。

[0059] 2. 使用上述设备获取 FP，并将其与签证或者其它证件的号码一起提交至适当的中心 AFIS 数据库。一旦在中心 AFIS 中完成验证，结果匹配或者不匹配就会返回该设备。如果不匹配，操作员将能够用已获取的信息执行其它前述的任何功能。

[0060] 上文概括性地说明了用于个人和 / 或文件的鉴定和验证的设备的更多重要特征，其中该设备包括多功能的鉴定服务，并且该设备与多个远程数据库进行数据通信；而且，位

于该设备本身内部的安全信息交互设备用于该设备的安全匹配和操作，数据传输介质用于向多个数据库发送对象的信息，从而根据其详细说明将更好的理解，并且更好地理解本发明对现有技术做出的贡献。下面将描述本发明的附加特征，这些附加特征构成本说明书所附权利要求的内容。

[0061] 对此，在详细说明本发明的至少一个实施例之前，应当理解，本发明不限于按下文说明或者附图所示的具体结构或者组件布置来实施。本发明能够以其它实施方式来实施，并且通过各种方式运用和执行。而且，应当理解，这里采用的短语和术语是出于说明的目的，而不应视为限制。

[0062] 这些与本发明的其它目的，以及作为本发明特点的各种新颖的特征在所附权利要求中被详细指出，并且构成本发明的一部分。为了更好地理解本发明、其操作优点及其使用所达到的具体目的，应当参照附图和本发明的优选实施例所示的描述内容。

附图说明

[0063] 图 1 是表示用于个人和文件的鉴定和验证的设备的框图，其中，该设备具有安全多功能鉴定服务并且与多个远程数据库进行数据通信。

[0064] 图 2 是表示组成本发明的基本结构的部件以及在使用本发明期间用于识别和验证的部件的框图。

[0065] 图 3 是表示操作员对本发明的操作和设备管理员对本发明的操作的一个实施例的流程图。

[0066] 图 4A 和图 4B 是表示本发明的设备管理的一对流程图。

[0067] 图 5A 是表示本发明的设备配对（优选设备与数据传输介质之间的设备配对）的方法。

[0068] 图 5B- 图 5H 是表示在设备与数据传输介质之间的设备配对过程中的各个步骤的流程图。

[0069] 图 6 是表示本发明的配置管理方法的流程图。

[0070] 图 7 是表示本发明的同步的流程图。

[0071] 图 8A 是表示本发明的操作员在识别查询期间的室外操作 (field operation) 的流程图。

[0072] 图 8B 是表示本发明的操作员在验证查询期间的室外操作的流程图。

[0073] 图 8C 是表示本发明的操作员在设备间的重新连接期间的室外操作的流程图。

[0074] 图 9 是表示本发明的数据库管理的流程图。

[0075] 图 10A 是表示本发明的操作员执行识别查询搜索的一个实施例的流程图。

[0076] 图 10B 是表示本发明的操作员执行验证查询搜索的一个实施例的流程图。

[0077] 图 10C 是表示设备通过本地和远程数据库进行用户证件获取和处理的过程的一个实施例的流程图。

[0078] 图 11 是表示本发明的设备、数据传输介质和多个用户界面之间的多个用于让操作员能够与每一层通信的框图。

具体实施方式

[0079] 本发明提供了一种具有包括数据存储功能的安全多功能鉴定服务的智能外围设备其中，该设备包括多功能的智能外围设备或者辅助设备，当在一个系统中实施时，所述多功能的智能外围设备或者辅助设备用于与受到所述设备控制的数据传输介质共同对该设备指示系统执行的一组处理进行控制。

[0080] 本发明用于执行个人和 / 或文件的鉴定和验证，其中，该设备具有多种数据存储功能，并且通过数据传输介质与多个远程数据库进行数据通信。此外，各个辅助设备具有安全多功能鉴定服务。

[0081] 因此，在一个实施例中，本发明用作如下设备，该设备能够鉴定对象及其相关的颁发证件，并且核实提供颁发证件的个人为真正的持有人。该设备能够通过使用任何数据传输介质以与多个远程数据库通信，从而实现该操作。可通过单个地或组合地使用生物统计数据搜索和人口统计数据搜索以及匹配功能来进行对象的鉴定。

[0082] 本发明还能够在设备和任何数据传输介质之间实现加密的无线连接，以用于设备与多个远程数据库之间的安全信息传输。该功能可通过硬件和嵌入有该设备的软件与数据传输介质的组合来实现。

[0083] 在本发明的一个实施例中，该设备和数据传输介质进行无线通信，该通信可以采用任何协议和技术。此外，能够向本发明所采用的实际通信协议或者技术提供加密保护，以作为自主层 (autonomous layer)。

[0084] 在本发明的另一实施例中，操作员具有对设备与数据传输介质的配对以及这些配对向该操作员的发送进行管理的能力。此外，该操作员具有对从中心数据库或者远程数据库下载到该设备的任何数据进行管理和控制的能力。

[0085] 图 1 是表示本发明 10 的框图，其中，设备 12 与数据传输介质 14 进行数据通信。在一个实施方式中，数据传输介质 14 可以是移动设备、手持通信设备、计算平台设备或者蓝牙®连接。在一个实施例中，设备 12 包括生物统计鉴定模块 16，鉴定模块 16 用于优选地获取对象的指纹，以便进行识别或者验证。此外，设备 12 包括机器可读区域 (Machine Readable Zone，MRZ) 读取器 18A、光学字符识别 (Optical Character Recognition，OCR) 读取器 18B 以及射频识别 (Radio Frequency Identification，RFID) 读取器 20，这些读取器用于获取并且处理对象所具有的各种文件，以优选用于鉴定查询。此外，光学文件扫描器 22 用于文件的分析，以用于鉴定。设备 12 还包括安全访问模块 24，安全访问模块 24 与数据传输介质 14 具有接口，以用于该设备与多个远程数据库之间的信息的安全传输。此外，设备 12 还具有多个数据存储器 26，数据存储器 26 例如优选具有本地指纹数据库的形式或者拒绝人员观察名单的形式。此外，设备 12 还具有相机 27、磁条读取器 31 和接触式读卡器 33，相机 27 能够使该设备的操作员确保对象的图像识别。

[0086] 在一个实施例中，设备 12 通过数据传输介质 14 与设备管理系统 28 进行数据通信，其中该数据通信的形式优选为无线通信。此外，设备 12 优选地与多个数据库 30 进行数据通信，以用于个人和 / 或文件的远程识别和验证。

[0087] 如上所述，通过软件和辅助设备硬件的专门配置功能，本发明能够按照操作员所要求的任何方式组合多个生物统计和非生物统计的搜索和匹配功能。下面列出了四种主要生物统计功能：

[0088] • 1:N 本地识别；

[0089] • 1:N 远程识别；

[0090] • 1:1 本地验证；

[0091] • 1:1 远程验证。

[0092] 下面列出了非生物统计功能（注意，对于每种功能，其应用能够根据各国各自的要求进行定制接口协议）：

[0093] • 姓名搜索（欧盟 (EU)- 申根识别系统 (SIS) 和 SISII，US- 州和国家犯罪信息中心 (NCIC)）；

[0094] • 车辆登记搜索 (EU-SIS+ 和 SISII，US- 州机动车辆局 (DMV)）；

[0095] • 武器登记搜索 (US- 州和 NCIC)；

[0096] • 驾驶执照搜索 (EU- 国家数据库以及 US- 州 DMV)；

[0097] • 车辆出厂号码 (VIN) 搜索 (EU-SIS+ 和 SISII，US- 州 DMV)；

[0098] • 签证搜索 (EU-VIS/BIS)；

[0099] • 政府或者私有部门颁发的任何其它证件。

[0100] 此外，特殊证件鉴定功能使得操作员能够获得被持有的安全证件的真实性有关的信息，这些安全证件包括但不限于：

[0101] • 电子护照和标准护照；

[0102] • 国家身份证；

[0103] • 驾驶执照；

[0104] • 政府或者私有部门颁发的任何其它证件。

[0105] 仅用受限设备的数据库进行识别

[0106] (1:N(N 为几个）和本地搜索）

[0107] 本实施例使观察名单指纹和 DPL 或者其它种类的子集数据库能够驻留在设备自身内。这使得操作员能够在诸如远程区域或者通信信号不可靠的建筑物等通信受限制的位置处识别对象。这也可以在对具体一组对象进行搜索时使用。该设备为操作员提供了用于更新数据传输介质上的本地数据库的手段，这些手段包括但不限于无线网络、办公室 WiFi、办公室 PC 的 USB 连接、或者办公室局域网连接。

[0108] 此外，各个设备是唯一识别的，使得能够确切地知道哪个设备获得了哪个数据库信息。与各个设备的安全相关地，驻留在设备 12 中的数据库在保存到该设备中时被加密，并且在被未经正确授权的操作员篡改时可以被自动删除。

[0109] 识别

[0110] (1:N 远程和中心数据库搜索）

[0111] 本实施例提供了如下功能：通过使用优选地利用无线技术从设备传输到多个远程数据库的记录，对数据库的指定部分进行搜索。1:N FP 功能使本发明的操作员能够获取该区域中的未知对象的指纹。一旦获取指纹，就将该指纹传输到中心 AFIS 网站以用于搜索。命中 / 未命中的响应返回至该设备，如果可用，则也会同时返回该个人的照片。

[0112] 此外，远程数据库搜索使操作员能够在室外获得对象的人口统计。该搜索能够在一个数据库或者多个不同的数据库中进行，这取决于操作员启动的哪个对象和该对象的可用信息的类型。操作员能够对他们被授权访问的数据库选择性进行搜索，并且他们能够选择数据库的搜索顺序。

[0113] 验证和鉴定

[0114] (1:1 本地和文件鉴定)

[0115] 本实施例通过生物统计验证和文件鉴定来确认个人的身份。这需要使用智能卡/电子护照或者其它机器可读的嵌入式生物统计手段。当对象具有这种形式的身份证明时，操作员可通过使用所提供的文件来验证对象的身份，并且还能够验证该文件的真实性。

[0116] 当通过不同政府颁发的有效文件的数据库对该文件进行鉴定时，该数据库以安全格式驻留在该设备内。当设备上保存有其它数据库时，该设备是可唯一识别的，从而能够确切地知道哪个设备获得了哪个版本的数据库信息。此外，数据库在保存到设备中时被加密，并且如果在未经正确授权的情况下篡改时会被自动删除。

[0117] 远程验证和鉴定

[0118] (1:1 远程和文件鉴定)

[0119] 本实施例在生物统计数据没有保存在证件本身而是保存在远程数据库中时，对新的申根签证或者其它政府/机构颁发的证件进行验证。操作员可将所获取的对象指纹提交并且将其发送至中心AFIS，在中心AFIS中，将该指纹与中心AFIS所保存的与申根签证号码或者其它政府/机构颁发的证件号码有关的指纹相比较。本发明还使用设备和鉴定应用程序对签证或者证件进行鉴定。

[0120] 图2表示组成本发明的基本结构的部件和在本发明的使用期间用于识别和验证的部件的框图。所述部件分成两组，即在该图的顶端所显示的基本结构对象，以及在该图底端的用于识别和验证的对象。

[0121] 基本结构对象

[0122] 如前所述，本发明包括用于个人和/或文件的鉴定和验证的设备12，设备12通过数据传输介质14与多个远程数据库30进行数据通信。此外，在一个实施例中，边界控制移动应用程序(Border Control Mobile Application，BCMA)32可安装在设备12上，BCMA 32允许对鉴定和验证过程进行控制。此外，BCMA 32优选通过蓝牙®与设备12进行数据通信，并优选通过移动电话网络与多个国家主机进行数据通信。

[0123] 在一个实施例中，BCMA 32和设备12包括配对过程之后的设备对象(将在下文说明)。在配对过程期间，多个通信证书34A和配置数据34B上传到各个设备；在一个实施例中，通信证书34A为X.509格式。在设备12上保存有多个本地数据库36，数据库36可包括多个数据库子集38A以及多个日志数据38B，数据库子集38A包括但不限于“热门列表(Hotlist)”，日志数据38B包括但不限于操作员的工作日志和事件日志。卡可验证(CV)证书40可选择性地保存在设备12上，并且在读取RFID芯片时使用。

[0124] 身份证明和验证对象

[0125] 查询对象42用于对本地数据库36和远程数据库30进行多个搜索。查询对象42在识别/验证过程中收集所有的必要数据；收集的数据的数量和类型取决于过程。证件44保存多个人口统计数据46A和证件号码46B。此外，证件44具有多个鉴定信息46C、多个生物统计数据46D和操作员的参考指纹46E，鉴定信息46C包括但不限于水印和其它可鉴定特性。在一个实施例中，为了让操作员鉴定证件44，BCMA 32采用能够在证件44上找到的用于描述鉴定信息以及信息读取方式的格式说明。

[0126] 图3表示操作员对本发明的操作以及设备管理员对本发明的操作的一个实施例。

工作流程具有两个并行分支：(1) 设备管理；和 (2) 室外操作，将在下文对其详细说明。

[0127] 图 4A 和图 4B 表示本发明的设备管理系统 28 的操作流程图，设备 12 的管理系统 28 用于接纳设备 12、数据传输介质 14 以及多个数据库子集 26。此外，设备管理系统 28 用于将应用程序、数据库子集和设备信息存入自己的数据库。

[0128] 此外，设备管理系统 28 用于创建多个数据库资料（热门列表）以及配置数据，并随后更新设备 12 上的应用程序和数据库资料。最后，设备管理系统 28 将设备与可用的数据传输介质 14 进行配对，并将设备交给操作员，然后设备管理系统 28 解除设备的配对，并从设备下载室外操作日志。

[0129] 图 5A 表示本发明的设备配对方法，优选在设备 12 和数据传输介质 14 之间进行配对，以在设备 12 和多个远程数据库 30 之间进行信息的安全传输。在一个实施例中，可由设备管理员进行所述配对和解除。首先，为了开始配对操作，设备 12 包括安全信息交互设备 (secure information exchange device，SIED)48，SIED 48 用于鉴定设备 12，并且与数据传输介质 14 进行数据通信。为了鉴定设备 12 和数据传输介质 14，SIED 48 用于读取和 / 或分析多个鉴定数据，鉴定数据包括但不限于设备 12 和数据传输介质 14 的识别信息和证书。在鉴定期间，SIED 48 将设备 12 和数据传输介质 14 的数字证书与外部的证书管理机构 (CA) 根证件进行比较。在一个实施例中，设备 12、数据传输介质 14 以及 SIED 48 都具有由同一 CA 颁发的数据证书，因此它们在同一证书链上。因此，当数字证书验证成功时，SIED 48 在设备数据库 50 中进行搜索，当设备数据库 50 中注册了设备 12 和数据传输介质 14 时，设备 12 和数据传输介质 14 的鉴定均被核准。或者，如果它们不在数据库 50 中，SIED 48 向设备管理员发出警告。因此，一旦完成鉴定，SIED 48 将设备 12 与数据传输介质 14 进行配对，以允许设备 12 与远程数据库 30 收发多个信息。

[0130] 首先，在步骤 100 中，配对请求发送至设备 12 和数据传输设备 14。在步骤 102 中，在设备 12 与数据传输介质 14 重新连接时，SIED 48 获取设备 12 的操作员的指纹以便鉴定查询，从而鉴定操作员。在步骤 104 中，SIED 48 将其自己的数字证书同时发送给设备 12 和数据传输介质 14。而且，设备 12 和数据传输介质 14 可使用外部 CA 的根证书来鉴定 SIED 证书。在 SIED 48 的验证以后，在步骤 106 中，设备 12 产生密钥对。在步骤 108 中，设备 12 向 SIED 48 发送公共密钥。在设备 12 和数据传输介质 14 通信期间使用公共密钥，其中设备 12 将通过使用数据传输介质 14 来鉴定设备 12 本身。在步骤 110 中，设备 12 将向 SIED 48 发送蓝牙®地址。在与设备 12 所执行上述步骤的同时，在数据传输介质 32 成功验证 SIED 48 的数字证书之后，在步骤 112 中，数据传输介质 14 产生其自己的密钥对，并在步骤 114 中向 SIED 48 发送公共密钥。如上所述，在设备 12 与数据传输介质 14 通信期间又使用该密钥，其中数据传输介质 14 将自我鉴定。在步骤 116 中，数据传输介质 14 向 SIED 48 发送数据传输介质 14 的蓝牙®地址。在步骤 118A 和步骤 118B 中，SIED 48 向外部 CA 发送设备 12 的公共密钥和数据传输介质 14 的公共密钥，以用于签名。在步骤 120 中，SIED 48 从外部 CA 接收签名的证书，在步骤 122 中，SIED48 通过使用 SIED 48 的私有密钥对每个证书进行签名。接下来，在步骤 124 中，SIED 48 优选地产生 16 个字符长度的随机字符串，以用作设备 12 和数据传输介质 14 所使用的蓝牙®密码。最后，在步骤 126A 和步骤 126B 中，SIED 48 上传各个设备 12 与数据传输介质 14 的配对信息，其中配对信息包括但不限于各个证书、各个蓝牙®地址和密码以及获取的操作员的指纹。

[0131] 图 5B- 图 5H 表示利用位于设备 12 中的 SIED 48 在设备 12 与数据传输介质 14 之间进行如图 5A 所示的设备配对过程中的各步骤以及其它可选的实施例。

[0132] 在本实施例中，在系统的操作员 52 开始室外操作之前，操作员将设备 12 与数据传输介质 14 进行配对。如上所述，使用之前的配对过程需要确保设备 12 及其操作员 52 和数据传输介质 14 之间的验证连接。配对过程向设备 12 和数据传输介质 14 提供基本信息以便能够建立安全的蓝牙®通信，并且提供了安全的鉴定和授权。此外，设备 12 的安全访问模块中保存的本地数据库的机密性也包括上述过程。

[0133] 在本实施例中，配对和解除配对是由设备管理员执行的。设备管理员管理优选地通过共同注册设备 12、数据传输介质 14、本地数据库 26 和操作员 52 来管理设备配对。

[0134] 图 5B 表示整个配对过程，其中图 5C- 图 5H 详细地说明了包括整个过程在内的各个步骤。

[0135] 图 5C- 图 5H 表示执行如下操作的过程的一个实施例 ：

[0136] • 发现设备

[0137] • 创建一对设备

[0138] • 更新软件应用程序

[0139] • 更新数据库

[0140] • 为每个设备创建证书

[0141] • 更新配置

[0142] 首先，配对过程从发现将会组成一对的各个设备 12 和数据传输介质 14 开始。设备 12 和对应的数据传输介质 14 通过 SIED 48 进行数据通信。如上所述，SIED 48 用作可信赖的主机，其中操作的各个元件 (设备 12 和数据传输介质 14) 信任 SIED 48 的真实性。SIED 48 执行随设备 12 一起提供的应用程序。在步骤 200A 和步骤 200B 中，SIED 48 分别鉴定设备 12 和数据传输介质 14。SIED 48 从设备 12 和数据传输介质 14 读取多个鉴定数据 (包括设备 ID、证书)。然后，SIED 48 用外部的 CA 根证书核对每个数字证书。如果数字证书验证成功， SIED 48 然后在设备数据库 50 中搜索设备 ID。如果在设备数据库 50 中注册了设备 12 和数据传输介质 14，则鉴定成功。在任何其它情况下，SIED 48 将会警告设备 ；在本实施例中，将在配对过程开始之前进行设备 12 和数据传输介质 14 的注册。

[0143] 在完成设备的鉴定之后，SIED 48 通过首先获取操作员 52 的指纹来执行配对 ；优选地，当设备 12 和数据传输介质 14 重新连接时，该指纹将用于鉴定操作员。接下来，SIED 48 将它自己的数字证书发送给设备 12 和数据传输介质 14 ；设备 12 和数据传输介质 14 用外部 CA 的根证书来鉴定 SIED 证书。在本实施例中，设备数据库 50 不是设备 12 自身的一部分，而优选地是操作员 52 或者设备管理员所具有的清单数据库。设备数据库的界面是设备 12 整体的一部分。终端用户通过使用它们的清单数据库的登记软件来进行设备的登记。

[0144] 如果设备 12 成功地验证了 SIED 数字证书，该设备生成密钥对 (即，公共密钥和私有密钥)，并且将公共密钥转发给 SIED 48。在设备 12 和数据传输介质 14 通信期间将会使用该公共密钥，其中设备 12 将向数据传输介质 32 鉴定自己。最后，设备 12 将向 SIED 48 发送设备 12 的蓝牙®地址。

[0145] 与设备 12 的验证类似，如果数据传输介质 14 成功验证了 SIED 数字证书，数据传输介质 14 产生密钥对，并且将公共密钥发送给 SIED 48。在设备 12 和数据传输介质 14 通

信期间将会使用该公共密钥，其中数据传输介质 14 将向设备 12 鉴定自己。最后，数据传输介质 14 将其蓝牙®地址发送给 SIED 48。

[0146] 如图 5A 所述，SIED 48 向外部 CA 发送公共密钥以用于签名。然后，SIED 48 产生十六个字符长的 ID，该 ID 将由设备 12 和数据传输介质 14 用作蓝牙密码。然后，SIED 48 将设备 12 证书、数据传输介质 14 证书、数据传输介质 14 蓝牙®地址和蓝牙®密码上传到设备 12。一旦成功配对，该配对将会存入 SIED 48 的数据库。在设备配对之后，如果需要的话，同步代理 (synchronization agent) 将会更新热门列表和软件应用程序。

[0147] 图 6 表示整个系统的配置管理的流程图，其中配置管理器负责用于创建多个配置数据以及规定哪个应用程序更新需要在同步过程中安装在设备 12 上 (见图 7)。在一个实施例中，可在配对过程期间上传配置数据。在步骤 202 中，配置管理器执行查询，以确定是否有新的配置数据可用。在步骤 204 中，如果有新的配置数据可用，则更新配置数据，并且随后在步骤 206 中，上传配置数据。然后，在步骤 208 中，新的配置数据保存在设备 12 的本地数据库的日志数据中。

[0148] 图 7 表示本发明的同步的流程图，其中在步骤 210 中，设备 12 或者数据传输介质 14 与 SIED 48 连接。在步骤 212 中，配置管理器鉴定图 5A 所示的连接设备。在步骤 214A 中，检查设备 12 的应用程序版本，以确定是否有更新 ；在步骤 214B 中，检查数据传输介质 14 的应用程序版本，以确定是否有更新。当设备 12 有应用程序更新时，在步骤 216A 中上传新的应用程序，并且在步骤 218A 中将应用程序数据记入日志。当数据传输介质 14 有应用程序更新时，在步骤 216B 中上传新的应用程序，并且在步骤 21 8B 中将应用程序数据记入日志。最后，SIED 48 用于核对数据库资料，并且如果该资料已经改变，SIED 48 将会在步骤 220 中更新数据库。

[0149] 图 8A- 图 8C 表示可由操作员执行的各种室外操作过程，其中所述过程包括但不限于 ：识别 ；验证 ；以及设备的重新连接。

[0150] 识别和验证过程可包括本地数据库搜索或者远程数据库搜索，这取决于具体情况和操作员的需要。在一个实施例中，在远程数据库上执行远程搜索，其中设备 12 优选地通过移动电话网络向国家主机 (NationalState Host Machine，NSHM) 发送搜索查询 ；优选使用传输层安全 (TransportLayer Security，TLS) 加密来确保 NSHM 和设备 12 之间的数据通信的安全。一旦从设备 12 发送搜索查询，NSHM 将向与数据查询对应的远程数据库发送查询 ；随后，优选使用上述通信方法将数据库搜索结果传输到设备 12。

[0151] 图 8A 表示识别查询和 / 或搜索过程的一个实施例，其中该过程的目的之一是确定查询 / 搜索的对象是否在热门列表、DPL 或者其它类似的数据库子集中。

[0152] 首先，在步骤 222 中，操作员从接受调查或查询的对象获取多个人口统计数据和 / 或生物统计数据。一旦从对象获得数据，在步骤 224 中，在多个远程数据库中搜索所获得的数据。如果如前所述由于操作员的位置不能进行远程搜索，则在步骤 226 中，对设备 12 内保存的多个数据库执行本地搜索。在步骤 228 中，获得查询结果，并将其提供给与对象的识别有关的操作员。

[0153] 图 8B 表示验证查询和 / 或鉴定过程的一个实施例，其中该过程的目的之一是鉴定对象所持有的多个证件，以确定所述证件是否属于该对象。

[0154] 首先，在步骤 230 中，操作员从对象获取的多个生物统计和鉴定信息，生物统计和

鉴定信息包括但不限于该对象的指纹、证件号码（即护照等）和其它鉴定信息。一旦获取对象的证件信息，在步骤 232 中，使用保存在辅助设备 12 上的多个本地数据库来鉴定对象的信息。在证件上保存了生物统计数据的情况下，在步骤 234 中，使用本地搜索 / 数据库查询来验证对象的证件。如果该证件上保存了参考指纹，设备 12 将参考指纹与获取的指纹进行比较。然而，在该证件没有保存生物统计数据的情况下，在步骤 236 中，使用远程搜索 / 数据库查询来验证对象的证件。如果证件上没有保存参考指纹，设备 12 通过数据传输介质 14 向远程数据库发送所获取的指纹和证件信息。在搜索 / 查询之后，在步骤 238 中，产生关于对象证件的真实性的查询结果。因此，如果鉴定失败，那么操作员将会被警告，然而在成功鉴定之后，过程可以继续。

[0155] 图 8C 表示当连接中断时设备 12 和数据传输介质 14 之间重新连接的过程的一个实施例的流程图。在现场操作期间，设备 12 和数据传输介质 14 之间的连接可能会中断。在这种情况下，操作员应当进行重新连接。在步骤 240 中，操作员必须提交指纹，其中在步骤 242 中，如前所述，主要通过操作员的指纹来鉴定操作员。在步骤 244 中，辅助设备 12 和数据传输介质 14 重新连接，以便使用。

[0156] 图 9 表示对保存在设备 12 内的多个本地数据库的数据库管理的一个实施例的流程图。位于设备 12 内的多个本地数据库使得操作员能够执行搜索，并且能够在远程连接出现问题的情况下或者当需要用于识别 / 验证请求的快速响应时利用该特征。

[0157] 本地数据库优选是较大的中心数据库 246 的一部分，其中所述中心数据库可包括黑名单 / 被通缉的人员、具有指纹数据的生物统计数据库、或者包括黑名单、护照、身份证的数据库。反之，位于设备 12 上的多个数据库是有限容量的数据库，其中多条基本信息将由操作员提供。这样，操作员可将设备 12 的本地数据库转换成将供操作员室外操作期间使用的格式。

[0158] 在步骤 248 中，在数据下载请求传输到中心数据库 246 之后下载多条数据。在接收到多条数据后，在步骤 250 中，根据基于下载的数据来生成多个本地数据库。在步骤 252 中，在由数据库管理器生成本地数据库后，使用由数据库管理器生成的密码来加密数据库。在步骤 254 中，数据库管理组件将加密的数据库文件以及相关的密码一起发送给同步代理。

[0159] 在一个实施例中，通过 SQL CE 将数据库保存到设备 12 上。通过由数据库引擎提供的 AES 128 方法将数据库文件加密。设备 12 对数据库密码进行加密并且将它们保存在内置 SAM 模块中。在设备 12 检测到蓝牙®连接可能受损（连接中断或者解耦）的情况下，设备 12 将密码从设备 12 的 RAM 删除。

[0160] 图 10A- 图 10C 表示通过对多个本地或者远程数据库进行识别 / 验证查询来获取对象的证件和 / 或生物统计数据的各种实施例。图 10A 和 10B 以图 8A 和图 8B 中所述的上述过程为基础并显示了该过程。

[0161] 图 10C 表示从设备 12 的角度来显示整个过程（优选从对象获取生物统计和人口统计数据，以及随后执行用于识别和 / 或验证目的的各种搜索查询）的流程图。

[0162] 首先，在步骤 256 中，设备 12 的操作员扫描对象的证件的 MRZ（在本实施例中，证件包括但不限于身份证明或者护照）。在扫描了对象证件的 MRZ 之后，设备 12 解码 MRZ，并且将这些内容放入对象的文件中。然后，在步骤 258 中，操作员确定对象的证件上是否存在要读取的芯片，并且将这些内容放入对象的文件中。在步骤 260 中，操作员确定是否需要获

取对象的指纹，如果需要，就扫描多个手指，然后将指纹扫描信息加入对象的文件。最后，在步骤 262 中，将对象的文件关闭、打包并且传输到数据传输介质 14。

[0163] 在步骤 264 中，数据传输介质 14 从设备 12 接收对象文件，并且将该文件解包。在设备 12 上可以显示工作流程选择列表，其中操作员具有确定要执行的搜索查询的能力。在一个实施例中，在步骤 266 中，操作员能够选择下列搜索中的一个搜索来执行 ：

[0164] • 姓名

[0165] • 其它人口统计资料

[0166] • FP 本地

[0167] • FP 远程

[0168] 在步骤 268 中，当操作员选择本地数据库搜索时，设备 12 发送搜索目标。在步骤 270 中，辅助设备 12 对本地数据库搜索产生响应，以供操作员查阅。在步骤 272 中，当操作员请求远程搜索时，对象的文件被打包并且传输到国家主机、中心数据库和 / 或 AFIS。最后，在步骤 274 中，对远程数据库搜索的响应被传输到设备 12，并且保存到对象的文件中。

[0169] 图 11 表示设备 12 和数据传输介质 14 和多个用于允许操作员与本发明的每一层通信的用户界面之间的各种界面的流程图。

[0170] 在一个实施例中，设备 12 具有可配置软件系统 278，其中当操作员使用时，软件和与该软件相关的各种功能用于支持该设备 12。优选地，可配置软件是由各种操作员（包括执法机构）使用，以优选地用于提供关于个人、多个车辆和 / 或财产的信息。在一个实施例中，可配置软件 278 用于提供与设备 12 的接口，以优选地便于从身份证明文件获取多个数据或者多个生物统计数据（包括对象的指纹）。如前述部分所述，能够可使用可配置软件 278 来处理由操作员从对象获得的信息，从而使得操作员能够进行关于该对象的本地搜索或者远程搜索。此外，可在中心数据库中执行搜索，或者通过使用设备 12 的本地数据库在本地执行搜索。

[0171] 在一个实施例中，可配置软件 278 和设备 12 之间的通信信道是 TCP/IP（可选择使用 UDP），其中带宽可低至 19.2 kbps。

[0172] 此外，在一个实施例中，可配置软件通过蓝牙®连接与设备 12 进行数据通信。在通过可配置软件与设备 12 建立连接之后，应用程序优选设计成易于使用，并且操作员不需要大量的操作培训。

[0173] 如前述章节所述，为了更好地使设备 12 操作，设备 12 应当与数据传输介质 14 配对，从而能够与多个远程数据库 30 通信 ；在一个实施例中，设备 12 能够与包括但不限于手提计算机 276 和数据传输介质 14 同时配对。在本实施例中，与手提计算机 276 的数据连接最好是通过数据传输介质 14。

[0174] 在一个实施例中，设备 12 具有多项功能和搜索查询，包括但不限于 ：

[0175] 鉴定

[0176] 在每次登录时，将通过使用设备 12 获取操作员的指纹并且执行与设备 12 内部保存的指纹之间的匹配，来执行基于生物统计的操作员鉴定。

[0177] 查询本地数据库或者州数据库

[0178] 可配置软件 278 将提供用户界面，以用于查询本地或者远程（联邦的或者州的）数据库。主要查询包括但不限于 ：

[0179] - 人员：通过使用他 / 她的身份证明文件、地理数据或者生物统计标识（指纹）来请求关于人员的 多条信息。

[0180] - 车辆：通过使用车辆标识（牌照、车辆出厂号码 VIN 等）请求关于车辆的多条信息。

[0181] - 财产：通过使用财产的序列号和类型来请求关于财产的多条信息。

[0182] - 枪支：通过使用枪支的序列号来请求关于枪支的多条信息。

[0183] 信息发送

[0184] 此外，位于设备 12 上的 SIED48 为多个操作员提供电子邮件信息发送特征，其中可配置软件 278 可提供用户界面用于信息发送，其中操作员可向多名其它操作员发送电子邮件消息。发送方可观察一个接收方或者多个接收方是否登录系统，当接收方或者一些接收方没有登录时，它们将在下次登录时接收该消息。优选地，仅通过操作员请求将消息保存到 SIED 48 或者从 SIED 48 删除。此外，SIED 48 在设备 12 的操作员之间传递非同步消息，其中消息发送业务优选为封闭系统，其中操作员能够仅仅在系统的边界发送和接收消息。

[0185] 人员有关的查询

[0186] 人员的身份，他 / 她在本地或者远程数据库上的存在能够通过各种方式实现。本章节说明可由可配置软件 278 实施的查询的类型。

[0187] AFIS

[0188] 基于 AFIS 的查询是指纹搜索，其中优选地，通过设备 12 获取两个食指。可配置软件 278 在设备 12 上实施用于表明人手形状的图形用户界面 280(GUI)，以用于指纹获取处理。获取的指纹将会作为电子邮件附件发送至 SIED 48 的合适服务，其中电子邮件的主题应当是人可读标识符。

[0189] 姓名搜索

[0190] 能够用关于人员的多条人口统计信息进行查询，其中可配置软件 278 将运行 GUI 用于姓名搜索处理。能够提供多个域，包括但不限于：

[0191] - 名、姓（必须输入的字段）。

[0192] - 州：可能具有该人员的记录的州。

[0193] 如果可以的话，应当填写如下数据字段，以便更好地过滤结果列表：

[0194] - 性别：应当可以从列表（女性、男性、未知）中选择。

[0195] - 种族：可从列表选择，包括但不限于：美国印地安人、亚洲人、黑人、未知、白人，和 / 或拉丁美洲人。

[0196] - 生日 (DoB)：应当按照州政府指定的格式输入。必须向操作员表明格式说明。

[0197] - 城市：该人员居住的城市。

[0198] 身份证明文件核查

[0199] 通过确认他 / 她的身份证明文件来核查人员的身份。也可以通过使用从身份证明文件获取的信息来执行进一步的查询。可配置软件 278 能够运行 GUI 以用于从身份证明文件获取信息，将获取的数据传递给操作员，并向操作员确认并且指示机器可读数据的结果。至少能够支持如下身份证明文档处理：

[0200] 旅行文件 / 护照核查

[0201] 生物统计护照或者电子护照组合了包含持有者的人口统计和生平数据的纸质和

电子的数据存储。设备 12 能够从护照本身采集该信息。在一个实施例中，用于信息收集的过程可包括如下步骤：

[0202] 1. 在选择护照选项之后，辅助设备首先扫描护照的机器可读区域 (MRZ)。这可以通过将正确的页面（包括 MRZ) 滑过设备 12 一侧的凹槽来实现。

[0203] 2. 如果该护照是电子护照，下一步是非接触式芯片的扫描，其通过将电子护照保持在设备 12 的包含 RFID 天线的区域来实现。

[0204] 3. 在扫描非接触式芯片之后，可获得现场的一个或者多个指纹。如果护照芯片包括指纹数据，这使设备 12 能够执行 1:1 指纹匹配查询。此外，获取的（现场的或者从芯片读取的）指纹能够在 AFIS 搜索期间使用。

[0205] 护照验证成功是指对象就是被扫描护照所描述的人，并且护照是有效的。此外，可通过采集到的涉及该人员的数据来进一步执行搜索。这些搜索包括但不限于：姓名搜索以及指纹搜索。

[0206] 人员 ID

[0207] 可通过扫描人员的个人身份证（个人 ID) 卡上的 MRZ 来启动查询。存储在身份证 MRZ 中的数据（姓名、出生日期等）可用于对州政府数据库进行搜索。

[0208] 驾驶执照

[0209] 如果操作员能够获取位于大多数美国驾驶员的执照上的条型码，就能够自动填写用于姓名搜索的字段。这项功能将会进行与姓名搜索相同的查询，只是加快了数据获取过程。

[0210] 车辆

[0211] 车牌

[0212] 可通过车牌信息对州数据库进行搜索。为了进行查询可能需要多个字段，上述多个字段包括但不限于：

[0213] - 车牌号码：该号码印在车牌上。

[0214] - 州：颁发该车牌的州。该州或者 / 州的缩写必须可以从下拉列表中选择。

[0215] 为了进一步细化搜索，在 GUI 280 中可以存在如下可选字段：

[0216] - 类型：车辆的类型应当可以从列表选择。可用的类型为：分段式车、商务车、摩托车、客车（应当作为默认选项来选择）、往返穿梭车、拖车、卡车。

[0217] - 年份：颁发汽车牌照的年份，默认值必须为本年度。

[0218] 针对指定车辆产生汽车牌照搜索结果。如果汽车牌照搜索产生结果，则应当容易对拥有者的记录进行搜索。

[0219] 车辆识别号码

[0220] 可执行搜索以找到不具有汽车牌照或者具有错误汽车牌照的车辆有关的数据记录。为了执行查询，应当提供多个数据字段，这些数据字段包括但不限于：

[0221] - 车辆识别号码 (VIN)：由制造商在汽车内输入的唯一识别号码。

[0222] - 州：可能具有该车信息的州。

[0223] 下列字段是可选的，但是可以填写以便提高正确度：

[0224] - 制造商：该车的制造商。应当可以从列表选择，但可以保留空白。

[0225] - 年份：登记车辆的年份，默认必须为本年度。

[0226] 船只

[0227] 操作员能够对关于船只的保存记录进行搜索。需要如下信息来进行该处理：

[0228] - 船号：由该船的制造商提供的序列号。

[0229] - 登记号：该船的登记号。

[0230] - 州：登记该船的州。

[0231] 通过使用船只的信息执行搜索来产生拥有该指定船只的机构的记录。

[0232] 财产有关的查询

[0233] 可执行搜索，以查找关于各种被盗物体的记录。必须填写的数据字段是：

[0234] - 序列号：由制造商提供的序列号。

[0235] - 类型：被搜索的物体的类型，应当可以从列表中选择。

[0236] 根据情况，查找到的数据记录描述了指定的物体及其状态（被盗 / 丢失财物、其它）。

[0237] 枪支有关的查询

[0238] 可执行搜索，以找到关于登记枪支的数据。该搜索将产生关于指定枪支的记录。必须输入如下数据字段以顺利地执行搜索：

[0239] - 序列号：该序列号嵌在枪身内。

[0240] 其它可选的数据字段包括但不限于：

[0241] - 口径：可以填写口径信息。该数据必须按照该州规定的格式提供。

[0242] - 制造商：枪的制造商。这应当可以从列表中选择，并且可以保留空白。

[0243] 使用枪的数据来执行查询，以产生关于指定武器的记录。

[0244] 查询回复

[0245] 当用于查询的回复到达时，操作员应当接收视频或者音频通知。通过搜索处理将回复进行分组，其中优选手动地删除回复，但当操作员退出登录时，所有数据应当从设备清除。此外，在一个实施例中，回复可以是文字数据，并且应当被解析，以便找到关键字并且将它们高亮显示。

[0246] 安全

[0247] 可配置软件 278 和设备 12 与多个敏感数据协同地工作；因此应当采取多项安全措施，以防止信息泄露。当操作员执行退出登录操作时，必须安全地删除这些回复。操作员将会阻止用设备 12 的未授权使用，但是在失窃的情况下，设备 12 优选在五分钟的不活动后执行对操作员的重新鉴定。此外，辅助设备 12 和 SIED 48 之间的传输会容易受到诸如窃听或者篡改等攻击，因此应当加密通信；该加密应当实现 FIPS 140-2 标准下的 256 位 AES 的安全。

[0248] 优选地，设备 12 使政府机构官员能够从对象的文件获取数据，或者在室外获取现场指纹。然后，这些数据能够被处理，以使官员能够进行关于该对象的搜索。

[0249] 为了实现这些功能，辅助设备 12 中必须存在如下软件组件：

[0250] - 传感器设备：要求进行数据获取的硬件集成到设备 12，如前所述，其包括：指纹读取器、OCR 读取器、条型码读取器、非接触式芯片读取器和接触式芯片读取器。为了能够使用传感器硬件，设备 12 中必须存在低级别的控制软件组件。

[0251] - 文件读取器组件：软件部分需要获取和处理嵌入在各种文件中的数据，或者执

行指纹获取过程。该组件包括用于处理具体文件的全部必要知识。

[0252] - 事务控制：为了执行（通过从文件读取或者通过用户输入获得）收集到的数据的搜索或者验证，需要事务控制组件。该软件组件在本地或者远程地协调查询的执行，并且处理这些事务的结果。

[0253] - 用户界面：用户界面组件提供了用于让操作员能够与系统交互的手段。系统能够通过这些用户界面与用户通信：

[0254] - 设备用户界面

[0255] - 手提计算机用户界面

[0256] - 数据传输介质界面

[0257] 事务控制组件驻留在数据传输介质 14 中，文件读取器组件位于辅助设备 12 中。设备 12 优选地提供该设备能够读取的一组文件，并且允许操作员选择其中一个文件。

[0258] 然后，设备 12 通过操作各种传感器设备来执行必要的步骤，以从文件读出所有数据。通过设备 12 获取的数据经过处理被填入数据字段中，以用于实际搜索。

[0259] 客户通信

[0260] 当辅助设备 12 和数据传输介质 14 之间建立了数据连接，操作员可仅使用设备 12 的特征。一旦建立数据连接，设备 12 可向多个远程数据库发送多个请求，以用于个人和 / 或文件的识别或者验证。由设备 12 产生的请求和回复可编码到个人消息中，且设备 12 对大部分请求发送回复消息，但是对一些请求不产生回复，或者可产生多个回复消息。

[0261] 层

[0262] 优选地，辅助设备 12 和数据传输介质 14 之间的通信信道被划分成不同层。这些层包括但不限于：

[0263] - 监牙®通信：通过蓝牙®连接来传输所有通信。

[0264] -TLS：通过 TLS 版本 1.2 来保护通信信道。

[0265] - 消息发送层：该层执行必要的消息序列化 / 反序列化。所述消息是 ASN.1 DER 编码的。

[0266] - 应用程序层：在该层中处理消息；该层包括所有的应用程序和业务逻辑。

[0267] 协议说明

[0268] 设备 12 等待多个输入连接请求，并然后使用如下协议阶段 (protocol phase) 进行通信，上述协议阶段包括但不限于：

[0269] - 连接：执行 TLS 握手操作，以通过打开的蓝牙信道来建立安全通信。设备 12 和数据传输介质 14 应当使用该配对过程中分配的通信证书。

[0270] - 访问特征：在该阶段中，数据传输介质 14 可访问由设备 12 提供的特征。这可通过安全信道交换消息来进行。设备 12 对大多数的请求产生单个回复，但对一些请求可产生多个回复或者甚至零回复。

[0271] - 断开连接：在关闭潜在的 TLS 和蓝牙信道之后，连接结束。

[0272] 因此，总之，本发明公开了用于通过设备上的安全信息交互设备在该设备和数据传输介质之间进行安全配对和操作的各种独特方案，该设备用作设备和数据传输介质所使用的信任元件，以便以安全加密方法进行创建和操作。

[0273] 尽管已经在优选实施例或者具体实施例中以示例的方式说明了本发明的各种变

型，显然在不脱离本发明的精神和范围或者本发明构思的情况下也可以设计其它实施例。然而，应当清楚地理解，这些变型和修改落在本发明的精神和范围内，并且包括但不限于下述附加的权利要求。

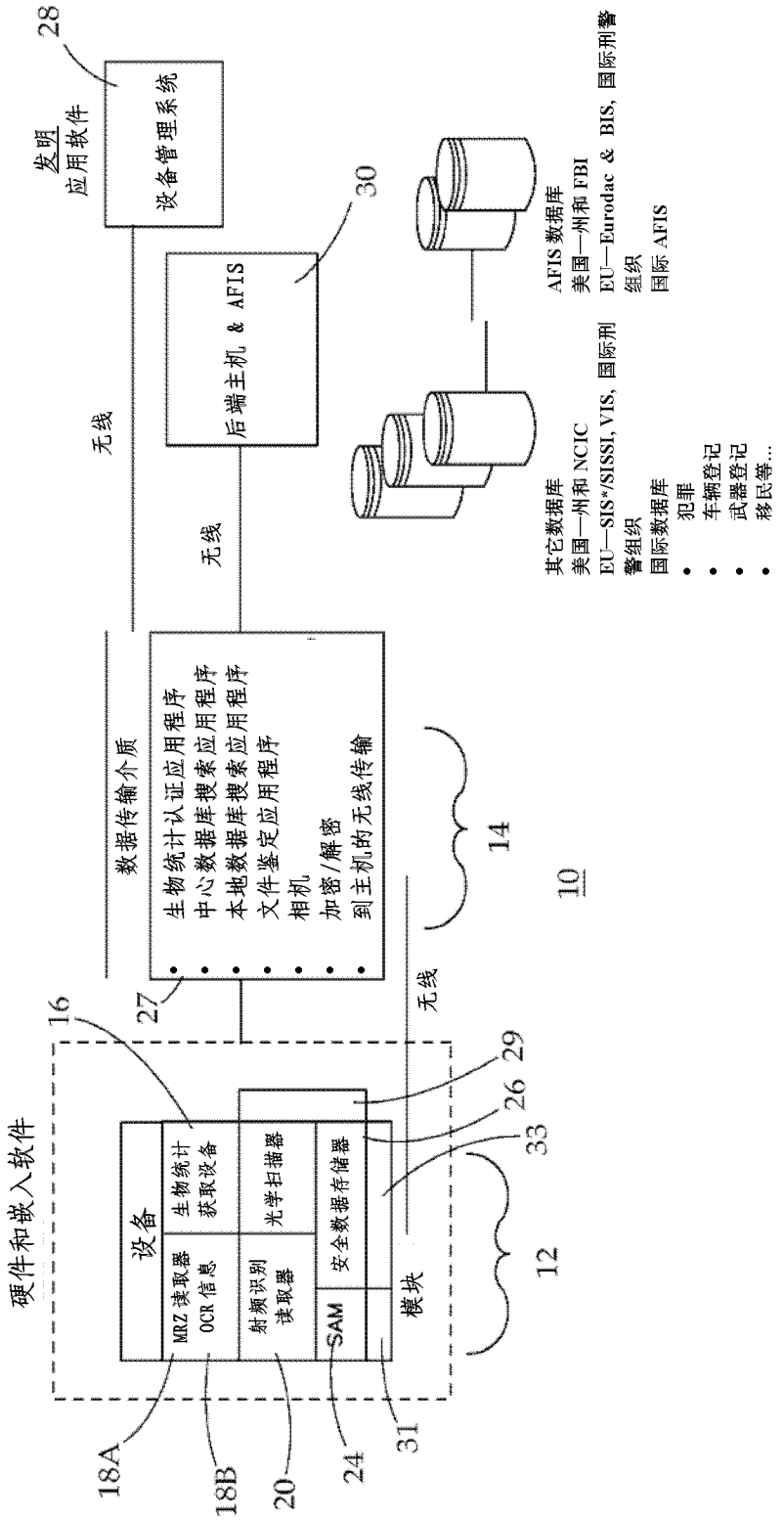

硬件和嵌入软件
设备
MRZ 读取器
OCR 信息
生物统计
获取设备
射频识别
读取器
光学扫描器
SAM
安全数据存储器
模块
16
18A
18B
20
24
31
12
33
26
29
27
数据传输介质
生物统计认证应用程序
中心数据库搜索应用程序
本地数据库搜索应用程序
文件鉴定应用程序
相机
加密/解密
到主机的无线传输
14
10
无线
无线
无线
发明
应用软件
28
设备管理系统
后端主机 & AFIS
30
AFIS 数据库
美国—州和 FBI
EU—Eurodac & BIS, 国际刑警组织
国际 AFIS
其它数据库
美国—州和 NCIC
EU—SIS*/SISSI, VIS, 国际刑警组织
国际数据库
犯罪
车辆登记
武器登记
移民等...

图 1

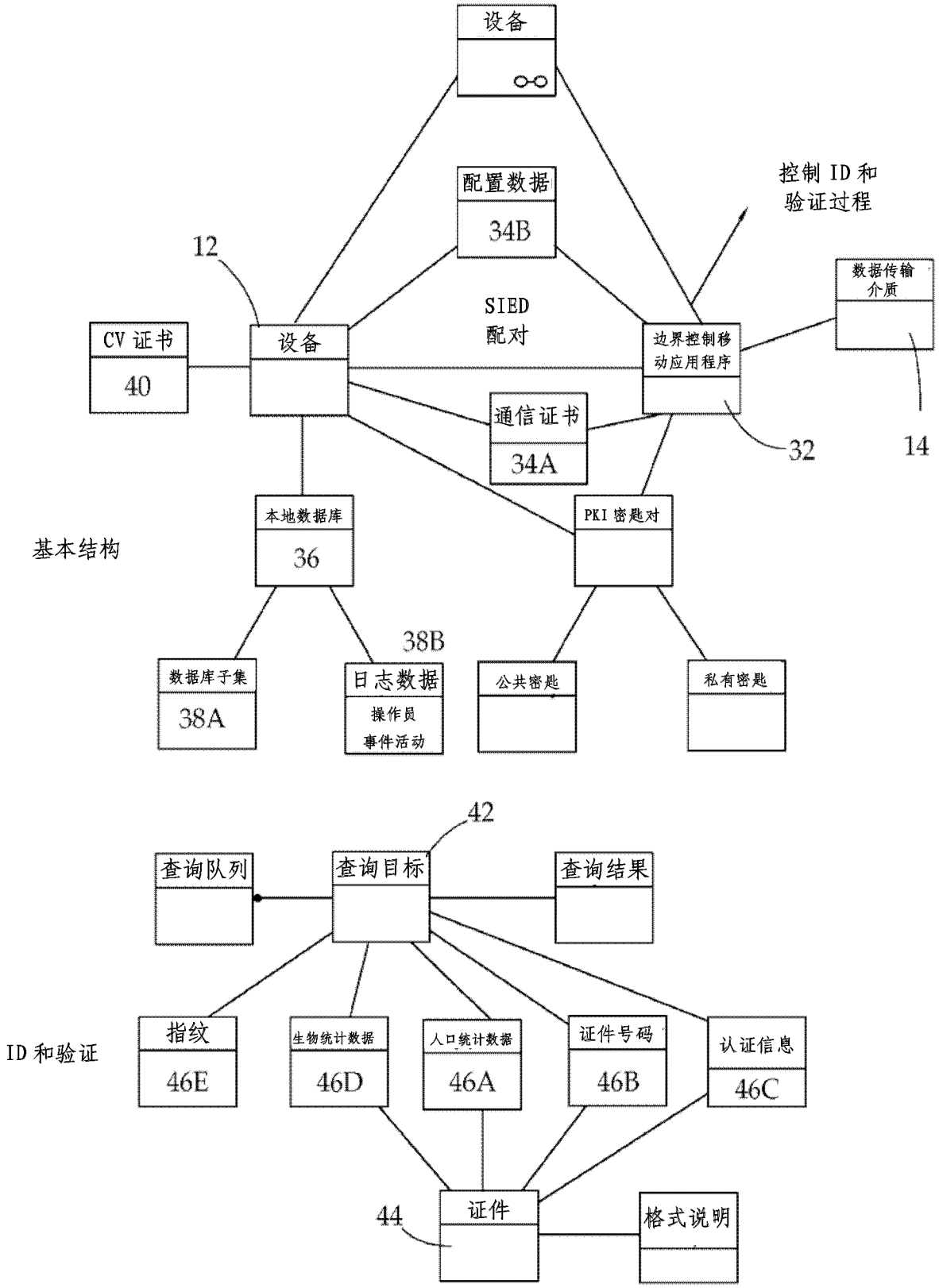

设备
配置数据
34B
控制 ID 和
验证过程
12
SIED
配对
数据传输
介质
CV 证书
40
设备
边界控制移
动应用程序
通信证书
34A
32
14
基本结构
本地数据库
36
PKI 密匙对
38B
数据库子集
38A
日志数据
操作员
事件活动
公共密匙
私有密匙
42
查询队列
查询目标
查询结果
ID 和验证
指纹
46E
生物统计数据
46D
人口统计数据
46A
证件号码
46B
认证信息
46C
44
证件
格式说明

图 2

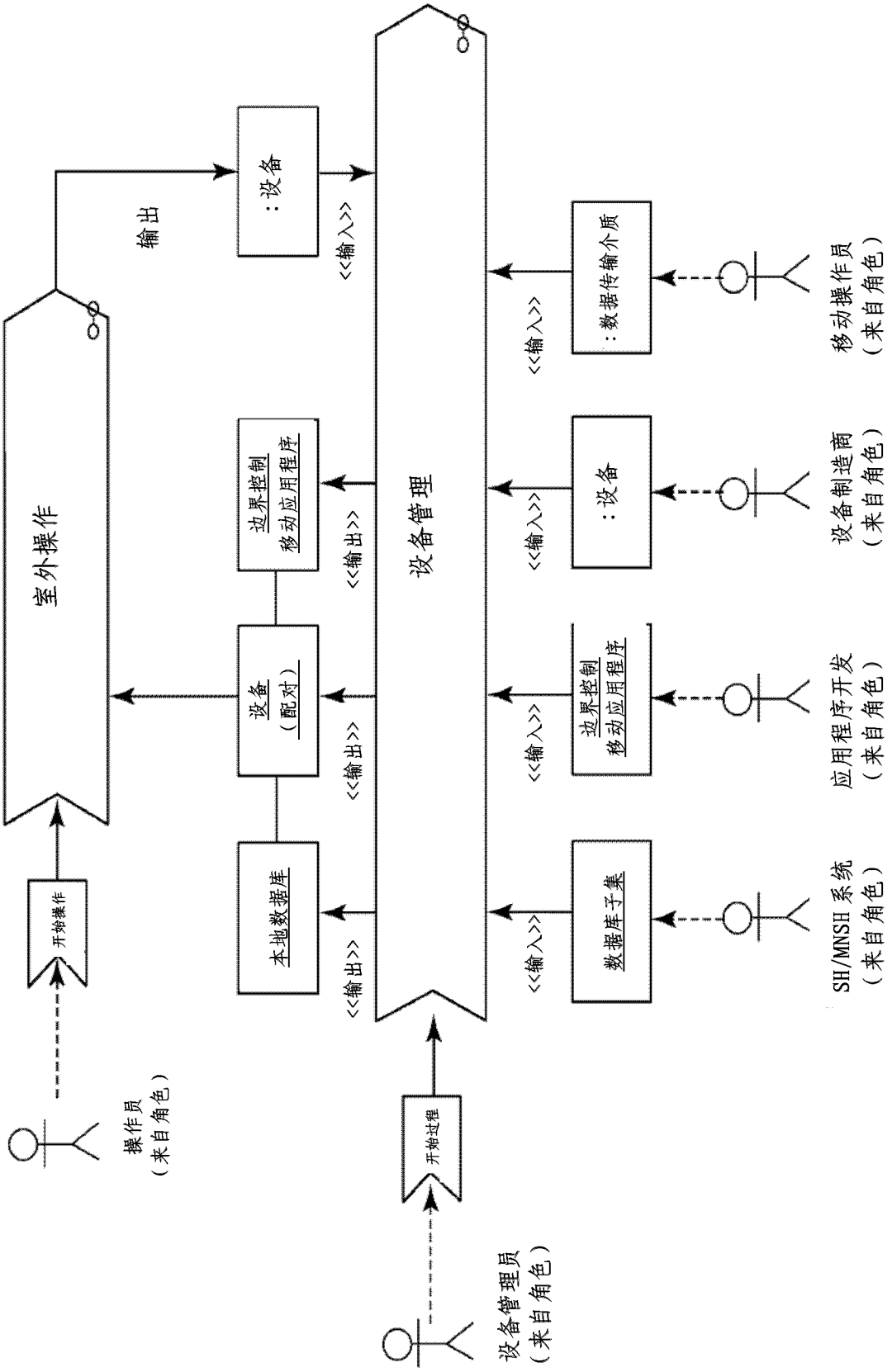

操作员
（来自角色）
开始操作
室外操作
输出
：设备
<<输入>>
设备管理
开始过程
设备管理员
（来自角色）
本地数据库
<<输出>>
设备
（配对）
<<输出>>
边界控制
移动应用程序
<<输出>>
数据库子集
<<输入>>
边界控制
移动应用程序
<<输入>>
：设备
<<输入>>
：数据传输介质
<<输入>>
SH/MNSH 系统
（来自角色）
应用程序开发
（来自角色）
设备制造商
（来自角色）
移动操作员
（来自角色）

图 3

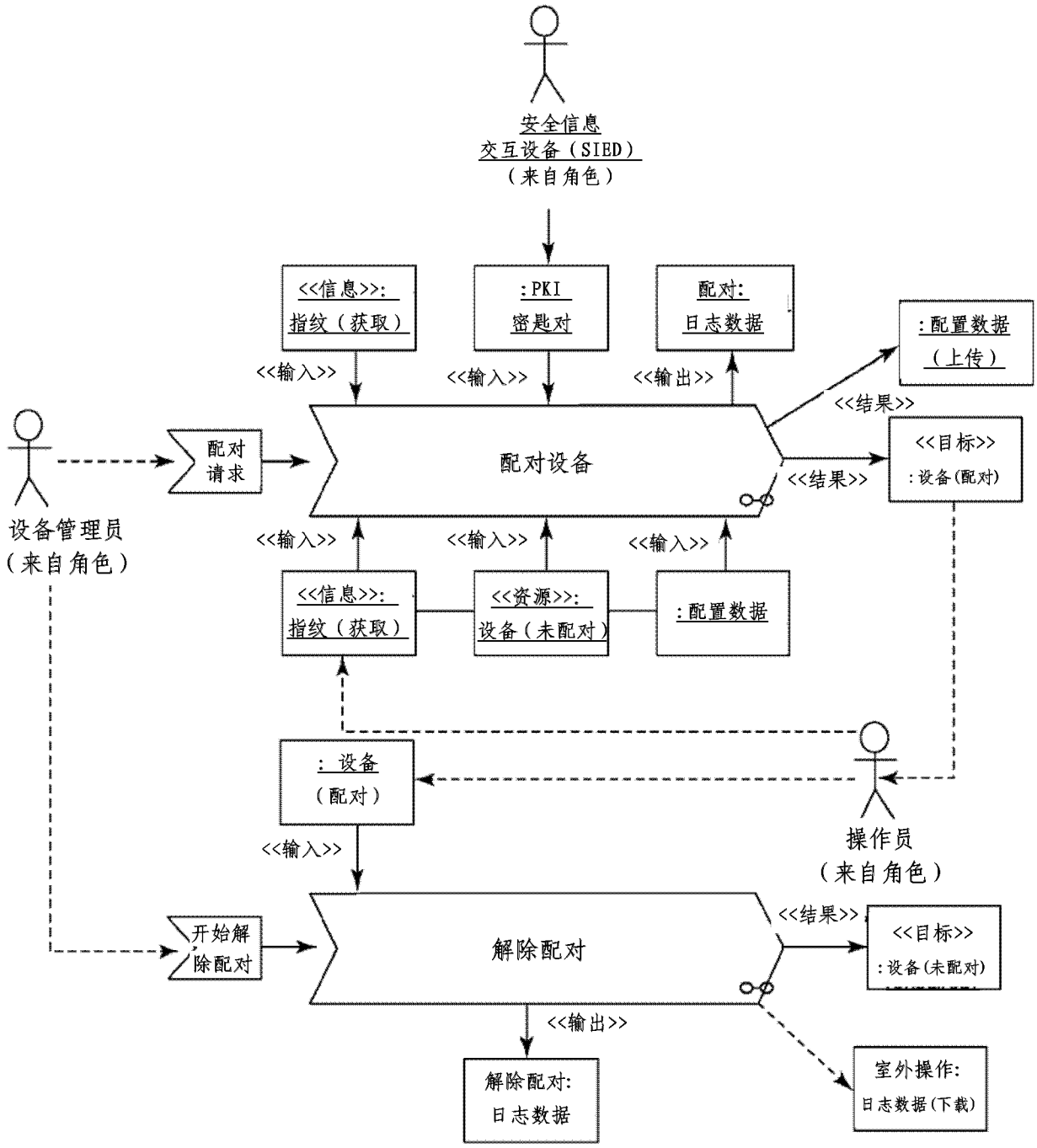

安全信息
交互设备（SIED）
（来自角色）
<<信息>>:
指纹（获取）
:PKI
密匙对
配对:
日志数据
:配置数据
（上传）
<<输入>>
<<输入>>
<<输出>>
<<结果>>
设备管理员
（来自角色）
配对
请求
配对设备
<<目标>>
:设备(配对)
<<结果>>
<<输入>>
<<输入>>
<<输入>>
<<信息>>:
指纹（获取）
<<资源>>:
设备（未配对）
:配置数据
: 设备
（配对）
操作员
（来自角色）
<<输入>>
开始解
除配对
解除配对
<<结果>>
<<目标>>
:设备(未配对)
<<输出>>
解除配对:
日志数据
室外操作:
日志数据(下载)

图 4A

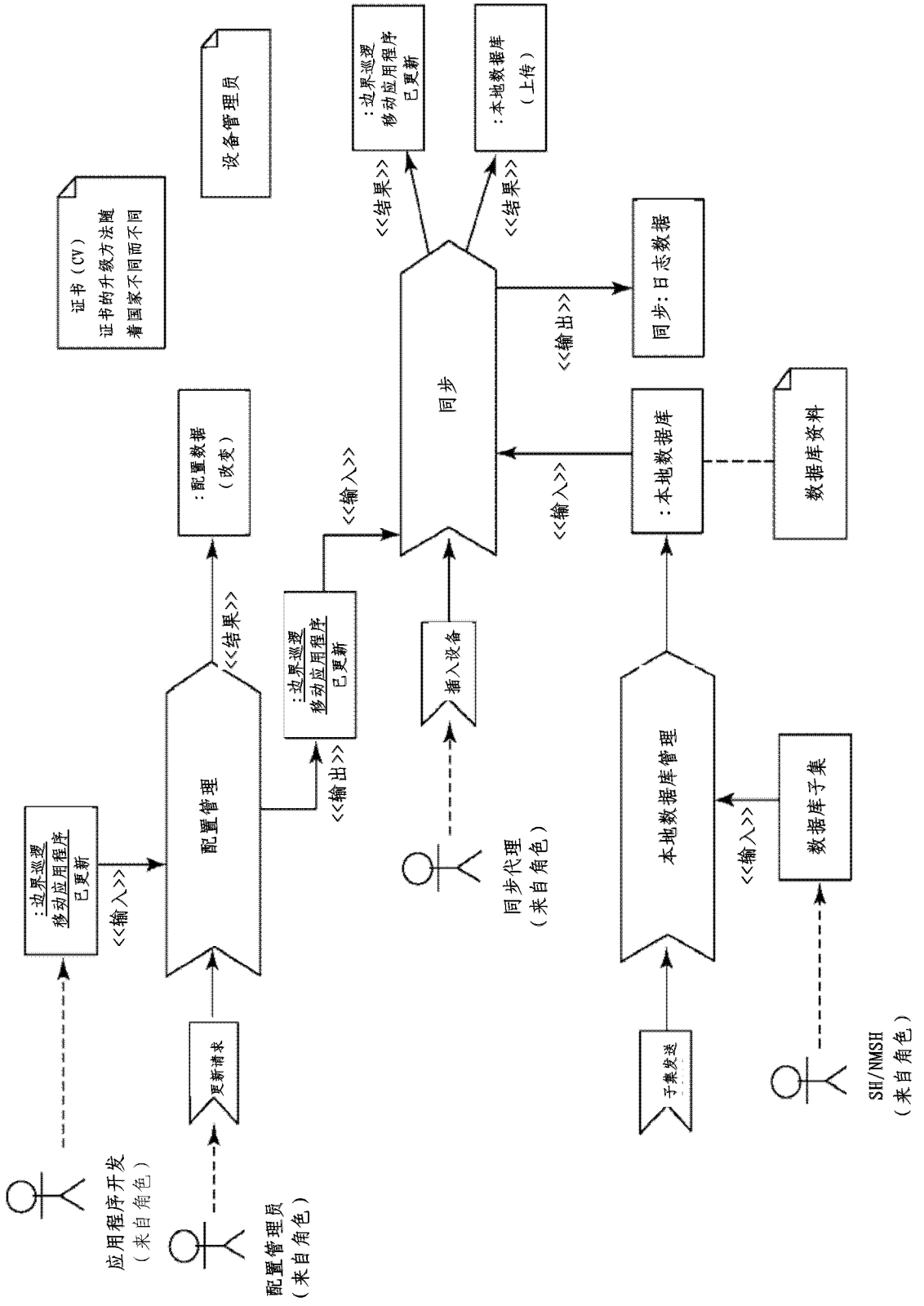

:边界巡逻
移动应用程序
已更新
<<输入>>
配置管理
<<结果>>
:配置数据
(改变)
<<输出>>
:边界巡逻
移动应用程序
已更新
<<输入>>
同步
<<结果>>
:边界巡逻
移动应用程序
已更新
<<结果>>
:本地数据库
(上传)
<<输出>>
同步:日志数据
<<输入>>
:本地数据库
数据库资料
本地数据库管理
<<输入>>
数据库子集
证书(CV)
证书的升级方法随
着国家不同而不同
设备管理员
更新请求
插入设备
子集发送
应用程序开发
(来自角色)
配置管理员
(来自角色)
同步代理
(来自角色)
SH/NMSH
(来自角色)

图 4B

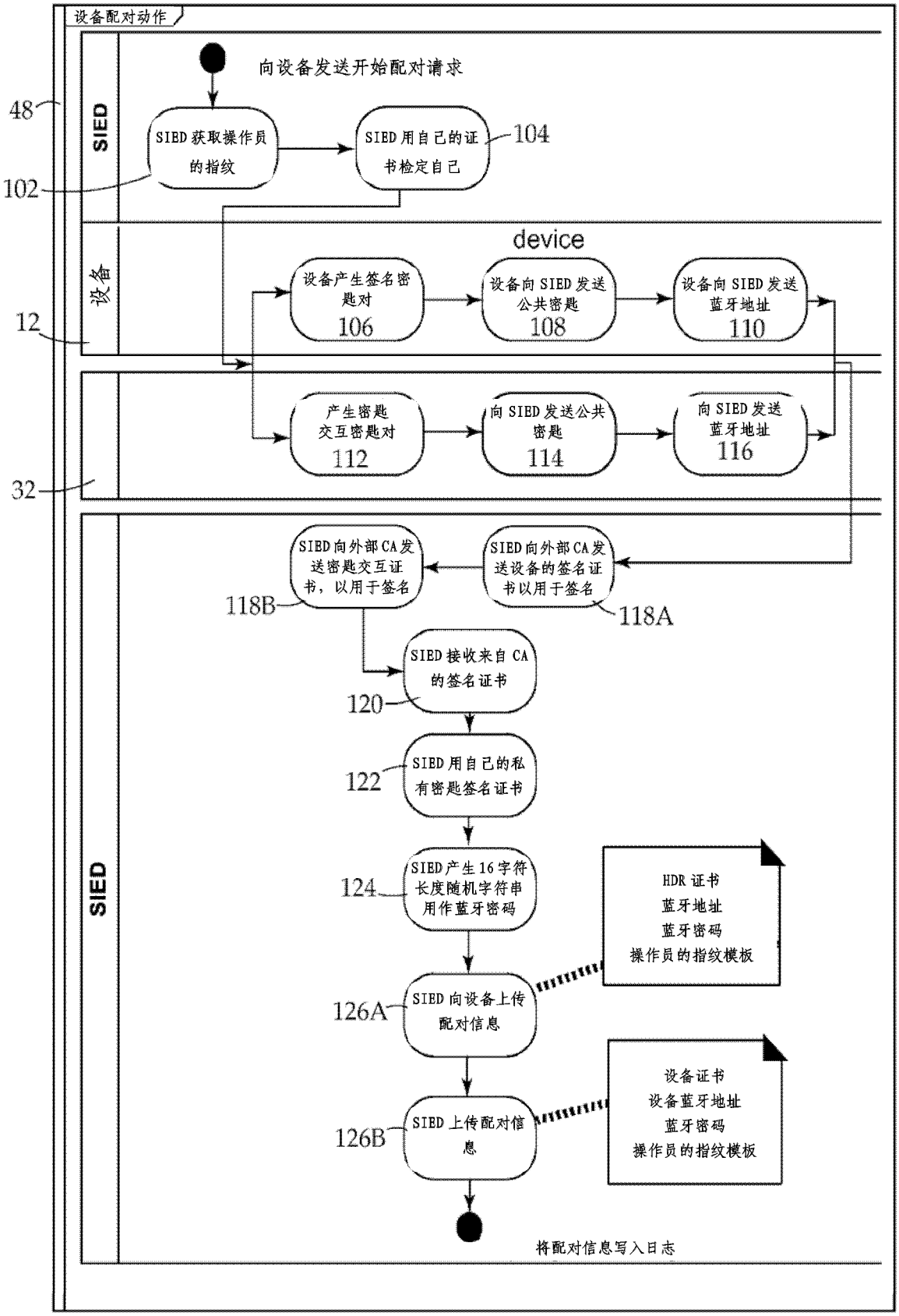

设备配对动作
SIED
向设备发送开始配对请求
48
SIED 获取操作员的指纹
102
SIED 用自己的证书检定自己
104
device
设备
设备产生签名密匙对
106
设备向 SIED 发送公共密匙
108
设备向 SIED 发送蓝牙地址
110
12
产生密匙交互密匙对
112
向 SIED 发送公共密匙
114
向 SIED 发送蓝牙地址
116
32
SIED
SIED 向外部 CA 发送密匙交互证书，以用于签名
SIED 向外部 CA 发送设备的签名证书以用于签名
118B
118A
SIED 接收来自 CA 的签名证书
120
SIED 用自己的私有密匙签名证书
122
SIED 产生 16 字符长度随机字符串用作蓝牙密码
124
HDR 证书
蓝牙地址
蓝牙密码
操作员的指纹模板
SIED 向设备上传配对信息
126A
设备证书
设备蓝牙地址
蓝牙密码
操作员的指纹模板
SIED 上传配对信息
126B
将配对信息写入日志

图 5A

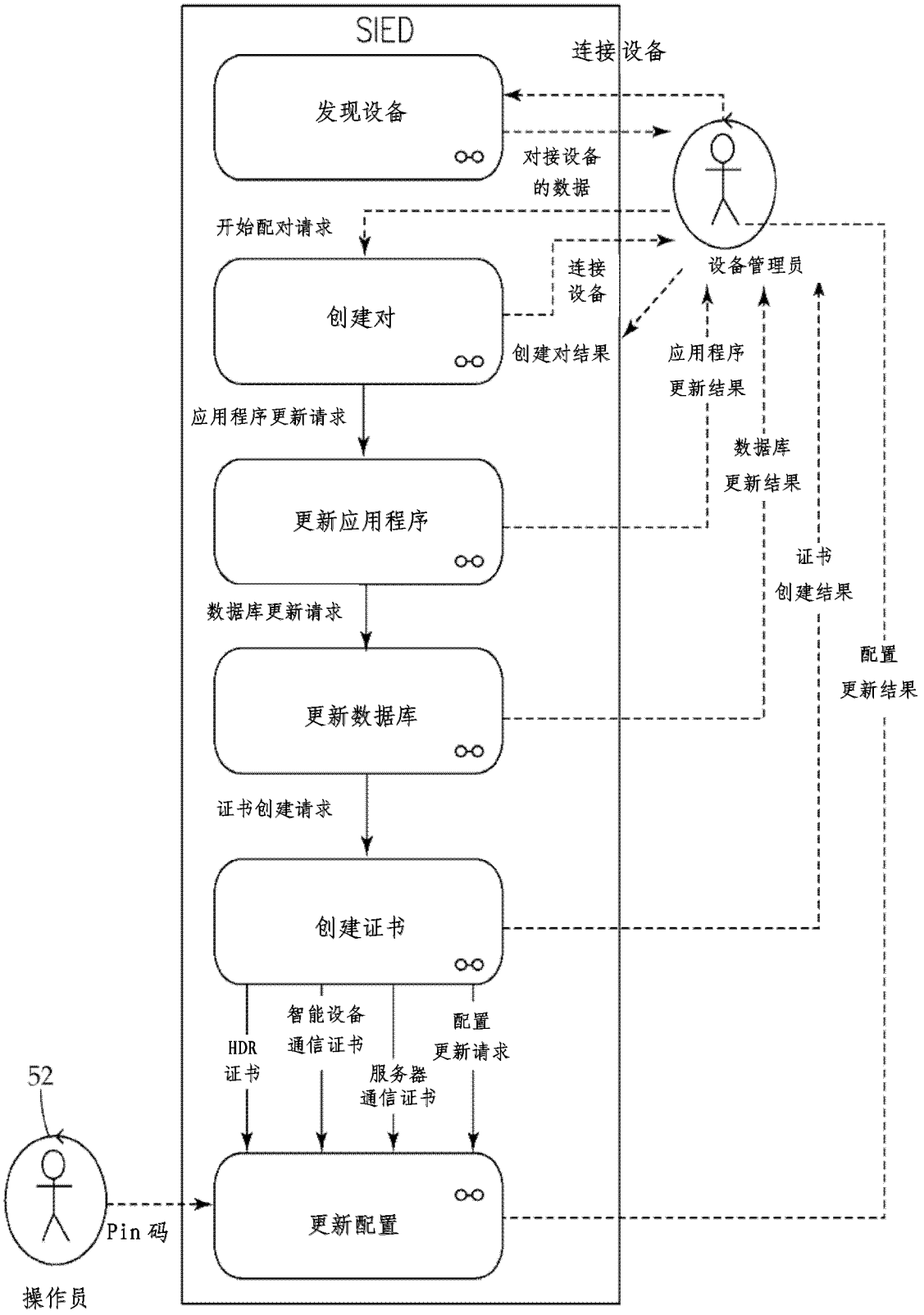

SIED
连接设备
发现设备
对接设备
的数据
开始配对请求
连接
设备
设备管理员
创建对
创建对结果
应用程序
更新结果
应用程序更新请求
数据库
更新结果
更新应用程序
证书
创建结果
数据库更新请求
配置
更新结果
更新数据库
证书创建请求
创建证书
智能设备
通信证书
配置
更新请求
HDR
证书
服务器
通信证书
52
Pin 码
更新配置
操作员

图 5B

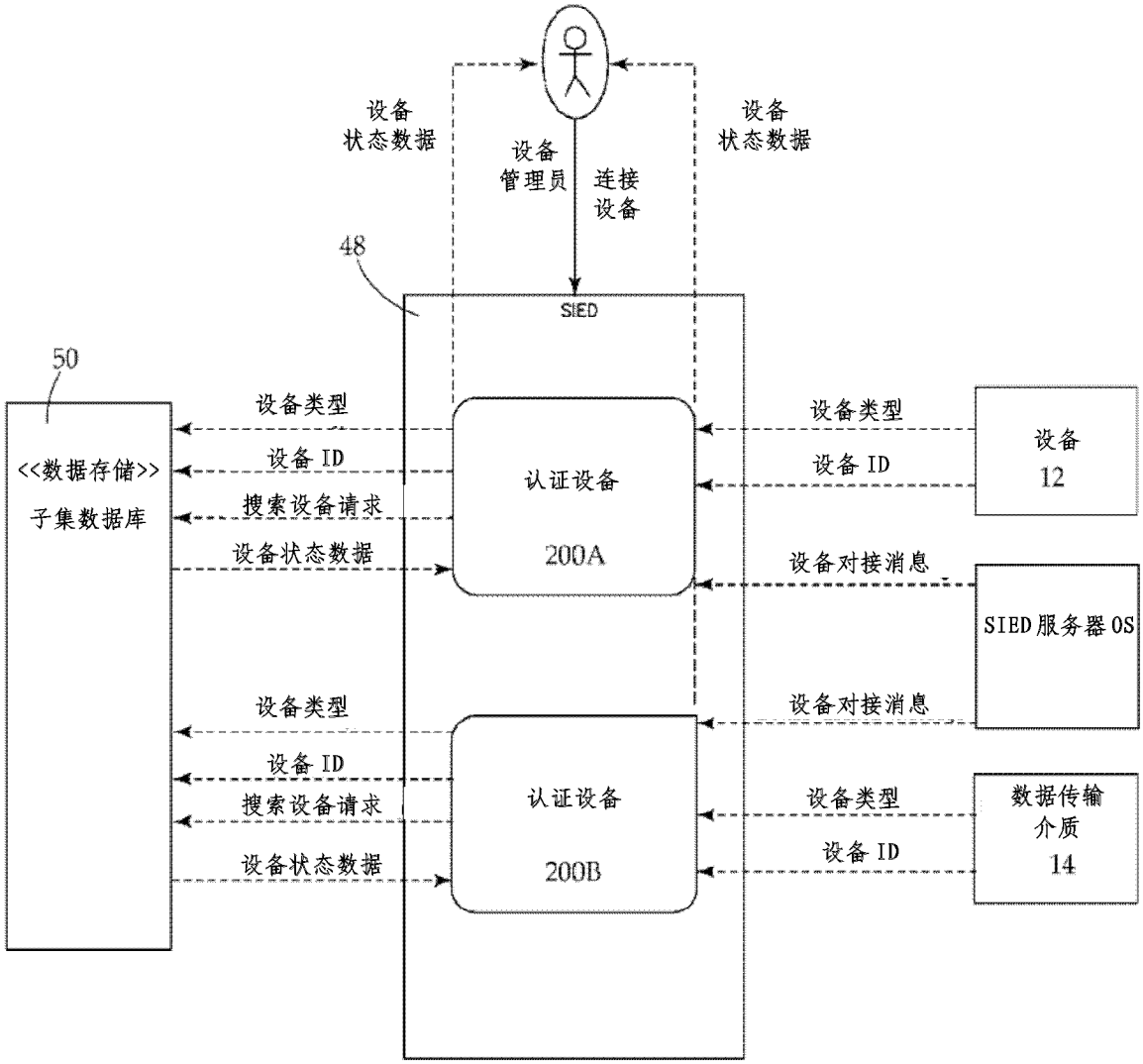

设备
状态数据
设备
管理员
连接
设备
设备
状态数据
48
SIED
50
<<数据存储>>
子集数据库
设备类型
设备 ID
搜索设备请求
设备状态数据
认证设备
200A
设备类型
设备 ID
设备
12
设备对接消息
SIED 服务器 OS
设备类型
设备 ID
搜索设备请求
设备状态数据
认证设备
200B
设备对接消息
设备类型
设备 ID
数据传输
介质
14

图 5C

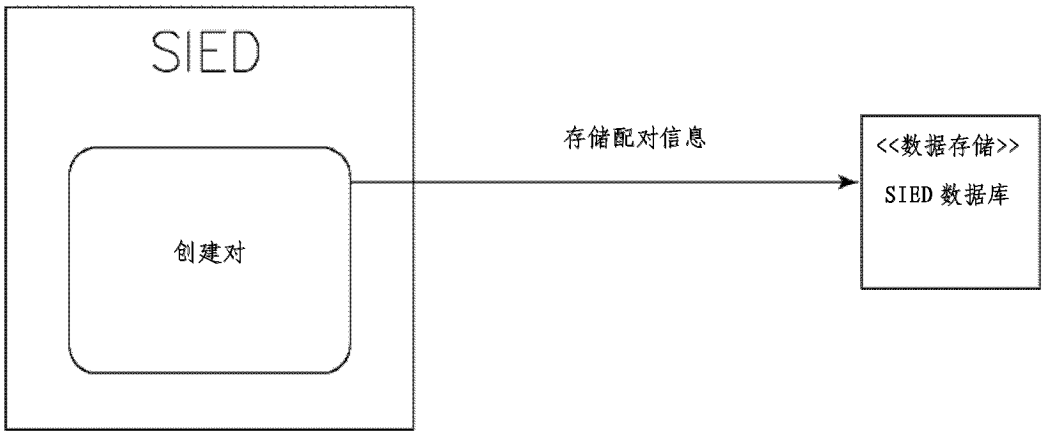

SIED
创建对
存储配对信息
<<数据存储>>
SIED 数据库

图 5D

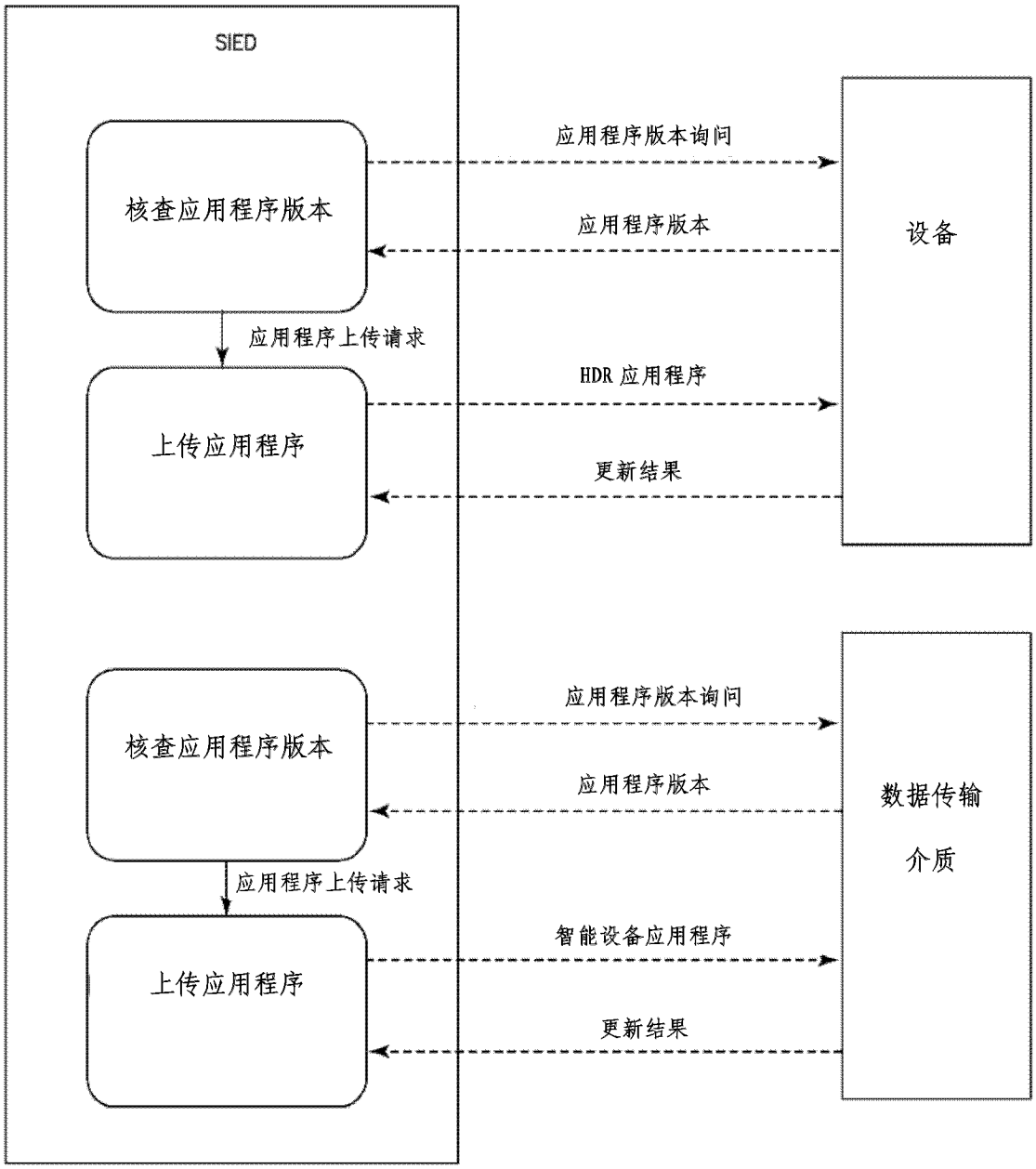

SIED
核查应用程序版本
应用程序版本询问
应用程序版本
设备
应用程序上传请求
上传应用程序
HDR 应用程序
更新结果
核查应用程序版本
应用程序版本询问
应用程序版本
数据传输
介质
应用程序上传请求
上传应用程序
智能设备应用程序
更新结果

图 5E

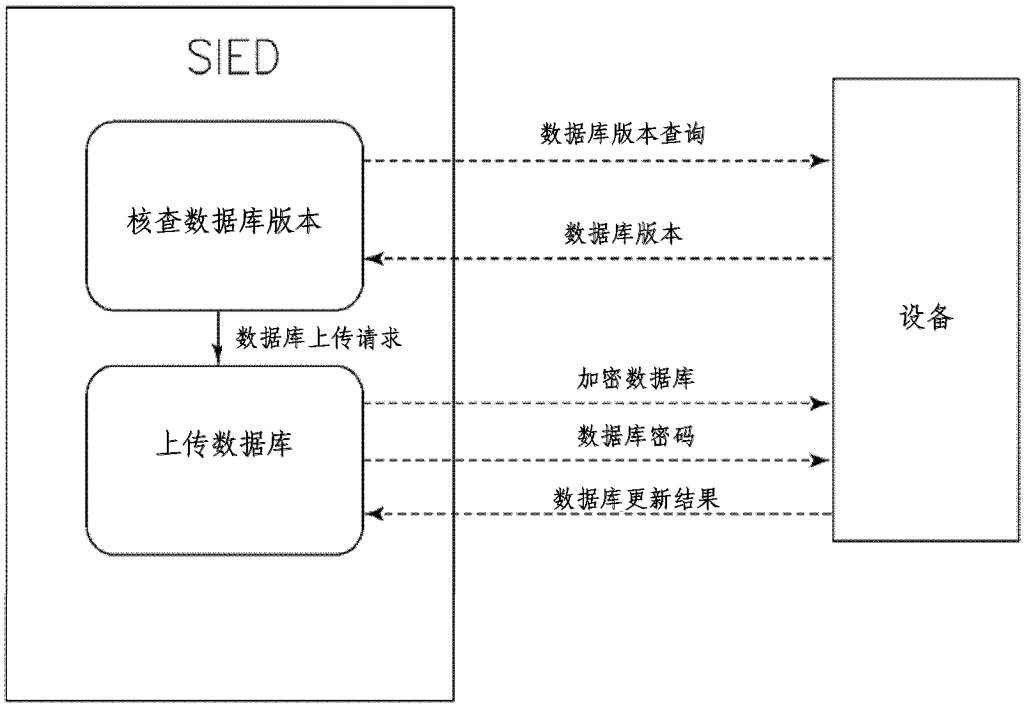

SIED
核查数据库版本
数据库上传请求
上传数据库
数据库版本查询
数据库版本
加密数据库
数据库密码
数据库更新结果
设备

图 5F

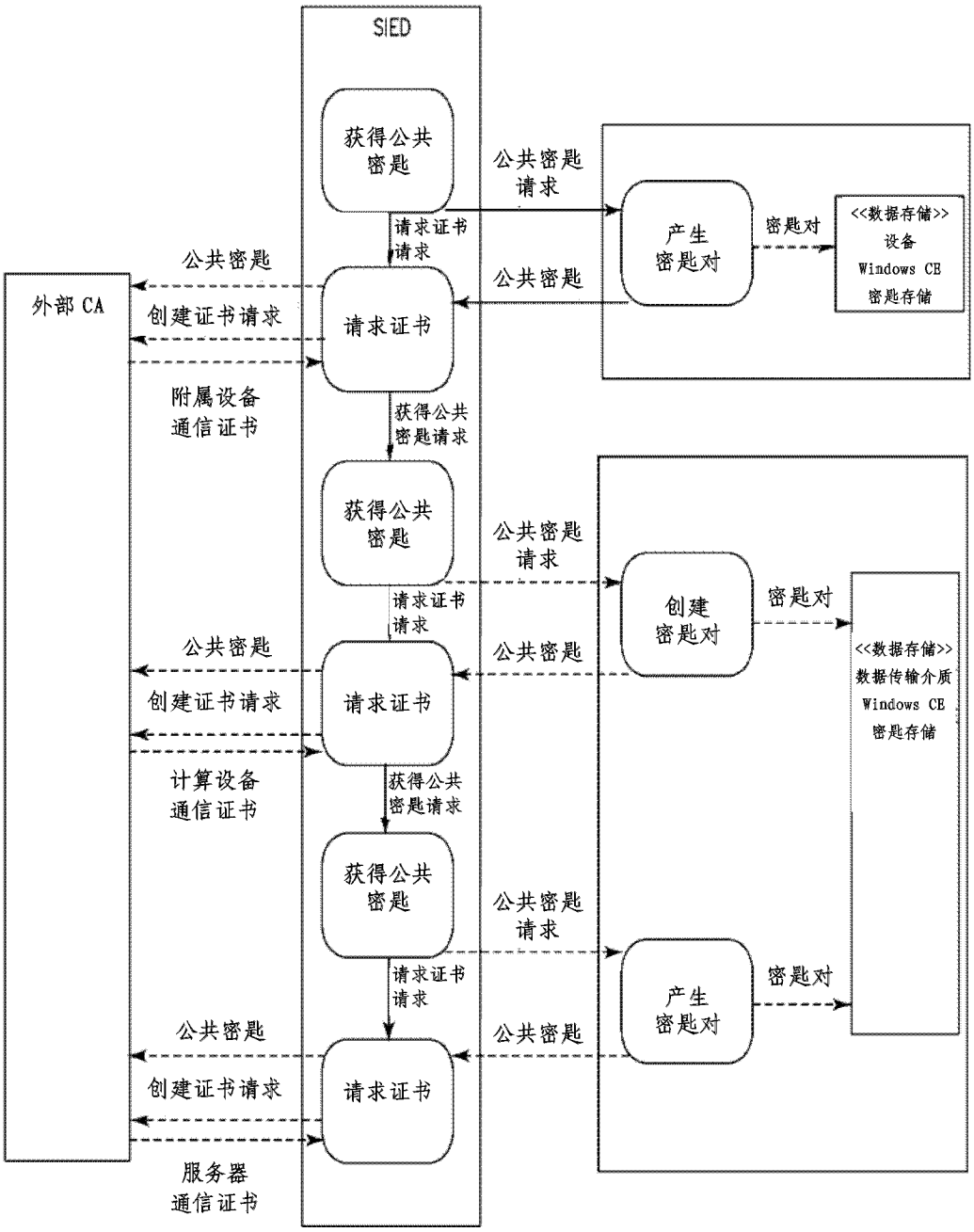

SIED
获得公共密匙
公共密匙请求
产生密匙对
密匙对
<<数据存储>>设备 Windows CE 密匙存储
请求证书请求
公共密匙
外部 CA
创建证书请求
请求证书
附属设备通信证书
获得公共密匙请求
获得公共密匙
公共密匙请求
创建密匙对
密匙对
<<数据存储>>数据传输介质 Windows CE 密匙存储
请求证书请求
公共密匙
创建证书请求
请求证书
计算设备通信证书
获得公共密匙请求
获得公共密匙
公共密匙请求
产生密匙对
密匙对
请求证书请求
公共密匙
创建证书请求
请求证书
服务器通信证书

图 5G

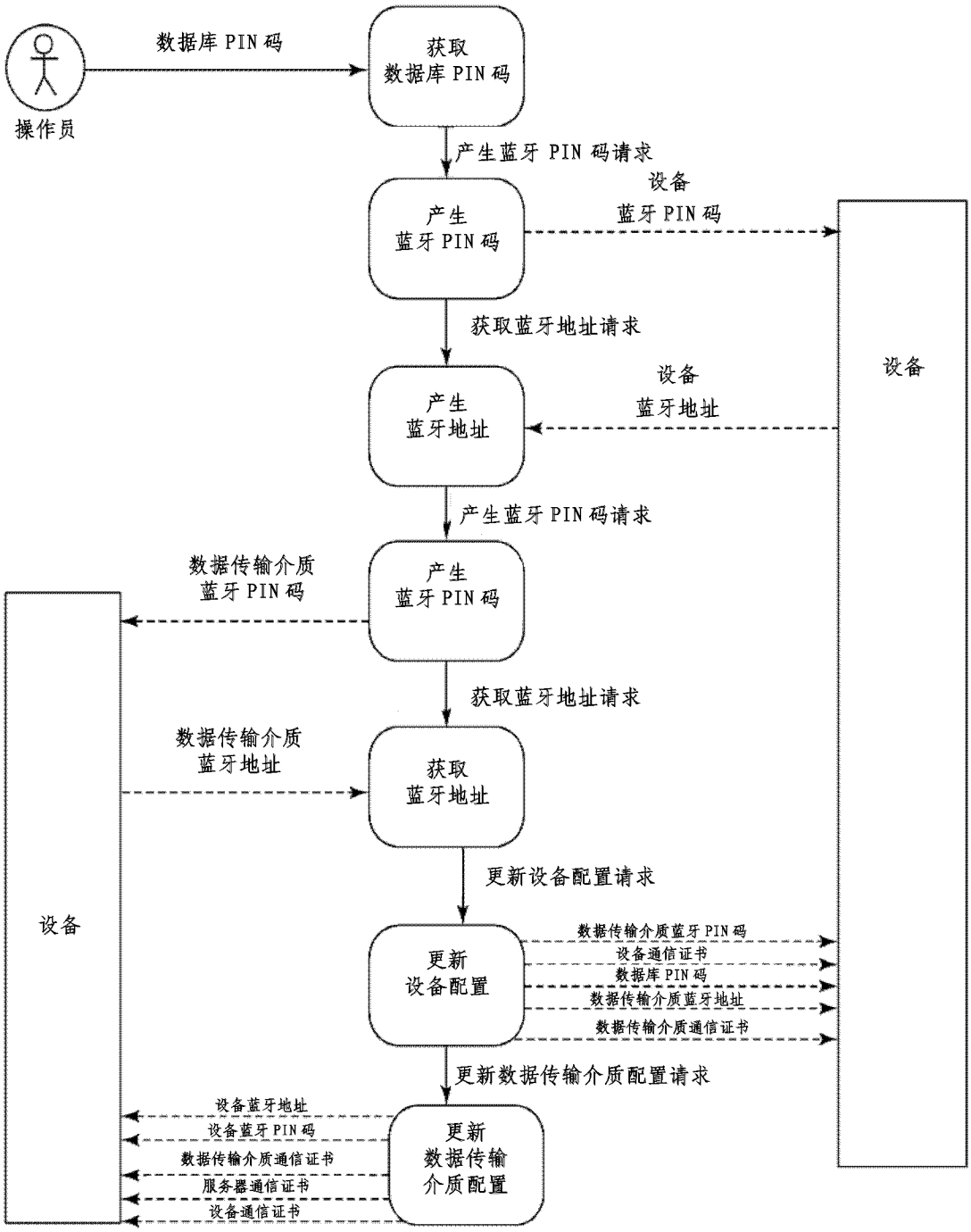

操作员
数据库 PIN 码
获取
数据库 PIN 码
产生蓝牙 PIN 码请求
产生
蓝牙 PIN 码
设备
蓝牙 PIN 码
设备
获取蓝牙地址请求
产生
蓝牙地址
设备
蓝牙地址
产生蓝牙 PIN 码请求
产生
蓝牙 PIN 码
数据传输介质
蓝牙 PIN 码
获取蓝牙地址请求
获取
蓝牙地址
数据传输介质
蓝牙地址
更新设备配置请求
更新
设备配置
数据传输介质蓝牙 PIN 码
设备通信证书
数据库 PIN 码
数据传输介质蓝牙地址
数据传输介质通信证书
更新数据传输介质配置请求
更新
数据传输
介质配置
设备蓝牙地址
设备蓝牙 PIN 码
数据传输介质通信证书
服务器通信证书
设备通信证书
设备

图 5H

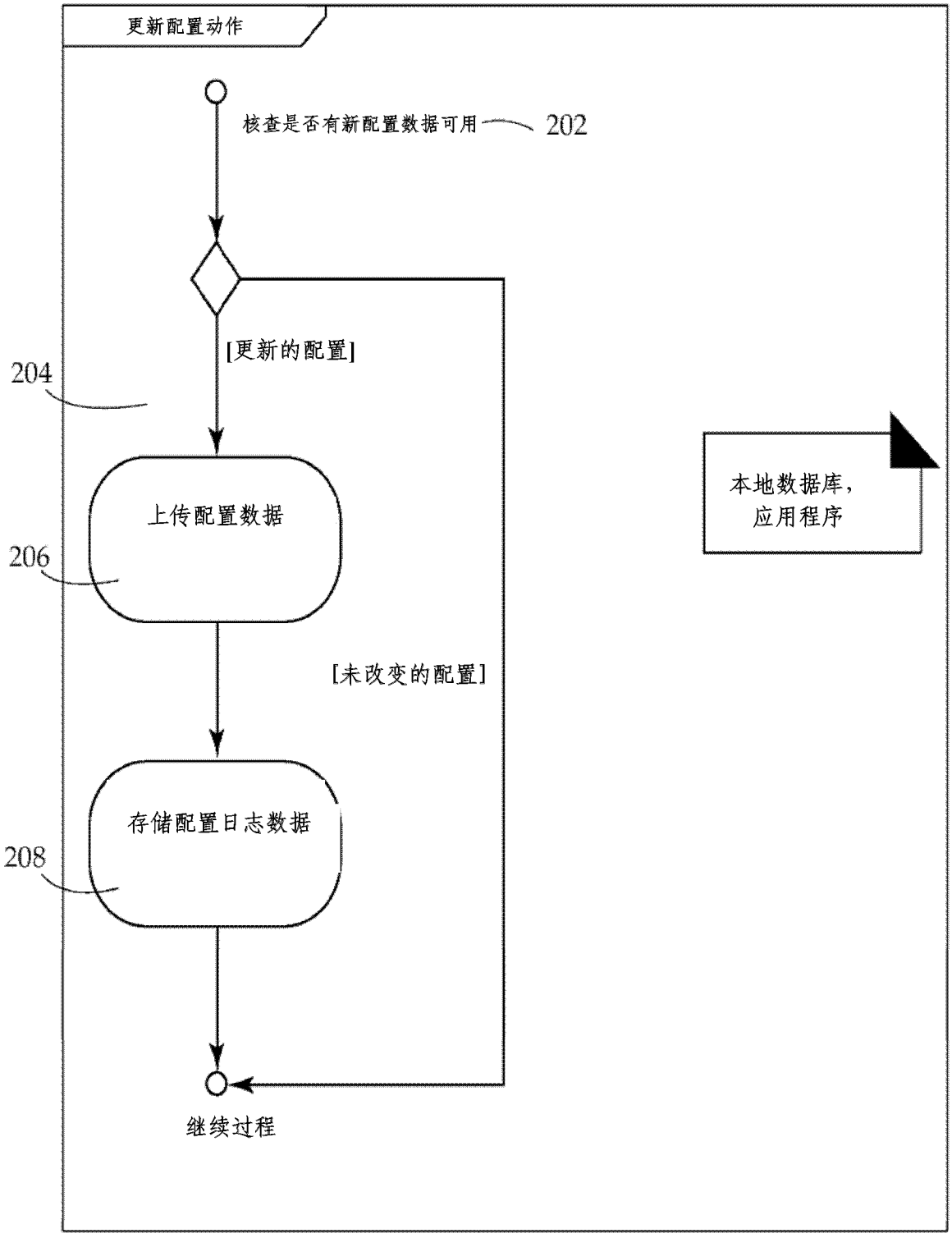

更新配置动作
核查是否有新配置数据可用
202
[更新的配置]
204
上传配置数据
206
[未改变的配置]
存储配置日志数据
208
继续过程
本地数据库，
应用程序

图 6

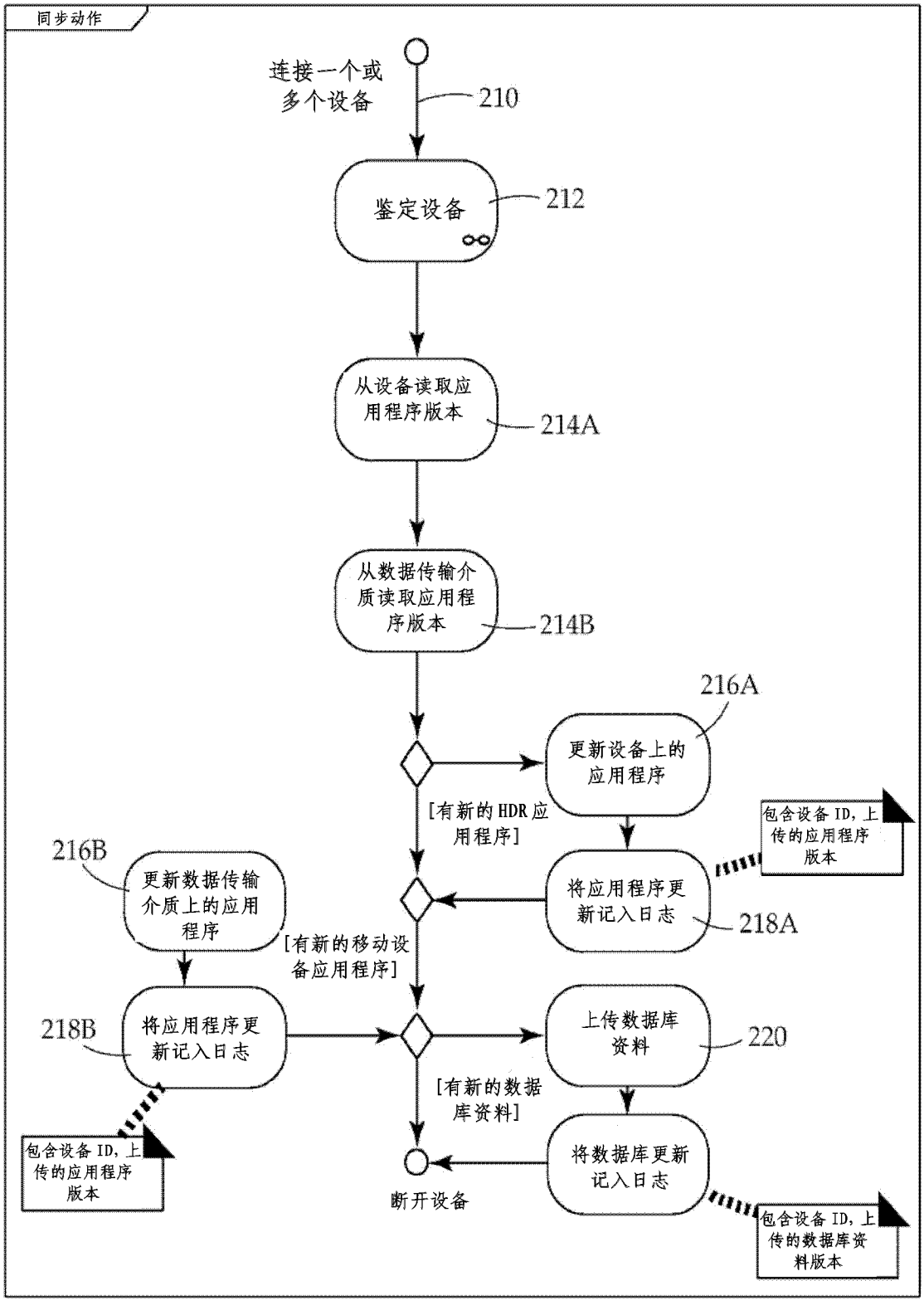

同步动作
连接一个或多个设备
210
鉴定设备
212
从设备读取应用程序版本
214A
从数据传输介质读取应用程序版本
214B
216A
更新设备上的应用程序
[有新的 HDR 应用程序]
包含设备 ID，上传的应用程序版本
216B
更新数据传输介质上的应用程序
将应用程序更新记入日志
218A
[有新的移动设备应用程序]
218B
将应用程序更新记入日志
上传数据库资料
220
[有新的数据库资料]
包含设备 ID，上传的应用程序版本
将数据库更新记入日志
断开设备
包含设备 ID，上传的数据库资料版本

图 7

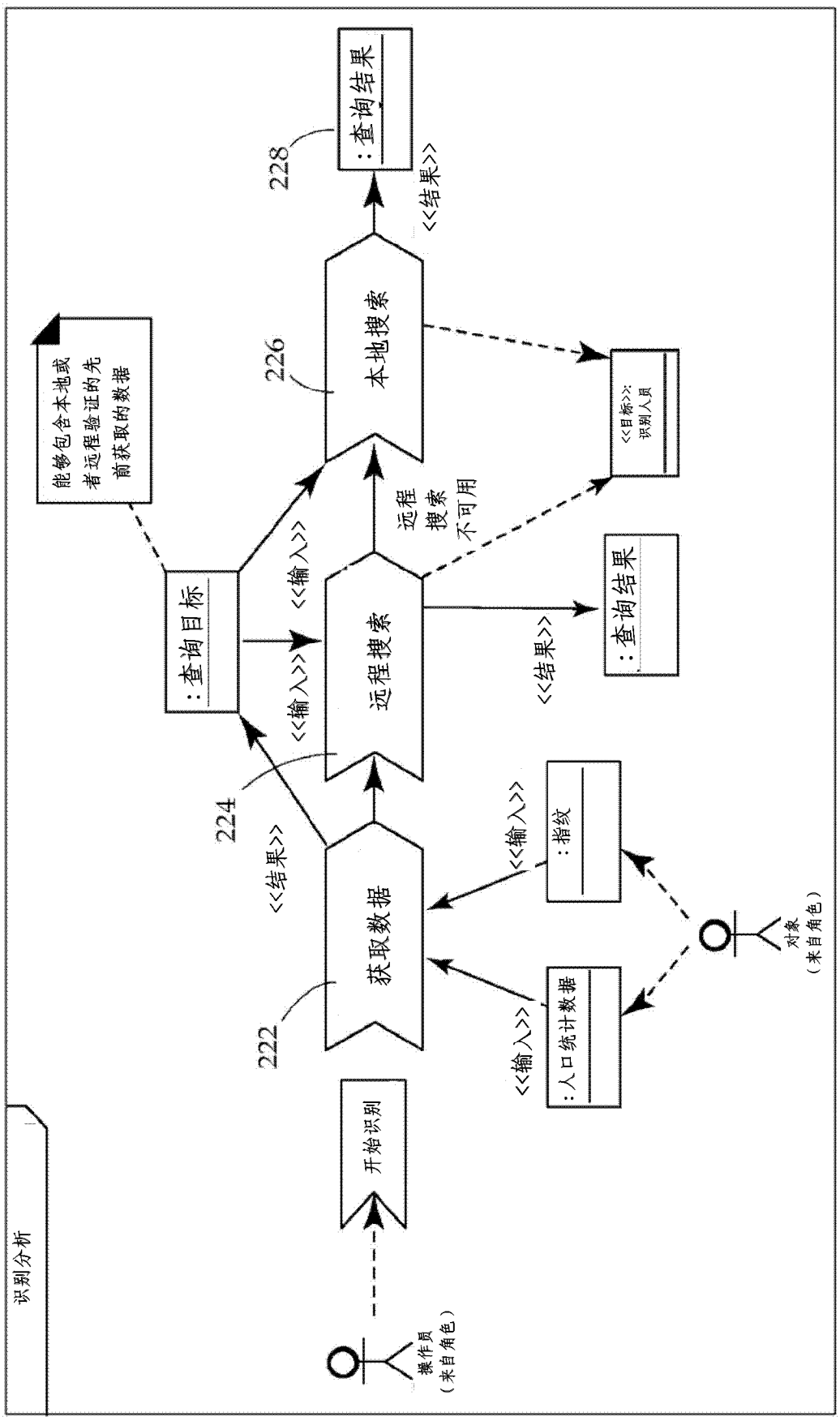

识别分析
开始识别
操作员
（来自角色）
222
获取数据
224
<<结果>>
:查询目标
<<输入>>
<<输入>>
远程搜索
远程
搜索
不可用
226
本地搜索
228
:查询结果
<<结果>>
能够包含本地或
者远程验证的先
前获取的数据
<<目标>>:
识别人员
:查询结果
<<结果>>
<<输入>>
:指纹
<<输入>>
:人口统计数据
对象
（来自角色）

图 8A

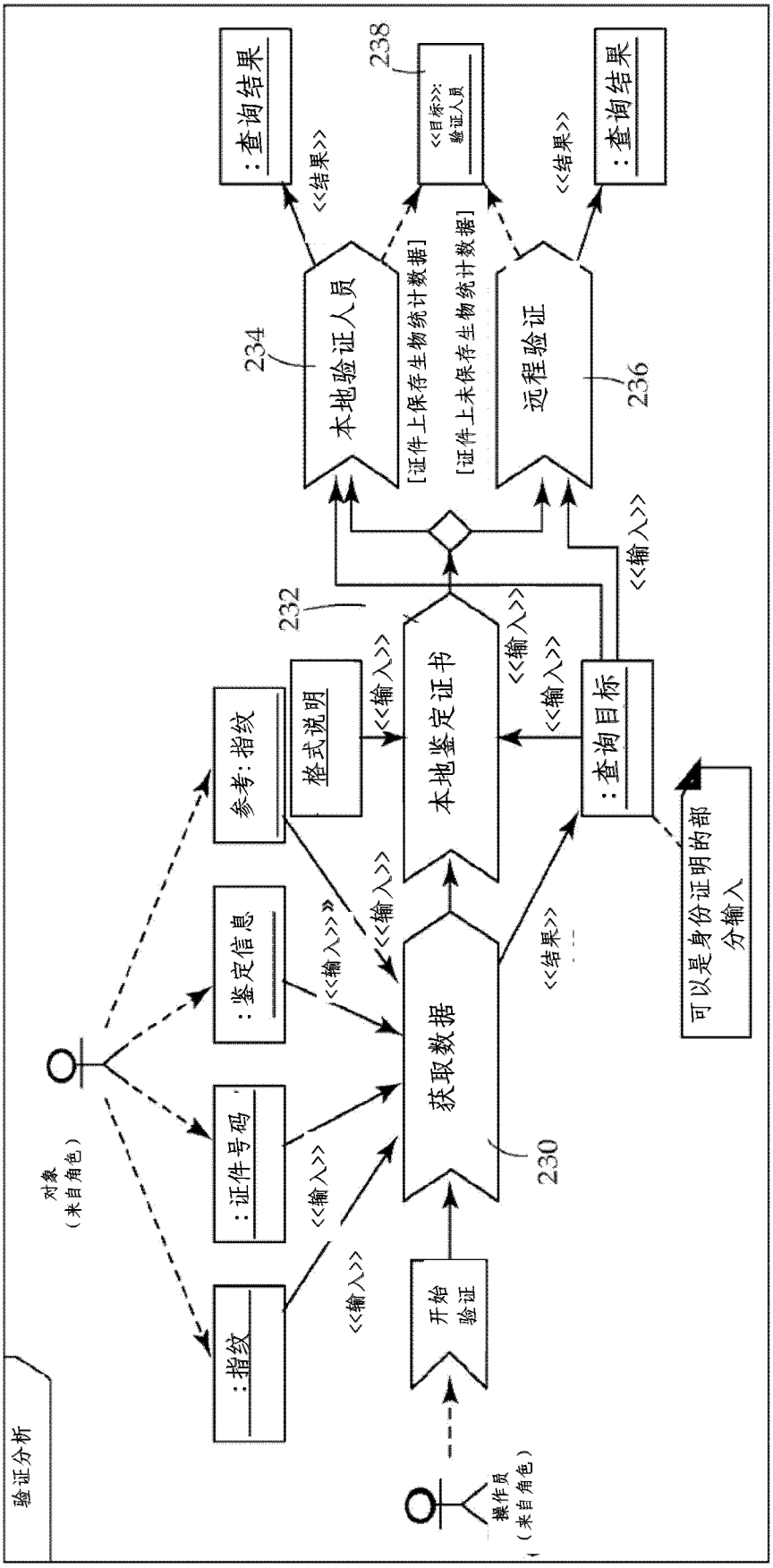

验证分析
对象
（来自角色）
操作员
（来自角色）
:指纹
:证件号码
:鉴定信息
参考: 指纹
格式说明
开始
验证
获取数据
230
本地鉴定证书
232
:查询目标
可以是身份证明的部分输入
本地验证人员
234
远程验证
236
:查询结果
:查询结果
238
<<目标>>:
验证人员
[证件上保存生物统计数据]
[证件上未保存生物统计数据]
<<输入>>
<<结果>>

图 8B

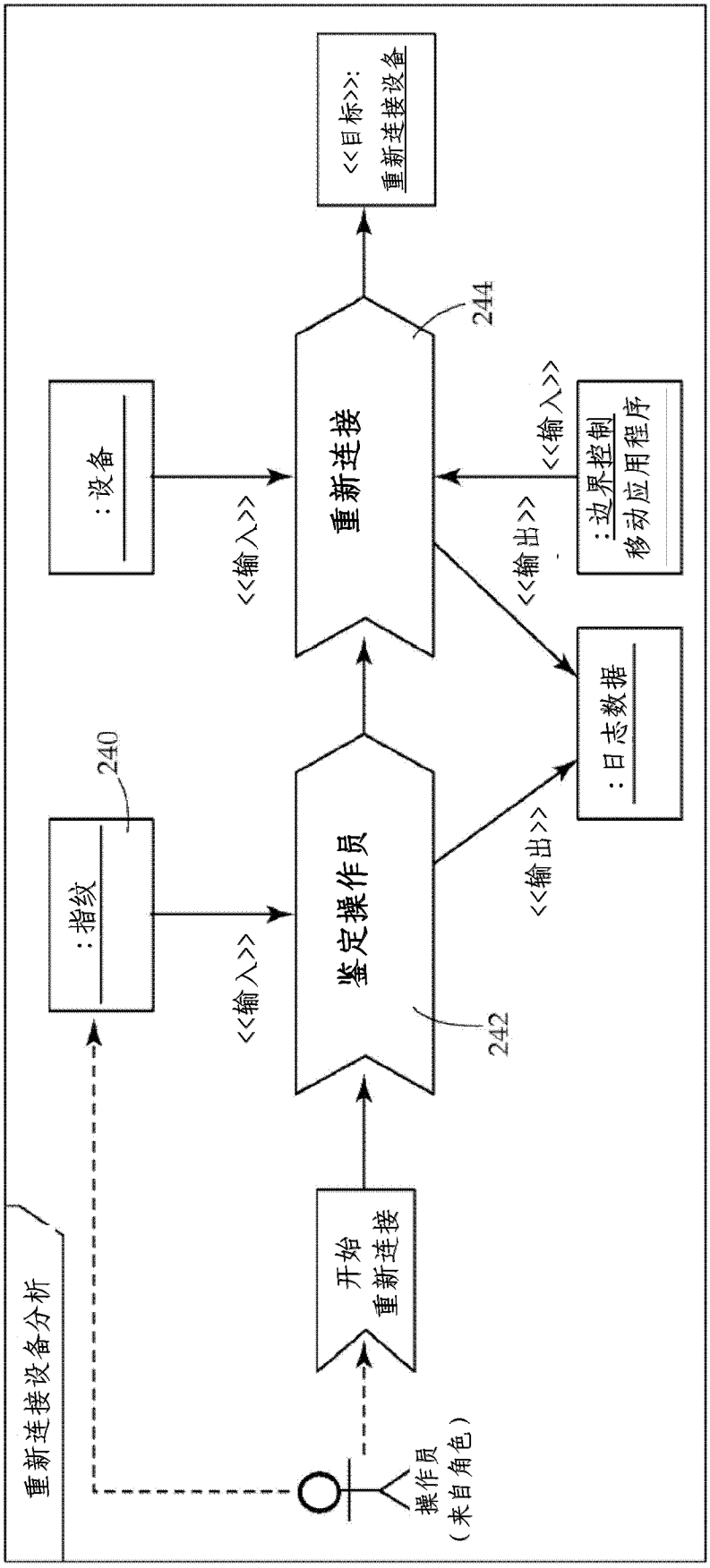

重新连接设备分析
操作员
（来自角色）
开始
重新连接
:指纹
240
:设备
<<输入>>
<<输入>>
鉴定操作员
242
重新连接
244
<<目标>>:
重新连接设备
<<输出>>
<<输出>>
:日志数据
<<输入>>
:边界控制
移动应用程序

图 8C

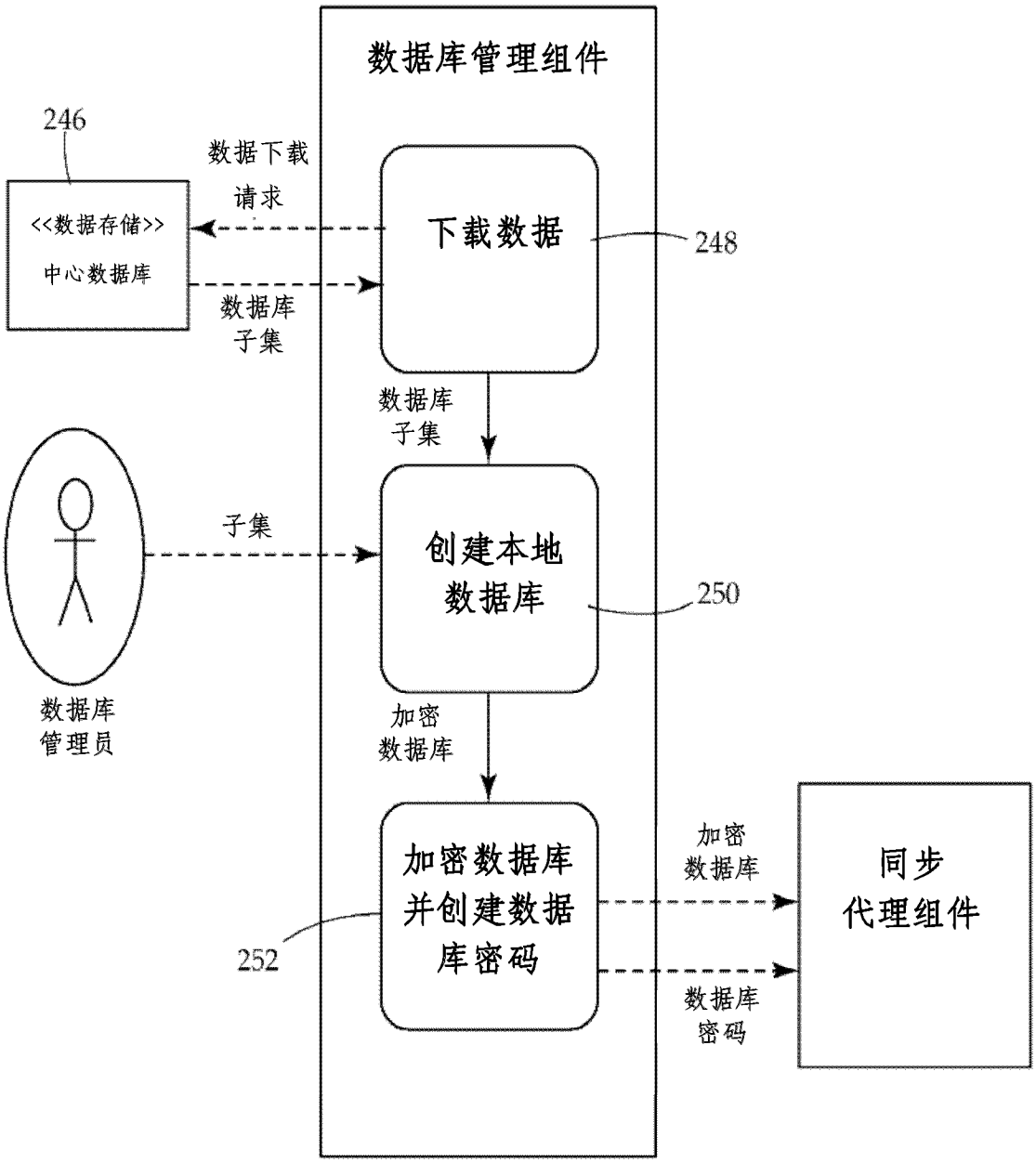

数据库管理组件
246
<<数据存储>>
中心数据库
数据下载
请求
数据库
子集
下载数据
248
数据库
子集
子集
创建本地
数据库
250
数据库
管理员
加密
数据库
加密数据库
并创建数据
库密码
252
加密
数据库
数据库
密码
同步
代理组件

图 9

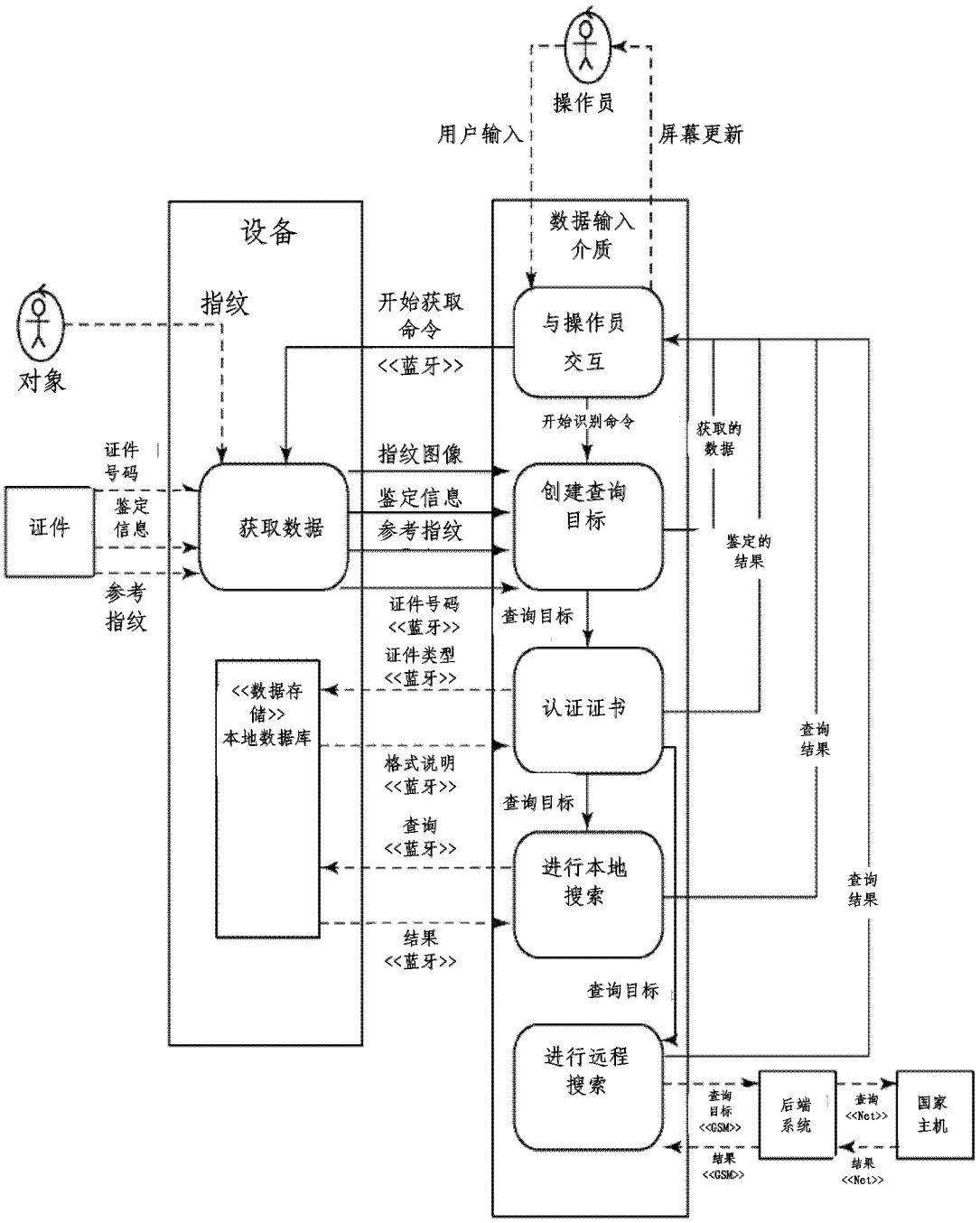

操作员
用户输入
屏幕更新
设备
数据输入介质
指纹
对象
开始获取命令
<<蓝牙>>
与操作员交互
开始识别命令
获取的数据
证件号码
证件
鉴定信息
参考指纹
获取数据
指纹图像
鉴定信息
参考指纹
创建查询目标
鉴定的结果
证件号码
<<蓝牙>>
查询目标
证件类型
<<蓝牙>>
<<数据存储>>
本地数据库
认证证书
查询结果
格式说明
<<蓝牙>>
查询目标
查询
<<蓝牙>>
进行本地搜索
查询结果
结果
<<蓝牙>>
查询目标
进行远程搜索
查询目标
<<GSM>>
后端系统
查询
<<Net>>
国家主机
结果
<<GSM>>
结果
<<Net>>

图 10A

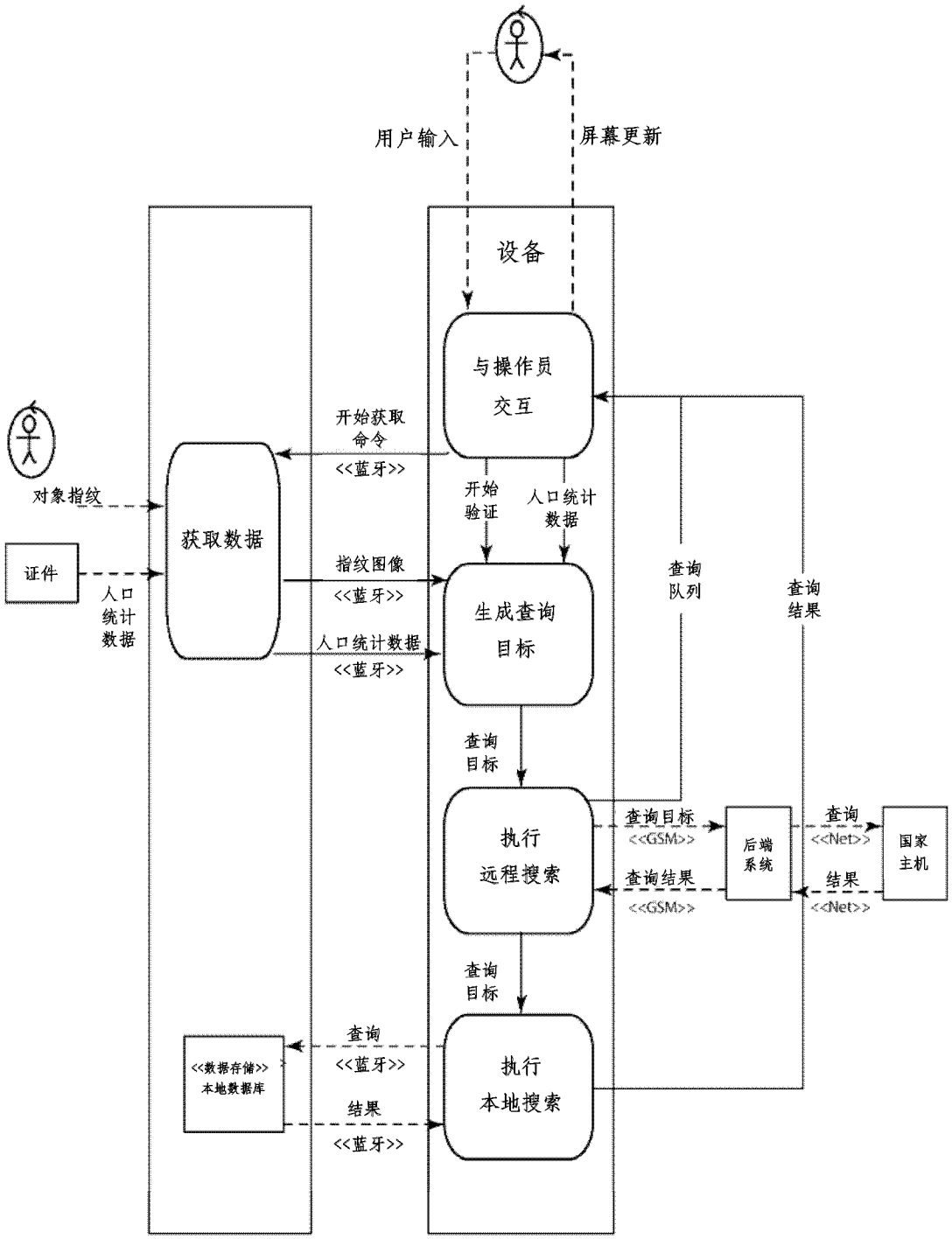

用户输入
屏幕更新
设备
与操作员
交互
开始获取
命令
<<蓝牙>>
对象指纹
证件
人口
统计
数据
获取数据
开始
验证
人口统计
数据
指纹图像
<<蓝牙>>
人口统计数据
<<蓝牙>>
生成查询
目标
查询
队列
查询
结果
查询
目标
执行
远程搜索
查询目标
<<GSM>>
查询结果
<<GSM>>
后端
系统
查询
<<Net>>
结果
<<Net>>
国家
主机
查询
目标
<<数据存储>>
本地数据库
查询
<<蓝牙>>
结果
<<蓝牙>>
执行
本地搜索

图 10B

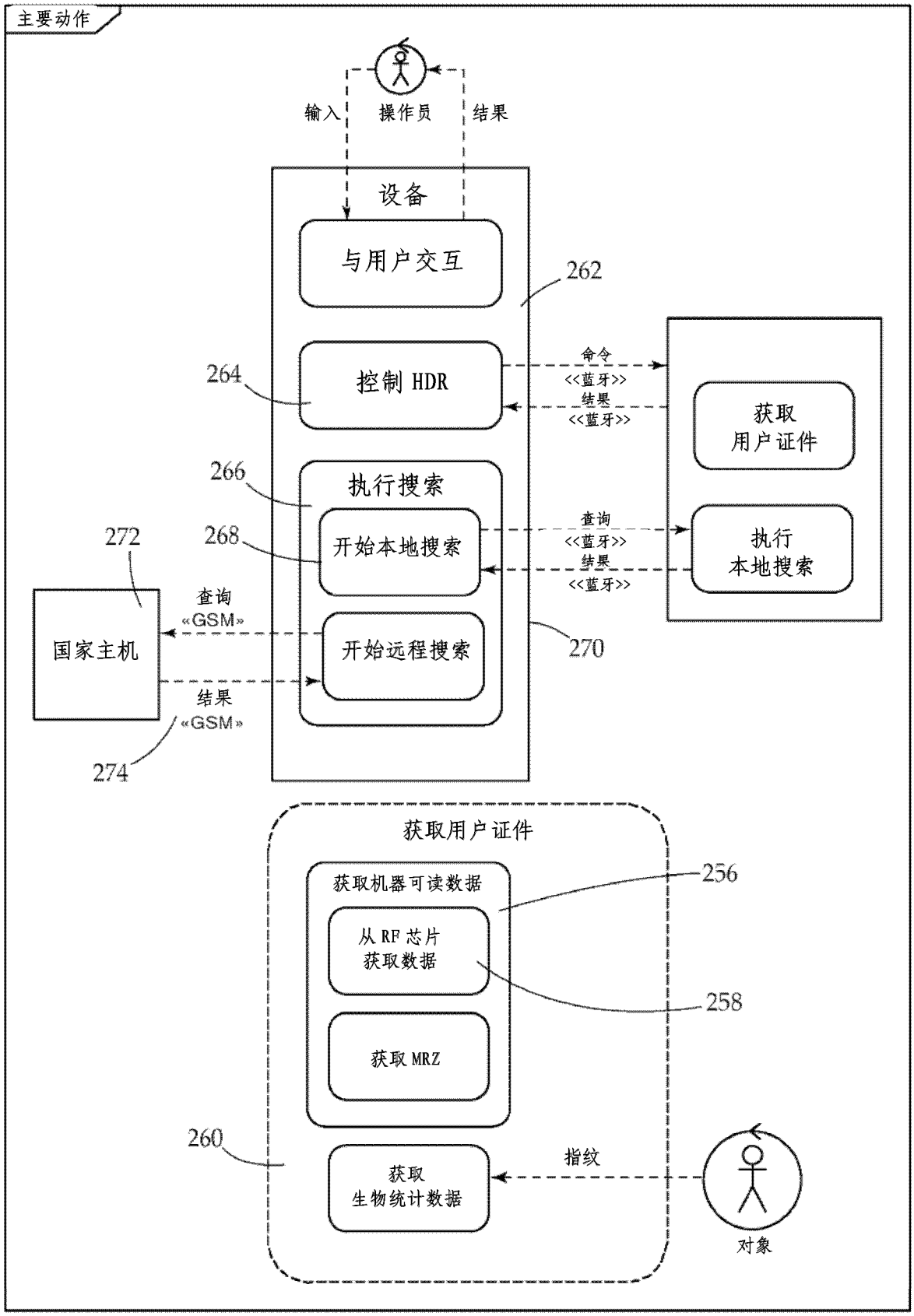

主要动作
输入
操作员
结果
设备
与用户交互
262
控制 HDR
264
命令
<<蓝牙>>
结果
<<蓝牙>>
获取
用户证件
执行搜索
266
开始本地搜索
268
查询
<<蓝牙>>
结果
<<蓝牙>>
执行
本地搜索
272
国家主机
查询
«GSM»
开始远程搜索
270
结果
«GSM»
274
获取用户证件
获取机器可读数据
256
从 RF 芯片
获取数据
258
获取 MRZ
260
获取
生物统计数据
指纹
对象

图 10C

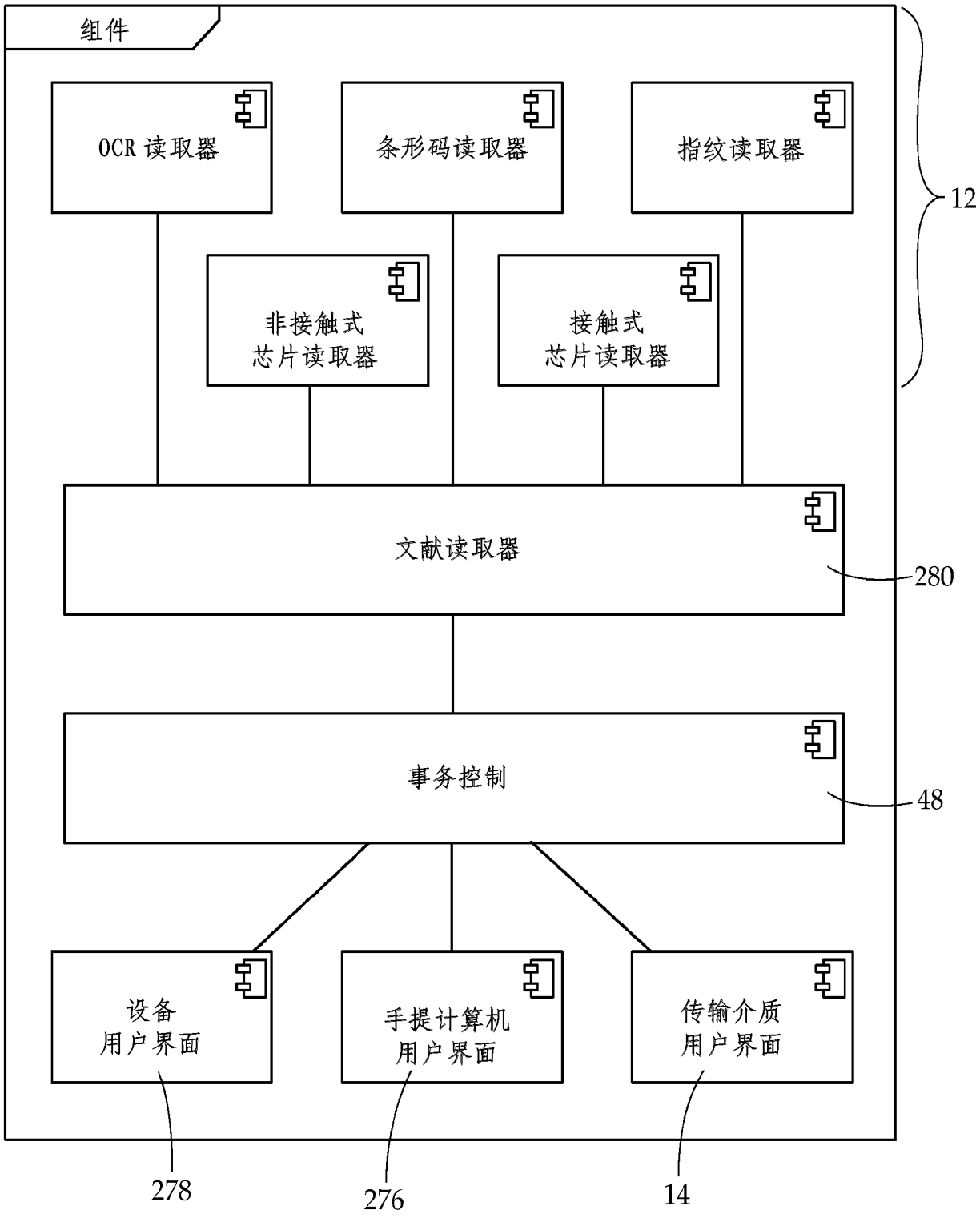

组件
OCR 读取器
条形码读取器
指纹读取器
12
非接触式
芯片读取器
接触式
芯片读取器
文献读取器
280
事务控制
48
设备
用户界面
手提计算机
用户界面
传输介质
用户界面
278
276
14

图 11