



(12) 发明专利申请

(10) 申请公布号 CN 115516420 A

(43) 申请公布日 2022. 12. 23

(21) 申请号 202180033676.9

(22) 申请日 2021.05.13

(30) 优先权数据

15/931,794 2020.05.14 US

(85) PCT国际申请进入国家阶段日

2022.11.07

(86) PCT国际申请的申请数据

PCT/US2021/032175 2021.05.13

(87) PCT国际申请的公布数据

W02021/231686 EN 2021.11.18

(71) 申请人 德州仪器公司

地址 美国德克萨斯州

(72) 发明人 B·谢尔谢斯 E·T·J·佩特斯

(74) 专利代理机构 北京律盟知识产权代理有限公司 11287

专利代理师 林斯凯

(51) Int.Cl.

G06F 8/65 (2006.01)

G06F 21/64 (2006.01)

H04L 9/30 (2006.01)

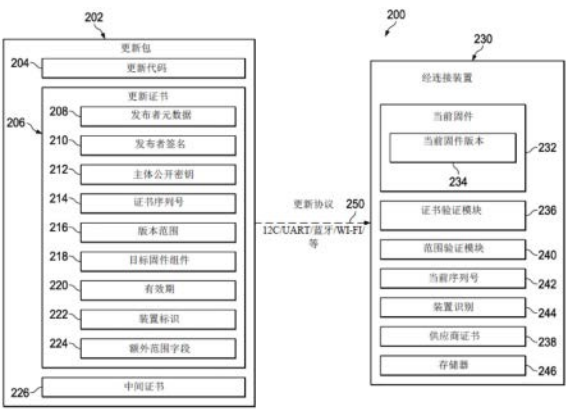
权利要求书2页 说明书7页 附图5页

(54) 发明名称

用于软件更新的认证密钥的可控范围

(57) 摘要

本发明提供用于更新客户端装置的技术,其包含:由客户端装置接收软件更新(204)及与所述软件更新(204)相关联的证书(206);由所述客户端装置基于所述客户端装置(230)的经存储公开密钥验证与所述软件更新(204)相关联的所述证书(206);从所述证书提取更新范围值(216到224);比较所述更新范围值(216到224)与所述更新的对应属性;以及基于所述比较应用所述软件更新或基于所述比较拒绝所述软件更新。



1. 一种用于更新客户装置的方法,其包括:
由客户端装置接收软件更新及与所述软件更新相关联的证书;
由所述客户端装置基于所述客户端装置的经存储公开密钥验证与所述软件更新相关联的所述证书;
从所述证书提取更新范围值;
比较所述更新范围值与所述更新的对应属性;及以下操作中的任一者:
基于所述比较应用所述软件更新;或
基于所述比较拒绝所述软件更新。
2. 根据权利要求1所述的方法,其中所述更新范围值包括证书更新序列号,且其中所述对应属性包括所述客户端装置的序列号。
3. 根据权利要求2所述的方法,其中所述比较包括验证所述证书更新序列号大于所述序列号,且
其中所述方法进一步包括:
用所述证书更新序列号替换所述客户端装置的所述序列号。
4. 根据权利要求1所述的方法,其中所述更新范围值包括版本号,其中所述对应属性包括所述软件更新的版本号,且其中所述比较包括验证所述版本号匹配所述软件更新的所述版本号。
5. 根据权利要求1所述的方法,其中所述更新范围值包括版本号范围,其中所述对应属性包括软件更新的版本号,且其中所述比较包括验证所述软件更新的所述版本号在所述版本号范围内。
6. 根据权利要求1所述的方法,其中所述更新范围值受到所述证书的数字签名的保护。
7. 根据权利要求1所述的方法,其中所述客户端装置的所述经存储公开密钥包括所述客户端装置的制造商的公开密钥。
8. 一种非暂时性程序存储装置,其包括存储在其上的指令,所述指令致使一或多个处理器:
产生更新范围值,所述更新范围值定义软件更新的属性;
产生保护更新范围值的数字签名;
产生包含所述数字签名及所述更新范围值的证书;以及
向客户端装置传输所述证书及所述更新范围值,其中更新范围值经配置以允许所述客户端装置比较所述更新范围值与所述更新的对应属性。
9. 根据权利要求8所述的非暂时性程序存储装置,其中所述更新范围值包括证书更新序列号,且其中所述对应属性包括所述客户端装置的序列号。
10. 根据权利要求8所述的非暂时性程序存储装置,其中所述更新范围值包括证书更新版本号,且其中所述对应属性包括所述软件更新的版本号,且其中所述指令进一步致使所述一或多个处理器验证所述版本号匹配所述软件更新的所述版本号。
11. 根据权利要求8所述的非暂时性程序存储装置,其中所述更新范围值包括版本号范围,其中所述对应属性包括所述软件更新的版本号,且其中所述比较包括验证所述软件更新的所述版本号在所述版本号范围内。
12. 根据权利要求8所述的非暂时性程序存储装置,其中所述更新范围值受到所述证书

的数字签名的保护。

13. 根据权利要求8所述的非暂时性程序存储装置,其中软件更新包括固件更新。

14. 一种装置,其包括:

存储器;以及

一或多个处理器,其可操作地耦合到所述存储器,其中所述一或多个处理器经配置以执行非暂时性指令,所述非暂时性指令致使所述一或多个处理器:

由所述装置接收软件更新及与所述软件更新相关联的证书;

由所述装置基于所述装置的经存储公开密钥验证与所述软件更新相关联的所述证书;

从所述证书提取一组更新范围值;

比较所述更新范围值与所述更新的对应属性;及以下操作中的任一者:

基于所述比较应用所述软件更新;或

基于所述比较拒绝所述软件更新。

15. 根据权利要求14所述的装置,其中所述更新范围值包括证书更新序列号,且其中所述对应属性包括所述装置的序列号。

16. 根据权利要求15所述的装置,其中所述比较包括验证所述证书更新序列号大于所述序列号,且

其中所述其中其上所存储的所述指令进一步致使所述一或多个处理器:

用所述证书更新序列号替换所述装置的所述序列号。

17. 根据权利要求14所述的装置,其中所述更新范围值包括版本号,其中所述对应属性包括所述软件更新的版本号,且其中所述比较包括验证所述版本号匹配所述软件更新的所述版本号。

18. 根据权利要求14所述的装置,其中所述更新范围值包括版本号范围,其中所述对应属性包括所述软件的版本号,且其中所述比较包括验证所述软件的所述版本号在所述版本号范围内。

19. 根据权利要求14所述的装置,其中所述更新范围值受到所述证书的数字签名的保护。

20. 根据权利要求14所述的装置,其中所述客户端装置的所述经存储公开密钥包括所述装置的制造商的公开密钥。

用于软件更新的认证密钥的可控范围

背景技术

[0001] 通常,能够连接到因特网的装置(在本文中称为经连接装置)由用户用预安装于所述装置上的已推出的软件版本获得。在许多情况下,在发行了已推出软件之后,用以增强或添加特征、修复错误、解决安全问题等的额外修改可能会作为对已推出软件的软件更新来进行。软件更新通过允许在经连接装置上运行的软件随环境演进而非在发行时保持固定来允许经连接装置适应不断变化的环境。

[0002] 通常,经连接装置更新过程包含下载或以其它方式获得软件更新包及认证所述软件更新包,例如通过验证与所述软件更新包相关联的数字签名及证书。此数字签名或证书使用经连接装置供应商的公开密钥来验证。然而,这些公开密钥及证书可能具有无限范围且可为可操作的,除非证书使用相对复杂的撤销机制来撤销。在某些情况下,期望降低或去除与撤销过程相关联的复杂性以有助于最小化应用软件更新所需的存储器、网络资源及处理功率的量。

发明内容

[0003] 本发明涉及更新软件。更特定来说,而非通过限制,本发明的方面涉及用于通过以下操作更新软件的技术:由客户端装置接收软件更新及证书;由所述客户端装置基于所述客户端装置的经存储公开密钥验证与所述软件更新相关联的所述证书;从所述证书提取更新范围值;比较所述更新范围值与所述更新的对应属性;以及基于所述比较应用所述软件更新或基于所述比较拒绝所述软件更新。

[0004] 本发明的另一方面涉及一种非暂时性程序存储装置,其包括存储在其上的指令,所述指令致使一或多个处理器:产生更新范围值,所述更新范围值定义软件更新的属性;产生保护更新范围值的数字签名;产生包含所述数字签名及所述更新范围值的证书;以及向客户端装置传输所述证书及所述更新范围值,其中更新范围值经配置以允许所述客户端装置比较所述更新范围值与所述更新的对应属性。

[0005] 本发明的另一方面涉及一种装置,其包含:存储器;以及一或多个处理器,其可操作地耦合到所述存储器,其中所述一或多个处理器经配置以执行非暂时性指令,所述非暂时性指令致使一或多个处理器:由所述装置接收软件更新及与所述软件更新相关联的证书;由所述装置基于所述装置的经存储公开密钥验证与所述软件更新相关联的所述证书;从所述证书提取一组更新范围值;比较所述更新范围值与所述更新的对应属性;以及基于所述比较应用所述软件更新或基于所述比较拒绝所述软件更新。

附图说明

[0006] 针对各个实例的详细描述,现将参考附图,其中:

[0007] 图1是说明数字证书链的框图。

[0008] 图2是说明在一些实例中的用于应用软件更新200的技术的框图。

[0009] 图3说明在一些实例中的用于更新软件的技术。

- [0010] 图4说明在一些实例中的用于更新软件的技术。
- [0011] 图5是在一些实例中的计算系统的实施例的示意图。
- [0012] 图6是在一些实例中的经连接装置的实施例的框图。

具体实施方式

[0013] 公开密钥密码学通常连同数字证书及签名一起使用。在公开密钥密码学中,一对密钥,即公开密钥及私密密钥使用单向函数在数学相关。公开密钥与私密密钥经相关使得使用公开密钥编码的消息仅可使用私密密钥来解码,且反之亦然。因此,数字文件(例如任何种类的文件)可通过将数字文件的位散列、使用私密密钥编码散列且接着将经编码散列与公开密钥一起附加到数字文件来数字地签名。接着,可通过使用公开密钥解码散列且接着比较经解码散列与数字文件的散列来执行验证。数字签名可用于验证特定软件更新是来自可信源,例如经连接装置或系统的供应商。

[0014] 某些经连接装置仅安装来自如通过数字签名验证的可信源的软件更新。通常,经连接装置包含与经连接装置的供应商相关联的公开密钥。此公开密钥或证书可被安装于经连接装置作为生产经连接装置的部分。当开发软件更新时,软件使用供应商的私密密钥来签名且将签名附加到软件更新包。在经连接装置接收到软件更新包之后,经连接装置通过用例如在经连接装置的制造期间预存储在经连接装置上的公开密钥或证书验证数字签名来验证软件更新。一旦软件更新的公开密钥或证书已被装置验证,那么软件更新就是可信的且可以应用。

[0015] 图1是说明数字证书链100的框图。在某些情况下,经连接装置的供应商可用作与供应商相关联的经连接装置的根证书颁发机构。根证书102包含根元数据104,例如根证书颁发机构的名称、标识符、证书的有效日期等。根证书102的公开密钥与根证书颁发机构的私密密钥相关联。根证书102还包含根公开密钥106及根签名108。根签名108可使用根证书颁发机构的私密密钥基于根元数据及根公开密钥106来计算,这是因为根证书102是自签名的。当供应商是根证书颁发机构时,根公开密钥106用作信任公开密钥根(ROTPK)。

[0016] 在供应商是根证书颁发机构的情况下,供应商可能不想使用根证书102直接发布证书以帮助维持根证书的安全性。在此类情况下,供应商可基于根证书102创建一或多个中间证书110。在本文,中间证书110包含中间元数据112,其可包含识别中间颁发机构(例如中间证书110用于谁或用于什么目的)的元数据。举例来说,中间元数据112可指示中间证书110是用于对固件更新进行签名的固件认证密钥(FWAK)且被发布到特定的人或团队。固件可指控制经连接装置的硬件的低级软件。当使用术语固件时,本文中描述的概念通常还可更加广泛地适用于软件及装置。中间元数据112还可识别根证书颁发机构,例如通过包含根公开密钥106或根证书颁发机构的名称。中间元数据112可使用根证书颁发机构的私密密钥来散列及签名以创建中间签名114。中间证书还含有基于中间颁发机构的私密密钥的中间公开密钥116。

[0017] 在某些情况下,供应商不可用作根证书颁发机构且根证书102被证书颁发机构(例如商业证书颁发机构)持有。在此类情况下,供应商可从证书颁发机构请求且获得第一中间证书110。接着,供应商还可基于第一中间证书110产生第二中间证书以用作FWAK。还可根据需求产生额外中间证书。第二中间证书可通过包含第一中间公开密钥116及/或第一中间证

书颁发机构的名称来识别中间证书颁发机构,其为第一中间证书被颁发给其的组织。

[0018] 在固件更新的开发及/或发行部分期间,可将数字签名应用到固件更新。创建此数字签名可能需要使用与中间证书110或根证书102相关联的私密密钥。在某些情况下,可能会潜在地破坏私密密钥的安全性,例如通过员工流动或违法行为,且可能有必要撤销及以其它方式替换私密密钥。然而,这些密钥的撤销对经连接装置来说可能很难,这是因为这些装置可能是离线的或难以用撤销信息更新。

[0019] 图2是说明在一些实例中的用于应用软件更新200的技术的框图。在某些情况下,更新包202包含用于更新经连接装置230的更新代码204以及更新证书206。更新证书206可为基于证书链(例如连同图1描述的证书链)以及更新代码204。举例来说,组织可用作中间证书颁发机构且向子组织(例如开发或更新团队)或甚至个人(例如开发人员)发布证书。作为更详细实例,开发人员可产生公共/私密密钥对且可将它们的公开密钥提交给中间证书颁发机构以请求证书。接着,组织可为开发人员颁发证书,例如包含开发人员的公开密钥(例如主体公开密钥212)及组织的数字签名(例如发布者签名210)。发布者签名210可为至少部分基于主体公开密钥212及主体元数据的散列。

[0020] 更新证书206还可包含范围字段,例如证书序列号214、固件版本216、目标固件组件218、有效期220、装置id 222。更新证书206可根据需要包含额外范围字段224。在某些情况下,范围字段可作为例如元数据包含于主体元数据中。举例来说,发布者元数据208可包含一或多个范围字段。范围字段定义固件更新的范围且含有识别固件更新的范围的额外信息。范围字段由数字签名进行签名且受到数字签名的保护。举例来说,范围字段包含于被散列且接着被发布者签名的证书的部分中,且更新证书206的范围是固定的。在某些情况下,可为每一更新证书设置如由范围字段内的值定义的不同范围。举例来说,证书可包含证书对其有效的更新代码204的特定版本,对照所述特定版本更新FW的每一构建。在某些情况下,范围字段的值可为基于由主体提供的或由发布者提供的更新代码的性质。

[0021] 在更新包202被经连接装置230接收之后,固件更新202可被存储于经连接装置230的存储器中。经连接装置230的证书验证模块236验证固件更新是来自可信源。举例来说,经连接装置230包含具有当前固件版本234的当前固件232。在固件更新202经由更新协议250接收之后,证书验证模块236通过使用发布者的公开密钥212验证发布者签名210来验证更新证书206。证书验证模块236可从固件更新202存取中间证书226以从中间证书226获得根公开密钥。接着,对照来自在经连接装置230的生产期间安装的供应商证书238的ROTPK确认所获得的此根公开密钥。对照ROTPK验证中间证书226允许经连接装置230验证发布者是可信源。如果固件更新来自可信源,那么可验证更新证书的范围。

[0022] 证书的范围定义必须被满足才能应用更新的一组条件。如由范围字段定义的固件更新202的范围由接收固件更新202的经连接装置230强制执行。经连接装置230的范围验证模块240可例如基于固件更新202的性质、装置的性质、应用更新的方式等验证如由证书对照更新的条件定义的范围。作为实例,更新的范围可为基于与证书相关联的序列号。在此实例中,序列号仅可使用一次且证书可与作为唯一的不断增加的序列号的证书序列号214一起产生。因此,每当产生新的证书时,就向新的证书提供不同证书序列号,其大于与先前证书相关联的证书序列号。当经连接装置230应用更新时,经连接装置230存储与更新相关联的序列号,在此实例中作为当前序列号242。当接收到下一更新时,范围验证模块240在对照所

存储ROTPK验证证书的数字签名之后,从更新证书206获得证书序列号214。范围验证模块240获得经连接装置230的当前序列号242且比较当前序列号242与固件更新的证书序列号214以对照当前序列号242验证所述证书序列号214。在证书序列号214超过当前序列号242的情况下,则证书及相关联更新可在范围内。在给定证书序列号可被多次使用的情况下,经连接装置230可包含计数器,每当使用特定序列号且将其与限值作比较时,都使计数器递增。

[0023] 作为另一实例,更新的范围可为基于固件版本。在此实例中,范围验证模块240可在对照所存储的ROTPK验证证书的数字签名之后从证书的范围字段获得版本范围216。此版本范围216在某些情况下指定版本或版本范围,证书对所述版本或版本范围来说是有效的。范围验证模块240还可获得经更新代码204的更新版本以及当前FW版本234。范围验证模块验证更新版本大于当前FW版本且还验证更新代码204的更新版本匹配版本范围216或在版本范围216的范围内。如果更新代码204的更新版本无法对照版本范围216来验证,那么拒绝更新代码204。

[0024] 作为另一实例,更新的范围可为基于经连接装置230的组件。在某些情况下,经连接装置230的固件可例如基于经连接装置的配置而有所不同。经连接装置的某些版本可支持不同特征,例如所支持的不同联网协议、可用传感器、位置特定的差异等。经连接装置的这些不同版本可基于所支持特征而具有不同固件组件。关于特定当前固件组件234的信息可包含于当前固件232中。范围验证模块240作为检查固件更新202的范围的部分可存取目标固件组件218的范围字段及当前固件组件234。范围验证模块240可比较当前固件组件234以确定目标固件组件218匹配当前固件组件234。在某些情况下,范围验证模块240可检查目标固件组件218包含至少一些当前固件组件234。

[0025] 作为另一实例,更新的范围可为基于装置标识符(ID) 244。在某些情况下,经连接装置230包含装置ID 224,其可在经连接装置230的生产期间安装。范围验证模块240可从固件更新202存取装置ID列表222以验证经连接装置230的装置ID 244在装置ID列表222中。

[0026] 在某些情况下,固件更新202的范围可由例如包含于额外范围字段224中的额外性质定义。举例来说,如果固件更新202经由特定更新协议250接收,那么额外范围字段224可指示经连接装置230可在范围内。此更新协议可定义更新是如何获得的,例如,使用网络协议获得更新,或更新是否直接被复制到装置,例如经由USB。更新协议可被识别且与固件更新202一起被存储于存储器246中。定义固件更新202的范围的其它性质也可包含例如于额外范围字段224中。

[0027] 图3说明在一些实例中的用于更新软件300的技术。在步骤302,客户端装置接收软件更新及与软件更新相关联的证书。举例来说,经连接装置可接收固件更新。固件更新可包含数字证书以及基于证书范围字段的散列的数字签名。在某些情况下,数字证书可与软件更新分开接收。在步骤304,客户端装置基于客户端装置上的经存储公开密钥验证与软件更新相关联的证书。举例来说,证书可包含中间颁发机构的公开密钥,其可用于提取签名,签名可由存储于经连接装置上的制造商的公开密钥解码以验证软件更新来源于制造商。此公开密钥可例如在装置被制造时存储于装置上。在步骤306,从证书提取更新范围值。举例来说,一或多个范围字段可包含于更新证书内。这些范围字段定义固件更新的范围。范围字段的实例包含证书序列号、软件版本号或范围及更新协议。在步骤308,比较更新范围值与更

新的对应属性。更新的属性可包含例如客户端装置的性质、环境值,例如用于获得更新的协议或技术、与更新相关联的元数据、证书与更新之间的关系等。举例来说,更新序列号可与和已经在经连接装置上的软件相关联的当前序列号作比较以验证更新序列号更大。其它实例包含验证更新版本号等于范围字段中的版本号或在范围字段的版本号的范围。在步骤310,基于比较应用软件更新或基于比较拒绝软件更新。举例来说,如果比较成功,那么可应用软件更新。在另一实例中,如果比较失败,例如如果软件更新超出了证书中定义的版本范围,那么拒绝软件更新。

[0028] 图4说明在一些实例中的用于更新软件400的技术。在步骤402,产生更新范围值,更新范围值定义软件更新的属性。如上文描述,更新的属性可包含例如客户端装置的性质、环境值,例如用于获得更新的协议或技术、与更新相关联的元数据、证书与更新之间的关系等。在某些情况下,可包含多个属性。在404,可产生保护更新范围值的数字签名。举例来说,范围值可包含于数字证书的一或多个字段中。数字签名可基于数字证书的字段(包含范围值)产生。接着,数字签名保护范围值。在某些情况下,数字签名可为证书的发布者的数字签名。在步骤406,产生包含数字签名及更新范围值的证书。在步骤408,向经连接装置传输软件更新及更新范围值,其中更新范围值经配置以允许客户端装置比较更新范围值与更新的对应属性。

[0029] 图5是计算系统500的实施例的示意图,其中本发明的实施例可在其中操作。计算系统500可包含经连接装置502A到502C(统称为502)、更新服务器504及网络506(例如因特网)。在一些实施例中,更新服务器504可并非是单个服务器,而是可为可由单个网络地址(例如统一资源定位器(URL))存取的一或多个服务器。在某些情况下,更新服务器504可为替代下载资源的列表,且可包含第三方服务器。URL可由分发软件更新的组织利用。尽管在图5中未明确说明,但更新服务器504还可包含一或多个数据中心。数据中心可包含多个服务器例子,其中每一服务器例子都可实施于物理计算系统(例如单个电子计算装置(例如单个物理硬件服务器))上或可呈多计算装置(例如多个物理硬件服务器)的形式。服务器例子可经由一或多个网络装置(例如网关或路由器)或装置的组合连接以将网络流量路由或引导到适当服务器。在某些情况下,服务器还可定位于局域网(LAN)内。

[0030] 经连接装置502可包含(但不限于)IoT装置、移动装置(例如智能电话、平板计算机等)、个人计算机、穿戴式装置等。某些经连接装置502(例如经连接装置502A及502B)耦合到更新服务器504且能够经由网络506与更新服务器504通信。某些经连接装置502C可耦合到一或多个其它经连接装置502D且能够经由一或多个其它经连接装置502D及网络506获得更新。网络506可包含现今可用的一或多个计算网络,例如LAN、广域网(WAN)、因特网及/或其它远程网络。网络506可含有在电域及/或光域中操作的有线及/或无线可编程装置。举例来说,网络506可包含有线网络(例如以太网、通用串行总线(USB)、光纤连接等)、无线网络(例如蜂窝网络(例如基于全球移动通信系统(GSM)的蜂窝网络))、无线保真(WiFi®(WiFi是Wi-Fi联盟公司拥有的注册商标))网络及/或如所属领域的一般技术人员在查看了本发明后应了解的其它合适的基于无线电的网络。网络506还可采用任何数目个网络通信协议,例如传输控制协议(TCP)及因特网协议(IP)。尽管在图5中未明确展示,但网络506可包含各种网络装置,例如经配置以经由网络传输数据的服务器、路由器、网络交换机及/或其它网络硬件装置。在某些情况下,更新服务器504可直接连接到经连接装置502。举例来说,更新服

务器504可经由直接串行接口、短程射频连接、平行电缆等连接。

[0031] 如图6中说明,经连接装置600包含处理元件,例如含有一或多个硬件处理器的处理器605,其中每一硬件处理器可具有单个或多个处理器核心。处理器的实例包含(但不限于)中央处理单元(CPU)或微处理器。尽管图6中未说明,但处理器605的处理元件还可包含一或多个其它类型的硬件处理组件,例如图形处理单元(GPU)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)及/或数字信号处理器(DSP)。

[0032] 图6说明存储器610可操作且通信地耦合到处理器605。存储器610可为经配置以存储各种类型的数据的非暂时性计算机可读存储媒体。举例来说,存储器610可包含一或多个易失性装置,例如随机存取存储器(RAM)。非易失性存储装置620可包含经设计以在断电或关闭操作之后维持数据达一持续时间的一或多个磁盘驱动器、光学驱动器、固态驱动器(SSD)、磁带驱动器、快闪存储器、电可编程只读存储器(EEPROM)及/或任何其它类型存储器。非易失性存储装置620还可用于存储在执行程序时加载到RAM中的此类程序。

[0033] 所属领域的一般技术人员意识到,软件程序可以各种计算语言开发、编码及编译以用于各种软件平台及/或操作系统中且随后由处理器605加载并执行。在一个实施例中,软件程序的编译过程可将以编程语言编写的程序代码变换成另一计算机语言使得处理器605能够执行编程代码。举例来说,软件程序的编译过程可产生可执行程序,其向处理器605提供经编码指令(例如,机器代码指令)以实现具体的、非通用的特定计算功能。

[0034] 在编译过程之后,接着,经编码指令可作为计算机可执行指令或过程步骤从存储装置620、从存储器610加载到处理器605及/或嵌入于处理器605内(例如,经由高速缓存或机载ROM)。处理器605可经配置以执行所存储指令或过程步骤以便执行指令或过程步骤来将计算装置变换成非通用的、特定的经专门编程的机器或设备。例如由存储装置620存储的数据的所有存储数据可在计算机可执行指令或过程步骤执行期间由处理器605存取以指示计算装置600内的一或多个组件。存储装置620可经分区或分割成可由不同软件程序存取的多个区段。举例来说,存储装置620可包含出于特定目的标示的区段,例如存储用于更新计算装置600的软件的程序指令或数据。在一个实施例中,将更新的软件包含计算装置的ROM或固件。在某些情况下,计算装置600可包含多个操作系统。举例来说,计算装置600可包含用于正常操作的通用操作系统。计算装置600还可包含用于执行特定任务的另一操作系统,例如引导加载程序,所述特定任务例如更新并恢复通用操作系统且允许在通过通用操作系统通常不可用的级别下存取计算装置600。通用操作系统及另一操作系统两者可存取经指定用于特定目的的存储装置620的区段。

[0035] 计算装置600还可包含一或多个通信接口625,其可通信地耦合到处理器605。一或多个通信接口可包含无线电通信接口以对接一或多个无线电通信装置。在某些情况下,耦合到处理器的元件可包含于与处理器共享的硬件上。举例来说,通信接口625、存储装置620及存储器610可与例如数字无线电的其它元件一起包含于单个芯片或封装中,例如包含于单芯片系统(SOC)中。计算装置600还可包含输入装置630。输入装置的实例包含传感器、相机及人类输入装置,例如鼠标、键盘、触摸屏等。经处理输入可经由通信接口625从计算装置600输出到一或多个其它装置。在某些情况下,计算装置600还可包含用于例如向用户提供输出的输出装置(未展示)。输出装置的实例包含显示器屏幕、触觉或运动产生器、扬声器、灯等。

[0036] 贯穿说明书使用术语“耦合”。术语可涵盖实现与本发明的描述一致的功能关系的连接、通信或信号路径。举例来说,如果装置A产生控制装置B执行动作的信号,那么在第一实例中,装置A耦合到装置B,或在第二实例中,如果中介组件C基本上未更改装置A与装置B之间的功能关系,那么装置A通过中介组件C耦合到装置B,使得装置B由装置A经由装置A产生的控制信号控制。

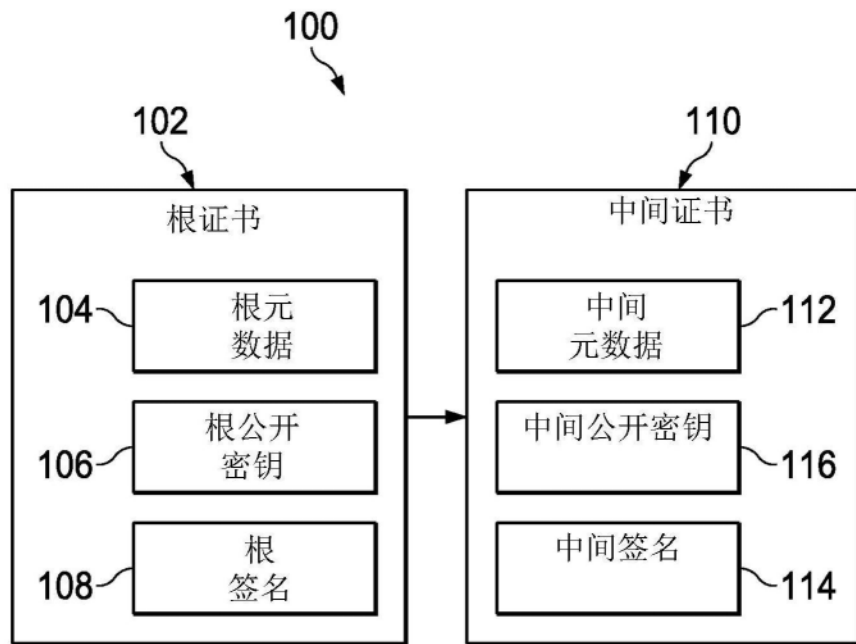


图1

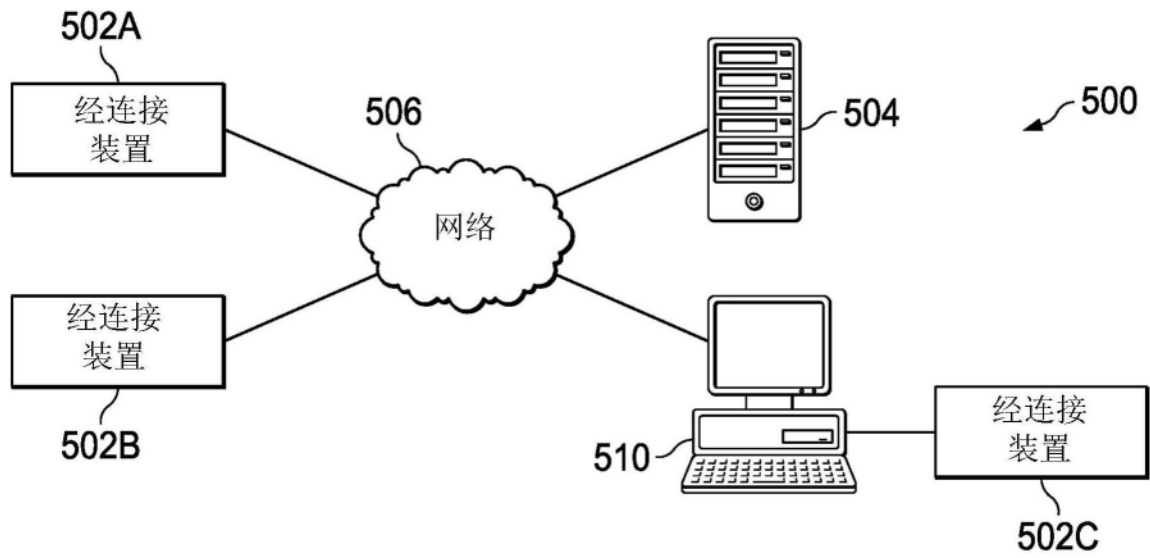


图5

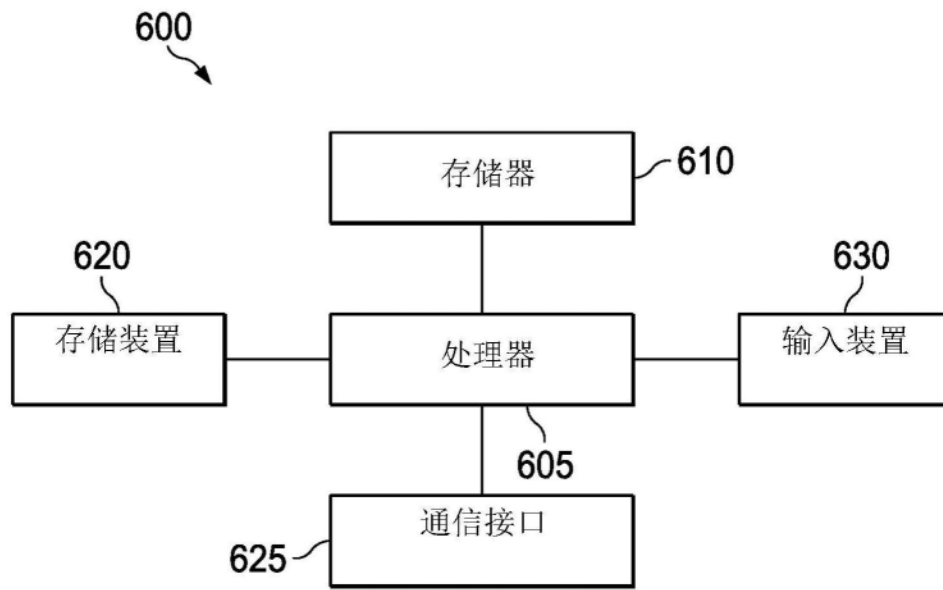


图6

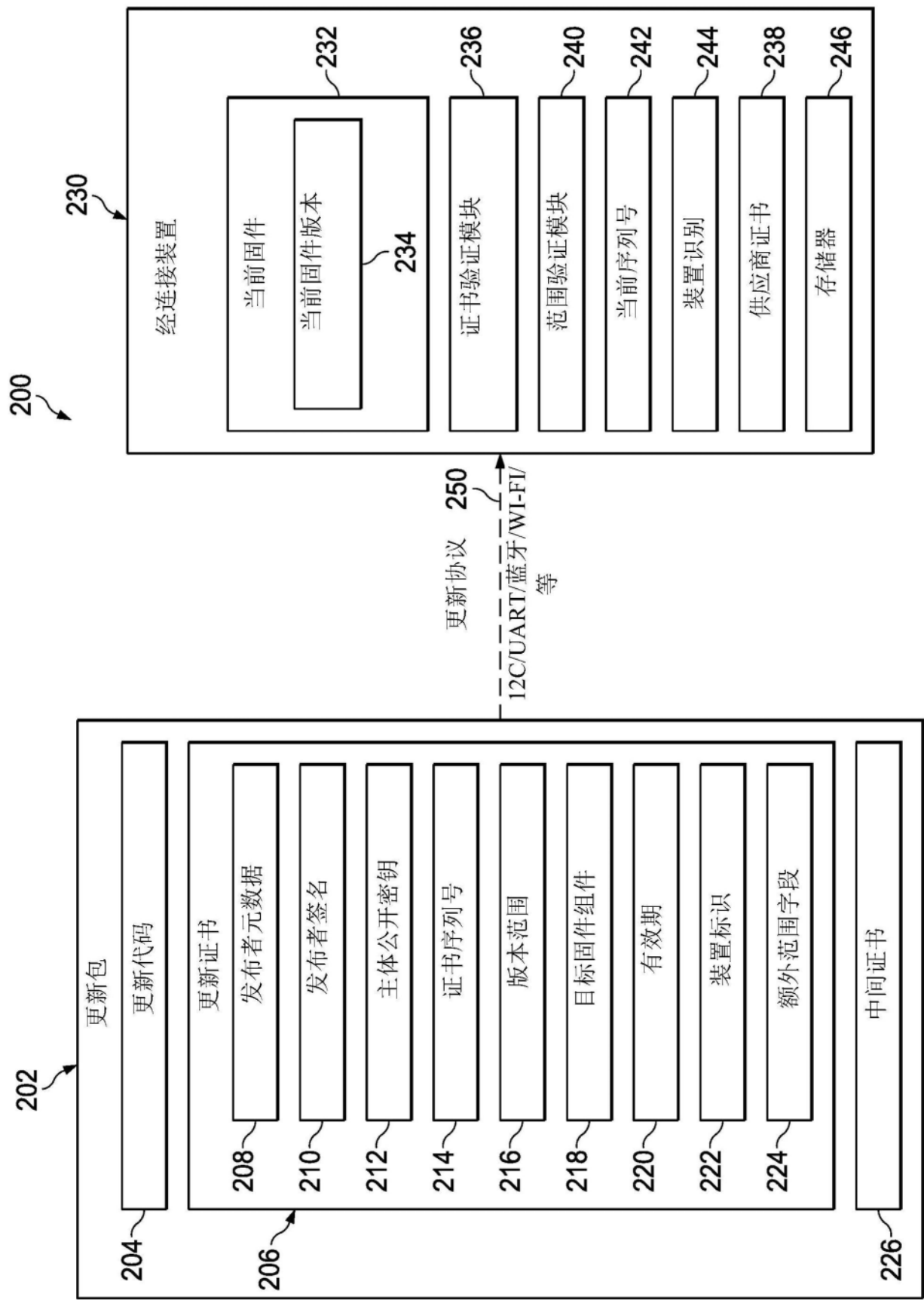


图2

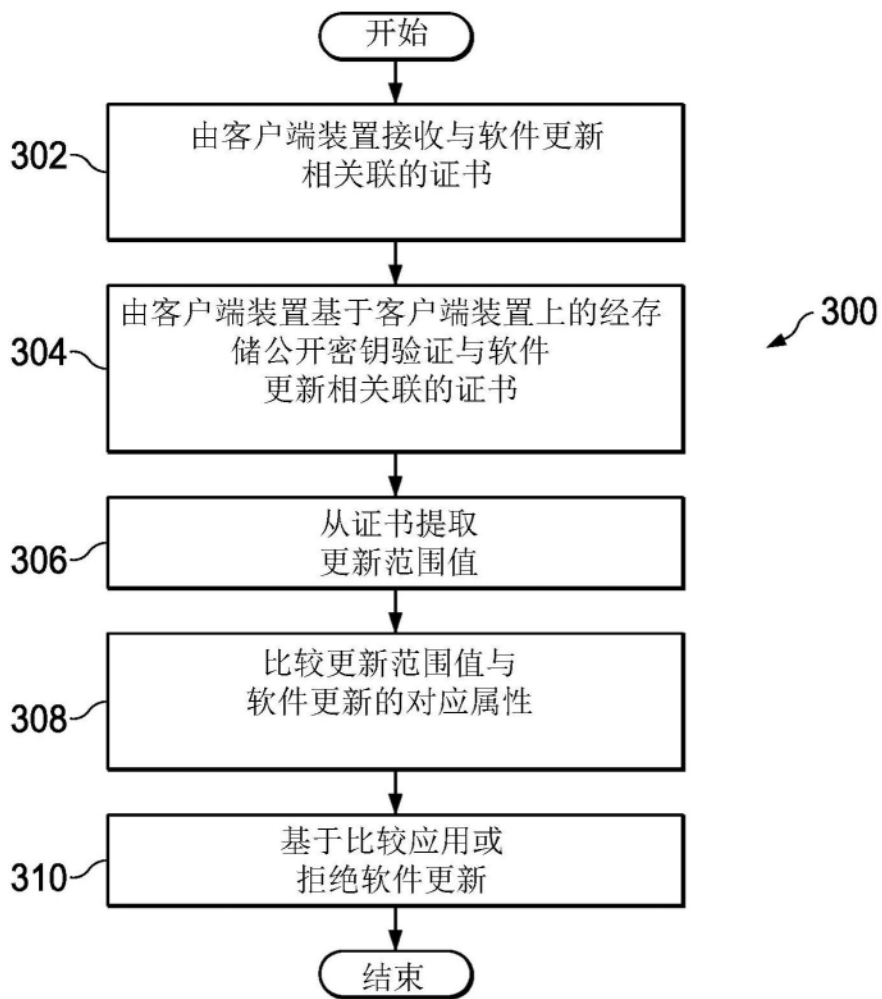


图3

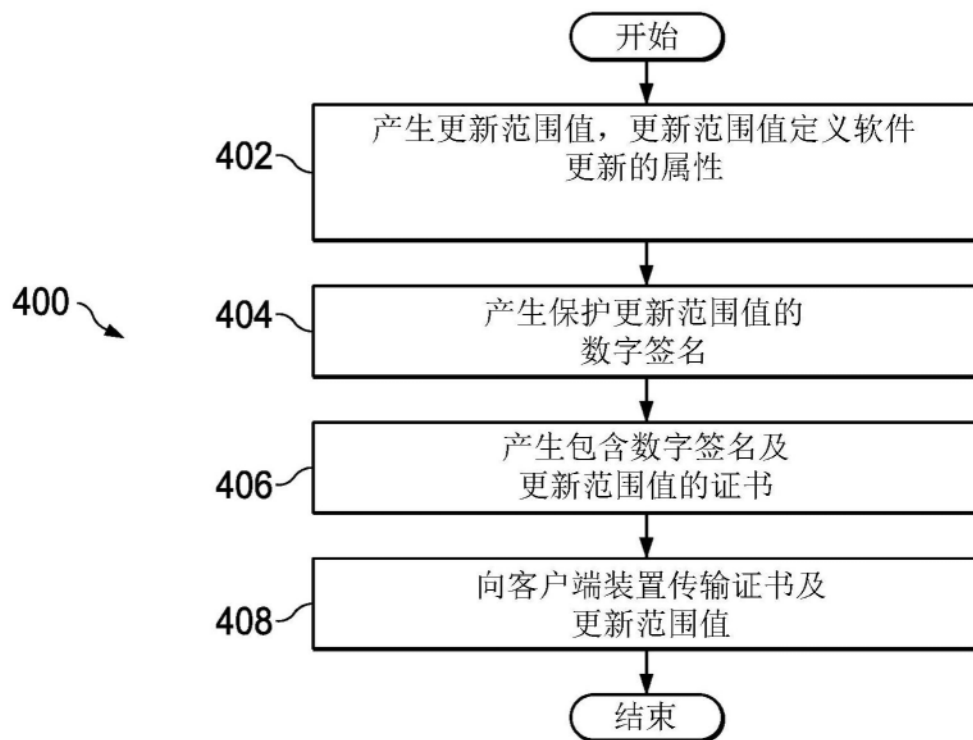


图4