

[19] 中华人民共和国国家知识产权局



## [12] 发明专利说明书

专利号 ZL 01814836.0

[51] Int. Cl.

G06F 12/14 (2006.01)

G06F 12/16 (2006.01)

H04L 9/00 (2006.01)

[45] 授权公告日 2006 年 12 月 20 日

[11] 授权公告号 CN 1291326C

[22] 申请日 2001.8.28 [21] 申请号 01814836.0

[30] 优先权

[32] 2000.8.28 [33] US [31] 09/649,838

[86] 国际申请 PCT/US2001/026634 2001.8.28

[87] 国际公布 WO2002/019598 英 2002.3.7

[85] 进入国家阶段日期 2003.2.28

[73] 专利权人 康坦夹德控股股份有限公司

地址 美国特拉华州

[72] 发明人 T·塔 X·王

审查员 胡徐兵

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 张政权

权利要求书 3 页 说明书 15 页 附图 10 页

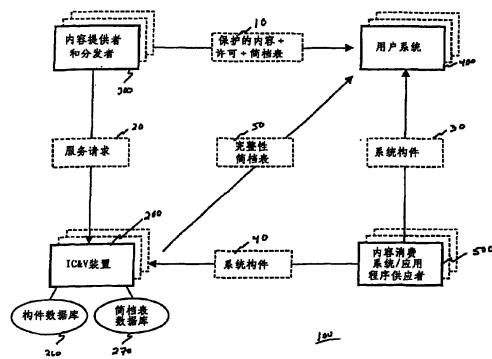
### [54] 发明名称

内容消费环境的完整性验证和确认的系统和方法

该信息在用户系统上的应用程序和/或系统构件与由内容消费系统/应用程序供应者分发的原始应用程序或系统构件之间，进行比较或完整性验证。

### [57] 摘要

诸如文档发行者或分发者的内容供应者，向用户提供例如被保护内容，以用于在信任的用户环境中的消费。通过提供完整性验证和确认设备，验证内容消费环境的真实性。内容供应者将包括例如许可协议和完整性简档表标识的被保护的数字内容版本，转送给用户。该简档表包括例如被允许与被保护内容结合使用的应用程序和系统构件。此外，内容供应者启动对完整性简档表的请求。该对完整性简档表的请求被转送到完整性验证和确认设备。如果不存在用于所请求的应用程序和/或系统构件的完整性简档表，则完整性验证和确认设备能够询问将系统构件供应给用户的内容消费系统/应用程序供应者。该供应者返回关于特定应用程序或系统构件的完整性验证和确认设备的验证信息。



1. 一种适于在内容消费环境中提供应用程序、系统或系统构件的完整性验证和确认的系统，所述系统包括用户系统、应用程序供应者以及完整性验证和确认设备，由此

所述应用程序供应者适于向所述用户系统分发应用程序、系统或系统构件，其特征在于，在所述系统中：

所述应用程序供应者适于向所述完整性验证和确认设备提供关于一个或多个应用程序、系统或系统构件的认证信息；

所述完整性验证和确认设备包含构件注册设备，它适于存储所述提供的关于一个或多个应用程序、系统或系统构件的认证信息；

所述完整性验证和确认设备适于确定并存储至少一个完整性简档表，该表包含可验证信息和用于定义一个或多个所述应用程序、系统或系统构件的环境的信息；以及

所述用户系统适于确定对内容的访问权，从而所述用户系统适于通过将由转送的完整性简档表定义的环境与所述一个或多个分发的应用程序、系统或系统构件进行比较，从而确认一个或多个所述分发的应用程序、系统或系统构件的完整性。

2. 如权利要求 1 所述的系统，其特征在于，所述完整性简档表包括具有由构件注册设备存储的认证信息的已注册应用程序、系统或系统构件的标识。

3. 如权利要求 1 所述的系统，其特征在于，所述完整性验证和确认设备包括维持完整性简档表的简档表数据库。

4. 如权利要求 1 所述的系统，其特征在于，还包括简档表验证设备，它适于通过将位于所述完整性简档表中的一个或多个应用程序、系统或系统构件标识与内容消费环境中的一个或多个应用程序、系统或系统构件相比较，以验证真实性。

5. 如权利要求 1 所述的系统，其特征在于，还包括注册应用程序设备，它适于从内容消费应用程序、系统或系统构件供应者中取得所述关于所述一个或多个应用程序、系统或系统构件的认证信息，并适于将所述认证信息提供到所述构件注册设备。

6. 如权利要求 1 所述的系统，其特征在于，所述完整性简档表包括所述环境的所述一个或多个应用程序、系统或系统构件的标识。

7. 如权利要求 1 所述的系统，其特征在于，还包括与所述内容消费环境耦合的内容供应者。

8. 如权利要求 1 所述的系统，其特征在于，如果简档表验证设备判定所述内容消费环境中的一一个或多个应用程序、系统或系统构件是非真实的，则禁止访问一个或多个文档。

9. 如权利要求 1 所述的系统，其特征在于，还包括简档表创建设备，它适于根据由构件注册设备存储的关于一个或多个应用程序、系统或系统构件的所述认证信息，创建所述完整性简档表。

10. 一种在内容消费环境中用于对应用程序、系统或系统构件的完整性验证和确认的方法，所述方法包括以下步骤：

取得用户系统的应用程序、系统或系统构件，所述应用程序、系统或系统构件由应用程序供应者分发；

其特征在于，所述方法包括以下步骤：

由所述应用程序供应者向完整性验证和确认设备提供关于一个或多个应用程序、系统或系统构件的认证信息；

由所述完整验证和确认设备确定完整性简档表，所述完整性简档表包括可验证信息和定义所述一个或多个应用程序、系统或系统构件的真实性环境的信息；以及

由所述用户系统确定对内容的访问权，所述确定包括通过将完整性简档表所定义的环境与所述内容消费环境中的所述一个或多个取得的应用程序、系统或系统构件相比较，来确认一个或多个所述取得的应用程序、系统或系统构件的完整性。

11. 如权利要求 10 所述的方法，其特征在于，还包括验证所述完整性简档表。

12. 如权利要求 10 所述的方法，其特征在于，所述访问权包括允许访问所述内容的权利或禁止访问所述内容的权利的至少一个。

13. 如权利要求 10 所述的方法，其特征在于，还包括数字化签名所述完整性简档表。

14. 如权利要求 10 所述的方法，其特征在于，还包括将已数字化签名的完整

性简档表转送到内容消费者。

15. 如权利要求 10 所述的方法，其特征在于，还包括在所述确定访问权的步骤前，建立防篡改环境。

16. 如权利要求 10 所述的方法，其特征在于，还包括验证所述完整性简档表。

17. 如权利要求 16 所述的方法，其特征在于，还包括在所述确定访问权的步骤前，加载经验证的完整性简档表。

18. 如权利要求 10 所述的方法，其特征在于，还包括确立所述内容消费环境的一个或多个应用程序、系统或系统构件至少不是监控、控制或记录过的一种。

## 内容消费环境的完整性验证和确认的系统和方法

### 技术领域

本发明涉及完整性（integrity）验证和确认。本发明具体涉及在内容消费环境中的完整性验证和确认。

### 背景技术

阻碍通过电子商务广泛分发数字文件的一个最重要的问题是，在如今数字文件的分发和使用中，缺乏对内容拥有者和供应者的知识产权保护。解决这个问题的工作被称为知识产权管理（IPRM），数字产权管理（DPRM），知识财产管理（IPM），数字权管理（DRM），权利管理（RM）和电子著作权管理（ECM）。

内容供应者经常希望他们的内容由具有所需特征和/或行为的验证应用程序和系统来消费。公开密钥基础结构（PKI）的直接使用，使应用程序和系统供应者能够确证他们自己的产品，使内容供应者能够验证用于消费其内容的应用程序和系统的完整性。

### 发明内容

不过，PKI 的直接使用产生了卖方和供应者间的多对多关系。这类关系可能标注得不完善，从而难以管理这类关系，难以有效实时地进行完整性验证。

内容供应者经常希望他们的内容由用希望的特征和行为的验证应用程序和系统来消费。通过控制内容消费环境的这些方面，内容供应者能够限制诸如复制，打印，嵌入，分发等使用。

例如，内容供应者可希望要求消费内容的系统带有某一等级完整性和权限管理能力，保护内容不被滥用。该内容供应者也可希望在用户系统上，保证没有诸如调试器，病毒，监听程序等，会挪用或“偷窃”内容或其它敏感信息的“异类”应用程序干扰内容消费应用程序。比如，在此处完全引用标题为“Document Distribution Management Method And Apparatus Using A Standard Rendering

“Engine And A Method And Apparatus For Controlling A Standard Rendering Engine”的代理号为 111325 000002 文件，在文中，通过控制用户系统的功能，限制用户访问和控制文件。

为了验证带有所需特征和行为的给定应用程序和系统，需要验证所有的应用程序和系统构件，来消费由验证应用程序确认的内容。

本发明描述了为内容消费环境提供验证和确认服务的系统和方法。在这样的系统中，内容供应者和内容消费系统/应用程序供应者间，引入了提供这些服务的完整性验证和确认设备。这个验证设备注册来自各个供应者的各个应用程序和/或系统，根据预定的选择确认这些应用程序和/或系统对内容供应者的完整性。通过使用这个设备，内容供应者能够“确信”(trust)完整性验证和确认系统。经过这个确信，供应者建立了允许消费其内容的一系列验证和确认设备的简档表，并且根据这个简档表，在用户系统上验证用户的这一系列应用程序和系统是真实的。

具体而言，这个发明的系统和方法为消费环境中的例如文档内容完整性提供了验证和确认服务。在这个环境中，在内容供应者、内容消费系统和应用程序供应者间，引入提供这些服务的完整性验证和确认设备，它们可以分布于诸如个人计算机，手提计算机，PDAs，多媒体显示装置，DVD 播放器，分布式网络电话，以及应用程序例如可以是文字处理器，文件浏览器，多媒体播放器等等。完整性验证和确认设备注册来自各个内容消费系统/应用程序供应者的各个应用程序和/或系统，并且对内容供应者证明这些应用程序和系统。用这个设备，内容供应者可以选择或确信这个完整性验证和确认设备，建立允许消费其内容的一系列应用程序和系统的简档表，并根据该简档表在用户系统上验证在其上的那个系列应用程序和系统是真实的。在这种方式中，可以对请求或提交的内容控制由用户访问或控制的范围。

在这里所述用的术语文档，是被分发或传送的任意信息主题单元，包括但不限于，信件，书，杂志，期刊，新闻报纸，其它报纸，软件，插件，照片和其它图像，音频和视频剪切，和其它多媒体表示。文档可以是纸张印刷形式，存储介质上的数据形式，或任意其它已知或未来将出现的各种介质或软件，例如包括光盘(CD)，数字视频光盘(DVD)，激光影碟，磁介质和磁光介质，等等。

本发明系统和方法提供完整性验证和确认服务。

本发明为内容消费环境分别提供用于完整性验证和确认服务的系统和方法。

本发明也为确定完整性简档表分别提供系统和方法。

本发明此外还为验证一个或更多系统环境的完整性分别提供系统和方法。

本发明也为管理完整性简档表，系统和系统构件信息提供系统和方法。

本发明另外还通过使用完整性简档表，提供在用户系统上执行完整性检查的系统和方法。

特别是诸如文档发布者或分发者的内容供应者，它启动对完整性简档表的请求，并转送到完整性验证和确认设备。如果还不存在用于请求的应用程序和系统构件的完整性简档表，完整性验证和确认设备将对例如向用户提供各种系统构件和/或应用程序的内容消费系统/应用程序供应者进行询问。内容消费系统/应用程序提供者返回关于特别应用程序或系统构件的完整性验证和确认设备的认证信息。在用户系统上的应用程序或系统构件和由内容消费系统/应用程序供应者分发的初始应用程序或系统构件之间，能够通过认证信息进行比较或完整性验证。

在构件数据库中存储用于系统应用程序和构件的认证信息，在简档表数据库中存储内容供应者所需的简档表。另一方面，内容消费系统/应用程序供应者也可以保持认证信息数据库，其中认证信息可以直接转送到完整性验证和确认设备各自的数据库，而无须完整性验证和确认设备来确定完整性简档表。接着，对应于确定的完整性简档表的完整性简档表的标识被返回给内容供应者。

诸如文档分发者的内容供应者例如向用户提供被保护的内容。内容供应者向用户转送被保护的数字内容版本，例如包括许可协议和完整性简档表标识。完整性简档表标识包括可与被保护内容联合使用的应用程序和系统构件，和用于那些系统/应用程序的完整性简档表标识。

在用户系统的请求下，拥有了从内容消费系统/应用程序供应者取得认证信息，完整性验证和确认设备将完整性简档表转送到用户系统。利用这个完整性简档表可执行用户系统的完整性验证。如果确定用户系统的构件/应用程序是真实的，则例如根据附加的简档表信息，就可由用户应用程序和系统访问由内容供应者提供的数字内容。

不过须注意，对完整性验证的请求发起不一定需要有供应者。反过来说，通过 嵌入在简档表识别信息中的随被保护内容从内容供应者转送到用户系统的软件应用程序，能够发起完整性请求。

另外，内容供应者也可以用作完整性验证和确认设备。在这种情况下，内容供应者通过取得适当的认证信息并确定完整性简档表是供内容供应者自己使用时，

自己就可以进行完整性验证和确认服务。

此外，内容消费应用程序/系统供应者也能够起到完整性验证和确认设备的作用。在这种情况下，该内容消费应用程序/系统供应者例如也可以提供完整性简档表和相应的应用程序和/或系统构件。

根据本发明的第一方面，提供一种适于在内容消费环境中提供应用程序、系统或系统构件的完整性验证和确认的系统，所述系统包括用户系统、应用程序供应者以及完整性验证和确认设备，由此所述应用程序供应者适于向所述用户系统分发应用程序、系统或系统构件，其中，在所述系统中：所述应用程序供应者适于向所述完整性验证和确认设备提供关于一个或多个应用程序、系统或系统构件的认证信息；所述完整性验证和确认设备包含构件注册设备，它适于存储所述提供的关于一个或多个应用程序、系统或系统构件的认证信息；所述完整性验证和确认设备适于确定并存储至少一个完整性简档表，该表包含可验证信息和用于定义一个或多个所述应用程序、系统或系统构件的环境的信息；以及所述用户系统适于确定对内容的访问权，从而所述用户系统适于通过将由传送的完整性简档表定义的环境与所述一个或多个分发的应用程序、系统或系统构件进行比较，从而确认一个或多个所述分发的应用程序、系统或系统构件的完整性。

根据本发明的第二方面，提供一种在内容消费环境中用于对应用程序、系统或系统构件的完整性验证和确认的方法，所述方法包括以下步骤：取得用户系统的应用程序、系统或系统构件，所述应用程序、系统或系统构件由应用程序供应者分发；其中，所述方法包括以下步骤：由所述应用程序供应者向完整性验证和确认设备提供关于一个或多个应用程序、系统或系统构件的认证信息；由所述完整验证和确认设备确定完整性简档表，所述完整性简档表包括可验证信息和定义所述一个或多个应用程序、系统或系统构件的真实性环境的信息；以及由所述用户系统确定对内容的访问权，所述确定包括通过将完整性简档表所定义的环境与所述内容消费环境中的所述一个或多个取得的应用程序、系统或系统构件相比较，来确认一个或多个所述取得的应用程序、系统或系统构件的完整性。

在下面较佳实施例的详细描述中，描述了本发明上述和其它的特征和优点。

## 附图说明

通过引用附图，将详细描述本发明的较佳实施例，其中：

图 1 是根据本发明，示出完整性验证和确认系统的第一个示范实施例的功能概图。

图 2 是根据本发明，示出完整性验证和确认系统的第一个示范实施例的功能方框图。

图 3 是根据本发明，示出完整性验证和确认系统的示范工作流程图。

图 4 是根据本发明，示出的完整性简档表的示范结构。

图 5 是根据本发明，示出的示范环境堆栈。

图 6 是根据本发明，示出的示范环境堆栈。

图 7 是根据本发明，示出的示范堆栈工作流程。

图 8 是根据本发明，示出的示范堆栈工作流程。

图 9 是根据本发明，示出的操纵堆栈的示范方法。

图 10 是根据本发明，通过使用调试防止动态篡改的示范方法。

图 11 是根据本发明，用于完整性验证和确认方法的一个示范实施例的概要流程图。

图 12 是根据本发明，用于注册应用程序和/或系统的方法的一个示范实施例的概要流程图。

图 13 是根据本发明，用于确定完整性简档表的方法的一个示范实施例的概要流程图。

图 14 是根据本发明，用于验证完整性认证器的完整性的方法的一个示范实施例的概要流程图。

### 具体实施方式

本发明提供了确定内容消费环境完整性的验证和确认服务的系统和方法。在该系统中一个或更多的内容供应者和一个或更多的内容消费系统及应用程序供应者间，引入了完整性验证和确认设备。该完整性验证和确认设备从内容消费供应者和/或系统供应者取得认证信息。该认证信息使内容供应者相信内容将被提供到的环境。这样，根据由内容消费应用程序和系统供应者接收的认证信息，建立完整性简档表。接着，这个简档表转送到用户系统，确认用户没有在未授权的方式下，改变，修改，或干涉内容供应者提供的数字内容。

图 1 示出用于执行完整性验证和确认的示范系统。具体而言，完整性验证和

确认系统 100 包括完整性验证和确认设备 200, 内容供应者和/或分发者 300, 用户系统 400, 内容消费环境/应用程序供应者 500, 构件数据库 260 和简档数据库 270。

在示范的操作环境中, 内容消费系统/应用程序供应者 500 为用户提供了应用程序, 系统和/或软件/硬件构件。用户系统 400 使文档等数字内容消费, 该内容由内容供应者和 300 分发者提供。为验证用户系统 400 的完整性, 完整性验证和确认设备 200, 采集并注册来自内容消费系统/应用程序供应者 500 的, 关于各个应用程序, 系统和/或软件/硬件构件的认证信息。使用这个认证信息, 根据来自内容供应者 300 的服务请求 20, 完整性验证和确认设备 200 确定并验证一个或更多的应用程序, 系统和/或系统构件的完整性简档表。然后, 这个确定的完整性简档表 50 转送到用户系统 400, 这样可以确定用户系统 400 的完整性。

在操作中, 内容供应者和分发者 300 提供文档等数字内容到用户系统 400。用户系统 400 包括一个或更多的系统构件, 诸如硬件构件和/或各种软件应用程序。这些应用程序和硬/软件构件通常由用户从一个或更多的内容消费系统/应用程序供应者 (诸如计算机供应商, 软件仓库, 应用程序供应者, 等等) 得到。这些应用程序以及硬件和软件构件, 随后, 如果没有完成组装, 将由用户在适当的时间候组装和安装, 使用户能消费文档等内容。

这样, 在使用用户环境的应用程序和硬件/软件的过程中, 用户可能想要查看文档等被保护的内容。这样, 用户 400 将从内容供应者 300 请求一个或更多的文件, 诸如电子书籍, 多媒体文件, 图像, 模板, 等等。收到这些请求后, 内容供应者和分发者 300 可以将在被保护形式中的所需内容和简档表标识 10 提供给最终用户 400。这个简档表标识 10 包括诸如关于从中可见到的应用程序被保护内容的细节, 和在特定软/硬件环境中被提供内容可以操作的范围。

此外, 内容供应者 300 可以把服务请求 20 转送到完整性验证和确认设备 200。该服务请求 20 可例如包括一个构件和/或软件应用程序的列表, 在其上列有内容供应者 300 允许用户系统 400 消费所分发的被保护内容。由完整性验证和确认设备 200 确定, 是否在服务请求 20 中标识的构件和应用程序/软件有存储在构件数据库 260 中和/或简档表数据库 270 中的相关认证信息, 如果没有这种信息, 则该设备 200 可向一个或更多的内容消费系统/应用程序供应者 500 请求关于特定应用程序, 系统, 硬/软件构件等的认证信息。用这个认证信息, 该设备 200 将在构件数据库 260 中存储属于应用程序和系统构件的信息。另外, 完整性验证和确认设备

200 可以为一个或更多的应用程序开发完整性简档表。用这个确认应用程序、系统和系统构件的认证的信息，该完整性验证和确认设备 200 将完整性简档表 50 转送到用户系统 400。这个完整性简档表 50 用于确认用户系统 400 的系统，系统构件和/或应用程序的真实性，如果被确定为真实的，则将被保护内容 10 解保护，从而用户系统 400 可依照完整性简档表，见到或操作被保护内容。

图 2 是根据本发明的一个示范实施例，示出的完整性验证和确认环境 100 的构件概图。具体而言，完整性验证和确认环境 100 包括一个或更多的内容供应者 300，一个或更多的用户系统 400，一个或更多的完整性验证和确认装置 200，和一个或更多的内容消费系统/应用程序供应者 500。

内容供应者 300 例如可包括控制器 310，存储器 320，I/O 控制器 330 和内容数据库 340。不过须注意，内容供应者 300 也可以用更常规的方式分发内容。例如，内容供应者可以分发含有内容的光盘，光盘可被通过邮政服务邮寄给用户。本发明的系统和方法可用任意类型的分发和分配处理。

完整性验证和确认设备 200 包括控制器 210，存储器 220 和 I/O 控制器 230，数字签名装置 240，构件注册装置 250，构件数据库 260，简档表数据库 270，简档表创建装置 280，简档表分发装置 290 和简档表验证装置 295。完整性验证和确认设备 200 提供下列服务：构件注册服务和完整性简档表服务。注册服务能够对来自各个供应者的应用程序，系统，和/或软/硬件作为真实的进行注册，并带有所需的特征，目的和/或行为。

完整性简档表服务为内容供应者提供服务，建立和检索完整性简档表。完整性简档表是一种具有任选项数字签名的文档，包含可验证的信息和一系列要消费被保护文档内容的已注册的系统构件。完整性简档表一旦创建，其标识会返回给内容供应者。内容供应者包括完整性简档表标识和任选项被保护文档的使用许可。当消费被保护文档的内容并需要传送给用户的系统和环境的本地完整性验证时，完整性简档表可从完整性验证和确认设备 200 检索到用户系统。

用户系统可 400 包括控制器 410，存储器 420，I/O 控制器 430，存储设备 440，完整性认证设备 450 和简档表存储设备 460。不过须理解，这个示范用户系统是基于计算机模型，而用户系统的构件可以依照例如所消费内容的类型而改变。通常本发明的系统和方法可包括任何带有完整性可被检验的部分的用户系统。

内容消费系统/应用程序供应者 500 可例如包括，控制器 510，存储器 520，

I/O 控制器 530, 注册应用程序设备 540, 应用程序数据库 550 和系统数据库 560。不过, 类似于内容供应者 300, 内容消费系统/应用程序供应者可以有几个不同的形式, 该形式依赖于内容消费系统/应用程序供应者 500 提供的系统和/或应用程序。例如, 如果内容消费系统/应用程序供应者 500 提供了特定的硬件构件, 内容消费系统/应用程序供应者 500 可以不保持应用程序和系统数据库。另外, 例如系统/设备构件供应者可以在盘片上直接发送认证信息到完整性验证和确认设备 200。

此外, 内容消费系统/应用程序供应者 500 可以和内容供应者 300 协调一起促进完整性简档表的确定。通常, 内容消费系统/应用程序供应者可以同样是能够提供硬件或软件和认证信息的任何实体。

虽然在这个示范实施例中, 内容消费系统/应用程序供应者 500 由不同的系统构件组成, 须理解内容消费系统/应用程序供应者 500 可以是计算机分配者, 软件开发者, 软件供应者, 软件分发者等等。这样, 内容消费系统/应用程序供应者 500 能够提供允许消费由内容供应者 300 提供的内容的设备和/或软件。

完整性验证和确认环境 100 的各种构件能够通过链路 5 互相通信, 链路 5 可以是有线或无线链路, 或任意其它已知或将来开发的, 能够从互连构件发送或接收电子数据的构件。例如链路 5 可以是一个或多个分布网络, 其依次连接到一个或多个附加的完整性验证和确认环境 100, 或连接到内容供应者 300, 用户系统 400, 内容消费系统/应用程序供应者 500 和完整性验证和确认设备 200 中任意一个或多个的多重实例。

##

在用户系统 400 的用户请求下, 内容供应者 300 将文档等内容分发到用户系统 400。具体而言, 从用户系统 400 的内容供应者 300 可以接收请求。这个请求, 通过 I/O 控制器 330 接收, 并由控制器 310 结合存储器 320 处理, 以从内容数据库 340 检索请求内容。比如, 内容供应者 300 可以是在线内容供应者, 书店, 软件供应者, 或任意其它希望将例如文档等内容提供给用户的内容供应者。

在接收到来自用户系统 400 的内容请求后, 内容供应者 300 将所请求内容和关于被保护内容的附加信息送回到用户系统。这个附加信息可以包括简档表标识。另外, 附加信息可以包括指示用户系统以请求简档表的信息, 和在启用内容前的完整性验证。

##

因而，在存储在一个或多个存储器 420 和存储设备 440 中的控制器 410 的指示下，用户系统 400 通过 I/O 控制器 430，接收一个或更多的所需内容，附加信息和简档表标识。

在一个示范实施例中，内容供应商 300 可以启动，诸如来自完整性验证和确认设备 260 的，对完整性简档表的服务请求 20。完整性验证和确认设备 260 通过 I/O 控制器 230 并结合控制器 210 和存储器 220，接收来自内容供应商 300 的服务请求。

如上所述，完整性验证和确认设备 200 包括构件数据库 260 和简档表数据库 270。构件数据库 260 存储属于系统和系统构件的，可以由一个或更多的内容消费系统/应用程序供应商 500 分发的认证信息。类似地，简档表数据库 270 为一个或多个单个内容供应商 300 存储可验证信息和一系列要消费被保护文件内容的注册系统构件。

这样，在为完整性简档表接收来自内容供应商 300 的请求后，在控制器 210 的指引下和存储器 220 的协助下，完整性验证和确认设备 200 查找构件数据库 260 和简档表数据库 270，确定是否已经存在对应于服务请求信息的认证信息。

另外，完整性验证和确认设备 200 可以执行在线验证服务。在线验证服务提供比如在完整性验证和确认设备 200 内实时执行在线完整性验证。为启动这个服务，将一个称作完整性认证器的软件转送到用户系统 400。完整性认证器采集本地软件和/或硬件构件的信息。另外，完整性认证器可以是专用设备，诸如图 2 所示的完整性认证设备。采集的关于本地软件和/或硬件构件信息和完整性简档表标识一起被返回给完整性验证和确认设备 200，从而执行在线完整性检验。构件注册设备 250 检查来自各自的供应者的软/硬件构件，并在构件数据库 260 中存储标识信息。属于软/硬件构件的信息可以被进行散列操作，又散列值可以用作真实软件/硬件的标识。但是须注意，标识各个软/硬件构件的信息可是任何已知的或未来将开发的能允许对硬件和/或软件的真实片段进行标识的方法。

在下面叙述特定软件和/或硬件构件的注册。例如，内容消费系统/应用程序供应商 500 可与完整性验证和确认设备 200 的通信以请求注册服务，或者，另一方面，标识和验证确认设备 200 也可与内容消费系统/应用程序供应商 500 通信以确保认证信息。在这个例子中，注册应用程序设备 540 结合控制器 510，存储器 520

和 I/O 控制器 530，查找一个或多个应用程序数据库 550 和系统数据库 560，以确保关于特定软件和/或硬件的信息，例如供应者名称，构件标识，诸如序列号，版本号，创建号等，或应用程序本身。

例如，在一个特别的操作情景中，完整性验证和确认设备 200 可以从内容消费系统/应用程序供应者 500 请求诸如软件应用程序的特定应用程序，而不是从该特定内容消费系统供应者 500 处获取认证信息。这样，完整性验证和确认设备 200 不需要认证信息，就可以直接从内容消费系统/应用程序供应者 500 确保特定的软件应用程序。

构件注册设备 250 验证构件信息，可任选地计算可被例如用于作为真实的软件和/或硬件标识的散列值。然后，构件注册设备 250 在构件数据库 260 中存储构件信息和散列值。

另一方面，内容消费系统/应用程序供应者 500 可以不发送软件和/或硬件构件到注册应用程序设备 540，而是连接到构件注册设备 250，以下载小的诸如注册应用程序的软件应用程序，并在本地执行这个程序。这个注册应用程序将检查目标软件/硬件构件，并且将属于这个软件/硬件构件的信息或许和诸如散列值的完整性数据一起，发送回到随后可能在构件数据库 260 中存储关于该构件的认证信息的构件注册设备 250。

另外，简档表创建设备 280 为软件创建完整性简档表。特别地，可以从构件数据库检索各个软件应用程序的诸如散列值的完整性数据并将其存储。该简档表还包括了任选的构件间的互动关系。这种关系用于标识构件的调用和返回次序，防止构件和其它构件发生不希望的交互动作。然后，对完整性简档表的内容作数字化签名，并把所产生的签名添加到完整性简档表。每个完整性简档表与唯一的标识相关联。

图 3 示出了由完整性验证和确认设备 200 提供的输入，输出，服务和操作的示范性工作流程。特别对于构件注册服务，可把关于特别构件的构件标识以及任选地把它的元信息转送到构件注册设备 250。构件注册设备 250 在构件数据库中注册该构件，并可带有所需的特征，目的和行为。然后，构件注册设备 250 将已注册的构件的标识返回到例如内容消费系统/应用程序供应者，并使该标识可用于例如内容供应者 300。

在简档表创建中，简档表创建设备 280 接收已注册构件的标识。已注册构件

标识可先与相关构件信息（如果有的话）结合，然后数字化签名并被存储到简档表数据库中。将完整性简档表标识返回给请求者。

类似的，简档表分发设备 290 接收完整性简档表标识。然后，询问简档表数据库 270，确定对应于完整性简档表标识的完整性简档表是否可供使用。如果可以，则将完整性简档表返回给请求者。不然，则在简档表创建设备 280 的辅助下，确定完整性简档表。

简档表验证设备 295 接收识别一个或更多的构件和完整性简档表标识的信息。简档表验证设备比较构件标识，完整性简档表标识和相应的完整性简档表，来确定验证数据。如果简档表与构件和标识符合，则验证了系统的完整性。不然，该系统就不是完整性简档表所指定的系统，或在某些方面被改动了。

图 4 示出了示范的完整性简档表。通过简档表创建设备 280 可以创建这个示范完整性简档表。为了给已认证的内容供应者建立完整性简档表，可开始请求创建一个完整性简档表。例如，供应者可以与完整性验证和确认设备 200 接触，请求创建完整性简档表，然后发送软件和/或硬件构件的名称清单给完整性验证和确认设备 200。接着，简档表创建设备 280，从构件数据库 260 检索诸如各个构件的完整性或散列值的标识。然后，该设备确定各个构件的包含诸如完整性或散列值的认证信息的完整性简档表，和其它信息，诸如完整性简档表标识，版本号，创建日期，构成日期，内容供应者名称，以及例如可任选的任何软件和/或硬件构件间的互动关系。

简档表创建设备 280 将已确定的完整性简档表转送到随后可对简档表内容签名的数字签名器 240。然后，简档表创建设备 280 在简档表数据库 270 中存储已签名简档表，并且将简档表标识返回内容供应者 300。

在创建例如用于被保护文档内容的使用许可时，内容供应者 300 能够任选地在使用许可中包括完整性简档表标识。在用户系统 400 上，完整性简档表将被用于验证鉴别在环境调用堆栈中的所有软件/硬件构件。这保证只能由授权的软件/硬件构件或任何它们的组合消费敏感信息。

简档表分发设备 290 接收为得到完整性简档表的请求，从简档表数据库 270 检索它们，并将完整性简档表返回到各个请求者。类似地，简档表验证设备 295 接收为一个或多个系统环境验证用户系统的请求。该简档表验证设备 295 根据完整性简档表，采集关于软件/硬件构件的信息，将信息与简档表核对，并且将核对后

的结果返回请求者。

用户系统 400 包括完整性认证设备 450。后者例如可在任何内容消费应用程序的顶层运行。

这样，图 5 示出在用户系统 400 上的验证系统完整性的示范系统环境堆栈。特别地，用户系统环境堆栈包括完整性认证器和一个或多个系统构件。

图 6 示出了环境堆栈的示例，它包括完整性认证器，插件，翻译(render)应用程序，操作系统，操作系统(OS)引导，和各个硬件。

在示范操作环境中，完整性认证设备 450 包含它自己的加密/解密密钥对和标识验证和确认设备的验证密钥。对于这个发明的防篡改方面，这些密钥可以隐藏在和/或嵌入在完整性认证设备 400 中。对那些需要使用用户信息或包含敏感文档和数据的应用程序，完整性认证设备 450 可以使用相关联的完整性简档表，来验证所有在用户系统环境的调用堆栈上的软件/硬件构件。

完整性验证设备 450 先用完整性验证和确认设备的验证密钥来验证简档表的签名。如图 7-9 所示，一旦验证了该签名，完整性认证设备 450 检查当前调用堆栈，并用在完整性简档表中提供的信息，开始认证在调用堆栈上的各个软件/硬件构件。该调用堆栈是由存储图像和所包含的函数或程序组成的连续存储块。该堆栈以后进先出的概念操作，且堆栈的基本操作是堆栈“压入”和堆栈“弹出”。压入用于把图像存储到堆栈上，推进到堆栈顶部的位置。弹出用于把数据从堆栈中移出，并将堆栈顶部恢复到先前的位置。

对于调用堆栈，当前执行的函数的图像处于堆栈顶部。在当前执行的函数启用或调用下一个函数后，下一个函数的存储图象压入到调用堆栈顶部，而调用堆栈的顶部指向下一个函数的图像。各部分堆栈图象在完成调用函数的执行后，将包含地址或返回指令。

图 10 示出怎样保护执行环境。特别为保护完整性认证器(IA)，由作为 IA 一部分的信任的应用程序监控该 IA 的执行。该监控进程，诸如应用程序，可以是防止 IA 被系统中任意其它进程或应用程序监测的调试器或特定进程。在这样的环境中，当进程只能由一个进程调试时，该信任的监控程序能够用作调试器。由于监控程序是信任的应用程序，监控程序的完整性必需处于当前完整性简档表中。因此，IA 在加载和运行前，将核对该信任的应用程序的完整性。信任的监控应用程序的一个功能是防止 IA 被其它进程监控，控制和捕获。该应用程序的另一个功能是监

控当前环境，并确定环境中的改变是否是有效的。不过和 IA 相似，也必需保护被信任的控应用程序，而 IA 则扮演了保护信任的监控应用程序不被其它应用程序监控，捕获和/或控制的监控器的角色。这样的双重保护机制创造了防止其它应用程序监控该完整性认证器运行的封闭系统。

图 11 示出操作完整性验证和确认设备的示范方法。具体而言，控制从步骤 S100 开始，接着执行步骤 S110。在步骤 S110，确定完整性简档表。在下面的步骤 S120，验证完整性简档表。其后，在步骤 S130，将完整性简档表转送给用户。然后控制进入步骤 S140。

在步骤 S140，核对用户系统的完整性。接着，在步骤 S150，确定用户系统是否是真实的。如果用户系统是真实的，则控制进入允许用户访问所需内容的步骤 S160。不然，控制跳到拒绝访问内容的步骤 S170。然后，控制进入控制流程结束的步骤 S180。

图 12 示出根据本发明的注册构件/硬件和/或软件的示范方法。具体而言，控制从步骤 S200 开始，进入步骤 S210。在步骤 210，开始注册服务。下面，在步骤 S220，构件供应者提供关于特定构件/硬件和/或软件的认证信息。然后，在步骤 230，验证关于特定构件/硬件和/或软件的信息。接着，控制进入步骤 S240。

在步骤 240，确定完整性值是否需要被确定。如果需要，则控制进入确定完整性值的步骤 250。不然，控制跳到存储关于构件/硬件和/或软件的认证信息的步骤 260。

下面，在步骤 S270，确定是否要存储完整性值。如果需要，控制进入存储完整性值的步骤 S280。不然，如果不需要存储完整性值，控制跳到控制流程结束的步骤 S290。

图 13 示出根据本发明确定简档表的示范方法。具体而言，控制从步骤 S300 开始，进入步骤 S310。在步骤 S310，开始确定简档表。下面在步骤 S320，得到诸如构件和/或硬件或软件的标识的名称。然后，在步骤 S330，检索用于构件/硬件或软件的标识。接着，控制进入步骤 S340。

在步骤 S340，确定完整性简档表。下面，在步骤 S350，数字化签名完整性简档表。然后，在步骤 S360，存储已数字签名的完整性简档表。接着，控制进入步骤 S370。

在步骤 S370，已签名的完整性简档表随后被转送到请求者，诸如内容消费系

统/应用程序供应者. 然后控制进入控制流程结束的步骤 S380。

图 14 示出了根据一个方面的验证完整性认证器的完整性的示范方法。控制从步骤 S400 开始，并进入步骤 S410。在步骤 S410，核对完整性认证器的完整性。下面，在步骤 S420，确定完整性认证器是否有效。如果有效，控制进入步骤 S430，不然，控制跳到步骤 S540。

在步骤 S430，建立防篡改环境。下面在步骤 S440，验证完整性简档表。然后，在步骤 S450，确定完整性简档表是否有效。如果有效，控制进入步骤 S460，不然，控制跳到步骤 S540。

在步骤 S460，加载完整性简档表。下面，在步骤 S470，构造关于图 6 示出的当前运行环境的调用堆栈。在调用堆栈的底部是一系列硬件和/或设备，而所有的软件构件朝着堆栈顶部。堆栈中的构件关系是，较低的构件调用就在其上的那个构件。一旦构建了调用堆栈，就定位了包含最近被执行构件的运行图象的堆栈顶部。这样，在堆栈中各个构件的执行图象帮助识别调用构件。然后，在步骤 S480，检索调用构件的标识。接着，控制进入步骤 S490。

在步骤 S490，将构件的完整性与完整性简档表核对。下面，在步骤 S500，确定构件是否有效。如果有效，控制进入步骤 S510。不然，控制跳到步骤 S540。

在步骤 S510，确定堆栈是否为空。如果堆栈为空，控制跳到步骤 S520。不然，控制跳到步骤 S530。在步骤 S520，定位堆栈中的下一个构件，并把该构件设置为当前堆栈帧。然后，控制回到步骤 S480 进行验证。

在步骤 S530，完成完整性验证，控制进入控制流程结束的步骤 S550。

在步骤 S540，完整性检查失败，控制进入控制流程结束的步骤 S550。

如图 1-2 所示，完整性验证和确认设备较佳地用单程序通用计算机或分立程序通用计算机来实现。不过，该设备也能够用专用计算机，编程微处理器或微控制器和外围集成电路，ASIC，或其它集成电路，数字信号处理器，诸如分立元件电路的硬布线电子或逻辑电路，诸如 PLA，PLD，FPGA，PAL 等的可编程逻辑设备来实现。一般而言，可实现有限状态机器的任何设备从而可实现图 11-14 中示出流程图，从而可用于实现完整性验证和确认设备。

此外，在各种计算机或工作站硬件平台中，提供可移植源代码的环境内，使用对象或面向对象软件开发技术的软件中，易于实现所述方法。另外，所揭示的完整性验证和确认设备可部分或完全地用标准逻辑电路或 VLSI 结构的硬件来实现。

---

是否使用软件或硬件来实现根据本发明系统和方法取决于系统需要的速度和/或效率，特定的功能以及准备使用的特定的硬件或软件系统，或微处理器或微型计算机系统。不过，本领域的普通技术人员，无需对所述功能描述进行过多试验，就可易于将上述完整性验证和确认设备和方法，采用任何已知的或未来将开发的系统、结构、设备和/或软件加上计算机技术的知识以硬件或软件来实现。而且，所揭示的方法易于作为在可编程的通用计算机，专用计算机，微处理器，服务器等设备上的被执行的软件而实现。在这种情况下，本发明的方法和系统可用作嵌入在个人计算机或服务器中的例行程序而实现，这种例行程序比如是作为服务器或图形工作站的资源的 JAVA®或 CGI 脚本，嵌入在专用完整性验证和确认设备，web 浏览器，web TV 界面，PDA 界面，多媒体演示设备等中。通过将该系统和方法物理结合到诸如图形工作站或专用完整性验证和确认设备的软件和/或硬件系统中，也可以实现该完整性验证和确认设备。

显然，本发明提供了用于完整性验证的系统和方法。本发明已描述了较佳的实施例，而对本领域的普通技术人员而言，相应的替换方案，修改和变化是显然的。因此，申请人认为，在本发明的精神和范围中包含了所有这样的替换方案，修改和变化。

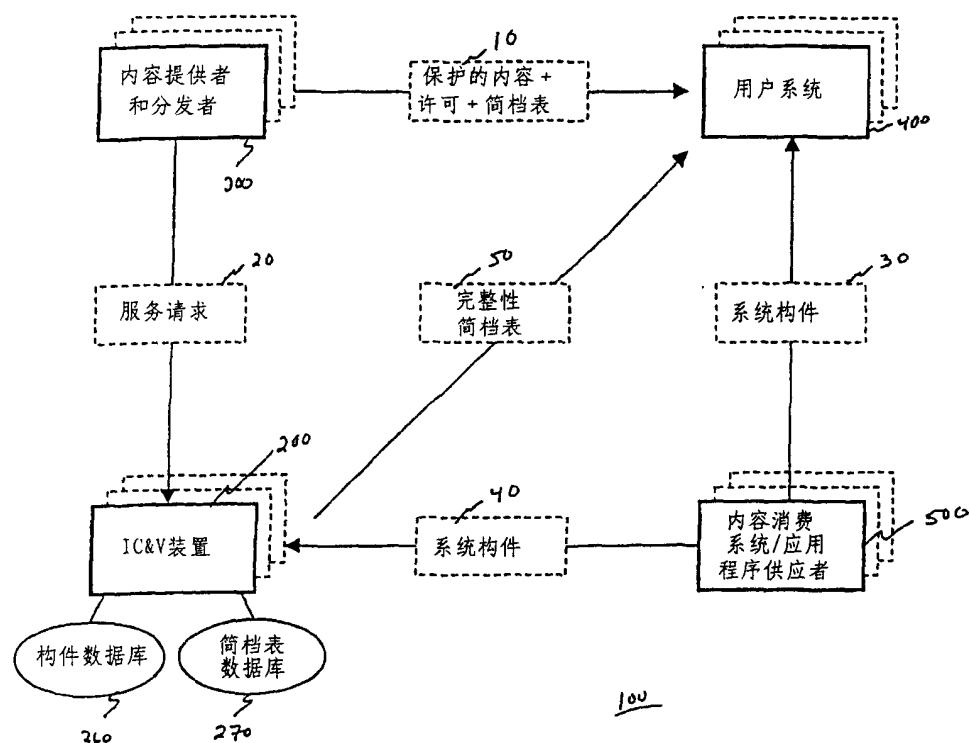
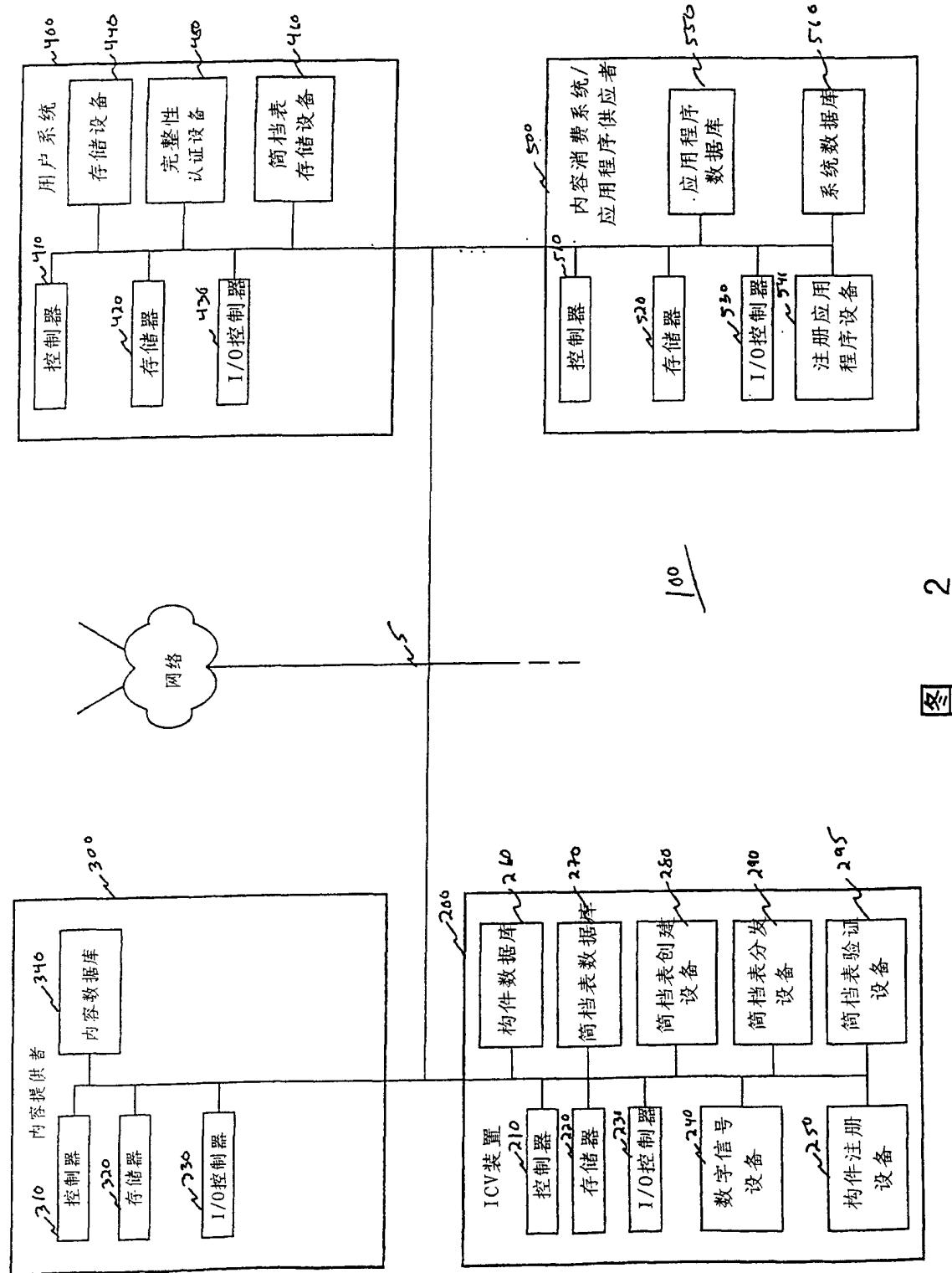


图 1



2

总

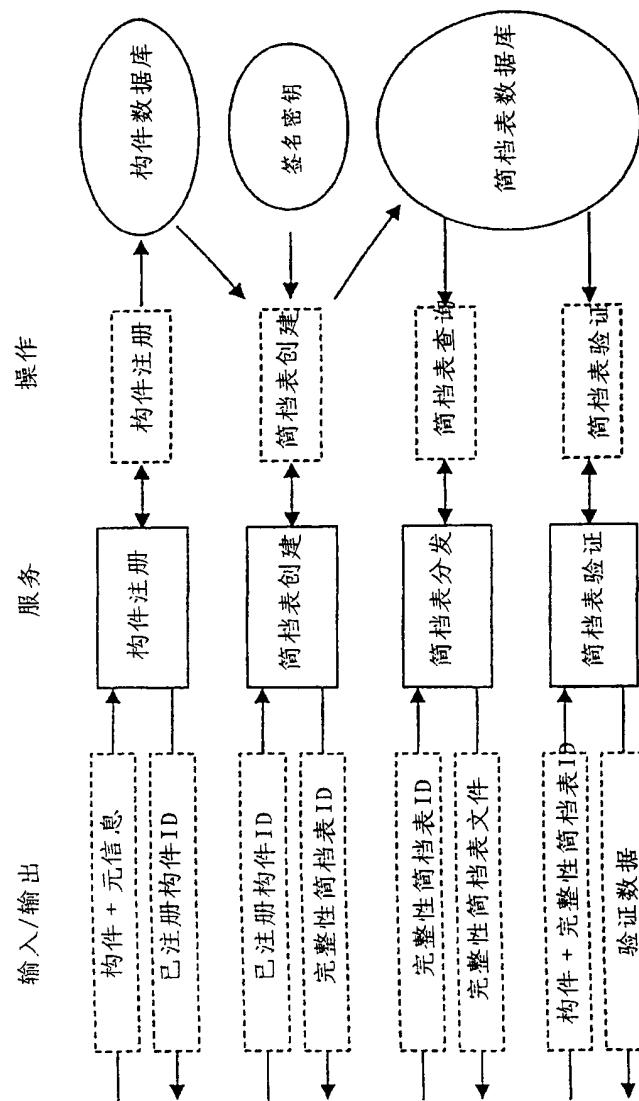


图 3

### 完整性简档表结构

完整性简档表标识
完整性简档表版本号
创建数据
创建者
内容供应者名称和ID
构件完整性值列表(例如无用散列值)
(任选项)构件间互动关系
完整性简档表数字签名

图 4

### 通用终端用户系统环境堆栈

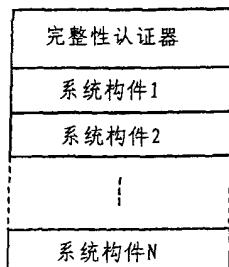


图 5

### 终端用户系统环境堆栈示例

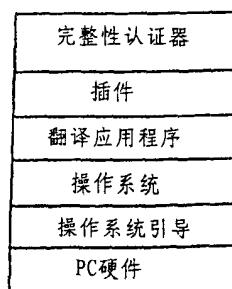


图 6

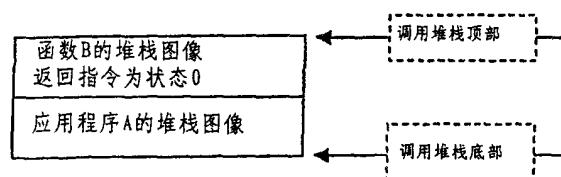


图 7

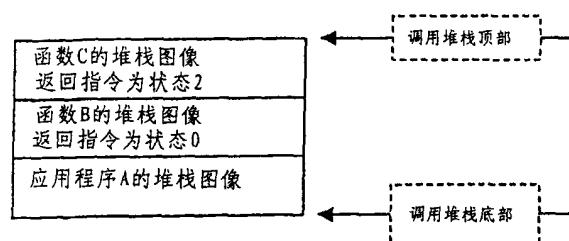


图 8

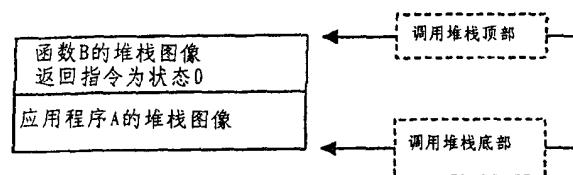


图 9

用防止诸如调试的监控的动态篡改，保护执行环境

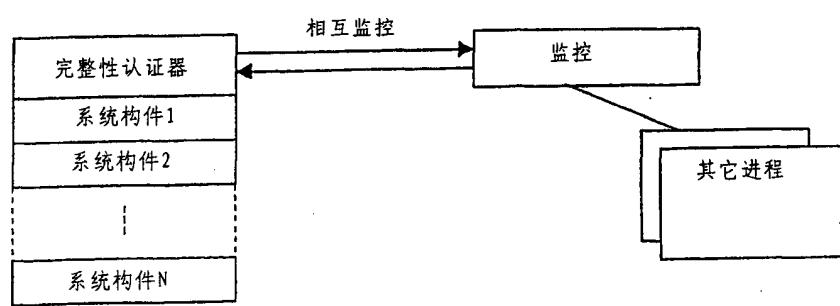


图 10

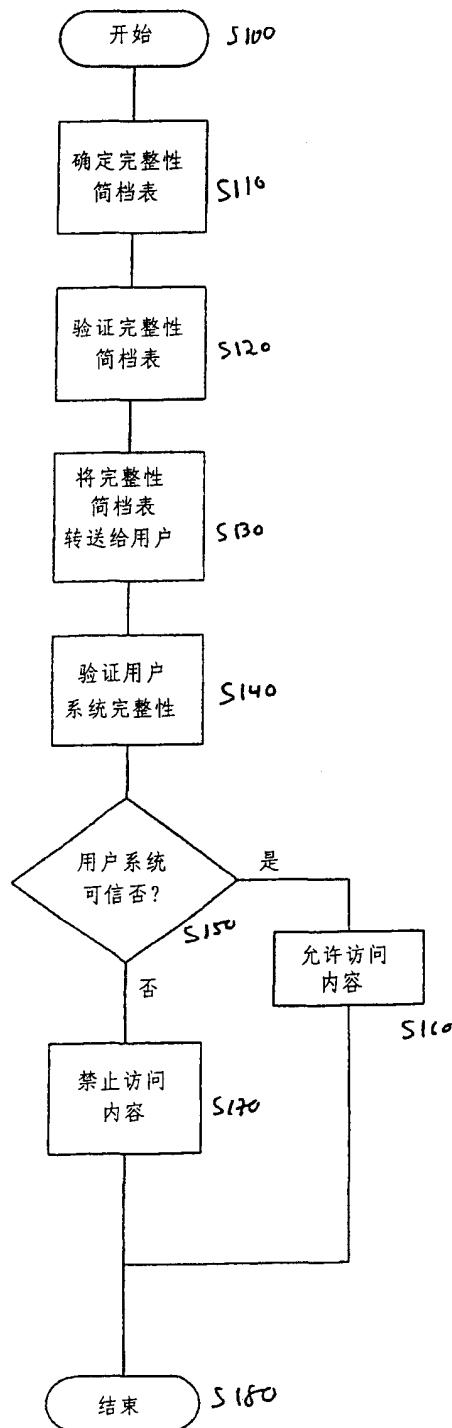


图 11

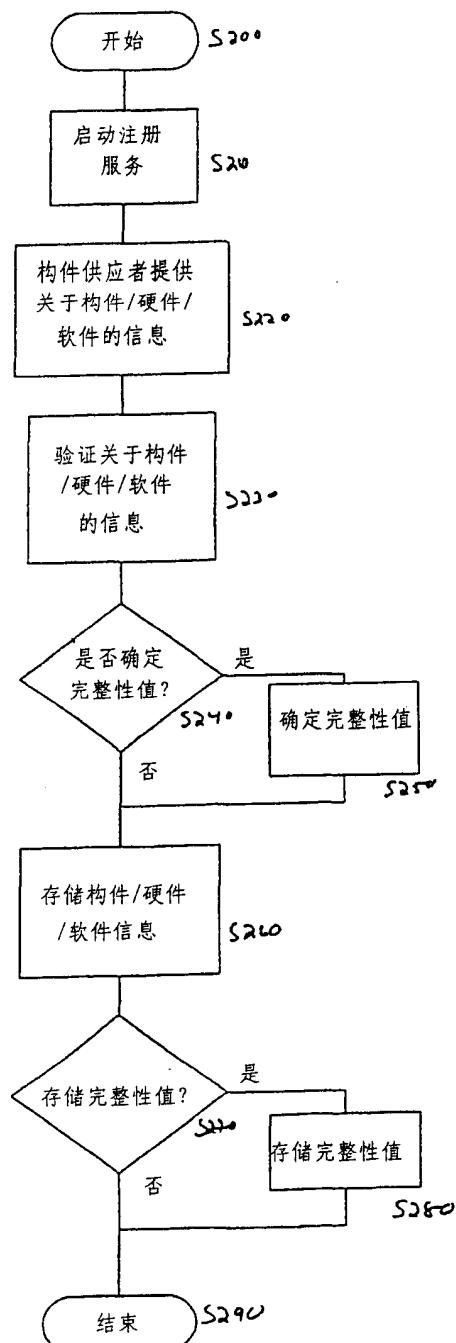


图 12

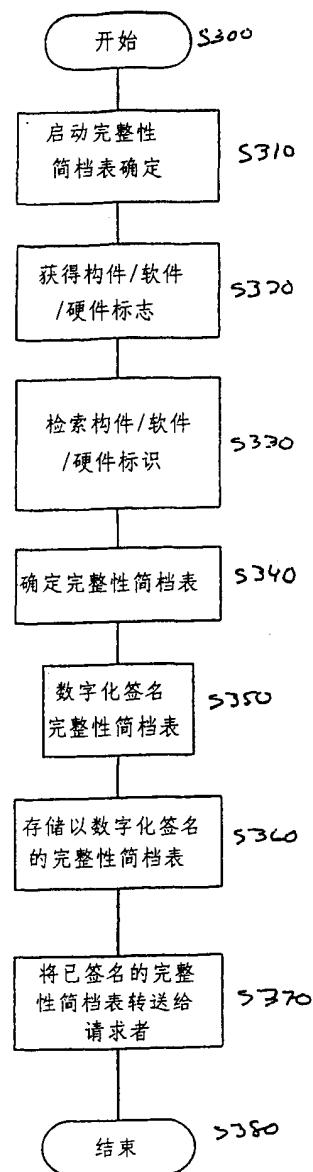


图 13

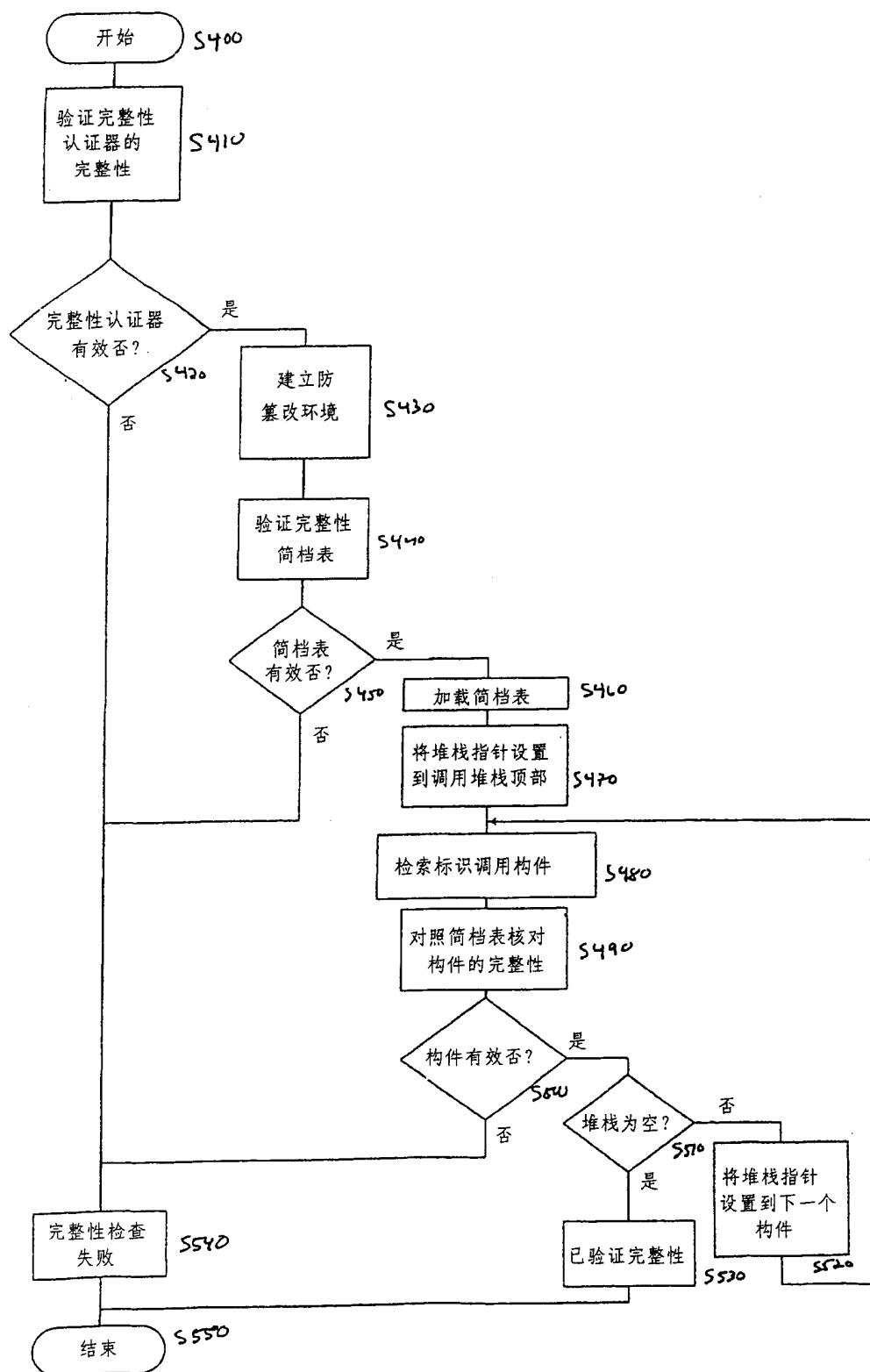


图 14