(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 11 月 28 日 (28.11.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/223751 A1

(51) 国际专利分类号:
G06F 21/54 (2013.01)

(21) 国际申请号: PCT/CN2019/088082

(22) 国际申请日: 2019 年 5 月 23 日 (23.05.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810516372.8 2018年5月25日 (25.05.2018) CN

(71) 申请人: 华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 季杰(**JI, Jie**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所 (普通合伙) (**SHENPAT INTELLECTUAL PROPERTY AGENCY**); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦B座18C2、18D、18E、18E2, Guangdong 518001 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** MULTI-CONTAINER-BASED TRUSTED APPLICATION PROCESSING METHOD, AND RELATED DEVICE

(54) 发明名称: 一种基于多容器的可信应用程序的处理方法及相关设备

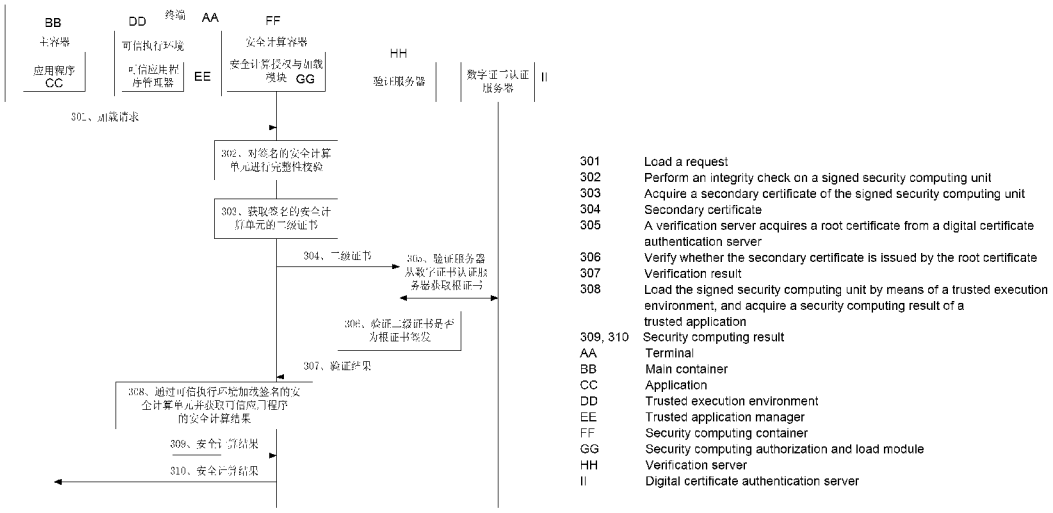

图 3

(57) **Abstract:** A multi-container-based trusted application processing method and a related device, for simplifying development and deployment processes of the trusted application, and improving the processing efficiency of the trusted application and the security of an access interface of a trusted execution environment (TEE). The method comprises: a terminal performing an integrity check on a signed security computing unit by means of a security computing container; if the signed security computing unit has passed the integrity check, the terminal performing a validity check on the signed security computing unit by means of the security computing container, and acquiring a check result; if the check result is valid, the terminal loading the signed security computing unit by means of the TEE or a security element (SE) and acquiring a security computing result of the trusted application.

WO 2019/223751 A1

[见续页]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：一种基于多容器的可信应用程序的处理方法及相关设备，用于简化可信应用程序的开发和部署流程，提高了对可信应用程序的处理效率和可信执行环境的访问接口的安全性。该方法包括：终端通过安全计算容器对签名的安全计算单元进行完整性校验；若签名的安全计算单元通过完整性校验，则终端通过安全计算容器对签名的安全计算单元进行合法性校验并获取校验结果；若校验结果为合法的，则终端通过可信执行环境TEE或安全元件SE加载签名的安全计算单元并获取可信应用程序的安全计算结果。

一种基于多容器的可信应用程序的处理方法及相关设备

本申请要求于 2018 年 05 月 25 日提交中国专利局、申请号为 201810516372.8、申请名称为“ 一种基于多容器的可信应用程序的处理方法及相关设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信领域，尤其涉及一种基于多容器的可信应用程序的处理方法及相关设备。

背景技术

目前，终端安全主要涉及五种领域：身份认证，准入控制，安全认证，业务授权，业务审计。对于安全认证领域，开始出现基于通用串行总线接口的硬件设备（universal serial bus key，USB Key）、可信执行环境（trusted execution environment，TEE）和安全元件（secure element，SE）等更为安全的解决方案，其中，可信执行环境 TEE 可以解决在移动支付场景下消费者、商户、移动运营商、第三方支付、金融机构等上下游参与方的各种不同安全诉求，是当前最具备发展潜力的技术之一。目前，TEE 技术已经在手机、机顶盒、平板和其它设备上广泛使用。

现有技术中，将在富执行环境（rich execution environment，REE）上执行的应用程序称为客户应用程序（client application，CA），例如，安卓（Android）等容易被攻击的传统操作系统，或第三方应用程序等；将在 TEE 上执行的应用程序称为可信应用程序（trusted application，TA），例如，执行签名、加解密计算等关键服务的程序。为了提升安全性，通过TEE将高安全敏感的TA与REE进行隔离，为TA提供专门的安全执行环境，并保护 TA 的资源和数据的保密性、完整性和访问权限。由于 TA 运行在 TEE/SE 中，TA 的部署/升级操作需要严格遵循 TEE/SE 发行方（通常是终端厂商）的安全验证规范。

由于目前的 TEE 的应用架构存在一些限制，不同终端厂商的 TEE 实现可信应用管理平台也存在较多差异，导致可信应用程序的开发及部署过程较为复杂，由于 TEE 技术的核心框架在于 REE 和 TEE 的隔离，由于 REE 侧容易遭受外界攻击，高安全级别的数据处理只能全部放在TEE侧实现。因为TEE需要通过对TA的安全计算单元进行数字签名等专有措施确保 TEE 真正可信，TA 的开发者必须联系各个 TEE 发行方(通常是终端厂商)进行合作开发，这种上下游（TA 开发者和 TEE 发行方）的耦合关系，会导致可信应用程序 TA 的处理效率低。

发明内容

本申请实施例提供了一种基于多容器的可信应用程序的处理方法及相关设备，用于简化可信应用程序的开发和部署流程，提高了对可信应用程序的处理效率和可信执行环境的访问接口的安全性。

本申请第一方面提供了一种基于多容器的可信应用程序的处理方法，包括：终端通过安全计算容器对签名的安全计算单元进行完整性校验，即确定该签名的安全计算单元是否被第三方篡改；若签名的安全计算单元通过完整性验证，即签名的安全计算单元未被第三方篡改，则终端通过安全计算容器对签名的安全计算单元进行合法性校验并获取校验结果；若校验结果为合法的，即二级证书所属的签名的安全计算单元是合法的，则终端通过可信执行环境 TEE 或安全元件 SE 加载签名的安全计算单元并获取可信应用程序的安全计算结果。通过引入安全计算容器的方式，避免了 TEE 的客户端应用程序受到攻击，达到了隔离主容器和 TEE 的安全效果，提高了可信执行环境的访问接口的安全性。

在一种可能的设计中，在本申请实施例第一方面的第一种实现方式中，终端通过安全计算容器对签名的安全计算单元进行合法性校验并获取校验结果包括：终端通过安全计算容器获取签名的安全计算单元的二级证书，该二级证书用于验证签名的安全计算单元的合法性；终端通过安全计算容器将二级证书发送至验证服务器；终端通过安全计算容器接收验证服务器发送的校验结果。通过给安全计算单元分配二级证书，使安全计算单元在主容器之外的安全计算容器中进行二级证书校验，认证与加载，既解决了可信应用程序开发的流程冗长的问题，降低了第三方开发者和终端厂商的接入成本，又保证了验证与加载安全计算单元的安全性。

在一种可能的设计中，在本申请实施例第一方面的第二种实现方式中，终端通过安全计算容器对签名的安全计算单元进行完整性校验包括：终端通过安全计算容器中的安全计算授权与加载模块从签名的安全计算单元中获取签名文件；终端通过安全计算授权与加载模块从签名的安全计算单元中获取安全计算单元文件元数据；终端通过安全计算授权与加载模块对安全计算单元文件元数据进行摘要计算，得到安全计算单元文件元数据的哈希值；终端通过安全计算授权与加载模块将哈希值和签名文件进行比对校验，即比较哈希值与签名文件的哈希值是否相同。对具体的完整性校验过程进行了细化，在可信应用程序的开发流程中，在签名的安全计算单元加载至可信执行环境之前，对签名的安全计算单元进行完整性验证，提高了签名的安全计算单元的可靠性和安全性。

在一种可能的设计中，在本申请实施例第一方面的第三种实现方式中，终端通过安全计算容器对签名的安全计算单元进行完整性校验之前，所述方法还包括：终端从主容器获取加载请求，该加载请求用于所述终端的安全计算容器加载签名的安全计算单元，该签名的安全计算单元用于对可信应用程序进行安全计算。增加了从主容器获取加载请求的过程，将对可信应用程序的安全计算功能拆分到安全计算单元中，定义安全计算的统一接口，达到一次开发，所有终端平台均可运行，避免了第三方开发者需要为每个终端平台定制 TA 的过程，降低了开发者和终端厂商的开发和分发成本。

在一种可能的设计中，在本申请实施例第一方面的第四种实现方式中，终端通过可信执行环境 TEE 或安全元件 SE 加载签名的安全计算单元并获取可信应用程序的安全计算结果之后，所述方法还包括：终端将安全计算结果传输至终端的主容器。将安全计算结果反馈至可信应用程序，实现对可信应用程序的安全计算。

在一种可能的设计中，在本申请实施例第一方面的第五种实现方式中，所述方法还包

括：若签名的安全计算单元没有通过完整性验证，则终端停止加载签名的安全计算单元的流程。增加了签名的安全计算单元没有通过完整性验证时，停止加载签名的安全计算单元的过程，确保了安全计算单元的有效性，提高了可信应用程序的开发过程的安全性。

在一种可能的设计中，在本申请实施例第一方面的第六种实现方式中，所述方法还包括：若校验结果为不合法的，则终端停止加载签名的安全计算单元的流程。增加了当二级证书为不合法的情况下，停止加载签名的安全计算单元的过程，确保了安全计算单元的合法性，提高了可信应用程序的开发过程的安全性。

在一种可能的设计中，在本申请实施例第一方面的第七种实现方式中，签名的安全计算单元的文件格式至少包括初始段、代码段和数据段。确定了签名的安全计算单元的具体组成，明确了统一的安全计算单元，简化了可信应用程序的开发过程。

本申请第二方面提供了一种基于多容器的可信应用程序的处理方法，包括：验证服务器接收终端发送的二级证书，该二级证书用于验证签名的安全计算单元的合法性；验证服务器从数字证书认证服务器获取根证书，该根证书与二级证书对应；验证服务器验证二级证书是否为根证书签发；若二级证书为根证书签发，则验证服务器确定签名的安全计算单元为合法的；若二级证书不为根证书签发，则验证服务器确定签名的安全计算单元为不合法的。通过验证服务器对安全计算单元的证书进行在线验证合法性，只有在证书有效的情况才会加载安全计算单元，保证了安全计算单元的合法性。

在一种可能的设计中，在本申请实施例第二方面的第一种实现方式中，所述方法还包括：验证服务器将验证结果发送至终端，该验证结果用于指示签名的安全计算单元是否为合法的。增加了将验证结果发送至终端的过程，使本申请实施例在步骤上更完善。

在一种可能的设计中，在本申请实施例第二方面的第二种实现方式中，验证服务器验证二级证书是否为根证书签发包括：验证服务器判断二级证书的公钥和根证书的公钥是否相同；若相同，则验证服务器确定二级证书为根证书签发；若不相同，则验证服务器确定二级证书不为根证书签发。细化了对二级证书的验证过程，增加了本申请实施例的实现方式。

本申请第三方面提供了一种终端，包括：校验单元，用于通过安全计算容器对签名的安全计算单元进行完整性校验；第一处理单元，若签名的安全计算单元通过完整性校验，则用于通过安全计算容器对签名的安全计算单元进行合法性校验并获取校验结果；第二处理单元，若校验结果为合法的，则用于通过可信执行环境 TEE 或安全元件 SE 加载签名的安全计算单元并获取可信应用程序的安全计算结果。通过引入安全计算容器的方式，避免了 TEE 的客户端应用程序受到攻击，达到了隔离主容器和 TEE 的安全效果，提高了可信执行环境的访问接口的安全性。

在一种可能的设计中，在本申请实施例第三方面的第一种实现方式中，第一处理单元具体用于：通过安全计算容器获取签名的安全计算单元的二级证书，该二级证书用于验证签名的安全计算单元的合法性；通过安全计算容器将二级证书发送至验证服务器；通过安全计算容器接收验证服务器发送的校验结果。通过给安全计算单元分配二级证书，使安全计算单元在主容器之外的安全计算容器中进行二级证书校验，认证与加载，既解决了可信

应用程序开发的流程冗长的问题，降低了第三方开发者和终端厂商的接入成本，又保证了验证与加载安全计算单元的安全性。

在一种可能的设计中，在本申请实施例第三方面的第二种实现方式中，所述校验单元具体用于：通过安全计算容器中的安全计算授权与加载模块从签名的安全计算单元中获取签名文件；通过安全计算授权与加载模块从签名的安全计算单元中获取安全计算单元文件元数据；通过安全计算授权与加载模块对安全计算单元文件元数据进行摘要计算，得到安全计算单元文件元数据的哈希值；通过安全计算授权与加载模块将哈希值和签名文件进行比对校验。对具体的完整性校验过程进行了细化，在可信应用程序的开发流程中，在签名的安全计算单元加载至可信执行环境之前，对签名的安全计算单元进行完整性验证，提高了签名的安全计算单元的可靠性和安全性。

在一种可能的设计中，在本申请实施例第三方面的第三种实现方式中，终端还包括：获取单元，用于从主容器获取加载请求，该加载请求用于终端的安全计算容器加载签名的安全计算单元，该签名的安全计算单元用于对可信应用程序进行安全计算。增加了从主容器获取加载请求的过程，将对可信应用程序的安全计算功能拆分到安全计算单元中，定义安全计算的统一接口，达到一次开发，所有终端平台均可运行，避免了第三方开发者需要为每个终端平台定制 TA 的过程，降低了开发者和终端厂商的开发和分发成本。

在一种可能的设计中，在本申请实施例第三方面的第四种实现方式中，终端还包括：传输单元，用于将安全计算结果传输至终端的主容器。将安全计算结果反馈至可信应用程序，实现对可信应用程序的安全计算。

在一种可能的设计中，在本申请实施例第三方面的第五种实现方式中，终端还包括：第一停止单元，若签名的安全计算单元没有通过完整性验证，则用于停止加载签名的安全计算单元的流程。增加了签名的安全计算单元没有通过完整性验证时，停止加载签名的安全计算单元的过程，确保了安全计算单元的有效性，提高了可信应用程序的开发过程的安全性。

在一种可能的设计中，在本申请实施例第三方面的第六种实现方式中，终端还包括：第二停止单元，若校验结果为不合法的，则用于停止加载签名的安全计算单元的流程。增加了当二级证书为不合法的情况下，停止加载签名的安全计算单元的过程，确保了安全计算单元的合法性，提高了可信应用程序的开发过程的安全性。

在一种可能的设计中，在本申请实施例第三方面的第七种实现方式中，签名的安全计算单元的文件格式至少包括初始段、代码段和数据段。确定了签名的安全计算单元的具体组成，明确了统一的安全计算单元，简化了可信应用程序的开发过程。

本申请第四方面提供了一种服务器，服务器为验证服务器，包括：接收单元，用于接收终端发送的二级证书，该二级证书用于验证签名的安全计算单元的合法性；获取单元，用于从数字证书认证服务器获取根证书；验证单元，用于验证二级证书是否为根证书签发；第一确定单元，若二级证书为根证书签发，则用于确定签名的安全计算单元为合法的；第二确定单元，若二级证书不为根证书签发，则用于确定签名的安全计算单元为不合法的。通过验证服务器对安全计算单元的证书进行在线验证合法性，只有在证书有效的情

况才会加载安全计算单元，保证了安全计算单元的合法性。

在一种可能的设计中，在本申请实施例第四方面的第一种实现方式中，服务器还包括：发送单元，用于将验证结果发送至终端，该验证结果用于指示签名的安全计算单元是否为合法的。增加了将验证结果发送至终端的过程，使本申请实施例在步骤上更完善。

在一种可能的设计中，在本申请实施例第四方面的第二种实现方式中，验证单元具体用于：判断二级证书的公钥和根证书的公钥是否相同；若相同，则确定二级证书为根证书签发；若不相同，则确定二级证书不为根证书签发。细化了对二级证书的验证过程，增加了本申请实施例的实现方式。

本申请第五方面提供了一种终端，包括：存储器、收发器和至少一个处理器，所述存储器中存储有程序代码，所述存储器、所述收发器和所述至少一个处理器通过线路通信，所述处理器运行所述代码以指令所述终端执行上述第一方面任一项所述的方法。

本申请第六方面提供了一种服务器，包括：存储器、收发器和至少一个处理器，所述存储器中存储有程序代码，所述存储器、所述收发器和所述至少一个处理器通过线路通信，所述处理器运行所述代码以指令所述服务器执行上述第二方面任一项所述的方法。

本申请的第七方面提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有程序代码，当其在计算机上运行时，使得计算机执行上述第一方面所述的方法。

本申请的第八方面提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有程序代码，当其在计算机上运行时，使得计算机执行上述第二方面所述的方法。

本申请的第九方面提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第一方面所述的方法。

本申请的第十方面提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第二方面所述的方法。

从以上技术方案可以看出，本申请实施例具有以下优点：

终端通过安全计算容器对签名的安全计算单元进行完整性校验，即确定该签名的安全计算单元是否被第三方篡改；若签名的安全计算单元通过完整性验证，即签名的安全计算单元未被第三方篡改，则终端通过所述安全计算容器对所述签名的安全计算单元进行合法性校验并获取校验结果；若校验结果为合法的，即二级证书所属的签名的安全计算单元是合法的，则终端通过可信执行环境 TEE 或安全元件 SE 加载签名的安全计算单元并获取可信应用程序的安全计算结果。本申请中，通过引入安全计算容器的方式，避免了 TEE 的客户端应用程序受到攻击，达到了隔离主容器和 TEE 的安全效果，改进了目前可信应用程序进行验证的流程，提高了可信执行环境的访问接口安全性。

附图说明

图 1 为现有方案应用的系统架构示意图；

图 2 为本申请实施例应用的系统架构示意图；

图 3 为本申请实施例中基于多容器的可信应用程序的处理方法的一个流程示意图；

图 4 为本申请实施例中基于多容器的可信应用程序的处理方法的另一个流程示意图；

图 5 为本申请实施例中终端的一个结构示意图；

图 6 为本申请实施例中终端的另一个结构示意图；

图 7 为本申请实施例中验证服务器的一个结构示意图；

图 8 为本申请实施例中验证服务器的另一个结构示意图；

图 9A 为本申请实施例中终端的另一个结构示意图；

图 9B 为本申请实施例中终端的另一个结构示意图；

图 10 为本申请实施例中终端的另一个结构示意图；

图 11 为本申请实施例中验证服务器的另一个结构示意图。

具体实施方式

本申请实施例提供了一种基于多容器的可信应用程序的处理方法及相关设备，用于简化可信应用程序的开发和部署流程，提高了对可信应用程序的处理效率和可信执行环境的访问接口的安全性。

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例进行描述。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”或“具有”及其任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

现有方案中提供了一种系统架构，如图 1 所示，在该系统架构中，包括可信执行环境（trusted execution environment，TEE）和富执行环境（rich execution environment，REE）。将高安全敏感的应用与通用的软件环境进行隔离，提供专门的可信执行环境 TEE，并保护应用的资源和数据的保密性、完整性和访问权限；对 Android 等容易被攻击的传统操作系统提供通用的富执行环境 REE。在 REE 侧执行的应用称为客户端应用程序（client application，CA），比如银行类应用等第三方支付应用，在 TEE 侧执行的应用称为可信应用程序（trusted application，TA），比如执行签名、加解密计算等关键服务的应用。由于 TA 运行在可信执行环境 TEE 中，TA 的部署/升级操作需要严格遵循 TEE 发行方（通常是终端厂商）的安全验证规范，比如使用数字签名等措施，确保 TEE 各个环节是真正可信的。可信执行环境 TEE 中包括可信执行环境内部应用程序编程接口（trusted execution environment internal application programming interface，TEE Internal API）和可信操作系统部件，TEE Internal API 的主要作用为：向上提供可信操作系统部件的功能、与客户端应用程序 CA 通信、实现 TA 与 TA 通信、提供安全存储、密码学功能、时间功能等；可信操作系统部件主要包括可信核心框架、可信功能、可信内核和可信执行环境 TEE 通信代理，其中，可信核心框架为 TA 提供类似操作系统的功能；可信功能为应用开发者

提供支持能力；可信内核用于与平台硬件中的可信设备进行交互；可信执行环境通信代理为 TA 和 CA 提供一个安全的通信通道，例如，可信执行环境通信代理通过平台硬件将消息传递至富执行环境通信代理，实现 TA 和 CA 的交互。富执行环境 REE 中包括可信执行环境客户端应用程序编程接口（trusted execution environment client application programming interface，TEE Client API）、可信执行环境功能应用程序编程接口（trusted execution environment functional application programming interface，TEE Functional API）和多媒体操作系统，多媒体操作系统部件主要包括公共设备驱动和富执行环境通信代理，其中，富执行环境通信代理用于与 TEE 进行通信，CA 和 TA 提供一个安全的通信通道，公共设备驱动用于驱动平台硬件中的公共设备。CA 使用 TEE Client API、TEE Functional API 接入到由 TA 提供的安全服务。

由于该系统架构存在一些限制，不同终端厂商的 TEE 实现可信应用管理平台也存在较多差异，导致 TA 的开发及部署过程较为复杂。由于 TEE 侧通过数字签名等专有措施确保 TEE 真正可信，具体的管控措施由具体的终端厂商（TEE 发行方）实施，可选应用程序 TA 的开发者必须联系各终端厂商进行合作开发，这种上下游的耦合关系，导致 TA 开发流程复杂和冗长。例如，支付宝应用程序的 TA，需要在每个终端厂商的设备上开发一套 TA，每个平台上的 TA 签名与系统接口都不一致，导致支付宝应用程序的 TA 研发流程和分发流程异常复杂，进而导致因流程不规范而存在的安全风险，同理，其他第三方开发者也会遇到同样的问题。

本申请实施例可应用于如图 2 所示的系统架构，在该系统架构中，包括终端 100、验证服务器 200 和数字证书认证（certificate authority，CA）服务器 300，其中，终端有三种应用环境，分别为：富执行环境（rich execution environment，REE）、可信执行环境（trusted execution environment，TEE）和安全元件（secure element，SE），终端包括主容器 101、安全计算容器 102、可信执行环境（trusted execution environment，TEE）和安全元件（secure element，SE）103、系统内核 104 和平台硬件 105，其中，主容器 101 中运行环境为 REE，主容器中包括多个应用程序，例如应用程序 1、应用程序 2 和应用程序 3；安全计算容器 102 包括安全计算授权与加载模块。其中，安全计算容器从主容器中独立出来，安全计算容器支持的硬件与主容器支持的硬件相同，例如，都是支持使用 REE 的硬件接口。CA 服务器 300 用于保存终端厂商提供的所有有效的证书，有效的证书包括二级证书和根证书，终端厂商可以在 CA 服务器 300 上管理这些有效的证书（可以对这些有效的证书进行查询、新增、吊销、失效、重新授权等操作）。验证服务器 200 用于为安全授权与加载模块提供对二级证书的有效性进行验证。本申请的系统架构可以应用在支付、加密存储等涉及安全计算的场景中，具体此处不做限定。

为便于理解，下面对本申请实施例的具体流程进行描述，请参阅图 3，本申请实施例中基于多容器的可信应用程序的处理方法的一个实施例包括：

301、终端从主容器获取加载请求。

终端从主容器获取加载请求，该加载请求用于指示终端的安全计算容器加载签名的安全计算单元，该签名的安全计算单元用于对可信应用程序 TA 进行安全计算，其中，安全

计算单元为可信应用程序中执行安全计算的功能模块。

在操作系统内核中隔离出多个相互独立的系统资源，即容器，每个容器都运行独立的OS，各个容器之间无法直接相互访问，本申请中提供了主容器和安全计算容器，其中主容器中的应用环境为REE。

可信应用程序 TA 向终端的安全计算容器中的安全计算授权与加载模块请求加载签名的安全计算单元。具体的，主容器中运行的是一个智能操作系统（比如 Android 系统），这个主容器中的应用程序（比如支付宝）需要进行安全计算，不再是直接向 TEE 发起调用，而是向安全计算容器进行发起调用，将签名的安全计算单元和参数传输至安全计算容器中的安全计算授权与加载模块，安全计算授权与加载模块会检查应用程序是否有权限发起此调用。

需要说明的是，在发送加载请求之前，需要用户先开发得到未签名的安全计算单元，在对该未签名的安全计算单元进行签名，得到签名的安全计算单元。开发得到未签名的安全计算单元的过程如下：

用户（第三方开发者）向终端厂商提交必要的资料，向终端厂商申请开发者证书，终端厂商在审核通过之后，给用户颁发开发者证书（二级证书），同时，将二级证书的公钥保存在 CA 服务器上。用户利用终端厂商提供的安全计算单元的软件开发工具包（software development kit，SDK）和编译器套件得到未签名的安全计算单元，其中，SDK 包含了 C 标准库和加解密计算库，编译器套件包含了编译器和链接脚本，链接脚本用于将编译之后的程序组装成一个标准的安全计算单元，例如，用户使用支付宝进行指纹支付时，因为指纹信息为重要的安全数据信息，需要在一个安全的环境中进行收集，因此支付宝需要对指纹采集的环境进行安全计算，将执行该功能的程序剥离出来重新编译得到未签名的安全计算单元，通过该未签名的安全计算单元对指纹采集的环境进行安全计算。该链接脚本具体用于将若干个输入文件根据一定的规则合并成一个输出文件，例如，链接脚本命令 ENTRY 指定了安全计算单元的入口函数为 compute 函数，这样 TEE 在加载安全计算单元时就能够将需要计算参数直接传递给 compute 函数，进行安全计算，获得计算结果。该链接脚本的代码如下所示：

```
ENTRY(compute)
SECTIONS
{
. =0×10000;
.text:{*(.text)}
. =0×8000000;
.data: {*(.data)}
.bss: {*(.bss)}
}
```

其中，经过编译器编译之后，未签名的安全计算单元的文件格式与动态库文件格式一样，有初始（init）段，代码段，数据段等。

对该未签名的安全计算单元进行签名的过程如下：

首先利用摘要算法对编译之后的未签名的安全计算单元文件进行摘要计算，得到安全计算单元的摘要文件，可选的，摘要算法可以采用安全哈希算法（secure Hash algorithm，SHA），例如SHA256，SHA512等；然后利用终端厂商颁发的二级证书中的公钥对摘要进行签名，生成签名文件，具体为 CERT.RSA 文件；将未签名的安全计算单元与签名文件进行合成，最终得到签名的安全计算单元。

可以理解的是，在开发得到未签名的安全计算单元之前，需要定义安全计算单元的同一格式，用户不用再考虑不同质终端厂家采用不同的 TEE 技术，实现开发一套安全计算单元，可以运行在各个终端平台的TEE之上。

302、终端通过安全计算容器对签名的安全计算单元进行完整性校验。

终端根据加载请求和安全计算授权与加载模块判断可信应用程序 TA 有权限发起此调用之后，终端通过安全计算容器中的安全计算授权与加载模块从签名的安全计算单元中获取密钥文件；终端通过所述安全计算授权与加载模块从签名的安全计算单元中获取安全计算单元文件元数据；终端通过安全计算授权与加载模块对安全计算单元文件元数据进行摘要计算，得到安全计算单元文件元数据的哈希值；终端通过安全计算授权与加载模块将哈希值和签名文件进行比对校验。若签名的安全计算单元通过完整性验证，即哈希值与签名文件的哈希值相同，则终端执行步骤 303。完整性是指在传输、存储信息或数据的过程中，确保信息或数据不被未授权的篡改或在篡改后能被迅速发现。

例如，安全计算授权与加载模块首先提取安全计算单元文件头部的 CERT.RSA 信息；接着提取安全计算单元中的安全计算单元文件元数据，安全计算单元文件元数据的起始地址为 CERT.RSA 的尾部，安全计算单元文件元数据的结束地址是安全计算单元文件的末尾；再利用 SHA256 算法对安全计算单元文件元数据进行摘要计算，得到安全计算单元元数据的哈希值；再根据。

需要说明的是，若签名的安全计算单元没有通过完整性验证，则终端可以认为此安全计算单元受到第三方篡改，停止加载签名的安全计算单元的流程。

可以理解的是，本申请在现有的“主容器”的基础上，增加了一个专门的“安全计算容器”，在该安全计算容器中将安全计算处理中后续容易产生变化的处理步骤剥离出来。该安全计算容器仍然位于 REE 侧，与 REE 侧的主容器使用相同的硬件，但是和主容器中的操作系统（Android 系统）相互隔离，安全计算容器中的数据安全性有较高保证，最高安全要求的计算处理步骤仍然由原TEE中的TA完成。例如，用户开发的支付宝程序不再直接使用 TEE 进行安全计算，而由安全计算容器来使用 TEE 进行安全计算，在新增的安全计算容器中，实现对支付宝的安全计算单元进行校验、认证与加载计算流程，这样能保证安全计算单元的安全性，解决了用户开发的 TA 分发的安全性问题；并且新增的安全计算容器，隔离了应用程序与 TEE 之间的联系，解决了 TA 容易遭受 CA 侧恶意调用，而导致 TEE 拒绝服务的风险。

303、终端通过安全计算容器获取签名的安全计算单元的二级证书。

终端通过通过安全计算容器中的安全计算授权与加载模块获取签名的安全计算单元的

二级证书，该二级证书用于验证签名的安全计算单元的合法性。

例如，终端通过安全计算授权与加载模块从签名的安全计算单元中提取二级证书，该二级证书用于指示该签名的安全计算单元的授权信息。

304、终端通过安全计算容器将二级证书发送至验证服务器。

终端通过安全计算容器中的安全计算授权与加载模块将二级证书发送至验证服务器。

需要说明的是，二级证书与存储在数字证书认证服务器上的根证书属于同源，二者具有同样的公钥，二级证书为根证书签发的。

305、验证服务器从数字证书认证服务器获取根证书。

验证服务器从数字证书认证服务器获取根证书。

具体的，验证服务器根据二级证书中携带的目标应用程序信息，向数字证书认证服务器发送根证书获取请求，该根证书获取请求中携带有目标应用程序信息；数字证书认证服务器根据目标应用程序信息将对应的根证书发送至验证服务器。

306、验证服务器验证二级证书是否为根证书签发。

验证服务器验证二级证书是否为根证书签发。

具体的，验证服务器判断二级证书的公钥和根证书的公钥是否相同；若相同，则验证服务器确定二级证书为根证书签发；若不相同，则验证服务器确定所二级证书不为根证书签发。若二级证书为根证书签发，则验证服务器确定签名的安全计算单元为合法的；若二级证书不为根证书签发，则验证服务器确定签名的安全计算单元为不合法的。

可以理解的是，通过公钥对证书进行验证为现有技术，具体此处不再赘述。还可以采用其他的验证方法验证二级证书的合法性，具体此处不做限定。

307、验证服务器将验证结果发送至终端。

验证服务器将验证结果发送至终端，该验证结果用于指示签名的安全计算单元是否为合法的。

需要说明的是，若校验结果为合法的，则终端执行步骤 308。若校验结果为不合法的，则终端停止加载签名的安全计算单元的流程。

308、终端通过可信执行环境加载签名的安全计算单元并获取可信应用程序的安全计算结果。

终端通过可信执行环境 TEE 加载签名的安全计算单元并获取可信应用程序的安全计算结果。具体的，终端的可信应用程序管理器（TA Manager）先检查签名的安全计算单元的二级证书是否合法，检查通过后，TAManager 调用签名的安全计算单元的通用接口，获取安全计算结果，将安全计算结果返回至安全计算容器。

需要说明的是，终端还可以通过安全元件 SE 调用签名的安全计算单元并获取 TA 的安全计算结果，终端通过 SE 调用签名的安全计算单元的过程与 TEE 调用签名的安全计算单元的过程类似，此处不再赘述。

309、终端通过可信执行环境 TEE 将安全计算结果传输至终端的安全计算容器。

终端通过可信执行环境 TEE 将安全计算结果传输至终端的安全计算容器中的安全计算授权与加载模块。

需要说明的是，终端还可以通过安全元件 SE 将安全计算结果传输至终端的安全计算容器中的安全计算授权与加载模块。

310、终端将安全计算结果传输至终端的主容器。

终端将安全计算结果传输至终端的主容器。具体的，终端的安全计算授权与加载模块将接收到的安全计算结果传输至主容器中的可信应用程序 TA。

本申请实施例中，通过二级证书、在安全容器中进行合法性校验的方法，解耦了目前 TA 开发流程冗长的问题，向第三方开发者开放了安全计算的能力，简化第三方开发者对 TA 的开发和部署流程，提高了对 TA 的处理效率；通过新增的安全计算容器，在安全计算容器中对安全计算单元进行校验、认证与加载，保证了验证与加载安全计算单元的安全性，改进了目前 TA 进行验证的流程，提高了 TEE 的访问接口安全性；规定了安全计算的统一接口，便于 TA 应用程序的开发。

请参阅图 4，本申请实施例中基于多容器的可信应用程序的处理方法的另一个实施例包括：

401、终端从主容器获取加载请求。

终端从主容器获取加载请求，该加载请求用于指示终端的安全计算容器加载签名的安全计算单元，该签名的安全计算单元用于对可信应用程序 TA 进行安全计算。

可信应用程序 TA 向终端的安全计算容器中的安全计算授权与加载模块请求加载签名的安全计算单元。具体的，主容器中运行的是一个智能操作系统（比如 Android 系统），这个主容器中的应用程序（比如支付宝）需要进行安全计算，不再是直接向 TEE 发起调用，而是向安全计算容器进行发起调用，将签名的安全计算单元和参数传输至安全计算容器中的安全计算授权与加载模块，安全计算授权与加载模块会检查应用程序是否有权限发起此调用。

402、终端通过安全计算容器对签名的安全计算单元进行完整性校验。

终端根据加载请求和安全计算授权与加载模块判断可信应用程序 TA 有权限发起此调用之后，终端通过安全计算容器中的安全计算授权与加载模块从签名的安全计算单元中获取密钥文件；终端通过所述安全计算授权与加载模块从签名的安全计算单元中获取安全计算单元文件元数据；终端通过安全计算授权与加载模块对安全计算单元文件元数据进行摘要计算，得到安全计算单元文件元数据的哈希值；终端通过安全计算授权与加载模块将哈希值和签名文件进行比对校验。若签名的安全计算单元通过完整性验证，即哈希值与签名文件的哈希值相同，则终端执行步骤 303。

403、终端通过安全计算容器获取签名的安全计算单元的二级证书。

终端通过通过安全计算容器中的安全计算授权与加载模块获取签名的安全计算单元的二级证书，该二级证书用于验证签名的安全计算单元的合法性。

404、终端通过安全计算容器将二级证书发送至验证服务器。

终端通过安全计算容器中的安全计算授权与加载模块将二级证书发送至验证服务器。

405、验证服务器从数字证书认证服务器获取根证书。

验证服务器从数字证书认证服务器获取根证书。

具体的，验证服务器根据二级证书中携带的目标应用程序信息，向数字证书认证服务器发送根证书获取请求，该根证书获取请求中携带有目标应用程序信息；数字证书认证服务器根据目标应用程序信息将对应的根证书发送至验证服务器。

406、验证服务器验证二级证书是否为根证书签发。

验证服务器验证二级证书是否为根证书签发。

具体的，验证服务器判断二级证书的公钥和根证书的公钥是否相同；若相同，则验证服务器确定二级证书为根证书签发；若不相同，则验证服务器确定所二级证书不为根证书签发。若二级证书为根证书签发，则验证服务器确定签名的安全计算单元为合法的；若二级证书不为根证书签发，则验证服务器确定签名的安全计算单元为不合法的。

407、验证服务器将验证结果发送至终端。

验证服务器将验证结果发送至终端，该验证结果用于指示签名的安全计算单元是否为合法的。

需要说明的是，若校验结果为合法的，则终端执行步骤 308。若校验结果为不合法的，则终端停止加载签名的安全计算单元的流程。

步骤 401 至步骤 407 与步骤 301 至步骤 307 类似，具体此处不再赘述。

408、终端通过安全元件加载签名的安全计算单元并获取可信应用程序的安全计算结果。

终端通过安全元件 SE 加载签名的安全计算单元并获取可信应用程序 TA 的安全计算结果。具体的，终端的可信应用程序管理器（TA Manager）先检查签名的安全计算单元的二级证书是否合法，检查通过后，TAManager 调用签名的安全计算单元的通用接口，获取安全计算结果，将安全计算结果返回至安全计算容器。

409、终端通过安全元件 SE 将安全计算结果传输至终端的安全计算容器。

终端通过安全元件 SE 将安全计算结果传输至终端的安全计算容器中的安全计算授权与加载模块。

410、终端将安全计算结果传输至终端的主容器。

终端将安全计算结果传输至终端的主容器。具体的，终端的安全计算授权与加载模块将接收到的安全计算结果传输至主容器中的可信应用程序 TA。

本申请实施例中，通过新增的安全计算容器，在安全计算容器中对安全计算单元进行校验、认证与加载，保证了验证与加载安全计算单元的安全性，改进了目前 TA 进行验证的流程，既降低第三方开发者和终端厂商的接入成本，又保证了验证与加载安全计算单元的安全性；通过二级证书、在安全容器中进行合法性校验的方法，解耦了目前 TA 开发流程冗长的问题，向第三方开发者开放了安全计算的能力，简化第三方开发者对 TA 的开发和部署流程，提高了对 TA 的处理效率。

上面对本申请实施例中基于多容器的可信应用程序的处理方法进行了描述，下面对本申请实施例中的终端和验证服务器进行描述，请参阅图 5，本申请实施例中终端的一个实施例包括：

校验单元 501，用于通过安全计算容器对签名的安全计算单元进行完整性校验；

第一处理单元 502，若签名的安全计算单元通过完整性校验，则用于通过安全计算容器对签名的安全计算单元进行合法性校验并获取校验结果；

第二处理单元 503，若校验结果为合法的，则用于通过可信执行环境 TEE 或安全元件 SE 加载签名的安全计算单元并获取可信应用程序的安全计算结果。

本申请实施例，通过引入安全计算容器的方式，避免了 TEE 的客户端应用程序受到攻击，达到了隔离主容器和 TEE 的安全效果，提高了可信执行环境的访问接口的安全性。

请参阅图 6，本申请实施例中终端的另一个实施例包括：

校验单元 601，用于通过安全计算容器对签名的安全计算单元进行完整性校验；

第一处理单元 602，若签名的安全计算单元通过完整性校验，则用于通过安全计算容器对签名的安全计算单元进行合法性校验并获取校验结果；

第二处理单元 603，若校验结果为合法的，则用于通过可信执行环境 TEE 或安全元件 SE 加载签名的安全计算单元并获取可信应用程序的安全计算结果。

在一个示例中，第一处理单元 602 具体用于：

通过安全计算容器获取签名的安全计算单元的二级证书，该二级证书用于验证签名的安全计算单元的合法性；

通过安全计算容器将二级证书发送至验证服务器；

通过安全计算容器接收验证服务器发送的校验结果。

在一个示例中，校验单元 601 具体用于：

通过安全计算容器中的安全计算授权与加载模块从签名的安全计算单元中获取签名文件；

通过安全计算授权与加载模块从签名的安全计算单元中获取安全计算单元文件元数据；

通过安全计算授权与加载模块对安全计算单元文件元数据进行摘要计算，得到安全计算单元文件元数据的哈希值；

通过安全计算授权与加载模块将哈希值和签名文件进行完整性校验。

在一个示例中，终端还可以包括：

获取单元 604，用于从主容器获取加载请求，该加载请求用于终端的安全计算容器加载签名的安全计算单元，该签名的安全计算单元用于对可信应用程序进行安全计算。

在一个示例中，终端还可以包括：

传输单元 605，用于将安全计算结果传输至终端的主容器。

在一个示例中，终端还可以包括：

第一停止单元 606，若签名的安全计算单元没有通过完整性验证，则用于停止加载签名的安全计算单元的流程。

在一个示例中，终端还可以包括：

第二停止单元 607，若校验结果为不合法的，则用于停止加载签名的安全计算单元的流程。

在一个示例中，签名的安全计算单元的文件格式至少包括初始段、代码段和数据段。

本申请实施例中，通过新增的安全计算容器，在安全计算容器中对安全计算单元进行校验、认证与加载，保证了验证与加载安全计算单元的安全性，改进了目前 TA 进行验证的流程，提高了 TEE 的访问接口安全性；通过二级证书、在安全容器中进行合法性校验的方法，解耦了目前 TA 开发流程冗长的问题，向第三方开发者开放了安全计算的能力，简化第三方开发者对 TA 的开发和部署流程，提高了对 TA 的处理效率；规定了安全计算的统一接口，便于 TA 应用程序的开发。

请参阅图 7，本申请实施例中验证服务器的一个实施例包括：

接收单元 701，用于接收终端发送的二级证书，该二级证书用于验证签名的安全计算单元的合法性；

获取单元 702，用于从数字证书认证服务器获取根证书；

验证单元 703，用于验证二级证书是否为根证书签发；

第一确定单元 704，若二级证书为根证书签发，则用于确定签名的安全计算单元为合法的；

第二确定单元 705，若二级证书不为根证书签发，则用于确定签名的安全计算单元为不合法的。

本申请实施例中，通过验证服务器对安全计算单元的证书进行在线验证合法性，只有在证书有效的情况才会加载安全计算单元，保证了安全计算单元的合法性。

请参阅图 8，本申请实施例中验证服务器的另一个实施例包括：

接收单元 801，用于接收终端发送的二级证书，该二级证书用于验证签名的安全计算单元的合法性；

获取单元 802，用于从数字证书认证服务器获取根证书；

验证单元 803，用于验证二级证书是否为根证书签发；

第一确定单元 804，若二级证书为根证书签发，则用于确定签名的安全计算单元为合法的；

第二确定单元 805，若二级证书不为根证书签发，则用于确定签名的安全计算单元为不合法的。

在一个示例中，服务器还包括：

发送单元 806，用于将验证结果发送至终端，该验证结果用于指示签名的安全计算单元是否为合法的。

在一个示例中，验证单元 803 具体用于：

判断二级证书的公钥和根证书的公钥是否相同；

若相同，则确定二级证书为根证书签发；

若不相同，则确定二级证书不为根证书签发。

本申请实施例中，通过验证服务器对安全计算单元的证书进行在线验证合法性，只有在证书有效的情况才会加载安全计算单元，这样保证了安全计算单元的合法性。

上面图 5 至图 8 从模块化功能实体的角度分别对本申请实施例中终端和验证服务器进行详细描述，下面从硬件处理的角度对本申请实施例中终端和验证服务器进行详细描述。

本申请实施例提供一种终端，如图 9A 所示，该终端具有存储器 901、收发器 902 和至少一个处理器 903，该存储器 901 存储程序代码和数据，例如该存储器中受保护区域可以存储 TEE 操作系统和可信应用程序，该存储器的非受保护区域可以存储 REE 操作系统和客户端应用程序，存储器 901、收发器 902 和至少一个处理器 903 通过总线 904 互相连接，总线 904 可以是外设部件互连标准（peripheral component interconnect，PCI）总线或扩展工业标准结构（extended industry standard architecture，EISA）总线等。该处理器 903 执行该存储器 901 中的程序代码以指令该终端完成上述方法实施例中的操作，简化可信应用程序的开发和部署流程，提高对可信应用程序的处理效率。

图 9B 是本申请实施例提供的一种终端的结构示意图，参考图 9B，终端 910 包括主容器 911、安全计算容器 912、可信执行环境（trusted execution environment，TEE）和安全元件（secure element，SE）913、系统内核 914 和平台硬件 915，其中，主容器 911 中运行环境为 REE，主容器 911 中包括多个应用程序，安全计算容器 912 包括安全计算授权与加载模块，可信执行环境和安全元件 913 中包括可信应用程序管理器。

图 10 示出的是与本申请实施例提供的终端的部分结构的框图。参考图 10，所述终端包括：射频（radio frequency，RF）电路 1010、存储器 1020、输入单元 1030、显示单元 1040、传感器 1050、音频电路 1060、无线保真（wireless fidelity，WIFI）模块 1070 和处理器 1080 等部件。本领域技术人员可以理解，图 10 中示出的终端结构并不构成对所述终端的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

处理器 1080 是终端的控制中心，在本申请实施例中，可以对签名的安全计算单元进行完整性验证，并加载签名的安全计算单元并获取可信应用程序的安全计算结果。

RF 电路 1010 通过总线与所述处理器 1080 连接，负责向互联网发送数据或者从互联网接收数据，还可用于收发信息过程中，信号的接收和发送，例如，向验证服务器发送二级证书；另外，终端在接收到验证服务器发送的验证结果后，将验证结果发送给处理器 1080 处理。通常，所述 RF 电路 1010 包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器（low noise amplifier，LNA）、双工器等。此外，所述 RF 电路 1010 还可以通过无线通信与网络和其他设备通信。上述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯系统 （global system of mobile communication，GSM）、通用分组无线服务（general packet radio service，GPRS）、码分多址（code division multiple access，CDMA）、宽带码分多址（wideband code division multiple access，WCDMA）、长期演进 （long term evolution，LTE）、电子邮件、短消息服务（short messaging service，SMS）等。

存储器 1020 可用于存储软件程序以及模块，所述处理器 1080 通过运行存储在所述存储器 1020 的软件程序以及模块，从而执行终端的各种功能应用以及数据处理。所述存储器 1020 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序（比如对签名的安全计算单元进行完整性验证等）等；存储数据区可存储根据终端的使用所创建的数据(比如安全计算结果等)等。此外，所述存储器 1020

可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

图 11 是本申请实施例提供的一种验证服务器的结构示意图，该验证服务器 1100 可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上处理器（central processing units，CPU）1101（例如，一个或一个以上处理器）和存储介质 1108，一个或一个以上存储应用程序 1107 或数据 1106 的存储介质 1108（例如一个或一个以上海量存储设备）。其中，存储介质 1108 可以是短暂存储或持久存储。存储在存储介质 1108 的程序可以包括一个或一个以上模块（图示没标出），每个模块可以包括对验证服务器中的一系列代码。更进一步地，处理器 1101 可以设置为与存储介质 1108 通信，处理器 1101 是验证服务器的控制中心，可利用各种接口和线路连接整个验证服务器的各个部分，通过运行或执行存储在存储介质 1108 内的软件程序和/或模块，以及调用存储在存储介质 1108 内的数据，验证服务器的各种功能和处理数据，从而完成对终端发送的二级证书的合法性验证。

存储介质 1108 可用于存储软件程序以及模块，处理器 1101 通过运行存储在存储介质 1108 的软件程序以及模块，从而执行验证服务器 1100 的各种功能应用以及数据处理。存储介质 1108 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序（比如判断二级证书是否合法等）等；存储数据区可存储根据验证服务器的使用所创建的数据(比如确定二级证书为合法的)等。此外，存储介质 1108 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。在本申请实施例中提供的基于多容器的可信应用程序的处理方法的程序和接收到的数据流存储在存储器中，当需要使用时，处理器 1101 从存储介质 1108 中调用。

验证服务器 1100 还可以包括一个或一个以上电源 1102，一个或一个以上有线或无线网络接口 1103，一个或一个以上输入输出接口 1104，和/或，一个或一个以上操作系统 1105，例如 Windows Serve，Mac OS X，Unix，Linux，FreeBSD 等等。本领域技术人员可以理解，图 11 中示出的验证服务器结构并不构成对验证服务器的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络

单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line，DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存储的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘（solid state disk，SSD））等。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory，ROM）、随机存取存储器（random access memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

权 利 要 求

1、一种基于多容器的可信应用程序的处理方法，其特征在于，包括：

终端通过安全计算容器对签名的安全计算单元进行完整性校验；

若所述签名的安全计算单元通过所述完整性校验，则所述终端通过所述安全计算容器对所述签名的安全计算单元进行合法性校验并获取校验结果；

若所述校验结果为合法的，则所述终端通过可信执行环境 TEE 或安全元件 SE 加载所述签名的安全计算单元并获取可信应用程序的安全计算结果。

2、根据权利要求 1 所述的处理方法，其特征在于，所述终端通过所述安全计算容器对所述签名的安全计算单元进行合法性校验并获取校验结果包括：

所述终端通过所述安全计算容器获取所述签名的安全计算单元的二级证书，所述二级证书用于验证所述签名的安全计算单元的合法性；

所述终端通过所述安全计算容器将所述二级证书发送至验证服务器；

所述终端通过所述安全计算容器接收所述验证服务器发送的校验结果。

3、根据权利要求 1 所述的处理方法，其特征在于，所述终端通过安全计算容器对签名的安全计算单元进行完整性校验包括：

所述终端通过所述安全计算容器中的安全计算授权与加载模块从所述签名的安全计算单元中获取签名文件；

所述终端通过所述安全计算授权与加载模块从所述签名的安全计算单元中获取安全计算单元文件元数据；

所述终端通过所述安全计算授权与加载模块对所述安全计算单元文件元数据进行摘要计算，得到所述安全计算单元文件元数据的哈希值；

所述终端通过所述安全计算授权与加载模块将所述哈希值和所述签名文件进行比对校验。

4、根据权利要求 1 所述的处理方法，其特征在于，所述终端通过安全计算容器对签名的安全计算单元进行完整性校验之前，所述方法还包括：

所述终端从主容器获取加载请求，所述加载请求用于所述终端的安全计算容器加载所述签名的安全计算单元，所述签名的安全计算单元用于对所述可信应用程序进行安全计算。

5、根据权利要求 1-4 任一所述的处理方法，其特征在于，所述终端通过可信执行环境 TEE 或安全元件 SE 加载所述签名的安全计算单元并获取可信应用程序的安全计算结果之后，所述方法还包括：

所述终端将所述安全计算结果传输至所述终端的主容器。

6、根据权利要求 1-4 任一所述的处理方法，其特征在于，所述方法还包括：

若所述签名的安全计算单元没有通过所述完整性校验，则所述终端停止加载所述签名的安全计算单元的流程。

7、根据权利要求 1-4 任一所述的处理方法，其特征在于，所述方法还包括：

若所述校验结果为不合法的，则所述终端停止加载所述签名的安全计算单元的流程。

8、一种基于多容器的可信应用程序的处理方法，其特征在于，包括：

验证服务器接收终端发送的二级证书，所述二级证书用于验证签名的安全计算单元的合法性；

所述验证服务器从数字证书认证服务器获取根证书；

所述验证服务器验证所述二级证书是否为所述根证书签发；

若所述二级证书为所述根证书签发，则所述验证服务器确定所述签名的安全计算单元为合法的；

若所述二级证书不为所述根证书签发，则所述验证服务器确定所述签名的安全计算单元为不合法的。

9、根据权利要求 8 所述的处理方法，其特征在于，所述方法还包括：

所述验证服务器将验证结果发送至所述终端，所述验证结果用于指示所述签名的安全计算单元是否为合法的。

10、根据权利要求 8 或 9 所述的处理方法，其特征在于，所述验证服务器验证所述二级证书是否为所述根证书签发包括：

所述验证服务器判断所述二级证书的公钥和根证书的公钥是否相同；

若相同，则所述验证服务器确定所述二级证书为所述根证书签发；

若不相同，则所述验证服务器确定所述二级证书不为所述根证书签发。

11、一种终端，其特征在于，包括：

校验单元，用于通过安全计算容器对签名的安全计算单元进行完整性校验；

第一处理单元，若所述签名的安全计算单元通过所述完整性校验，则用于通过所述安全计算容器对所述签名的安全计算单元进行合法性校验并获取校验结果；

第二处理单元，若所述校验结果为合法的，则用于通过可信执行环境 TEE 或安全元件 SE 加载所述签名的安全计算单元并获取可信应用程序的安全计算结果。

12、根据权利要求 11 所述的终端，其特征在于，所述第一处理单元具体用于：

通过所述安全计算容器获取所述签名的安全计算单元的二级证书，所述二级证书用于验证所述签名的安全计算单元的合法性；

通过所述安全计算容器将所述二级证书发送至验证服务器；

通过所述安全计算容器接收所述验证服务器发送的校验结果。

13、根据权利要求 11 所述的终端，其特征在于，所述校验单元具体用于：

通过所述安全计算容器中的安全计算授权与加载模块从所述签名的安全计算单元中获取签名文件；

通过所述安全计算授权与加载模块从所述签名的安全计算单元中获取安全计算单元文件元数据；

通过所述安全计算授权与加载模块对所述安全计算单元文件元数据进行摘要计算，得到所述安全计算单元文件元数据的哈希值；

通过所述安全计算授权与加载模块将所述哈希值和所述签名文件进行比对校验。

14、根据权利要求 11 所述的终端，其特征在于，所述终端还包括：

获取单元，用于从主容器获取加载请求，所述加载请求用于所述终端的安全计算容器加载所述签名的安全计算单元，所述签名的安全计算单元用于对所述可信应用程序进行安全计算。

15、根据权利要求 11-14 任一所述的终端，其特征在于，所述终端还包括：

传输单元，用于将所述安全计算结果传输至所述终端的主容器。

16、根据权利要求 11-14 任一所述的终端，其特征在于，所述终端还包括：

第一停止单元，若所述签名的安全计算单元没有通过所述完整性校验，则用于停止加载所述签名的安全计算单元的流程。

17、根据权利要求 11-14 任一所述的终端，其特征在于，所述终端还包括：

第二停止单元，若所述校验结果为不合法的，则用于停止加载所述签名的安全计算单元的流程。

18、一种服务器，其特征在于，所述服务器为验证服务器，包括：

接收单元，用于接收终端发送的二级证书，所述二级证书用于验证签名的安全计算单元的合法性；

获取单元，用于从数字证书认证服务器获取根证书；

验证单元，用于验证所述二级证书是否为所述根证书签发；

第一确定单元，若所述二级证书为所述根证书签发，则用于确定所述签名的安全计算单元为合法的；

第二确定单元，若所述二级证书不为所述根证书签发，则用于确定所述签名的安全计算单元为不合法的。

19、根据权利要求 18 所述的服务器，其特征在于，所述服务器还包括：

发送单元，用于将验证结果发送至所述终端，所述验证结果用于指示所述签名的安全计算单元是否为合法的。

20、根据权利要求 18 或 19 所述的服务器，其特征在于，所述验证单元具体用于：

判断所述二级证书的公钥和根证书的公钥是否相同；

若相同，则确定所述二级证书为所述根证书签发；

若不相同，则确定所述二级证书不为所述根证书签发。

21、一种终端，其特征在于，包括：

存储器、收发器和至少一个处理器，所述存储器中存储有程序代码，所述存储器、所述收发器和所述至少一个处理器通过线路通信，所述处理器运行所述代码以指令所述终端执行如权利要求 1-7 任一项所述的方法。

22、一种服务器，其特征在于，包括：

存储器、收发器和至少一个处理器，所述存储器中存储有程序代码，所述存储器、所述收发器和所述至少一个处理器通过线路通信，所述处理器运行所述代码以指令所述服务器执行如权利要求 8-10 任一项所述的方法。

23、一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行如权利要求 1-10 任意一项所述的方法。

24、一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行如权利要求 1-10 任意一项所述的方法。

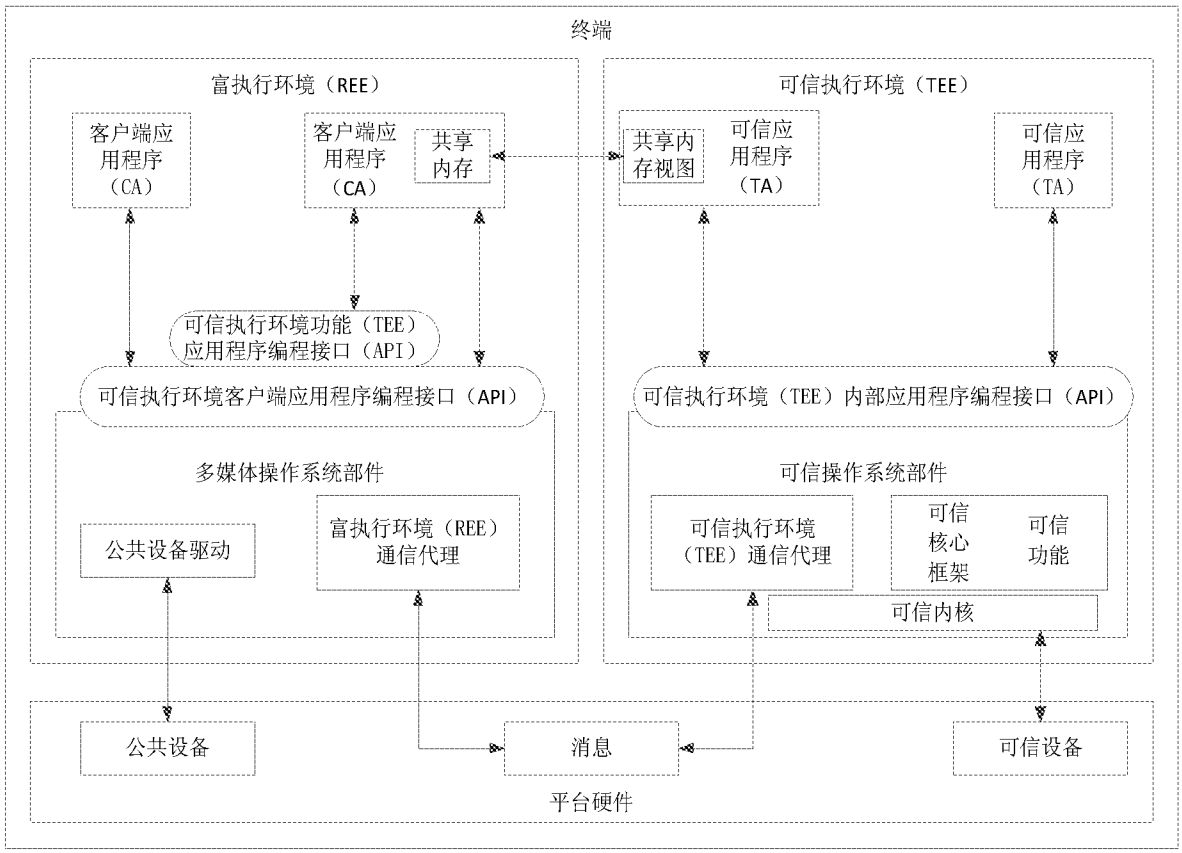
终端
富执行环境（REE）
可信执行环境（TEE）
客户端应用程序（CA）
客户端应用程序（CA）
共享内存
共享内存视图
可信应用程序（TA）
可信应用程序（TA）
可信执行环境功能（TEE）应用程序编程接口（API）
可信执行环境客户端应用程序编程接口（API）
可信执行环境（TEE）内部应用程序编程接口（API）
多媒体操作系统部件
可信操作系统部件
公共设备驱动
富执行环境（REE）通信代理
可信执行环境（TEE）通信代理
可信核心框架
可信功能
可信内核
公共设备
消息
可信设备
平台硬件

图 1

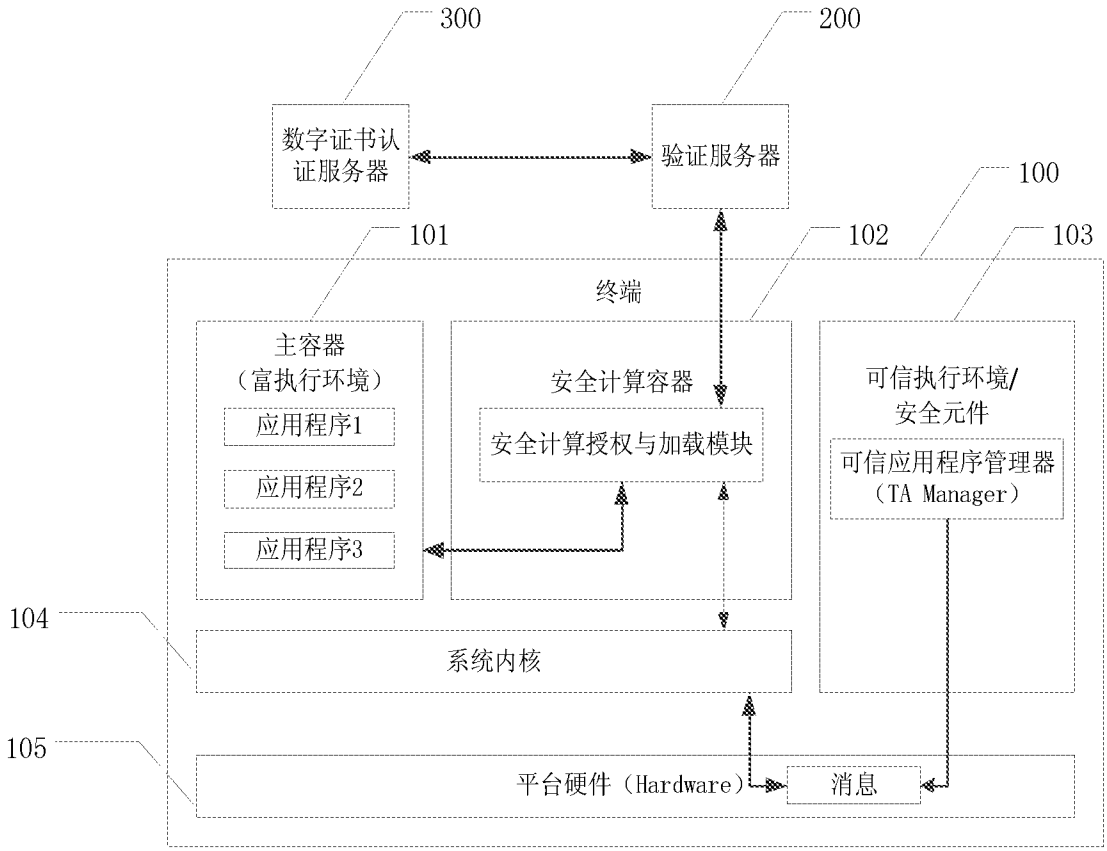
300
200
数字证书认证服务器
验证服务器
100
101
102
103
终端
主容器
（富执行环境）
应用程序1
应用程序2
应用程序3
安全计算容器
安全计算授权与加载模块
可信执行环境/
安全元件
可信应用程序管理器
（TA Manager）
104
系统内核
105
平台硬件（Hardware）
消息

图 2

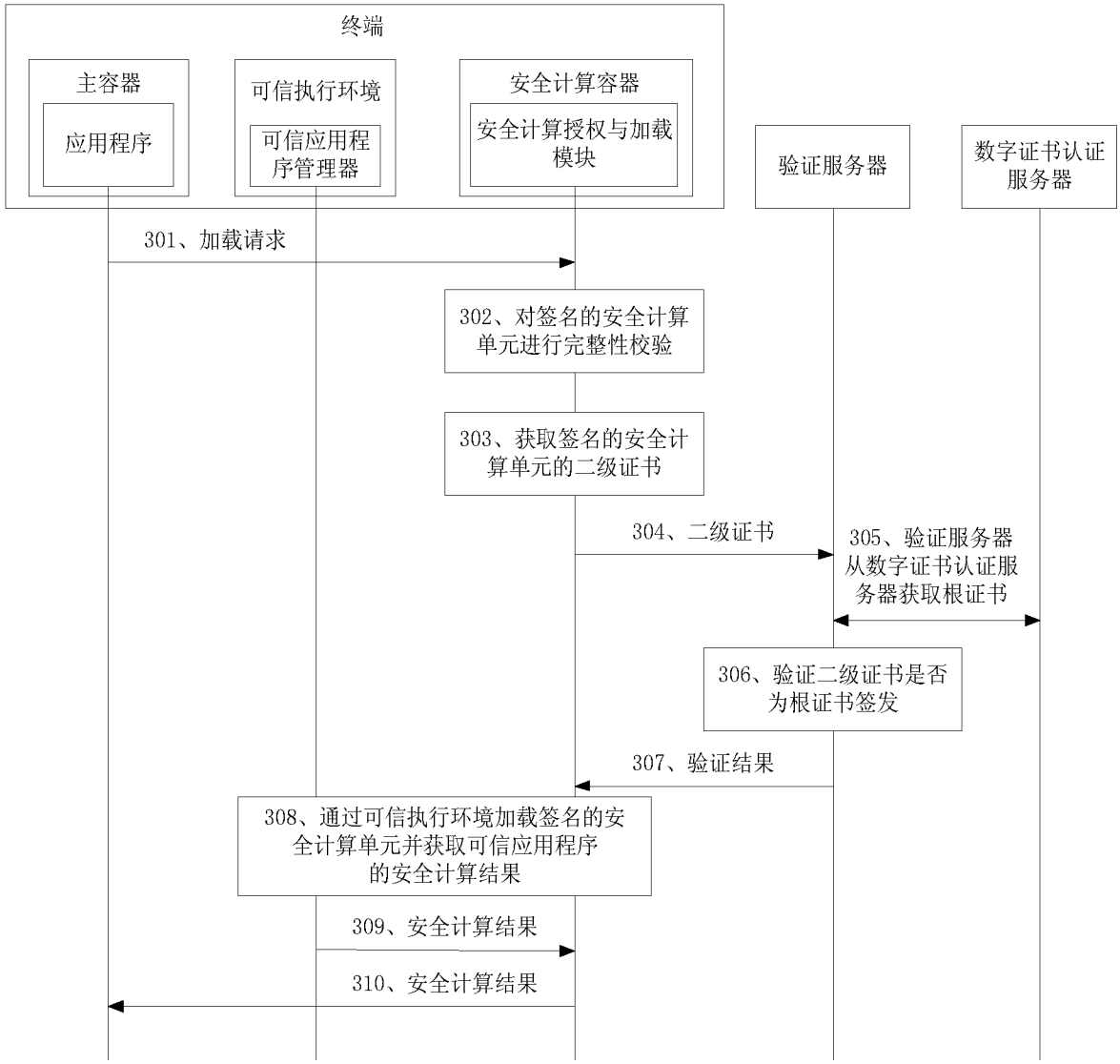
终端
主容器
应用程序
可信执行环境
可信应用程序管理器
安全计算容器
安全计算授权与加载模块
验证服务器
数字证书认证服务器
301、加载请求
302、对签名的安全计算单元进行完整性校验
303、获取签名的安全计算单元的二级证书
304、二级证书
305、验证服务器从数字证书认证服务器获取根证书
306、验证二级证书是否为根证书签发
307、验证结果
308、通过可信执行环境加载签名的安全计算单元并获取可信应用程序的安全计算结果
309、安全计算结果
310、安全计算结果

图 3

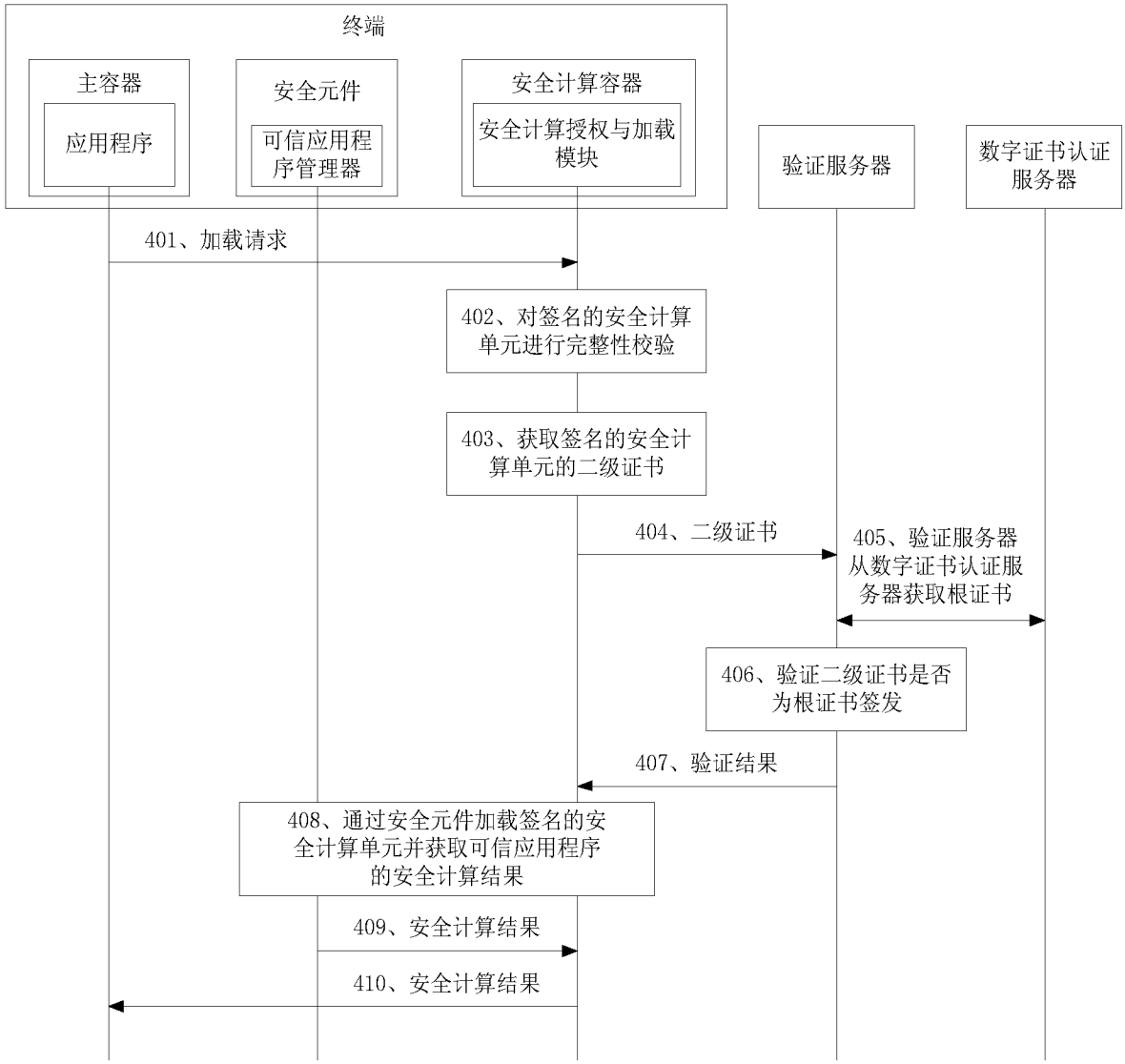
终端
主容器
应用程序
安全元件
可信应用程序管理器
安全计算容器
安全计算授权与加载模块
验证服务器
数字证书认证服务器
401、加载请求
402、对签名的安全计算单元进行完整性校验
403、获取签名的安全计算单元的二级证书
404、二级证书
405、验证服务器从数字证书认证服务器获取根证书
406、验证二级证书是否为根证书签发
407、验证结果
408、通过安全元件加载签名的安全计算单元并获取可信应用程序的安全计算结果
409、安全计算结果
410、安全计算结果

图 4

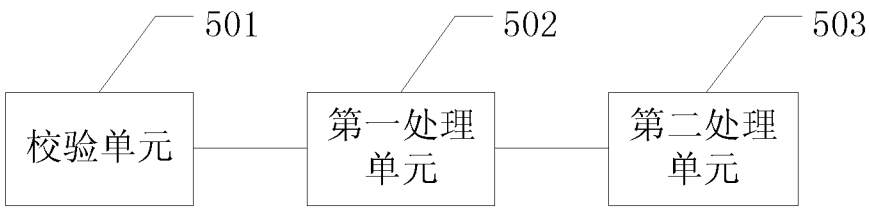
501
502
503
校验单元
第一处理单元
第二处理单元

图 5

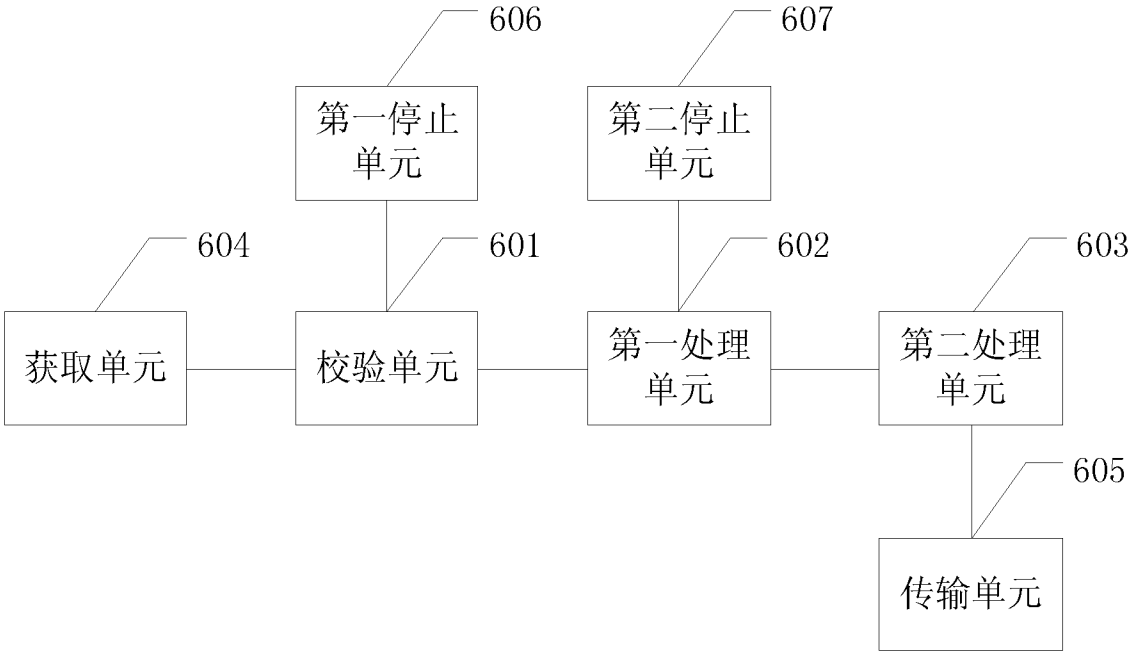
606
607
第一停止单元
第二停止单元
604
601
602
603
获取单元
校验单元
第一处理单元
第二处理单元
605
传输单元

图 6

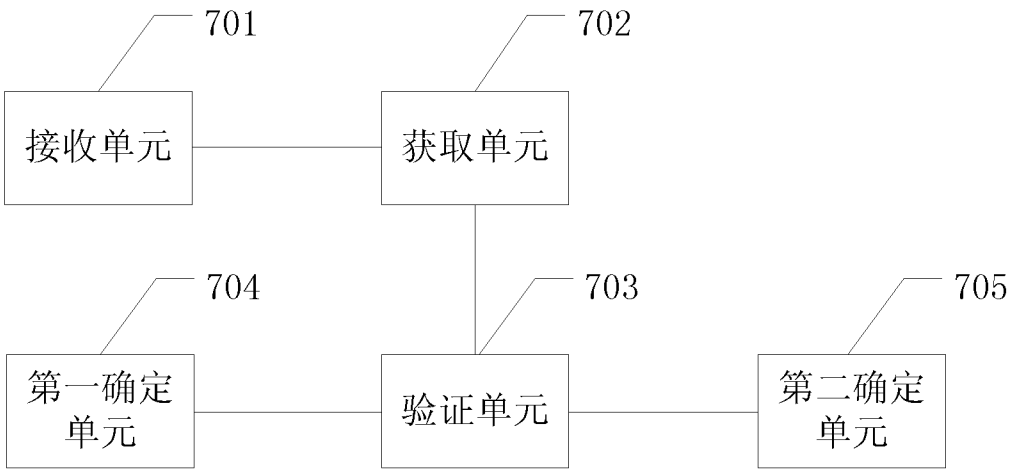
701
702
接收单元
获取单元
704
703
705
第一确定单元
验证单元
第二确定单元

图 7

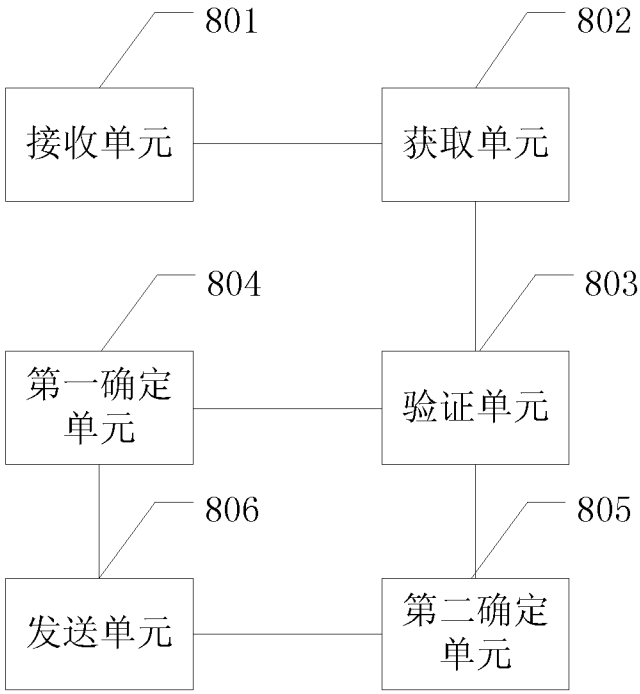
801
802
接收单元
获取单元
804
803
第一确定单元
验证单元
806
805
发送单元
第二确定单元

图 8

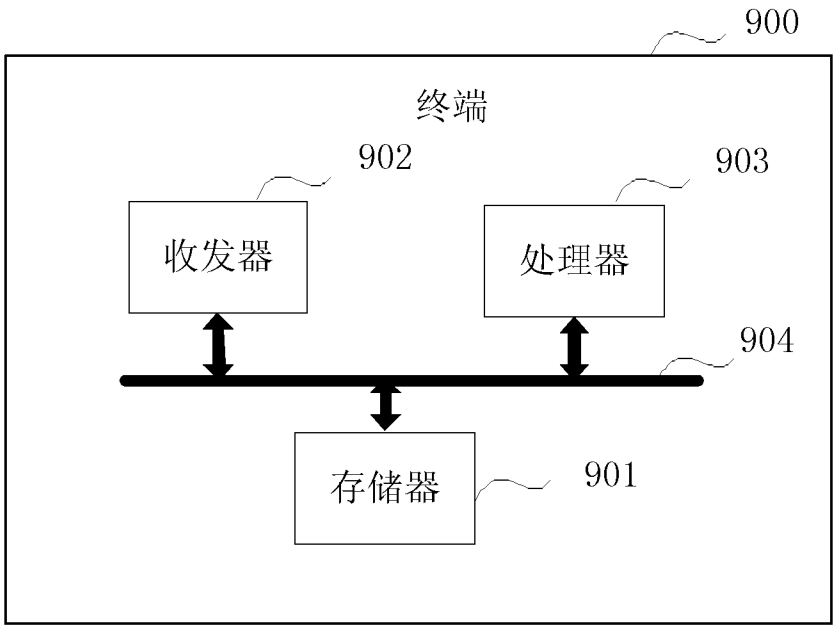
900
终端
902
903
收发器
处理器
904
存储器
901

图 9A

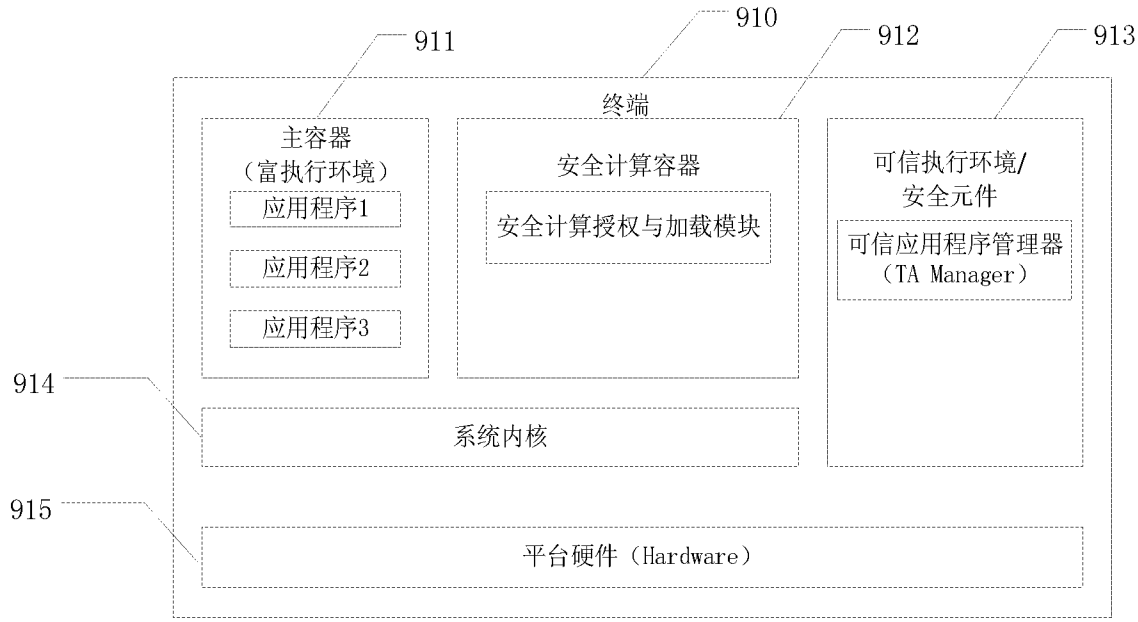
910
911
912
913
终端
主容器
（富执行环境）
应用程序1
应用程序2
应用程序3
安全计算容器
安全计算授权与加载模块
可信执行环境/
安全元件
可信应用程序管理器
（TA Manager）
914
系统内核
915
平台硬件（Hardware）

图 9B

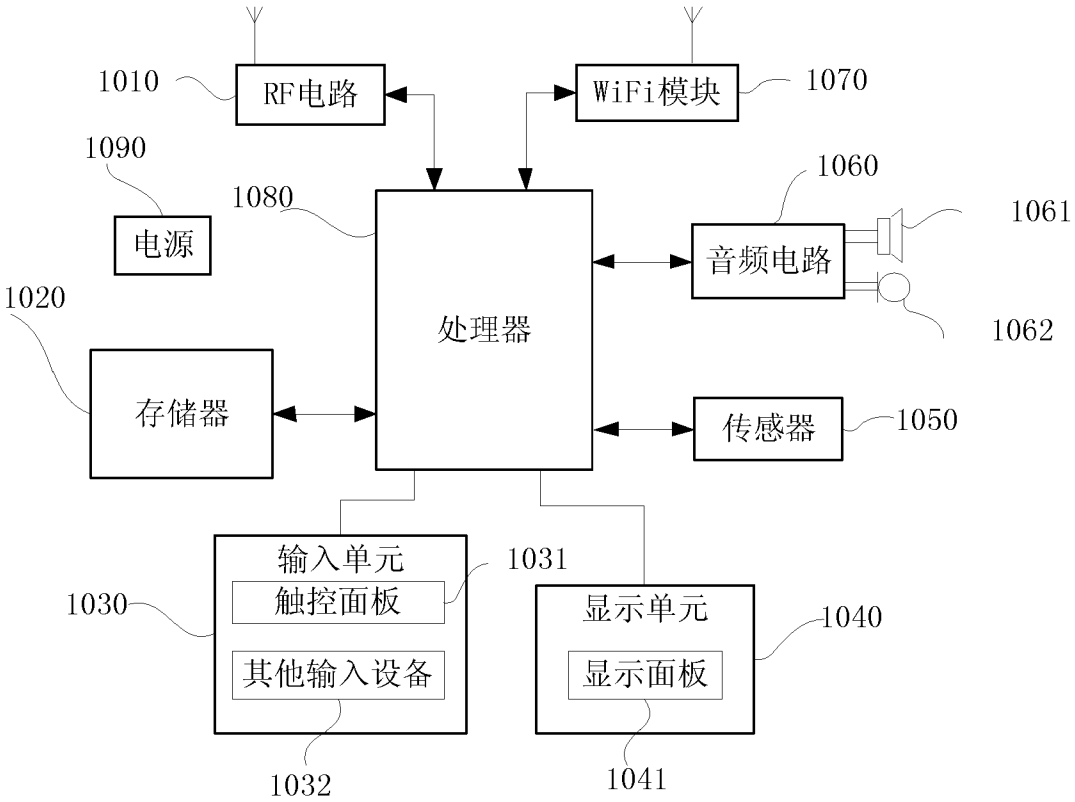
1010
RF电路
WiFi模块
1070
1090
电源
1080
处理器
1060
音频电路
1061
1062
1020
存储器
传感器
1050
输入单元
1031
触控面板
1030
其他输入设备
1032
显示单元
1040
显示面板
1041

图 10

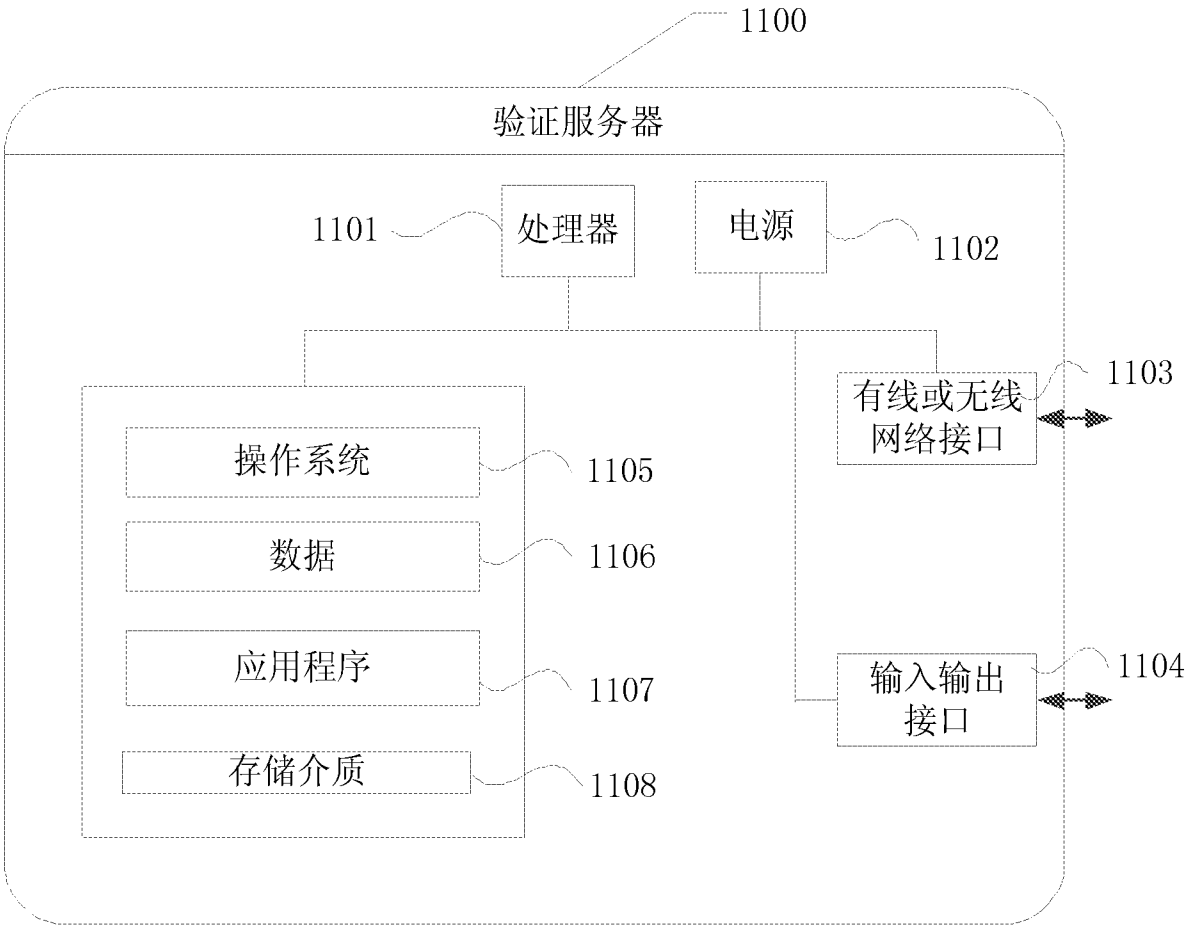
1100
验证服务器
1101
处理器
电源
1102
1103
有线或无线
网络接口
操作系统
1105
数据
1106
应用程序
1107
存储介质
1108
输入输出
接口
1104

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/088082

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/54(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, IEEE: 完整, 安全, 合法, 可信, 签名, 证书, 容器, 校验, 验证, 应用, 软件, 程序, 服务器, 摘要, 哈希值, TEE, SE, REE, integrality, safe, validity, certificate, server, signature, container, check, verification, abstract

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 107277020 A (GUOMIN CERTIFICATION TECHNOLOGY (BEIJING) CO., LTD.) 20 October 2017 (2017-10-20) description, paragraphs [0038]-[0074], and figures 1 and 2	8-10, 18-20, 22-24
A	CN 107567629 A (INTEL CORPORATION) 09 January 2018 (2018-01-09) entire document	1-24
A	CN 106815494 A (CHINA SOFT INFORMATION SYSTEMS ENGINEERING CO., LTD.) 09 June 2017 (2017-06-09) entire document	1-24
A	CN 105429760 A (SHENZHOU RONG"AN SCIENCE AND TECHNOLOGY (BEIJING) CO., LTD.) 23 March 2016 (2016-03-23) entire document	1-24
A	US 2018113817 A1 (INTEL CORPORATION) 26 April 2018 (2018-04-26) entire document	1-24

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 July 2019	**21 August 2019**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/088082

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 107277020 A	20 October 2017	None	
CN 107567629 A	09 January 2018	US 2016275290 A1	22 September 2016
		EP 3271818 A1	24 January 2018
		WO 2016148827 A1	22 September 2016
CN 106815494 A	09 June 2017	None	
CN 105429760 A	23 March 2016	CN 109150548 A	04 January 2019
US 2018113817 A1	26 April 2018	US 2016364341 A1	15 December 2016
		EP 3308317 A1	18 April 2018
		WO 2016204892 A1	22 December 2016
		CN 107667350 A	06 February 2018

国际检索报告

国际申请号
PCT/CN2019/088082

A. 主题的分类

G06F 21/54(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, WPI, EPODOC, CNKI, IEEE: 完整，安全，合法，可信，签名，证书，容器，校验，验证，应用，软件，程序，服务器，摘要，哈希值，TEE, SE, REE, integrality, safe, validity, certificate, server, signature, container, check, verification, abstract

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 107277020 A (国民认证科技北京有限公司) 2017年 10月 20日 (2017-10-20) 说明书第[0038]-[0074]段，附图1-2	8-10、18-20、22-24
A	CN 107567629 A (英特尔公司) 2018年 1月 9日 (2018-01-09) 全文	1-24
A	CN 106815494 A (中软信息系统工程有限公司) 2017年 6月 9日 (2017-06-09) 全文	1-24
A	CN 105429760 A (神州融安科技北京有限公司) 2016年 3月 23日 (2016-03-23) 全文	1-24
A	US 2018113817 A1 (INTEL CORPORATION) 2018年 4月 26日 (2018-04-26) 全文	1-24

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 7月 8日	2019年 8月 21日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	周亚楠
传真号 (86-10)62019451	电话号码 86-(10)-53961530

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/088082

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	107277020	A	2017年 10月 20日	无			
CN	107567629	A	2018年 1月 9日	US	2016275290	A1	2016年 9月 22日
				EP	3271818	A1	2018年 1月 24日
				WO	2016148827	A1	2016年 9月 22日
CN	106815494	A	2017年 6月 9日	无			
CN	105429760	A	2016年 3月 23日	CN	109150548	A	2019年 1月 4日
US	2018113817	A1	2018年 4月 26日	US	2016364341	A1	2016年 12月 15日
				EP	3308317	A1	2018年 4月 18日
				WO	2016204892	A1	2016年 12月 22日
				CN	107667350	A	2018年 2月 6日