(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 105190640 B
(45)授权公告日 2019.04.05

(21)申请号 201480025833.1
(22)申请日 2014.02.17
(65)同一申请的已公布的文献号
申请公布号 CN 105190640 A
(43)申请公布日 2015.12.23
(30)优先权数据
13/888,747 2013.05.07 US
(85)PCT国际申请进入国家阶段日
2015.11.06
(86)PCT国际申请的申请数据
PCT/US2014/016697 2014.02.17
(87)PCT国际申请的公布数据
WO2014/182359 EN 2014.11.13
(73)专利权人 波音公司
地址 美国伊利诺伊州
(72)发明人 G•A•金伯利
(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 赵蓉民 徐东升
(51)Int.Cl.
G06F 21/57(2006.01)
G06F 21/64(2006.01)
H04L 9/32(2006.01)
(56)对比文件
EP 1879122 A1,2008.01.16,
US 2007/0234047 A1,2007.10.04,
US 2009/0106560 A1,2009.04.23,
审查员 张剑峰

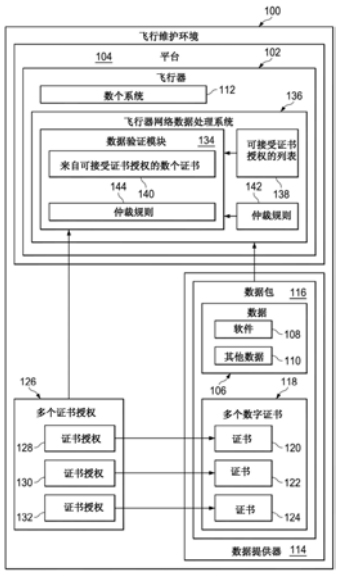
权利要求书2页 说明书10页 附图7页

(54)发明名称

响应于盗用的数字证书来验证飞行器信息

(57)摘要

本申请公开一种用于验证在飞行器上使用的数据的方法和装置。通过处理器单元接收与数据相关联的多个数字证书。处理器单元确定多个数字证书中的一个数字证书是否被盗用。处理器单元响应于确定多个数字证书中的一个数字证书被盗用而选择多个数字证书中的选择数量的数字证书。处理器单元使用多个数字证书中的选择数量的数字证书来验证在飞行器上使用的数据。



CN 105190640 B

1.一种用于验证在飞行器(102)上使用的数据(106)的方法,包含:

通过处理器单元(804)接收与所述数据(106)相关联的多个数字证书(118);

通过所述处理器单元(804)确定所述多个数字证书(118)中的一个数字证书是否被盗用;

通过所述处理器单元(804)选择仲裁规则(144),其中所述仲裁规则(144)是响应于确定所述多个数字证书(118)中的任何一个均没有被盗用而选择的第一仲裁规则以及响应于确定所述多个数字证书(118)中的一个数字证书被盗用而选择的第二仲裁规则;以及

通过所述处理器单元(804)使用由所述仲裁规则(144)限定的所述多个数字证书(118)中的选择数量的数字证书来验证在所述飞行器(102)上使用的数据(106)。

2.根据权利要求1所述的方法,其中所述多个数字证书(118)来自于多个证书授权(126)。

3.根据权利要求1或2所述的方法,其中使用所述多个数字证书(118)中所述选择数量的数字证书来验证在所述飞行器(102)上使用的所述数据(106)包含确定所述多个数字证书(118)中的所述选择数量的数字证书中的至少指定数量的数字证书是否有效。

4.根据权利要求3所述的方法,其中所述指定数量由仲裁规则(144)限定。

5.根据权利要求4所述的方法,进一步包含:

响应于确定所述多个数字证书(118)中的所述一个数字证书被盗用,从多个仲裁规则(142)中选择所述仲裁规则(144)。

6.根据权利要求5所述的方法,其中所述数据(106)包含在所述飞行器(102)上使用的软件(108)。

7.根据权利要求6所述的方法,其中所述处理器单元(804)是所述飞行器(102)上的飞行器网络数据处理系统(136)中的处理器单元(804)。

8.一种用于验证在飞行器(102)上使用的数据(106)的装置,包含:

数据验证模块(134),其经配置以:接收与在飞行器(102)上使用的数据(106)相关联的多个数字证书(118);确定所述多个数字证书(118)中的一个数字证书是否被盗用;通过所述处理器单元(804)选择仲裁规则(144),其中所述仲裁规则(144)是响应于确定所述多个数字证书(118)中的任何一个均没有被盗用而选择的第一仲裁规则以及响应于确定所述多个数字证书(118)中的一个数字证书被盗用而选择的第二仲裁规则;以及使用所述多个数字证书(118)中由所述仲裁规则(144)限定的选择数量的数字证书来验证在所述飞行器(102)上使用的所述数据(106)。

9.根据权利要求8所述的装置,其中所述多个数字证书(118)来自于多个证书授权(126)。

10.根据权利要求8或9所述的装置,其中所述数据验证模块(134)经配置以确定所述多个数字证书(118)中的所述选择数量的数字证书中的至少指定数量的数字证书是否有效。

11.根据权利要求10所述的装置,其中所述指定数量由仲裁规则(144)限定。

12.根据权利要求11所述的装置,其中所述数据验证模块(134)经配置以响应于确定所述多个数字证书(118)中的所述一个数字证书被盗用,从多个仲裁规则(142)中选择所述仲裁规则(144)。

13.根据权利要求8所述的装置,其中所述数据(106)包含在所述飞行器(102)上使用的

软件(108)。

14.根据权利要求8所述的装置,其中所述数据验证模块(134)被实施在所述飞行器(102)上的飞行器网络数据处理系统(136)中的处理器单元(804)内。

响应于盗用的数字证书来验证飞行器信息

技术领域

[0001] 本公开总体涉及用于验证在飞行器上使用的信息的真实性与完整性的系统和方法。更具体地，本公开涉及当获知或怀疑与信息相关联的数字证书被盗用(compromised)时验证在飞行器上使用的信息的真实性与完整性。

背景技术

[0002] 现代飞行器是极为复杂的。例如，飞行器可以具有多种类型的机载电子系统。这些系统通常采用外场可更换单元(LRU)的形式。外场可更换单元是可以从飞行器中去除且替换的物品。外场可更换单元被设计为易于替换。

[0003] 外场可更换单元可以采用各种形式。飞行器上的外场可更换单元可以是，例如但不限于，飞行管理系统、自动驾驶仪、飞行娱乐系统、通信系统、导航系统、飞行控制器、飞行记录器、防碰撞系统、支持维护功能的系统或支持机组人员处理的系统。飞行器上的各种外场可更换单元可以是飞行器网络数据处理系统的部件。

[0004] 外场可更换单元可以使用软件或编程以提供针对各种操作和功能的逻辑或控制。通常。飞行器上的软件被视为一个或多个独立的部件或与硬件部件相结合，并且所述飞行器上的软件在不改变硬件部件数量的情况下是不可变化的。被视为飞行器部件的飞行器软件可以被称为可装载飞行器软件部件或飞行器软件部件。飞行器软件部件是飞行器的配置的部件。

[0005] 飞行器操作者是操作飞行器的实体。飞行器操作者还可以负责飞行器的维护和维修。飞行器操作者的示例包括航空公司和军事单位。当飞行器操作者接收飞行器时，飞行器软件部件可能已经被安装到了飞行器的外场可更换单元内。

[0006] 飞行器操作者还可以接收已加载飞行器软件部件的复制品以防部件需要被重新安装或重新加载到飞行器的外场可更换单元中。可以要求对飞行器软件部件进行重新加载，例如，如果替换了或维修了在其中使用了该软件的外场可更换单元。此外，飞行器操作者还可以时常接收飞行器软件部件的更新。这些更新可以包括在当前安装的飞行器软件部件中并不存在的附加的特征，并且可以被认为是对一个或多个外场可更换单元的升级。在对飞行器上的飞行器软件部件进行加载期间，可以遵循规定的程序，从而获知该飞行器的当前配置，包括加载到飞行器上的所有飞行器软件部件。

[0007] 可能期望的是，在飞行器上仅可以使用来自被信任的供应商的仅被批准的软件和其他数据。未批准的软件和其他的数据可以包括被损坏的数据、被植入病毒的数据，或其他未批准的数据。未批准的软件和其他数据可能以不期望的方式影响飞行器的操作。

[0008] 数据处理网络可以采用公钥基础设施中的数字证书以确保在网络上使用仅被批准的软件和其他数据。这种数字证书还可以被称为公开密钥证书或身份证书。通过网络所信任的证书授权机构来发布数字证书。该数字证书以可以被信任的方式来识别(确认)到达网络的软件或其他数据的来源。网络可以使用数字证书以确定是否将在该网络上使用软件或其他数据。

[0009] 对于在完全基于地基的计算机网络上使用的用于验证软件和其他数据的真实性与完整性的当前系统和方法可能无法有效地应用于移动系统，诸如飞行器。运行和维护飞行器上的网络数据处理系统的特定环境可能使得难以或不可能使用此类当前方法来验证在飞行器网络数据处理系统上使用的软件或其他数据。

[0010] 因此。期望的是拥有考虑一个或多个上述问题以及可能的其他问题的方法和装置。

发明内容

[0011] 本公开的实施例提供用于验证在飞行器上使用的数据的方法。通过处理器单元接收与数据相关联的多个数字证书。处理器单元确定多个数字证书中的一个数字证书是否被盗用。处理器单元响应于确定多个数字证书中的一个数字证书被盗用而选择所选择数量的多个数字证书。处理单元使用所选择数量的多个数字证书来验证在飞行器上使用的数据。

[0012] 本公开的另一个实施例提供包含数据验证模块的装置。数据验证模块经配置以：接收与在飞行器中使用的数据相关联的多个数字证书；确定多个数字证书中的一个数字证书是否被盗用；响应于确定多个数字证书中的一个数字证书被盗用而选择所选择数量的多个数字证书；以及使用所选择数量的多个数字证书来验证在飞行器上使用的数据。

[0013] 本公开的另一个实施例提供用于验证在飞行器上使用的数据的方法。通过处理器单元接收与数据相关联的多个数字证书。处理单元确定多个数字证书中的一个数字证书是否被盗用。处理器单元选择仲裁规则，其中该仲裁规则是响应于确定多个数字证书中的任何一个均没有被盗用而选择的第一仲裁规则以及响应于确定多个数字证书中的一个被盗用而选择的第二仲裁规则。处理器单元使用由仲裁规则限定的所选择数量的多个数字证书来验证在飞行器上使用的数据。

[0014] 特征和功能可以在本公开的各种实施例中被独立地实现，或者可以在其他实施例中被结合，其中参考下列描述和附图可以获知进一步的细节。

附图说明

[0015] 在所附的权利要求中记载了被认为是说明性实施例特性的新颖特征。然而，当结合附图阅读时，通过参照本公开说明性实施例的以下详细描述，将更好地理解说明性实施例与优选的使用模式、进一步目的及其特征，其中：

[0016] 图1是根据说明性实施例的飞行器维护环境的框图的图示；

[0017] 图2是根据说明性实施例的仲裁规则的框图的图示；

[0018] 图3是根据说明性实施例使用多个数字证书和一系列可接受证书授权机构进行数据验证的框图的图示；

[0019] 图4是根据说明性实施例使用多个数字证书和仲裁规则进行数据验证的框图的图示；

[0020] 图5是根据说明性实施例响应于被盗用的证书授权进行数据验证的框图的图示；

[0021] 图6是根据说明性实施例对数据进行签名以便在飞行器上使用的过程的流程图的图示；

[0022] 图7是根据说明性实施例对数据进行验证以便在飞行器上使用的过程的流程图的

图示；

[0023] 图8是根据说明性实施例的数据处理系统的图示。

具体实施方式

[0024] 不同说明性实施例认识并考虑了数个不同的考虑方面。在本文中使用的关于物品的“数个”意味着一个或多个物品。例如，“数个不同的考虑方面”意味着一个或多个不同的考虑方面。

[0025] 不同的说明性实施例认识并考虑到可以围绕源自单一的根证书授权的证书(singular root certificate authority-derived certificates)来构造当前的公钥基础设施系统。使用单一证书可以创造一种系统，在该系统内的错误配置或攻击可以有效地使得系统停止操作。

[0026] 不同的说明性实施例还认识并考虑到飞行器的操作者可以优选某些证书授权并且可以不信任其他的证书授权。因此。可能期望的是允许飞行器操作者使用来自对操作者可接受的证书授权的证书来验证在由操作者操作的飞行器上使用的软件和其他数据。

[0027] 不同的说明性实施例还认识并考虑到审计技术可以存在，审计技术使得发现根证书授权的盗用成为可能。可能期望的是针对在飞行器中使用的软件或其他数据的验证考虑已被获知或者被怀疑的证书授权的盗用。

[0028] 因此，一个或多个说明性实施例提供了系统和方法，所述系统和方法使用来自多个证书授权的多个数字证书来确认在飞行器中使用的软件和其他数据的真实性与完整性有效。根据说明性实施例，如果确定满足仲裁规则的与数据相关联的多个证书中数个是有效的，则软件或其他数据被确认有效以便在飞行器上使用。可以响应于规定证书授权可能已被盗用的确定来选择限定了确认有效所需的仲裁的规则。

[0029] 现在转向图1，其根据说明性实施例描绘了飞行器维护环境的框图的图示。在该示例中，飞行器维护环境100可以经配置以便维护飞行器102。

[0030] 飞行器102可以是任何合适类型的飞行器。例如，但不限于，飞行器102 可以是商用或私人客运飞行器、货运飞行器、军用或其他政府飞行器、或针对任何适合目的或任务而配置的任何其他飞行器。飞行器102可以是固定机翼的、旋转机翼的，或轻于空气的飞行器。飞行器102可以是有人驾驶飞行器或无人驾驶的航空器。

[0031] 飞行器102是平台104的一个示例，在平台104内可以实施说明性实施例。平台104可以是交通工具或其他移动结构。例如但不限于，平台104可以是能够通过空气行进或在太空中行进或能够通过空气行进并且能够在太空中行进的航空航天交通工具。作为另一个示例，但不限于，平台104可以是能够在陆地上、在水面、在水下或在任何其他介质内或介质的组合中行进的交通工具。在另一个说明性实施例中，平台104可以是静态系统。例如，但不限于，平台104可以是工业控制系统或其他一般不移动的系统。

[0032] 飞行器102可以使用数据106来操作飞行器102。例如，数据106可以包括软件108、其他数据110，或数据的各种组合。例如，但不限于，软件108 可以包括在飞行器102上外场可更换单元上使用的飞行器软件部件。例如，但不限于，其他数据110可以包括映射数据或其他数据或由飞行器102使用的数据的组合。

[0033] 数据106可以被飞行器102上的数个系统112使用。例如，但不限于，数个系统112可

以包括自动驾驶仪系统、飞行管理系统、通信系统、卫生管理系统、其他系统或用于执行飞行器102上的各种功能的系统的各种组合。

[0034] 可以通过数据提供器114来提供数据106。数据提供器114可以是有权提供在飞行器102上使用的数据106或有权将数据106加载在飞行器102上的任何实体。例如，但不限于，数据提供器114可以包括软件供应商、飞行器维护实体、飞行器操作者、飞行器制造商，或授权以提供在飞行器102上使用的数据106的任何其他实体或实体的组合。数据提供器114可以是负责维护飞行器102的任何实体或实体的组合。数据提供器114可以是或可以不是飞行器102的拥有者。数据提供器114可以包括作为飞行器102的拥有者的代表提供在飞行器102上使用的数据106的实体。

[0035] 数据提供器114可以以数据包116提供数据106以便加载到飞行器102 上。例如，数据包116可以包括数据106连同用于数据106的多个数字证书 118。在该示例中，但不限于，多个数字证书118可以包括证书120、证书122 以及证书124。多个数字证书118可以包括任何合适数量的数字证书。例如，多个数字证书118可以包括两个或多于三个的数字证书。

[0036] 多个数字证书118可以来自多个证书授权126。例如，证书120可以来自证书授权128。证书122可以来自证书授权130。证书124可以来自证书授权 132。

[0037] 数据验证模块134可以经配置以使用多个数字证书118来验证在飞行器 102上使用的数据106。例如，可以在飞行器102上的飞行器网络数据处理系统136中实施数据验证模块134。

[0038] 数据验证模块134可以经配置以使用可接受证书授权138的列表来识别来自可接受证书授权140的数个证书，以便用来验证在飞行器102上使用的数据106。可以由仲裁规则142限定多个数字证书118的数量，该多个数字证书118必须被确定为是有效的以用于将被验证的数据106。数据验证模块134 可以经配置以基于数据106将在其上被使用的数个系统112、当数据106被加载到飞行器上时的飞行器102的位置、其他因素或因素的各种组合来从用于数据106的验证的多个仲裁规则142中选择仲裁规则144。

[0039] 图1的图示不意味着表明对不同说明性实施例可以被实施所采用的方式的物理或架构限制。可以使用除所示组件外的、替换所述组件的或除所示组件外并替换所示组件的其他组件。在一些说明性实施例中，一些组件是非必需的。此外，方框被呈现以说明一些功能性组件。当在不同的说明性实施例中实施这些方框时，可以将这些方框中的一个或多个组合或划分成不同的方框。

[0040] 现在转向图2，其根据说明性实施例描绘了仲裁规则的框图的图示。在该示例中，仲裁规则200可以是图1中的仲裁规则142的一种实施方式的示例。

[0041] 可以针对飞行器的各种特性或状态来限定仲裁规则200。例如，但不限于，可以针对飞行器的经营者202、针对飞行器维护实体204、针对飞行器类型206、针对数据将在其上被使用的飞行器系统208、针对飞行器位置210，或针对飞行器的各种其他特性或特性的组合来限定仲裁规则200。具体的仲裁规则200 可以被限定以便针对响应于被获知或被怀疑的证书授权盗用212而使用。

[0042] 现在转向图3，其根据说明性实施例描绘了使用多个数字证书和可接受证书授权的列表来进行数据验证的框图的图示。例如，可以使用图1中的数据验证模块134来执行数据验证300。

[0043] 在该示例中，将被验证的数据包302可以包括证书A304、证书B 306、和证书C 308。可接受证书授权的列表310可以指示仅来自证书授权A312和证书授权B 314的证书是可接受的以便用于数据验证300。在这种情况下，证书C 308既不是来自证书授权A312又不是来自证书授权B 314。因此，证书 C 308将不用于数据验证300。在该示例中，可以响应于证书A或B有效316 的确定来验证数据包302。

[0044] 现在转向图4，其根据说明性实施例描绘了使用多个数字证书和仲裁规则来进行数据验证的框图的图示。例如，可以使用图1中的数据验证模块134 来执行数据验证400。

[0045] 在该示例中，将被验证的数据包402可以包括证书A404、证书B 406和证书C 408。仲裁规则410可以指示如果三个证书中的至少两个是有效的412，则数据包402可以被验证。因此，在该示例中，可以响应于证书A和B有效 414、证书A和C有效416、证书B和C有效418、或证书A和B和C有效 420的确定来验证数据包402。

[0046] 现在转向图5，其根据说明性实施例描绘了响应于被盗用的证书授权来进行数据验证的框图的图示。例如，可以使用图1中的数据验证模块134来执行数据验证500。

[0047] 在该示例中，将被验证的数据包502可以包括证书A504、证书B 506、和证书C 508。仲裁规则510可以指示如果三个证书中的至少两个是有效的 512，则数据包502可以被验证。但是，在这种情况下，可用信息指示证书授权A被盗用514。仲裁规则510还指示了如果证书授权被盗用516，则将使用的适当的仲裁规则将从三个证书中的至少两个有效512改变为没有被盗用的全部证书有效518。因此，在该示例中，只有响应于证书B和C有效520的确定，数据包502才可以被验证。

[0048] 现在转向图6，其根据说明性实施例描绘了对数据签名以便在飞行器上使用的过程的流程图的图示。例如，但不限于，可以通过图1中的数据提供器 114来执行过程600。

[0049] 用于飞行器的数据可以被接收(操作602)。数据可以被签有来自多个证书授权的多个数字签名(操作604)。然后，数据和多个证书可以被发送到飞行器(操作606)，之后该过程结束。

[0050] 现在转向图7，其根据说明性实施例描绘了验证数据以便于在飞行器上使用的过程的流程图的图示。在该示例中，可以通过图1中的数据验证模块134 来执行过程700。

[0051] 接收包括多个数字证书的数据包(操作702)。可以确定是否有任一证书不是来自可接受证书授权(操作704)。如果确定有任一证书不是来自可接受证书授权，则仅来自可接受证书授权的证书可以被用来验证数据包(操作 706)。否则，所有已接收的数字证书都可以用来验证(操作708)。

[0052] 用于验证的适当的仲裁规则可以被选择(操作710)。可以确定是否存在证书授权可能已经被盗用的任何指示(操作712)。响应于确定证书授权可能已经被盗用，可以选择替换的仲裁规则以便验证(操作714)。否则，在操作 710中选择的仲裁规则可以用于验证(操作716)。

[0053] 随后可以确定是否满足所选择的仲裁规则(操作718)。如果满足了所选择的仲裁规则，则数据真实性与完整性可以被认为经过验证(操作720)，之后该过程结束。否则，数据真实性与完整性可以是没有经过验证(操作722)，之后该过程结束。

[0054] 现在转向图8，根据说明性实施例描绘了数据处理系统的图示。在该示例中，数据处理系统800是图1中飞行器网络数据处理系统136上的数据处理系统的一个实施方式的示

例。数据处理系统800是图1中的数据验证模块134 可以被实施在其上的数据处理系统的一个实施方式的示例。

[0055] 在该说明性示例中，数据处理系统800包括通信结构802。通信结构802 提供处理单元804、存储器806、永久性存储808、通信单元810、输入/输出 (I/O)单元812以及显示器814之间的通信。存储器806、永久存储808、通信单元810、输入/输出(I/O)单元812以及显示器814是处理器单元804经由通信结构802可访问的资源的示例。

[0056] 处理器单元804用作运行可以被加载到存储器806内的软件的指令。处理器单元804可以是数个处理器、多处理器核，或一些其他类型的处理器，这取决于特定的实施方式。此外，可以使用数个异构处理器系统来实施处理器单元804，在所述异构处理器中主处理器与二级处理器一起存在于单个芯片上。作为另一个说明性示例，处理器单元804可以是包含多个相同类型的处理器的对称多处理器系统。

[0057] 存储器806和永久性存储808是存储设备816的示例。存储设备是能够存储信息(例如，但不限于，数据、函数形式的程序代码，以及临时性的或永久性的其他合适信息)的任何一种硬件。在这些示例中，存储设备816还可以被称为计算机可读存储设备。在这些示例中，存储器806可以是例如，随机存取存储器或任何其他合适的易失性或非易失性存储设备。永久性存储 808可以根据具体的实施例采用各种形式。

[0058] 例如，永久性存储808可以包含一个或多个组件或设备。例如，永久性存储808可以是硬盘驱动器、闪速存储器、可重写光盘、可重写磁带或以上一些的组合。永久性存储808所使用的媒介还可以是可去除的。例如，可去除的硬盘驱动器可以用于永久性存储808。

[0059] 在这些示例中，通信单元810提供与其他数据处理系统或设备的通信。在这些示例中，通信单元810是网络接口卡。通信单元810可以通过使用物理或无线通信链路或物理和无线通信链路两者来提供通信。

[0060] 输入/输出单元812允许用可以被连接到数据处理系统800的其他设备输入和输出数据。例如，输入/输出单元812可以通过键盘、鼠标和/或其他合适的输入设备来为用户输入提供连接。此外，输入/输出单元812可以将输出发送给打印机。显示器814提供将信息显示给用户的机制。

[0061] 操作系统、应用程序和/或程序的指令可以位于存储设备816中，所述存储设备816通过通信结构802与处理器单元904通信。在这些说明性示例中，指令以函数的形式位于永久性存储808上。这些指令可以被加载到存储器806 中以便处理器单元804执行。通过使用计算机实施的指令，处理器单元804 可以对不同的实施例进行处理，所述计算机实施的指令可以位于存储器内，诸如存储器806。

[0062] 这些指令被称为程序指令、程序代码、计算机可用程序代码、或可以被处理器单元804中的处理器读取且执行的计算机可读程序代码。不同实施例中的程序代码可以被编入不同的物理或计算机可读存储媒介内，诸如存储器 806或永久性存储808。

[0063] 程序代码818以函数的形式位于计算机可读介质820上，所述程序代码 818是选择性可去除的并且可以被加载到数据处理系统800上或被转移到数据处理系统800以便处理器单元804执行。在这些示例中，程序代码818和计算机可读媒介820形成计算机程序产品822。在一个示例中，计算机可读介质 820可以是计算机可读存储介质824或计算机可读信号介质826。

[0064] 计算机可读存储介质824可以包括，例如被插入或被放入驱动器或其他设备内的光盘或磁盘，所述其他设备是用于转移到是永久性存储808的部件的一种存储设备(诸如硬盘驱动器)的永久性存储808的部件。计算机可读存储介质824还可以采用被连接到数据处理系统800的永久存储的形式，诸如硬盘驱动器，拇指驱动器或闪速存储器。在一些实例中，计算机可读存储介质824不可以从数据处理系统800中去除。

[0065] 在这些示例中，计算机可读存储介质824是被用于存储程序代码818的物理或有形存储设备，而不是传输或传递程序代码818的介质。计算机可读存储介质824还被称为计算机可读有形存储设备或计算机可读物理存储设备。换句话说，计算机可读存储介质824是人可以触摸的介质。

[0066] 替换的，可以使用计算机可读信号介质826将程序代码818传递到数据处理系统800。计算机可读信号介质826可以是，例如，包含程序代码818的传播数据信号。例如，计算机可读信号介质826可以是电磁信号、光信号、或任何其他合适类型的信号。可以经由通信链路(诸如无线通信链路、光纤电缆、同轴电缆、导线、或任何其他合适类型的通信链路)来传递这些信号。换句话说，在说明性示例中通信链路或连接可以是物理的或无线的。

[0067] 在一些说明性实施例中，通过计算机可读信号介质826可以从另一种设备或数据处理系统经由网络将程序代码818下载到永久性存储808以便在数据处理系统800中使用。例如，存储在服务器数据处理系统中的计算机可读存储介质内的程序代码可以经由网络从服务器下载到数据处理系统800。提供程序代码818的数据处理系统可以是服务器计算机、客户端计算机、或能够存储和传递程序代码818的一些其他设备。

[0068] 所述的用于数据处理系统800的不同组件不意味着提供了对实施不同实施例可以采用的方式的架构限制。可以在数据处理系统中实施不同的说明性实施例，该数据处理系统包括除所述的用于数据处理系统800的那些组件之外的组件或替换所述的用于数据处理系统800的那些组件的组件。图8中显示的其他部件可以不同于所示的说明性示例。通过使用能够运行程序代码的任何硬件设备或系统，可以实施不同的实施例。作为一个示例，数据处理系统800可以包括与无机组件整合的有机组件和/或可以完全由排除人类之外的有机组件组成。例如，存储设备可以由有机半导体组成。

[0069] 在另一个说明性实施例中，处理单元8 04可以采用具有若干电路的硬件单元的形式，所述电路被制造或配置以用于特定用途。这种类型的硬件可以执行操作而不需要从存储设备加载到存储器内的被配置为执行该操作的程序代码。

[0070] 例如，当处理器单元804采用硬件单元的形式时，处理器单元804可以是电路系统、专用集成电路(ASIC)、可编程逻辑设备，或经配置以执行数个操作的一些其他合适类型的硬件。关于可编程逻辑设备，该设备可以被配置以执行数个操作。该设备可以在日后被重新配置或者被永久配置为执行数个操作。可编程逻辑设备的示例包括，例如可编程逻辑阵列、可编程阵列逻辑、现场可编程逻辑阵列、现场可编程门阵列以及其他合适的硬件设备。在这种类型的实施方式中，程序代码818可以被忽略，其原因在于不同实施例的处理可以被实施在硬件单元中。

[0071] 还在另一个说明性示例中，可以使用可在计算机和硬件单元中存在的处理器的组合来实施处理器单元804。处理器单元804可以具有数个硬件单元和经配置以运行程序代码818的数个处理器。在该描绘的示例中，可以在数个硬件单元中实施一些处理，而在数个处

理器中可以实施其他的处理。

[0072] 在另一个示例中，总线系统可以用于实施通信结构802并且可以由一个或多个总线(诸如，系统总线或输入/输出总线)组成。当然，可以使用任何合适类型的架构来实施总线系统，所述合适类型的架构提供附接到总线系统的不同组件或设备之间的数据的传输。

[0073] 此外，通信单元810可以包括传输数据、接收数据或传输和接收数据的数个设备。通信单元810可以是，例如，调制解调器或网络适配器、两个网络适配器，或其中的一些组合。此外，存储器可以是，例如在可以存在于通信结构802中的接口和内存控制器集线器内找到的存储器806或高速缓存器。

[0074] 为说明和描述的目的，已经呈现了不同说明性实施例的描述，并且该不同说明性实施例的描述不意旨详尽或者限制公开形式的实施例。许多修改和变体对本领域的技术人员将是明显的。进一步，当与其他说明性实施例比较时，不同说明性实施例可以提供不同的特征。为了更好地解释实施例、实际应用的原理，以及能够使本领域的其他普通技术人员理解对于具有各种修改的各种实施例的本公开也适合于预期的特定用途，选取并描述了所选择的单个实施例或者多个实施例。

[0075] 注意：下列段落描述了发明的进一步的方面：

[0076] A1.一种用于验证在飞行器(102)上使用的数据(106)的方法，包括：

[0077] 通过处理器单元(804)接收与所述数据(106)相关联的多个数字证书 (118)；以及

[0078] 通过所述处理器单元(804)使用所述多个数字证书(118)中选择数量的数字证书来验证在所述飞行器(102)上使用的所述数据(106)。

[0079] A2.根据权利要求A1所述的方法，其中所述多个数字证书(118)来自于多个证书授权(126)并且进一步包含使用可接受证书授权的列表(138)来选择所述多个数字证书(118)中的所述选择数量的数字证书。

[0080] A3.根据权利要求A1所述的方法，其中使用所述多个数字证书(118)中所述选择数量的多个数字证书来验证在所述飞行器(102)上使用的所述数据 (102)包括确定所述多个数字证书(118)中所述选择数量的数字证书中的至少指定数量的数字证书是否有效。

[0081] A4.根据权利要求A3所述的方法，其中所述指定数量由仲裁规则(144) 限定。

[0082] A5.根据权利要求A4所述的方法，进一步包含：

[0083] 基于所述数据(106)将在其上被使用的所述飞行器(102)上的系统从多个仲裁规则(142)中选择所述仲裁规则(144)。

[0084] A6.根据权利要求A4所述的方法，进一步包含：

[0085] 基于所述飞行器(102)的位置从多个仲裁规则(142)中选择所述仲裁规则(144)。

[0086] A7.根据权利要求A1所述的方法，其中所述数据(106)包含在所述飞行器(102)上使用的软件(108)。

[0087] A8.根据权利要求A1所述的方法，其中所述处理器单元(804)是所述飞行器(102)上的飞行器网络数据处系统(136)中的处理器单元(804)。

[0088] A9.一种装置，包含：

[0089] 数据验证模块(134)，其经配置以接收与在飞行器(102)上使用的数据 (106)相关联的多个数字证书(118)并且使用所述多个数字证书(118)中选择数量的数字证书来验证在所述飞行器(102)上使用的所述数据(106)。

[0090] A10.根据权利要求A9所述的装置,其中所述多个数字证书(118)来自于多个证书授权(126)并且其中所述数据验证模块(134)进一步经配置以使用可接受证书授权的列表(138)来选择所述多个数字证书(118)中的所述选择数量的数字证书。

[0091] A11.根据权利要求A9所述的装置,其中所述数据验证模块(134)经配置以确定所述多个数字证书(118)中的所述选择数量的数字证书中的至少指定数量的数字证书是否有效。

[0092] A12.根据权利要求A11所述的方法,其中所述指定数量由仲裁规则(144) 限定。

[0093] A13.根据权利要求12所述的装置,其中所述数据验证模块(134)经配置以基于所述数据(106)将在其上被使用的所述飞行器(102)上的系统从多个仲裁规则(142)中选择所述仲裁规则(144)。

[0094] A14.根据权利要求A12所述的装置,其中所述数据验证模块(134)经配置以基于所述飞行器(102)的位置从多个仲裁规则(142)选择所述仲裁规则 (144)。

[0095] A15.根据权利要求A9所述的装置,其中所述数据(106)包含在所述飞行器(102)上使用的软件(108)。

[0096] A16.根据权利要求A9所述的装置,其中所述数据验证模块(134)被实施在所述飞行器(102)上的飞行器网络数据处理系统(136)内。

[0097] A17.一种用于验证在飞行器(102)上使用的数据(106)的方法,包括:

[0098] 通过所述处理器单元(804)接收在所述飞行器102上使用的所述数据 (106);

[0099] 通过所述处理器单元(804)生成用于所述数据(106)的多个数字证书 (118);以及

[0100] 将所述数据(106)和所述多个数字证书(118)发送给所述飞行器(102)。

[0101] A18.根据权利要求A17所述的方法,其中所述多个数字证书(118)来自多个证书授权(126)。

[0102] A19.根据权利要求A17所述的方法,其中所述数据(106)包含在所述飞行器(102)上使用的软件(108)。

[0103] A20.根据权利要求A17所述的方法,进一步包括:

[0104] 通过所述飞行器(102)上的飞行器网络数据处理系统(136)接收所述多个数字证书(118);以及

[0105] 通过所述飞行器网络数据处理系统(136)使用所述多个数字证书(118) 中选择数量的多个数字证书来验证在所述飞行器(102)上使用的所述数据 (106)。

[0106] B15.一种用于验证在飞行器(102)上使用的数据(106)的方法,包含:

[0107] 通过处理器单元(804)接收与所述数据(106)相关联的多个数字证书 (118);

[0108] 通过所述处理器单元(804)确定所述多个数字证书(118)中的一个数字证书是否被盗用;

[0109] 通过所述处理器单元(804)选择仲裁规则(144),其中所述仲裁规则(144) 是响应于确定所述多个数字证书(118)中的任何一个均没有被盗用而选择的第一仲裁规则以及响应于确定所述多个数字证书(118)中的一个数字证书被盗用而选择的第二仲裁规则;以及

[0110] 通过所述处理器单元(804)使用由所述仲裁规则(144)限定的所述多个数字证书(118)中的选择数量的数字证书来验证在所述飞行器(102)上使用的所述数据(106)。

[0111] B16.根据权利要求B15所述的方法,其中所述多个数字证书(118)来自于多个证书

授权(126)。

[0112] B17.根据权利要求B15所述的方法,其中使用所述多个数字证书(118) 中的所述选择数量的多个数字证书来验证在所述飞行器(102)上使用的所述数据(106)包含确定被所述仲裁规则(144)限定的所述多个数字证书(118) 中的所述选择数量的多个数字证书中的至少指定数量的数字证书是否有效。

[0113] B18.根据权利要求B17所述的方法,其中:

[0114] 所述第一仲裁规则指示所述多个数字证书(118)中的所述选择数量的多个数字证书中的所述指定数量的数字证书少于所述选择数量的多个数字证书;以及

[0115] 所述第二仲裁规则指示所述多个数字证书(118)中的所述选择数量的多个数字证书中的所述指定数量的数字证书等于所述选择数量的多个数字证书。

[0116] B19.根据权利要求B15所述的方法,其中所述数据(106)包含在所述飞行器(102)上使用的软件(108)。

[0117] B20.根据权利要求B15所述的方法,其中所述处理器单元(804)是在所述飞行器(102)上的飞行器网络数据处理系统(136)中的处理器单元(804)。

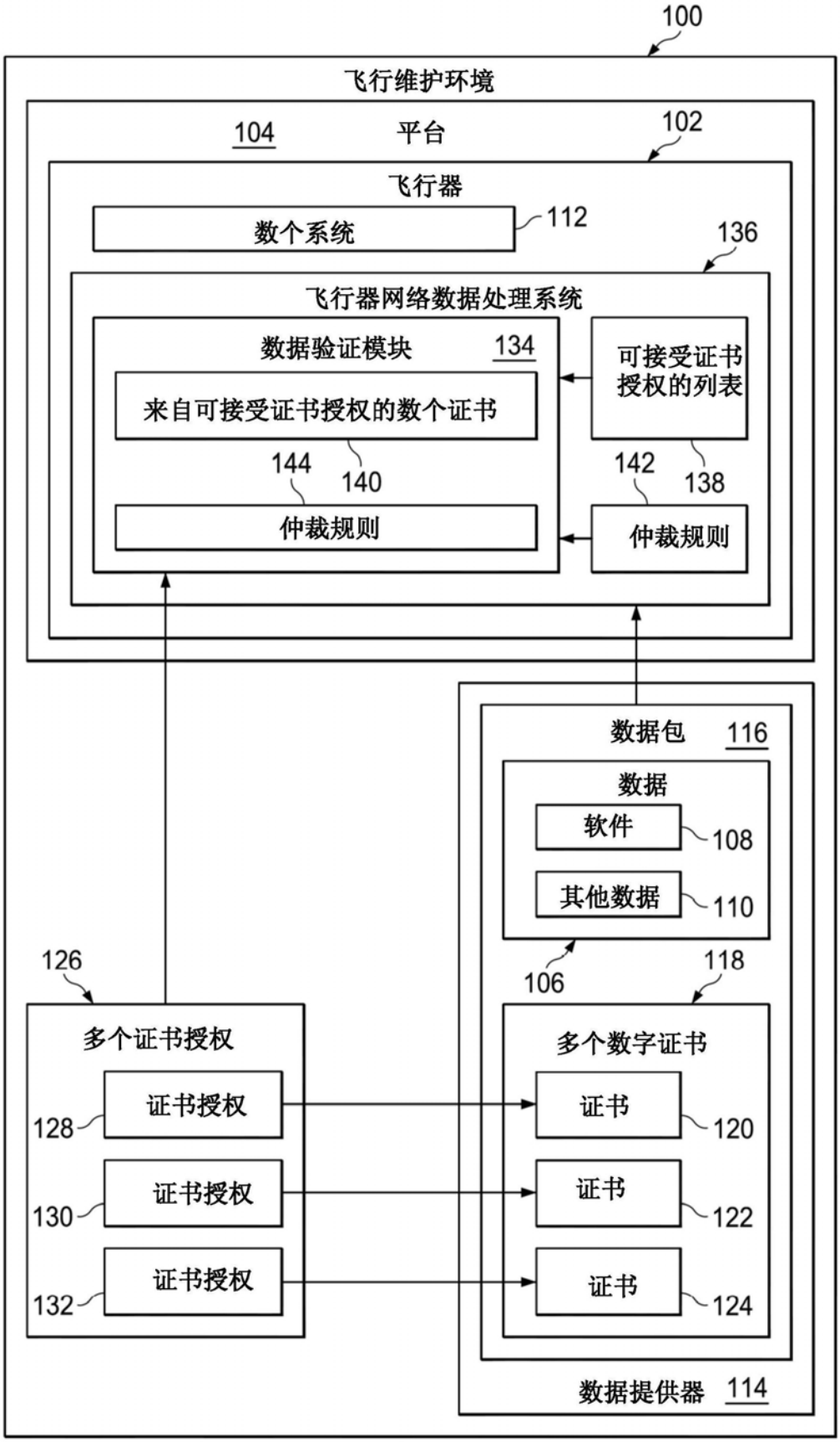

100
飞行维护环境
104
平台
102
飞行器
数个系统
112
136
飞行器网络数据处理系统
数据验证模块
134
来自可接受证书授权的数个证书
144
140
仲裁规则
可接受证书授权的列表
142
138
仲裁规则
数据包
116
数据
软件
108
其他数据
110
126
106
118
多个证书授权
证书授权
128
证书授权
130
证书授权
132
多个数字证书
证书
120
证书
122
证书
124
数据提供器
114

图1

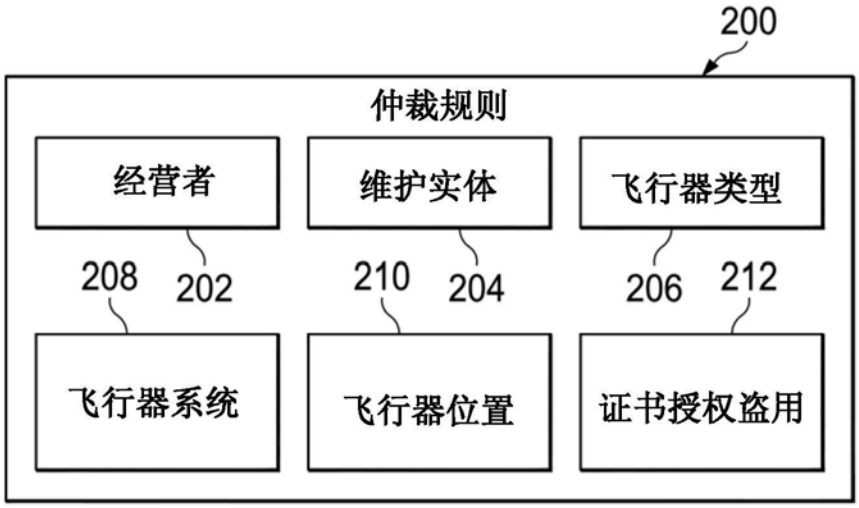

200
仲裁规则
经营者
维护实体
飞行器类型
208
202
210
204
206
212
飞行器系统
飞行器位置
证书授权盗用

图2

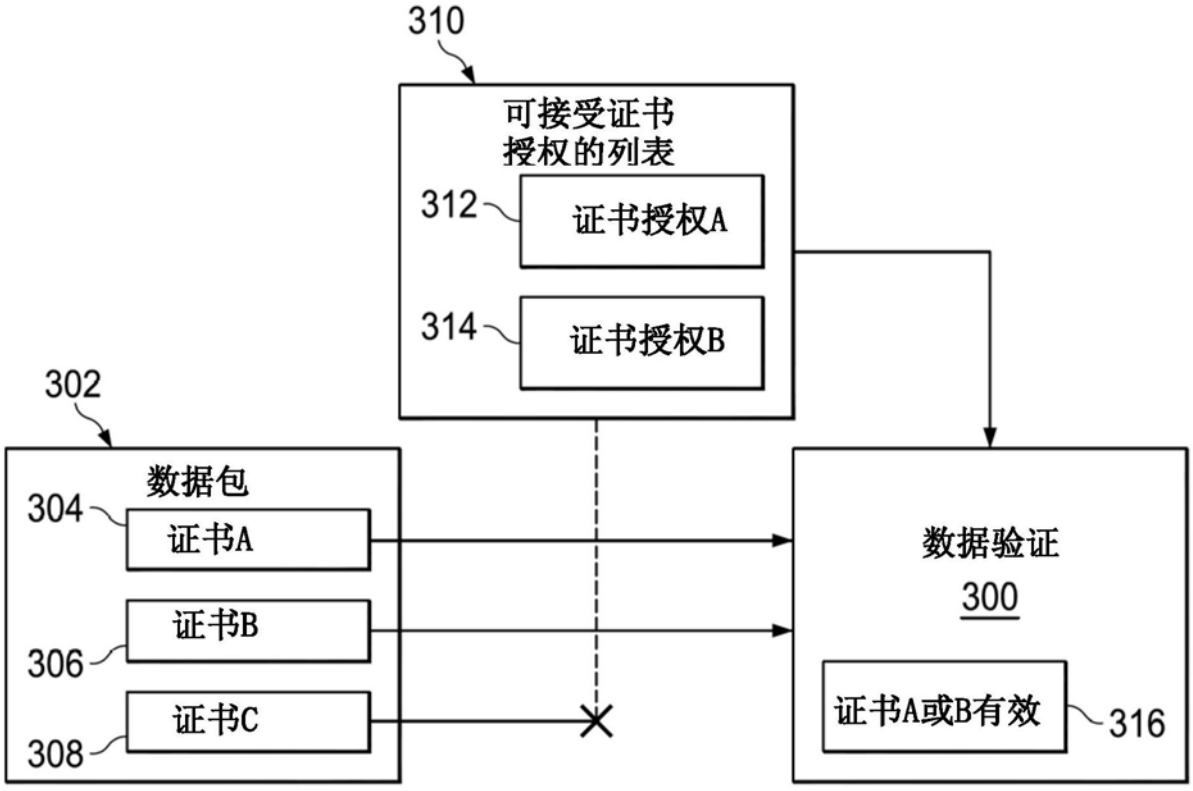

310
可接受证书
授权的列表
312
证书授权A
314
证书授权B
302
数据包
304
证书A
证书B
306
证书C
308
数据验证
300
证书A或B有效
316

图3

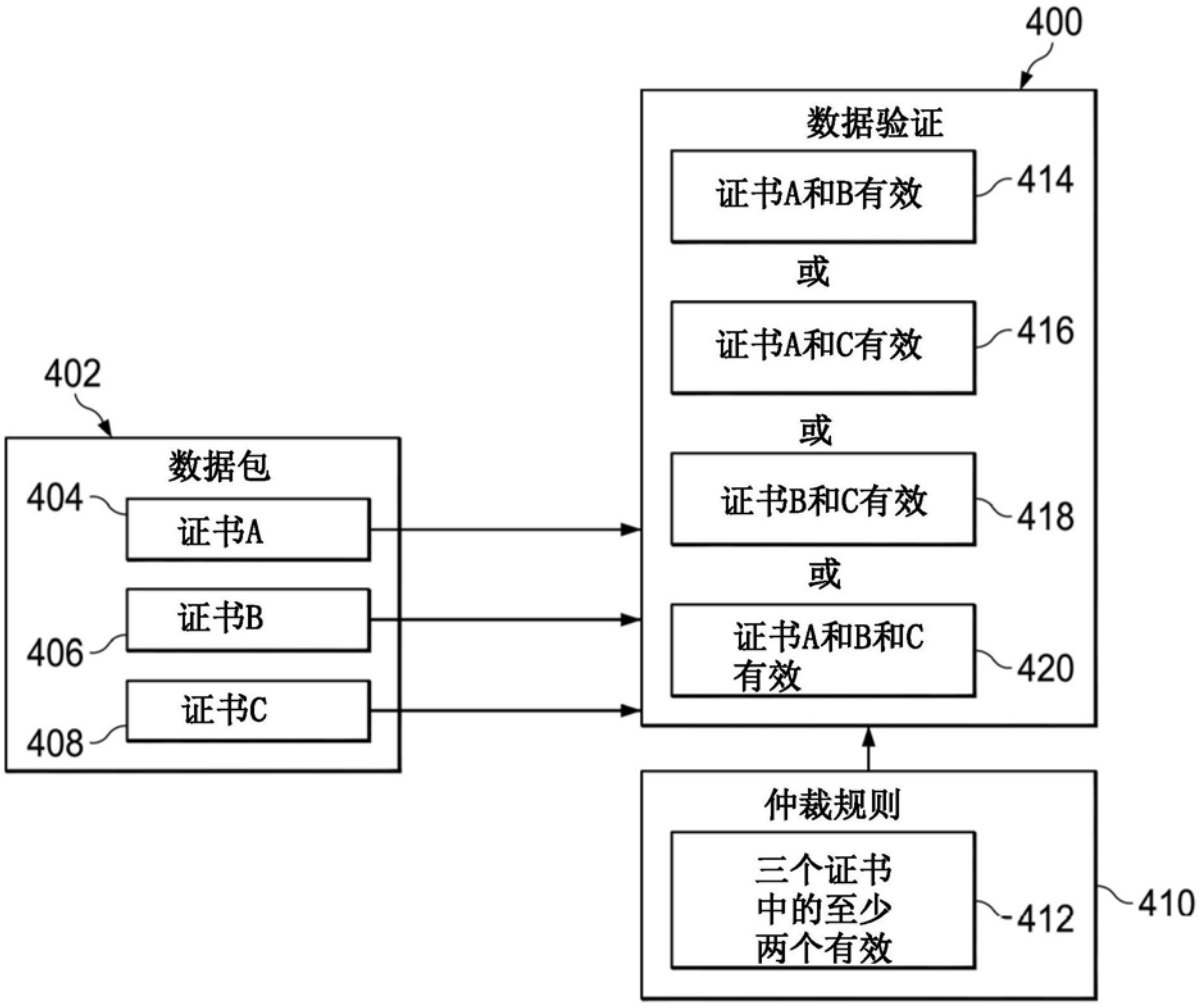

400
数据验证
证书A和B有效
414
或
证书A和C有效
416
或
证书B和C有效
418
或
证书A和B和C有效
420
402
数据包
404
证书A
证书B
406
证书C
408
仲裁规则
三个证书中的至少两个有效
412
410

图4

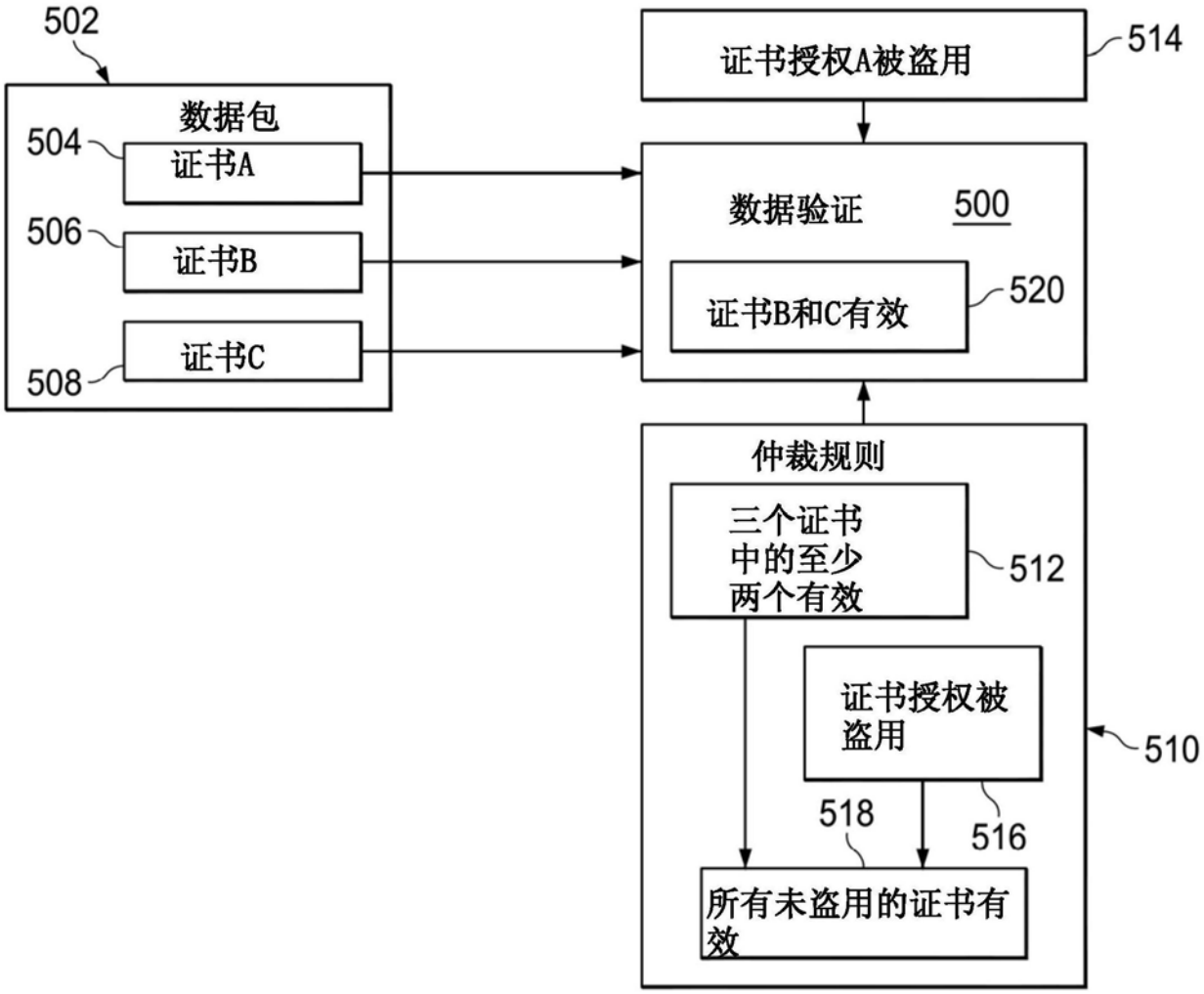

502
数据包
504
证书A
506
证书B
508
证书C
证书授权A被盗用
514
数据验证
500
证书B和C有效
520
仲裁规则
三个证书中的至少两个有效
512
证书授权被盗用
510
518
516
所有未盗用的证书有效

图5

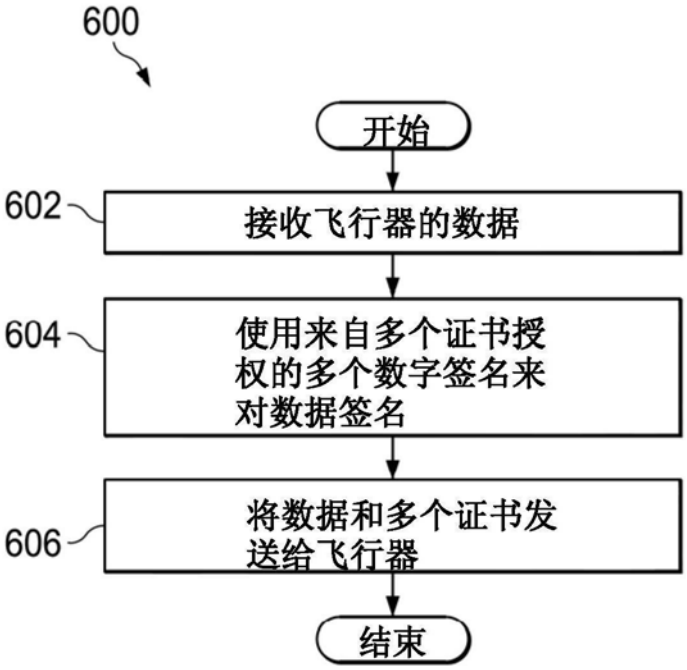

600
开始
602
接收飞行器的数据
604
使用来自多个证书授权的多个数字签名来对数据签名
606
将数据和多个证书发送给飞行器
结束

图6

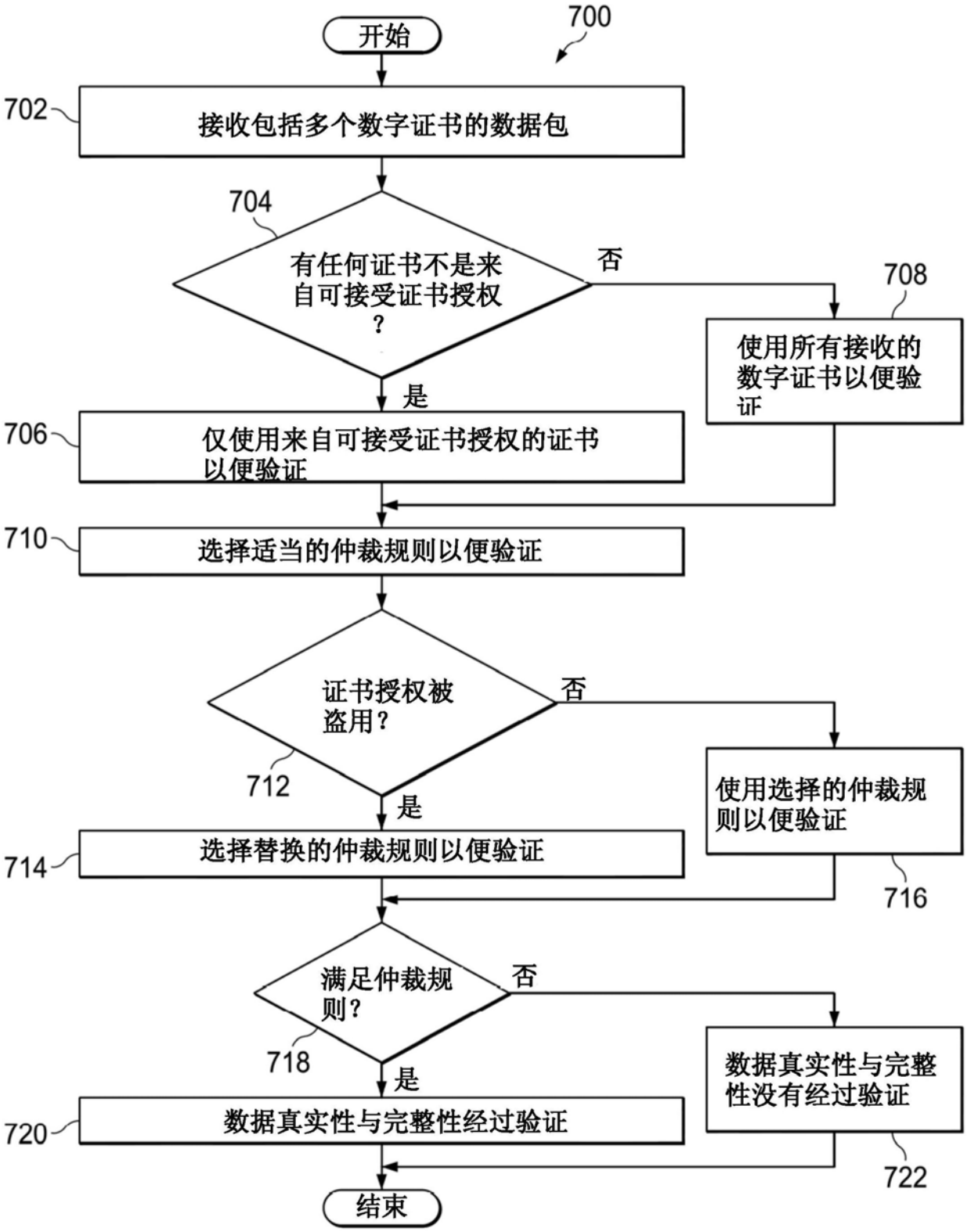

700
开始
702
接收包括多个数字证书的数据包
704
有任何证书不是来自可接受证书授权？
否
是
708
使用所有接收的数字证书以便验证
706
仅使用来自可接受证书授权的证书以便验证
710
选择适当的仲裁规则以便验证
证书授权被盗用？
否
是
712
使用选择的仲裁规则以便验证
714
选择替换的仲裁规则以便验证
716
满足仲裁规则？
否
是
718
数据真实性与完整性没有经过验证
720
数据真实性与完整性经过验证
722
结束

图7

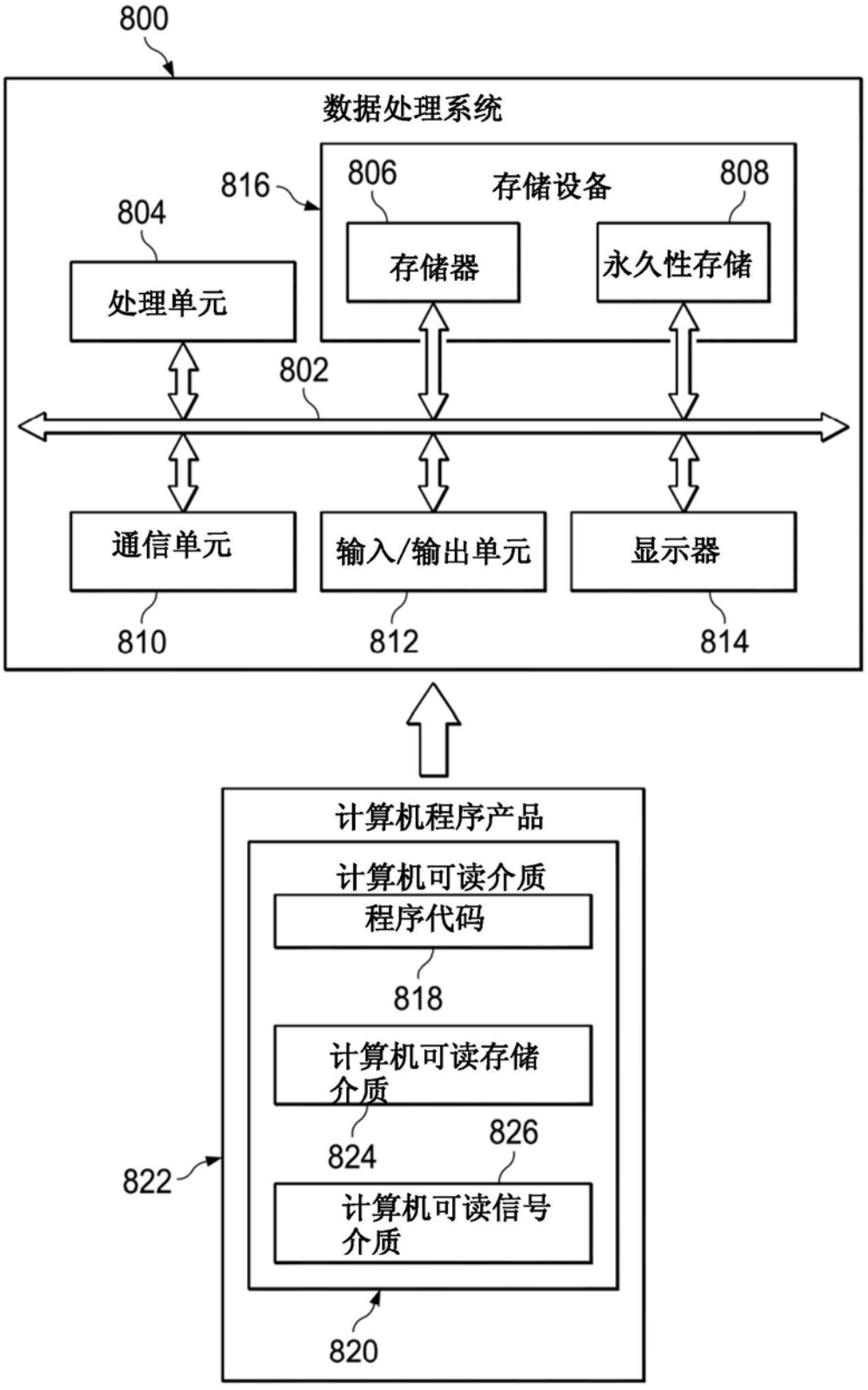

800
数据处理系统
816
806
存储设备
808
804
存储器
永久性存储
处理单元
802
通信单元
输入/输出单元
显示器
810
812
814
计算机程序产品
计算机可读介质
程序代码
818
计算机可读存储介质
824
826
822
计算机可读信号介质
820

图8