(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 101263478 B
(45)授权公告日 2012.10.10

(21)申请号 200680033092.7

(22)申请日 2006.09.06

(30)优先权数据
11/223,255 2005.09.09 US

(85)PCT申请进入国家阶段日
2008.03.10

(86)PCT申请的申请数据
PCT/US2006/034581 2006.09.06

(87)PCT申请的公布数据
WO2007/032968 EN 2007.03.22

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 M·德麦罗 M·A·戴拉

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌

(51)Int.Cl.
G06F 17/00(2006.01)

(56)对比文件
CN 1490736 A,2004.04.21, 全文.
US 6321339 B1,2001.11.20, 全文.
CN 1536871 A,2004.10.13, 说明书第2页第20行-第14页第15行.
US 6862696 B1,2005.03.01, 全文.

审查员 苏珊珊

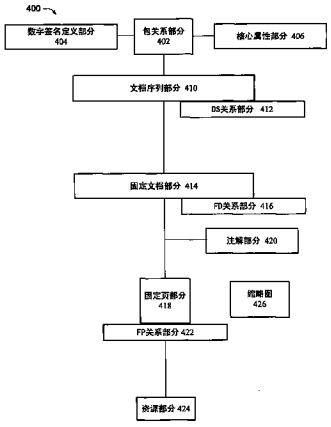
权利要求书 2 页 说明书 9 页 附图 8 页

(54)发明名称

数字签署策略的系统和方法

(57)摘要

描述了涉及有指导的数字签署策略的技术。在一实例中,一种系统包括用于将文档作为多个逻辑部分来存储的装置。该系统还包括用于建立当将数字签名应用于该文档时的文档配置的装置,以及用于指示该文档配置随后是否被更改的装置。



CN 101263478 B

1. 一种用于数字签署策略的系统，包括：

用于将文档作为多个逻辑部分来存储的装置；

用于从各逻辑部分之间的相互关系以及各逻辑部分内的数据建立当将一数字签名应用于所述文档时的文档配置的装置；以及

用于指示所述文档配置随后是否被更改的装置，

其中所述用于从各逻辑部分之间的相互关系以及各逻辑部分内的数据建立当将一数字签名应用于所述文档时的文档配置的装置包括一组数字签署策略规则，所述规则定义了所述逻辑部分中对所述文档配置作出贡献的一子集，使得如果所述子集的单独逻辑部分被更改，则所述文档配置被认为被更改。

2. 如权利要求 1 所述的系统，其特征在于，所述用于将文档作为多个逻辑部分来存储的装置包括 XML 纸件规范文档格式。

3. 如权利要求 1 所述的系统，其特征在于，所述用于从各逻辑部分之间的相互关系以及各逻辑部分内的数据建立当将一数字签名应用于所述文档时的文档配置的装置定义所述多个逻辑部分中的哪些部分要以所述数字签名来签署。

4. 如权利要求 1 所述的系统，其特征在于，所述一组数字签署策略规则还定义了所述逻辑部分中可在不更改所述文档配置的情况下被更改的第二子集。

5. 如权利要求 4 所述的系统，其特征在于，所述用于从各逻辑部分之间的相互关系以及各逻辑部分内的数据建立当将一数字签名应用于所述文档时的文档配置的装置还允许用户应用所述数字签名来指定所述第二子集中当被更改时被认为更改所述文档配置的的单独部分。

6. 如权利要求 1 所述的系统，其特征在于，所述用于指示所述文档配置随后是否被更改的装置包括被配置成指示在所述文档配置被更改的情况中所述数字签名为无效的界面。

7. 一种用于数字签署策略的方法，包括：

依据一数字签署策略来确定一文档中要以用户的数字签名来包括的部分；和

在从各部分之间的相互关系以及各部分内的数据建立的当前文档配置中向所述文档应用所述数字签名，其中所述数字签署策略定义了所述部分中对所述文档配置作出贡献的一子集，使得如果所述子集的单独部分被更改，则所述文档配置被认为被更改。

8. 如权利要求 7 所述的方法，其特征在于，所述部分包括所述文档中所包含的所有文档序列部分和相关联的关系部分、所有固定文档部分和相关联的关系部分、所有固定页部分和相关联的固定页关系部分、所有资源部分、以及所有数字签名定义部分。

9. 如权利要求 7 所述的方法，其特征在于，还包括验证所述数字签名。

10. 如权利要求 7 所述的方法，其特征在于，还包括在所述部分中的任一个随后被更改时使所述用户的数字签名无效。

11. 如权利要求 7 所述的方法，其特征在于，还包括允许用户指定核心属性、注解和数字签名中任何一个或多个可否在不使所述用户的数字签名无效的情况下被改变。

12. 如权利要求 11 所述的方法，其特征在于，在用户指定改变核心属性使用户的数字签名无效并且核心属性部分存在的情况中，则所述应用包括将所述用户的数字签名应用于所述核心属性部分。

13. 如权利要求 11 所述的方法，其特征在于，在用户指定改变核心属性不会使用户的

数字签名无效并且核心属性部分存在的情况中，则所述应用不包括将所述数字签名应用于所述核心属性部分。

14. 如权利要求 11 所述的方法，其特征在于，在用户指定改变核心属性不会使用户的数字签名无效并且核心属性部分不存在的情况中，则在数字地签署之前创建所述核心属性部分。

数字签署策略的系统和方法

技术领域

[0001] 本发明涉及数字签名。

[0002] 背景技术

[0003] 无纸化技术的采用已经因许多用户不愿意采用数字签名来签署文档而受到阻碍。这些用户中的大部分对于文档的数字签名实际表示什么意思感到困惑。用户还察觉出一旦该文档离开了用户的直接控制则对已签署的文档失去控制。例如，尽管文档上有用户的数字签名，但恶意的第三方仍可操控该文档。结果，数字文档通常被打印出来然后用惯例的笔墨方式来签署。在这一点上，不管该文档是扫描的还是作为硬拷贝来处理的，许多潜在的优势都消失。

[0004] 发明内容

[0005] 描述了涉及有指导的数字签署策略的技术。在一实例中，一种系统包括用于将文档作为多个逻辑部分来存储的装置。该系统还包括用于在将数字签名应用于该文档时建立文档配置的装置，以及用于指示该文档配置随后是否被更改的装置。

[0006] 提供本概述以便以简化的形式介绍将在以下详细描述中进一步描述的一些概念。本概述并非意在确定所要求保护的主题的关键或必要特征，也并非意在用来帮助确定所要求保护的主题的范围。

[0007] 附图说明

[0008] 图 1 示出了根据一实现的其上能实施数字签署策略的一示例性系统。

[0009] 图 2-6 示出了根据一实现的其中能实施数字签署策略的示例性文档配置。

[0010] 图 7 示出了根据一实现的其上能实施数字签署策略的环境中的示例性系统、设备及组件。

[0011] 图 8 示出了根据一实现的涉及数字签署策略的示例性流程图。

[0012] 具体实施方式

[0013] 概要

[0014] 所描述的技术涉及用于维持如数字地签署时的电子文档的数字签署策略。例 如，发布用户可撰写文档并当他或她对其配置满意时决定数字地签署该文档。该数字签署策略运作于基础数据级上来确立文档的哪些部分用数字签名来包括以便维持文档处于被用户签署时的配置。当根据数字签署策略来应用数字签名时，对文档的违反该策略的任何后续操纵都使得该数字签名无效。因此，数字签名的继续存在作为该文档自从被数字地签署以来没有被更改过的证明。因此，该数字签署策略促进了已签署文档的内容的更高级别的确定度，即该文档是否具有当应用数字签名时所具有的相同配置。涉及文档配置的这一增加的确定度级别有助于在诸如合同谈判和合作文档写作等各种各样的场景中提高成效。

[0015] 所述的签署策略与文档包 (document package) 和 / 或将文档的数据存储在离散的逻辑实体或部分之中的文档类型一起使用。这种配置的一个示例是具有可标识根部分及用于根部分的有效处理的相关联部分的树结构。在这种配置中，某些部分存储与内容有关的数据，而其它部分，例如根部分，存储传达其它部分的相互关系的数据。例如，一个部分可

以与给定页的内容相关，而另一部分可以与给定页相对于其它页的位置有关。鉴于此，该数字签署策略指定了文档或包的哪些基础部分可以被包括以便维持展示给用户的文档配置。换言之，该数字签署策略用来在文档被数字地签署时有效地记录文档的配置，以使该配置能被用来检测对该文档的后续改变。该数字签署策略能够检测到这种改变并能响应地使用户的签名无效。至少某些实现还允许用户指定文档的哪些其它部分能被今后的用户更改以及以何种形式更改。例如，发布用户在签署文档的时候可以指定消费用户能例如在不使发布用户的签名无效的情况下向文档增加注解。

[0016] 示例性系统

[0017] 图 1 示出了被配置成实现用于确定电子文档 101 是否保持与其被数字地签署时的文档配置一致的签署策略的示例性系统 100。系统 100 包括通过数字数据交换平台 106 耦合至消费器 104 的发布器 102。该数字数据交换平台可包括用于传输数字数据的任何装置。例如，可利用各种类型的网络来传输电子文档 101。在另一示例中，该电子文档可被存储在某种类型的存储介质上，例如磁盘或闪存设备，并以物理方式从一人交达另一人。在此情况中，发布器 102 包括在物理计算设备上操作的程序或软件，用来为发布用户 114 创建用户界面。类似地，消费器 104 包括在物理计算设备上操作的程序或软件，用来为消费用户 124 创建用户界面。

[0018] 系统 100 被配置成允许发布用户 114 与发布器 102 交互以生成随后能被展示给消费用户 124 的文档 101。在文档写作过程期间的某个时刻，发布用户可获得发布用户期望数字地签署的文档配置。在发布器 102 上操作的数字签署策略指定哪些基础文档部分要包括在发布用户的数字签名之内以便足以维持文档 101 的配置。消费用户 124 随后可访问文档 101。消费器 104 打开文档 101 并依据数字签署策略来检查该文档。在发布用户的数字签名保持有效的情况中，有效签名的存在向消费用户确保文档与发布用户的预期配置保持一致。在数字签名被无效的情况中，消费用户可基于对文档已被更改的了解进行相应的行动。类似地，如果文档随后被返回给发布用户，则发布器可评估发布用户的数字签名是否仍然有效。之后，发布用户可在得知该文档是否已被更改后进行相应的行动。

[0019] 图 2 示出了根据一实现的其上能实现数字签署策略的示例性文档格式 200 的一个一般示例。在此实例中，文档格式 200 将数据存储在多个离散的逻辑部分中。当被发布器或消费器解析后，这些逻辑部分共同创建如在 202 处一般所表示的展示给用户的文档配置。该文档可包括文本、图像和 / 或任何其它惯例的文档内容。在此实例中，逻辑部分被例示为第一文档部分 204、第二文档部分 206 和第三分档部分 208。当然，在此示例之外，其它示例性文档格式可以不同的方式来组织逻辑部分。例如，下文描述逻辑部分的一种树型组织的示例。

[0020] 出于解释的目的，考虑其中作者或发布用户期望向文档 202 以其当前的形式或配置应用他 / 她的数字签名。数字签署策略指定该文档的哪些部分被数字签名包括以用来建立当前配置。例如，假定在此示例中，数字签署策略以数字签名包括了所有三个文档部分 204、206 和 208。对指定部分中的任一个的任何后续更改使得发布用户的数字签名被无效。因此，有效的数字签名指示该文档以其曾经被签署的配置存在。在某些实现中，该数字签署策略可允许发布用户在不使他们的数字签名无效的情况下指定能被添加到该文档的附加的数据。此种实现的示例联系图 4 在以下描述。作为选择地或另外地，在某些实现中，该数

字签署策略定义了需要被数字签名包括来确保文档配置没有在不使签署用户的数字签名无效的情况下被更改的减少的或最低数量的文档部分。

[0021] 图 3-4 示出了图示出根据一实施例的能在其上实现数字签署策略的文档格式的文档。其上能实现这些文档的一种这样的文档格式是由华盛顿州雷德蒙市的微软公司开发的 XML 纸件规范 (XPS) 文档格式。关于 XPS 文档格式的详细内容可以至少从 http://www.microsoft.com/whdc/Device/print/metro.mspx 公开地获得。

[0022] 在这特定的示例中，该数字签署策略指定了对于被认为要签署的文档哪些文档部分要被数字签名所包括。如果数字签名包括比指定的少的文档部分，则该文档可能随后在不使数字签名无效的情况下被更改，并且因此造成了关于在应用数字签名之时的文档配置的模糊性。换言之，该数字签署策略的功能是指定哪些部分被数字签名所包括以便有效地创建在签署时刻的文档配置的快照。图 3-4 提供了该数字签署策略可如何在特定情形中实现的具体示例。其它情形应被本领域的技术人员所认识到。

[0023] 图 3 示出了包括包关系部分 301、文档序列部分 302 和相关联的文档序列 (DS) 关系部分 303、以及至少一个固定文档部分的的文档 300。单独的固定文档部分与单独的固定文档 (FD) 关系部分相关联。在此示例中，示出了三个固定文档部分 304、306 和 308，但其它示例可以有任何个数的固定文档部分。由于呈现图 3 的纸张的物理限制，仅对固定文档部分 304 示出 FD 关系部分 309。

[0024] 包关系 301 是其目标为一个部分，而其源是作为整体的一个包的关系。文档序列部分 302 包含引用固定文档部分 304、306 和 308 的标记。换言之，文档序列是列出了文档 300 中包含了什么固定文档的部分。对固定文档部分 304、306 或 308 中的一个或多个的任何删除被反映在文档序列部分 302 中。类似地，对新的固定文档部分的任何添加被反映在该文档序列部分中。

[0025] 单独的固定文档部分引用固定页部分。换言之，固定文档部分包含其各自的固定页的列表。由于呈现图 3 的物理页的空间限制，仅示出了与固定文档部分 304 有关系的固定页部分。在此实例中，示出了两个固定页部分 310、312，但是任何个数的固定页部分可以被单独的固定文档部分引用。对固定页部分的任何删除或添加被反映在相关联的固定文档部分中。

[0026] 单独的固定页部分通过一关系部分被链接至其资源部分，该关系部分指定了单独的页所链接至的所有资源。例如，固定页部分 310 通过固定页 (FP) 关系部分 320 关联到资源部分 322、324。由于附图页的物理限制，关于固定页部分 312 没有示出关系部分及资源部分。对来自固定页部分的内容的任何删除或添加被反映在该固定页部分和 / 或相关联的关系部分中。此外，对给定资源的任何变化被反映在该资源中。

[0027] 该数字签署策略用来建立在应用数字签名时的文档 300 的配置或内容。在该特定示例中，该数字签署策略指定了数字签名必须包括包关系部分 301、文档序列部分 302、固定文档部分 304、306 和 308、固定页部分 310、312、资源部分 322、324 及相关联的关系部分 303、309 和 320。该数字签署策略规则提供了确保将数据作 为多个逻辑部分来存储的文档被维持在由用户数字地签署的配置中的机制。在文档作为逻辑部分来存储的情况中，文档配置是从各部分之间的相互关系以及各部分内的数据中建立的。由此，该数字签署策略用来建立部分间关系以及部分内数据两者。在文档配置通过更改部分间关系和部分内数据中

的任一项或两者来更改的情况中，该数字签署策略使数字签名无效。这一数字签署策略机制允许作者或随后的用户确定该文档是否与同数字签名相关联的配置保持一致。

[0028] 出于解释的目的，假定文档 300 由发布用户依据上述指定的数字签署策略来数字地签署，使得该数字签名包括了包关系部分 301、文档序列部分 302 以及其文档序列关系部分 303、固定文档部分 304、306 和 308 以及其各自的固定文档关系部分（仅特别地指定了 FD 关系部分 309）、固定页部分 310、312 和固定页关系部分 320 以及资源部分 322、324。在这一实例中，在签署时对发布用户表示的文档配置被由数字签署策略指定的签名部分有效地包括。还假定随后的用户试图向文档 300 添加一新的固定文档。该新文档将被表示在文档序列部分 302 中。对该文档序列部分的这个改变将依据数字签署策略使得发布用户的数字签名被无效。在该特定实现中，数字签名被无效的事实可以用一种容易被用户察觉的方式在视觉上表示。其它实现可向用户提供它们将要进行的动作将使该文档的数字签名无效的警告。然而，在此实现中，数字签署策略并不能防止消费用户添加新的文档以及使数字签名无效。相反，这一动作只能使数字签名无效，并且系统将此信息给予用户以便根据他们认为合适的来行动。例如，如果消费用户接收了具有被无效的发布用户的签名的文档，则消费用户可以将该文档视为已被篡改，并且向发布用户请求一新的经签署的文档。

[0029] 类似于上面的示例，考虑其中随后的用户试图移除被一特定的固定页部分引用的资源并用一不同的资源来代替该资源的情形。例如，资源可以是用户试图用第二个不同图像来代替的图像。这一动作导致发布用户的数字签名被无效，因为该动作试图作更改（在此实例中，删除文档的经签署的部分）。在此示例中，响应于改变所引用的图像而使数字签名无效与数字签署策略的功能相一致。出于示例的目的，假定文档 300 是建筑者为给定价格建造房屋的要约。还假设所引用的图像是包括在要约中的房屋的设计图。要约的价格是基于该特定设计图的。因此，建筑者不愿意让某些人，例如财产所有人，能够用不同的设计图替换以至于看上去建筑者是基于该替换的设计图做出要约的。数字签署策略用于通知建筑者和 / 或财产所有人，该要约保留在建筑者在要约中签署的配置中，或是该要约已被更改以至于它不再与建 筑者签署的配置相一致。

[0030] 图 4 示出了另一文档 400，对于该文档，数字签署策略指定哪些文档部分要被数字签名包括以使该文档被认为是已签署的。如果该文档依据数字签署策略被数字地签署，则该数字签名捕捉当该文档被数字地签署时的文档配置。换言之，在此实现中，数字签名策略指定了包的哪些部分一定不能改变以使内容被认为是原封不动的。为了确保有效性，某些客户机应用程序和 / 或其用户可要求包中的所有部分和关系被签署并生效。其它则可要求仅选中的部分或关系被签署并生效来指示内容没有被改变。该数字签名策略对于定义将要被签署的内容同时允许包的一些部分保持可变提供了灵活性。文档 400 提供了签署用户可指定文档的特定内容能在不破坏用户的数字签名的情况下改变的实例的情形的示例。

[0031] 文档 400 包括包关系部分 402、数字签名定义部分 404 及核心属性部分 406。在此实例中，数字签名定义部分、核心属性部分及包关系部分在包级定义，并由此在文档级继承，并且由数字签署策略来维护。包关系 402 是其目标为一个部分，而其源为作为整体的一个包的关系。数字签名定义部分 404 允许发布用户定义要数字地签署该文档的被请求的一组人以及与每个被请求的数字签名相关联的条件或定义。核心属性部分涉及用户能在文档中定义的一个或多个属性。例如，一个这样的核心属性可以是用户能以其所期望的任何名

字或笔名自由指定的“文档作者”。

[0032] 文档 400 还包括具有相关联的文档序列 (DS) 关系部分 412 的文档序列部分 410，以及具有相关联的固定文档 (FD) 关系部分 416 的固定文档部分 414。固定文档部分 414 引用固定页部分 418 和注解部分 420。如在固定页 (FP) 关系部分 422 中所指示的，固定页部分 418 链接至资源部分 424。此特定实现还包括以下将更详细讨论的缩略图部分 426。

[0033] 数字签署策略用来建立当应用数字签名时文档 400 的内容。在该实现中，该数字签署策略为将依据数字签署策略的文档指定该数字签名包括包关系部分 402、文档序列部分 410 及其 DS 关系部分 412、固定文档部分 414 及其 FD 关系部分 416、固定页部分 418 及其 FP 关系部分 422 以及资源部分 424。数字签署策略还规定当存在缩略图 426 时数字签名包括缩略图 426。当然，虽然仅示出了上述部分中的每一个的单个示例，但是许多实现将具有部分 414-426 中的多个实例。

[0034] 在该实例中，签署包关系 402 防止随后的用户在不使签署用户的数字签名无效的情况下改变包关系。类似地，签署文档序列部分 410 及其 DS 关系部分 412 防止在不使数字签名无效的情况下移除现有的固定文档或添加新的固定文档。签署固定 文档部分 414 及其 FD 关系部分 416 防止对各页在固定文档中的顺序的改变或添加或删除固定页。签署固定页部分 418 及其 FP 关系部分 422 用来防止页的内容被改变。签署资源部分 424 防止移除或替换资源部分。类似地，当缩略图部分存在时，例如在该所示的实现中，签署缩略图部分防止在不破坏签名的情况下替换或删除缩略图 426。同样地，如果数字签名定义部分 404 存在，例如在此所指示的，则数字签署策略用数字签名来包括该数字签名定义部分。该数字签署策略功能性地签署这些组件中的每一个以总体提供关于该文档是否从所签署的配置更改的指示。

[0035] 在该实现中，数字签署策略允许签署用户决定该文档的特定部分的内容能否在不使签署用户的数字签名无效的情况下操纵。例如，签署用户是否希望随后的用户能够在不使签署用户的数字签名无效的情况下向文档添加内容？在一个这样的实例中，签署用户能够决定是否允许随后的用户向文档添加数字签名。在另一实例中，签署用户能够决定是否允许随后的用户改变文档的核心属性。在又一实例中，签署用户能够决定是否允许随后的用户向文档添加注解。这些选项中的每一个都独立于其它选项，并且签署用户能够不允许对文档的任何可任选添加或者任何期望的组合。

[0036] 图 5 示出了以关于核心属性的逻辑表 500 的形式的数字签署策略的一示例。逻辑表 500 涉及两个互斥的情形。在第一个情形中，签署用户希望允许核心属性改变，如 502 处所指示的。在第二个情形中，签署用户不希望允许核心属性改变，如 504 处所指示的。关于这两个情形 502、504，两个情况中的一个存在。或者如 506 处所指示的核心属性部分存在，或者如 508 处所指示的核心属性部分不存在。

[0037] 如 510 处所指示的，在签署用户希望允许核心属性改变并且核心属性部分存在的情况中，则当用户数字地签署该文档时，数字签名策略保持核心属性部分不被签署，但该策略将用户的数字签名应用于关于图 4 所描述的包关系。该包关系包含了到核心属性部分的链接，这样，随后的用户可以在不使用户的签名无效的情况下改变核心属性。

[0038] 如 512 处所指示的，在签署用户希望允许核心属性改变并且核心属性部分不存在的情况中，则数字签署策略在用户数字地签署该文档之前创建一核心属性部分。该核心属

性部分可以在此时为空，但在签署之前创建它允许随后添加内容。该核心属性部分然后被保持不被签署，以便能对该核心部分做随后的改变。如上所述，用户的数字签名被应用于包关系来防止资料被改变或删除。

[0039] 如 514 处所指示的，如果签署用户不希望允许核心属性添加并且核心属性存 在，则数字签署策略以用户的数字签名签署该核心属性部分以及包关系。在这一情形中，用户的数字签名包括核心属性部分，使得对该核心属性部分的任何改变将使用户的签名无效。

[0040] 最后，如 516 处所指示的，如果签署用户不希望允许核心属性添加并且核心属性部分不存在，则数字签署策略不在用户数字地签署文档之前创建核心属性部分。如其它情形中一样，数字签名被应用于包关系。在此情形中，随后添加核心属性则必须添加核心属性部分。添加核心属性部分改变了包关系部分，这使得用户的签名无效。

[0041] 共同参考图 4-5，数字签署策略能够以类似于如上关于核心属性所述的方式来处理注解。注解被添加到被固定文档部分 414 引用的注解部分 420。如果注解部分被用户的数字签名包括，则添加注解将使该签名无效。如果注解部分不存在，则在应用数字签名后创建该部分将改变固定文档部分并使签名无效。如果签署用户希望允许添加注解，则注解部分应当在签署时存在并且应该保持不被签署。注解部分可以在数字地签署文档之前被创建。在这一实例中，新创建的注解部分在应用用户的数字签名时可以为空。

[0042] 图 6 涉及例如可与图 4 所示的文档 400 相关联的数字签名部分。在该实现中，数字签名部分包括签名起源部分 602、签名部分以及证书部分。在这一实例中，表示了两个签名部分 604、606 以及两个证书部分 608、610。本实现将证书部分 608、610 表现为分开且不同的部分。在其它实现中，证书部分可被嵌入在相关联的签名部分内。签名起源部分 602 提供了用于导航文档的可用数字签名的起始点。包含了包括由数字签署策略指定的部分的数字签名并且被适当验证的签名部分，如 606 或 608，可被认为是有效的。例如，系统验证依据数字签署策略签署了正确的部分。系统还验证可任选地签署的部分（诸如上述核心属性）的状态，以及可任选地签署的部分的状况是如何影响用户的。系统还验证，对于所签署的部分，签名是否有效。例如，如本领域技术人员应该认识到的，系统检查散列计算是否匹配。

[0043] 换言之，如果签名部分包括与数字签署策略相一致的文档部分并且签名验证是成功的，则该文档可被认为是有效的已签署文档，例如 XPS 文档。在这一实例中，用户可以认为这一文档具有与应用该有效数字签名时存在的相同的配置。

[0044] 该数字签署策略提供了关于附加资料能否被添加至文档的一种灵活的解决方案。该解决方案允许发布用户指定什么（如果有）可任选材料可以在不使其数字签名被无效的情况下添加。该数字签署策略然后考虑文档的当前配置并相应地进行行 动以如上在图 4-6 中所述地创建或签署各部分。至少某些实现类似于开关。例如，如果作者打开签名保护并且有人添加了一数字签名，则数字签署策略破坏该作者的数字签名。如果作者不希望签名保护，则有人可以在不影响作者的数字签名的情况下添加数字签名。相同的原理可应用于其它可任选的添加，例如注解和核心属性。所以，该方案很灵活，因为它让签署用户来定义策略参数并且数字签署策略相应地操作以使得随后的用户能够在不破坏签署用户的数字签名的情况下添加内容。然而，尽管有其灵活性，但该数字签署策略继续防止任何人在不破坏消费用户的数字签名的情况下更改文档的配置。在最终用户级，所述的数字签署策略提供了关于拥有用户的数字签名的文档保持与用户曾数字地签署的配置相一致的增加的置

信度。该数字签署策略还可用于建立能被可与依据数字签署策略的文档及文档格式交互的其它软件产品所依据并理解的数字签署策略。该数字签署策略定义了关于什么被已签署文档实际包括、如何生成依据数字签署策略的已签署文档、和 / 或如何评估接收到的文档以确定该文档的数字签名是否有效的标准。总之，该数字签署策略定义了被数字地签署的文档实际表示了什么意思。

[0045] 示例性计算环境

[0046] 图 7 示出了其上能实现数字签署策略的示例性系统或计算环境 700。系统 700 包括第一机器 701 和第二机器 702 形式的通用计算系统。

[0047] 第一机器 701 的组件可包括，但不限于，一个或多个处理器 704（例如，微处理器、控制器等中的任一个）、系统存储器 706 及耦合各系统组件的系统总线 708。一个或多个处理器 704 处理各种计算机可执行指令来控制第一机器 701 的操作并与其它电子和计算设备通信。系统总线 708 代表任何个数的几种总线结构，包括存储器总线或存储器控制器、外围总线、加速图形端口、及采用各种总线体系结构中的任一种的处理器或局部总线。

[0048] 系统 700 包括各种计算机可读介质，其可以是可由第一机器 701 访问的任何介质，并包括易失性和非易失性介质、可移动和不可移动介质两者。系统存储器 706 包括诸如随机存取存储器 (RAM)710 等易失性存储器形式的计算机可读介质，和 / 或诸如只读存储器 (ROM)712 等非易失性存储器形式的计算机可读介质。基本输入 / 输出系统 (BIOS)714 维护帮助例如在启动期间在第一机器 701 内的组件之间的信息传输的基本例程，并被存储在 ROM 712 中。RAM 710 通常包含一个或多个处理器 704 直接可访问和 / 或当前正在操作的数据和 / 或程序模块。

[0049] 第一机器 701 可包括其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质。作为示例，硬盘驱动器 716 读取和写入不可移动、非易失性磁介质（未示出），磁盘驱动器 718 读取和写入可移动、非易失性磁盘 720（例如，“软盘”），而光盘驱动器 722 读取和 / 或写入可移动、非易失性光盘 724，例如 CD-ROM、数字多功能盘 (DVD) 或任何其它类型的光学介质。在该示例中，硬盘驱动器 716、磁盘驱动器 718 和光盘驱动器 722 各自通过一个或多个数据介质接口 726 连接至系统总线 708。盘驱动器和相关联的计算机可读介质为第一机器 701 提供了对计算机可读指令、数据结构、程序模块及其它数据的非易失性存储。

[0050] 任何数目的程序模块可以被存储在硬盘 716、磁盘 720、光盘 724、ROM 712 和 / 或 RAM 710 中，包括例如操作系统 726、一个或多个应用程序 728、其它程序模块 730 和程序数据 732。这些操作系统 726、应用程序 728、其它程序模块 730 和程序数据 732 中的每一个（或其某一组合）可以包括此处所描述的系统和方法的一个实施例。

[0051] 用户可以通过任何数目的不同输入设备，例如键盘 734 和定点设备 736（例如“鼠标”）与第一机器 701 接口。其它输入设备 738（未具体示出）可以包括话筒、操纵杆、游戏手柄、控制器、圆盘式卫星天线、串行端口、扫描仪等等。这些及其它输入设备通过耦合至系统总线 708 的输入 / 输出接口 740 连接至处理器 704，但也可通过其它接口和总线结构，例如并行端口、游戏端口、和 / 或通用串行总线 (USB) 来连接。

[0052] 监视器 742 或其它类型的显示设备可以通过诸如视频适配器 744 等接口连接至系统总线 708。除了监视器 742 之外，其它输出外围设备可包括诸如扬声器（未显示）和打印机 746 等组件，它们可通过输入 / 输出接口 740 连接至第一机器 701。

[0053] 第一机器 701 可采用与诸如第二机器 702 等一个或多个远程计算机的逻辑连接在联网环境中操作。例如，第二机器 702 可以是个人计算机、便携式计算机、服务器、路由器、网络计算机、对等设备、或其它常见的网络节点等等。第二机器 702 被示作可包括许多或全部此处关于第一机器 701 所描述的元件或特征的便携式计算机。

[0054] 第一机器 701 和第二机器 702 之间的逻辑连接被描绘为局域网 (LAN)750 和通用广域网 (WAN)752。这样的网络连接环境在办公室、企业范围计算机网络、内联网和因特网中是常见的。当在 LAN 网络连接环境中实现时，第一机器 701 通过网络接口或适配器 754 连接至局域网 750。当在 WAN 网络连接环境中实现时，第一机器 701 通常包括调制解调器 756，或用于通过广域网 752 建立通信的其它装置。可内置或外置于第一机器 701 的调制解调器 756 可通过输入 / 输出接口 740 或其它合适的机制连接至系统总线 708。所示出的网络连接是示例性的，并且可以利用在第一机器 701 和第二机器 702 之间建立通信链路的其它手段。

[0055] 在例如随系统 700 示出的联网环境中，关于第一机器 701 所描述的程序模块或其部分可以被存储在远程存储器存储设备中。作为示例，远程应用程序 758 以第二机器 702 的存储器设备来维护。出于图示的目的，应用程序和诸如操作系统 726 等其它可执行程序组件在此被示为分立的框，尽管可以认识到，这样的程序和组件在不同的时刻驻留在第一机器 701 的不同存储组件中，并由第一机器的处理器 704 来执行。

[0056] 示例性过程

[0057] 图 8 示出了关于数字签署策略的示例性过程 800。描述该过程的顺序不意在被解释为限制，并且任何数目的所述过程框可以按任何顺序组合来实现该过程。另外，该过程可以用任何合适的硬件、软件、固件或其组合来实现。

[0058] 在框 802 处，该过程确定依据数字签署策略要以用户的数字签名来包括的文档的部分。在某些实现中，数字签署策略可指定文档的所有部分被数字地签署。在其它实现中，该数字签署策略可以指定各部分的一个子集被数字地签署。例如，在一实现中，该数字签署策略被应用于对在签署时刻所表示的文档配置作出贡献的部分。在这一实例中，该数字签署策略用来通知用户和 / 或其他用户，文档在签署后是否以将文档配置从用户所签署的文档配置进行改变的方式被更改。

[0059] 在框 804 处，该过程对在框 802 处确定的部分应用数字签名。用户的数字签名被有效地应用于由数字签署策略指定的所有部分，使得如果任一部分被更改，则该数字签名就被破坏或无效。破坏与任一部分有关的数字签名破坏了作为整体的文档的数字签名。基本原理是更改任一指定部分会改变文档配置。

[0060] 该过程可表示数字签名是否保持有效，以使用户和 / 或随后的用户可关于如何处理该文档作出更明智的决定。该数字签署策略有效地创建了具有对用户更高程度的确定度的环境。例如，如果发布用于对特定的文档配置满意并数字地签署了该文档，则数字签署策略确保只要他 / 她的数字签名保持有效，发布用户和任何消费用户均可在他们正在查看曾被发布用户数字地签署的文档配置的自信中行动。这可在其中发布用户数字地签署了期望的文档配置然后将该文档发送至诸如可在合同谈 判中相遇的相反的消费方的情形中特别有价值。如果消费用户接着将该文档发送回发布用户，则发布用户可以对消费方对文档作出的某些难以检测但重要的改变很机警。该数字签署策略功能允许发布用户容易地确定所

返回的文档是否具有他数字地签署的相同配置。由于数字签署策略为用户创建了更高级别的确定度，因此它可以培养对数字文档的更高级别的接受度，特别是在被用户认为重要的事情中。另外，当以系统的角度来看时，该数字签署策略促进可与依据数字签署策略的文档交互或支持其的软件产品之间的互操作性。

[0061] 尽管用对结构特征和／或方法专用的语言描述了涉及数字签署策略的实现，但应该理解，所随权利要求的主题并不必然局限于所描述的具体特征或方法。相反，这些具体特征和方法为上述和以下的概念提供了实现的示例。

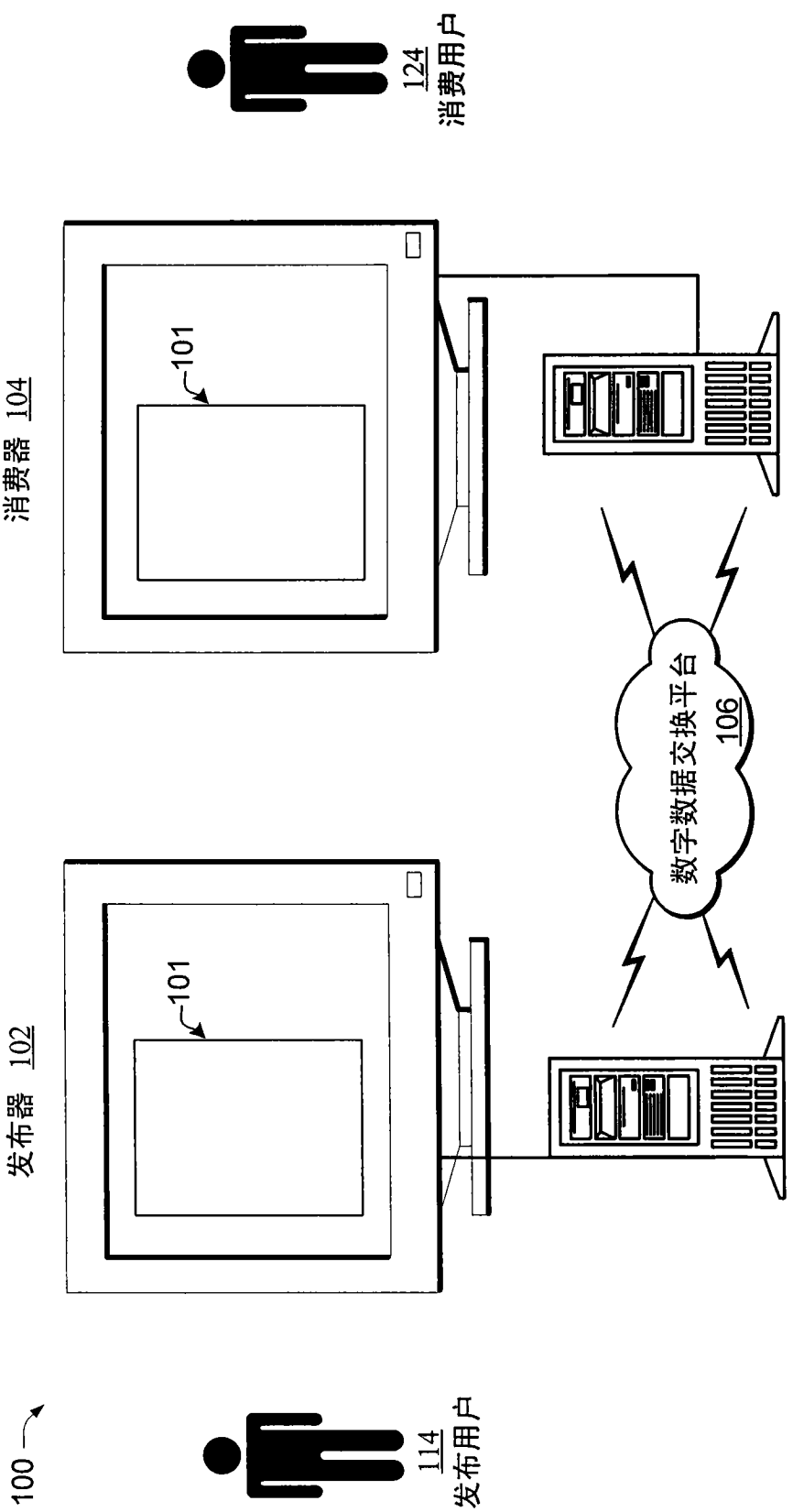


图 1

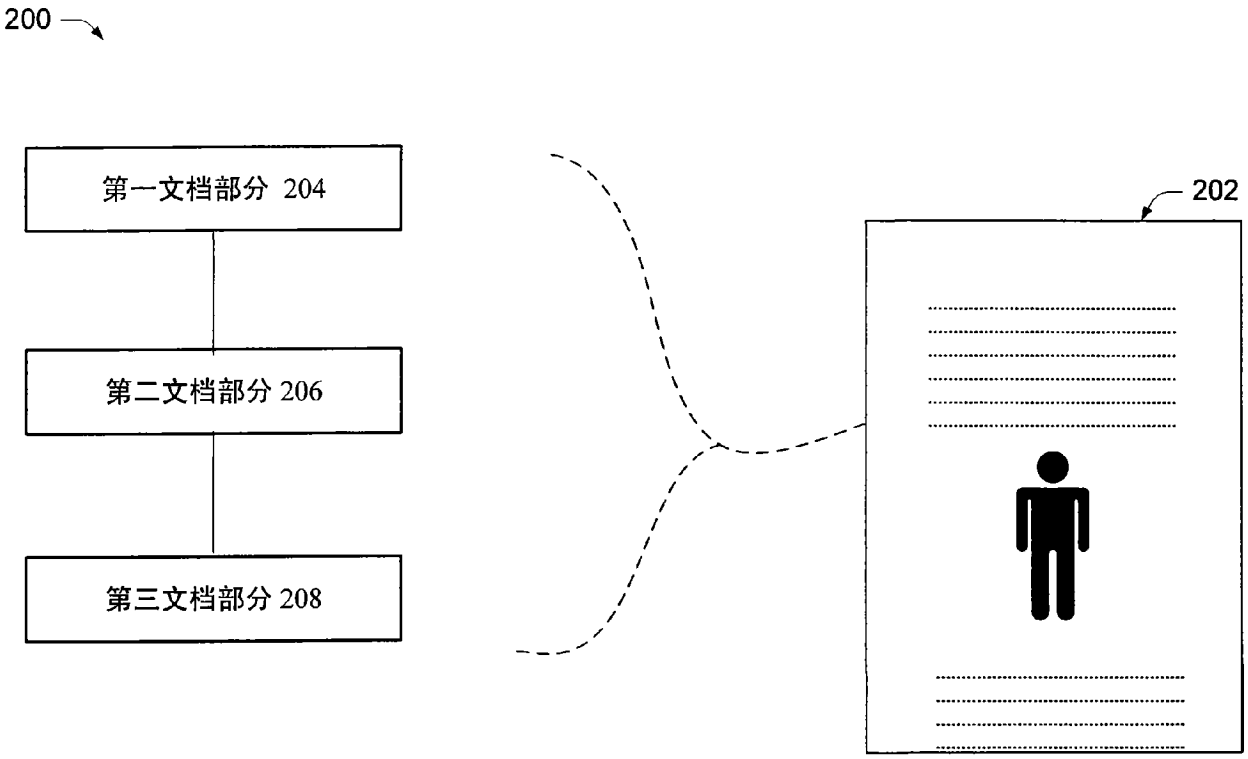


图 2

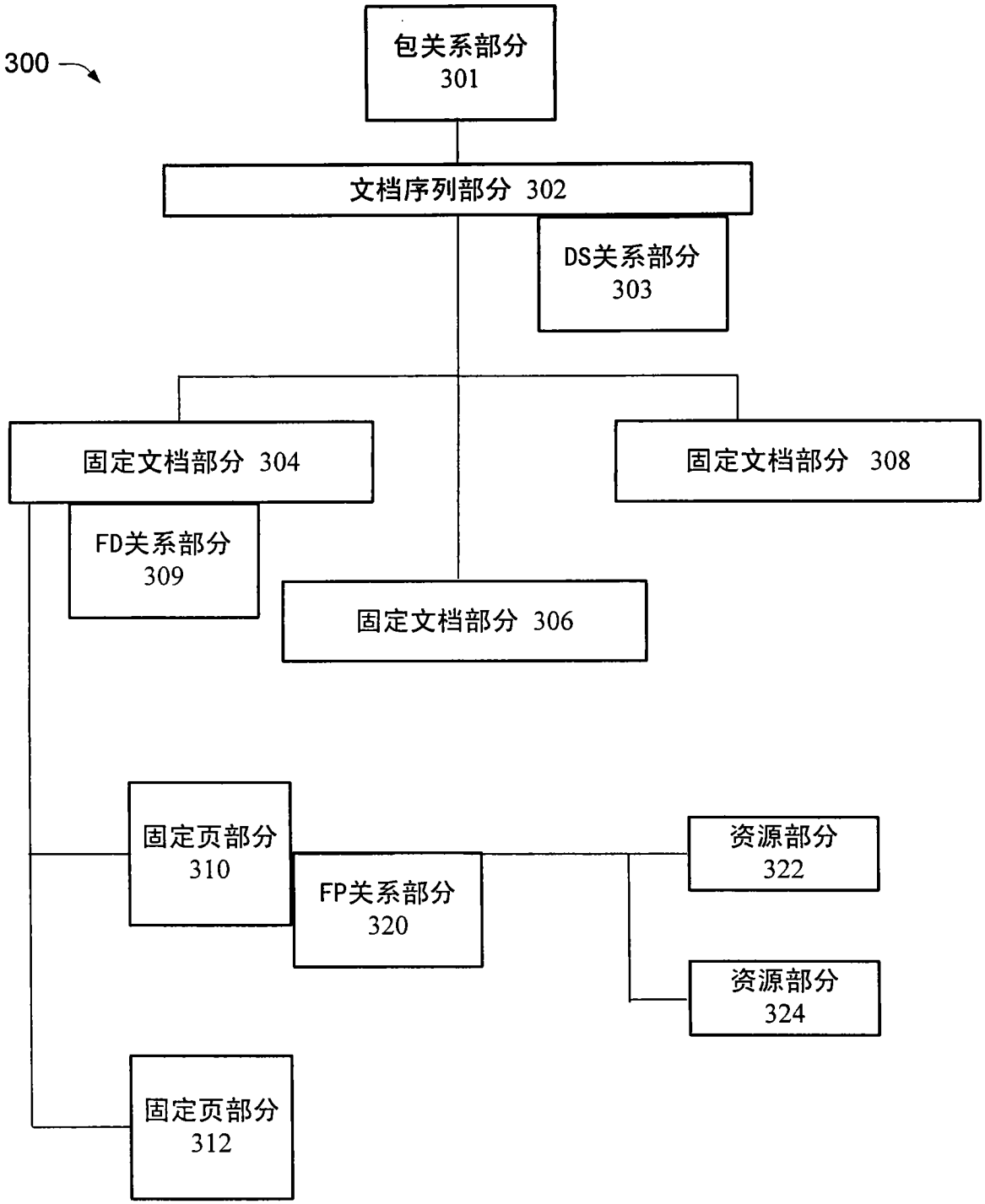

300
包关系部分
301
文档序列部分 302
DS关系部分
303
固定文档部分 304
固定文档部分 308
FD关系部分
309
固定文档部分 306
固定页部分
310
FP关系部分
320
资源部分
322
资源部分
324
固定页部分
312

图 3

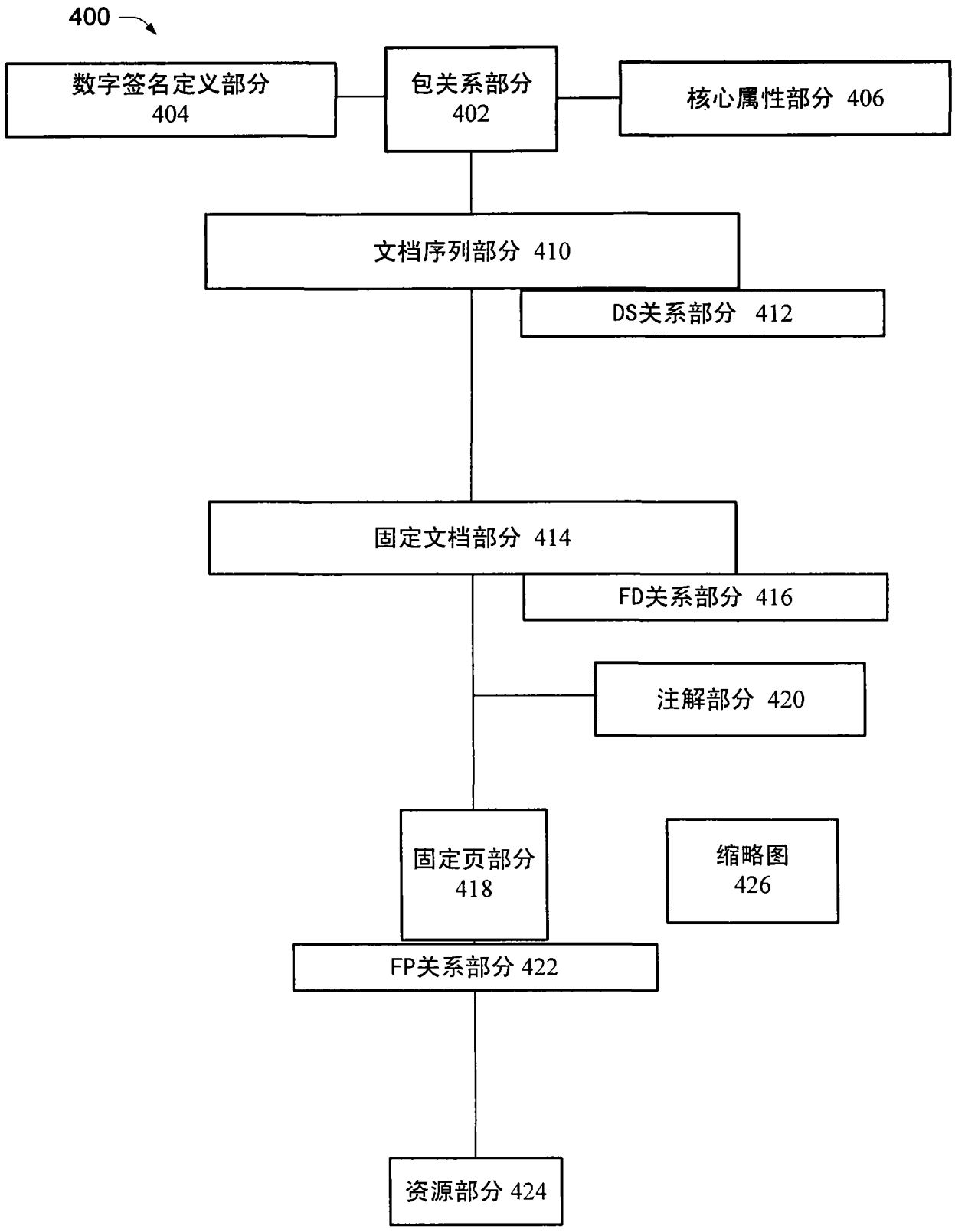

400
数字签名定义部分 404
包关系部分 402
核心属性部分 406
文档序列部分 410
DS关系部分 412
固定文档部分 414
FD关系部分 416
注解部分 420
固定页部分 418
缩略图 426
FP关系部分 422
资源部分 424

图 4

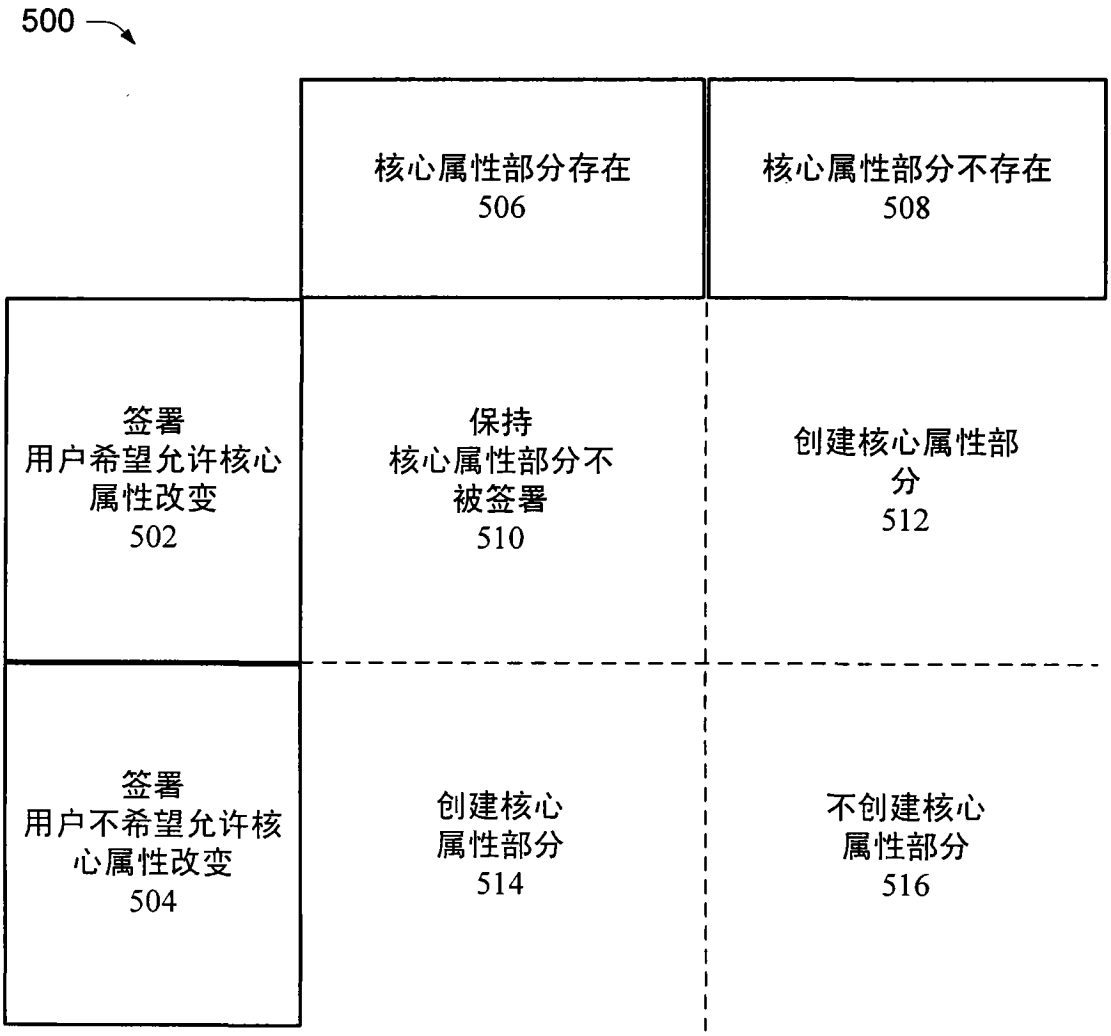

500
核心属性部分存在
506
核心属性部分不存在
508
签署
用户希望允许核心
属性改变
502
保持
核心属性部分不
被签署
510
创建核心属性部
分
512
签署
用户不希望允许核
心属性改变
504
创建核心
属性部分
514
不创建核心
属性部分
516

图 5

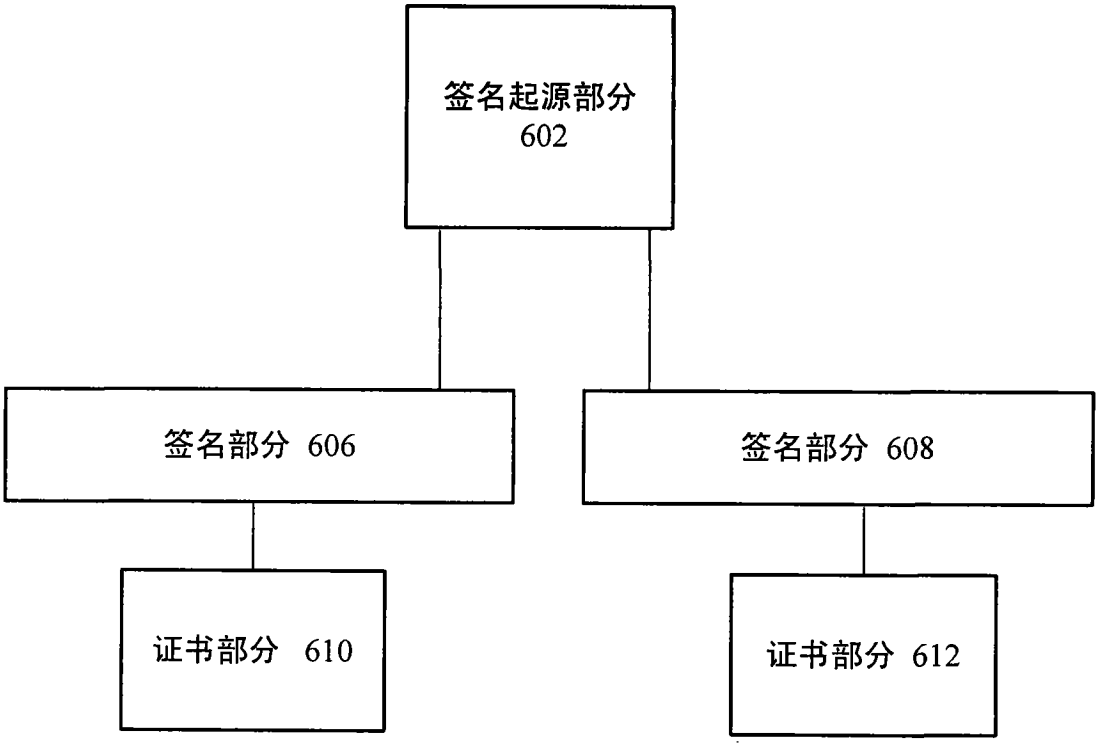


图 6

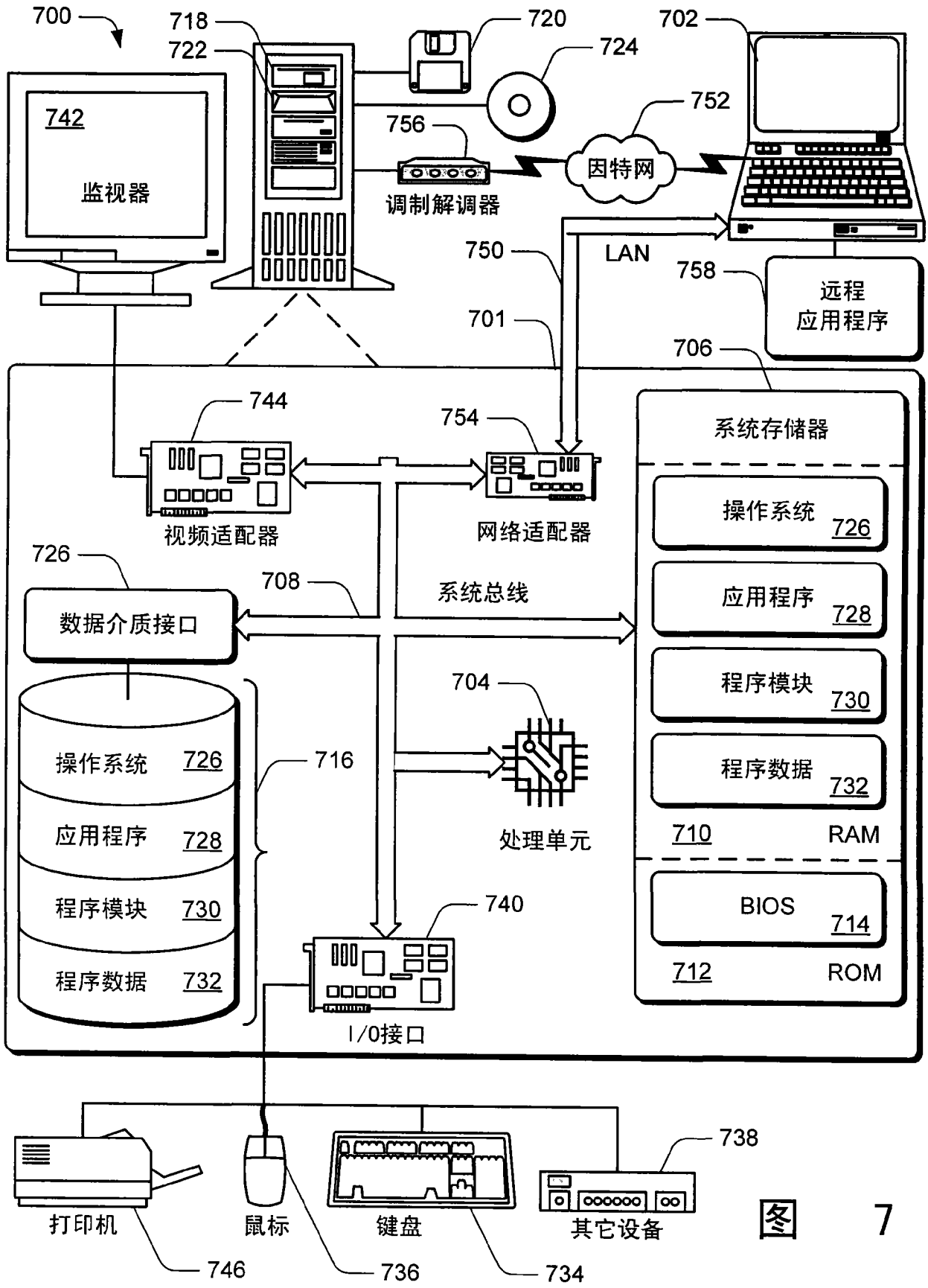

700
718
722
720
724
702
742
监视器
752
756
因特网
调制解调器
750
LAN
758
远程
应用程序
701
706
744
754
系统存储器
操作系统 726
视频适配器
网络适配器
726
708
系统总线
数据介质接口
应用程序 728
程序模块 730
704
程序数据 732
716
处理单元
710 RAM
操作系统 726
应用程序 728
程序模块 730
程序数据 732
740
BIOS 714
712 ROM
I/O接口
738
打印机
鼠标
键盘
其它设备
746
736
734

图 7

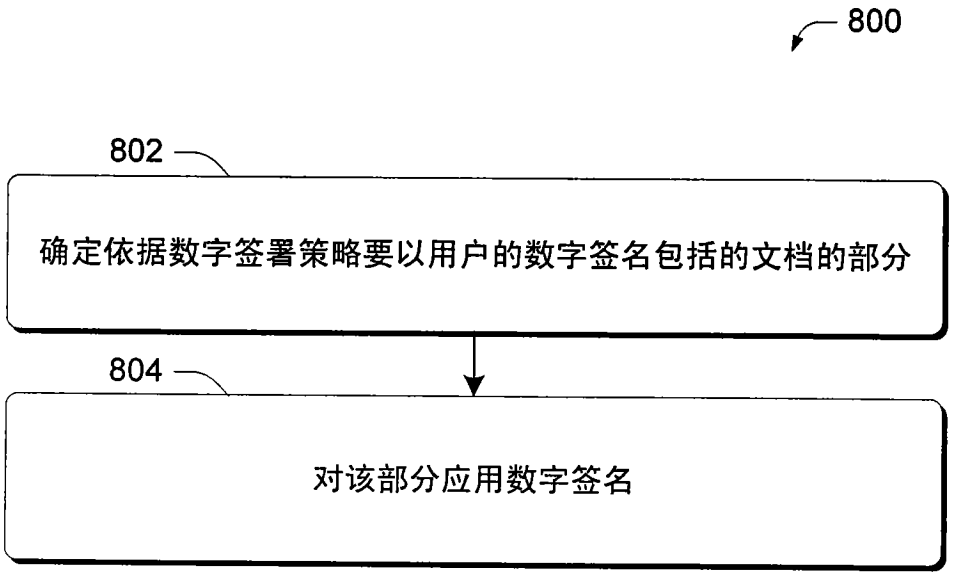


图 8