(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
2016 年 5 月 6 日 (06.05.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/065749 A1

(51) 国际专利分类号:
G06F 21/44 (2013.01)

(21) 国际申请号: PCT/CN2015/071248

(22) 国际申请日: 2015 年 1 月 21 日 (21.01.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410602394.8 2014 年 10 月 31 日 (31.10.2014) CN

(71) 申请人: **小米科技有限责任公司 (XIAOMI INC.)** [CN/CN]; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层, Beijing 100085 (CN)。

(72) 发明人: **洪锋 (HONG, Feng)**; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。 **林俊琦 (LIN, Junqi)**; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。 **朱毅凡 (ZHU, Yifan)**; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。

(74) 代理人: **北京律智知识产权代理有限公司 (BEIJING INTELLEGAL INTELLECTUAL PROPERTY AGENT LTD.)**; 中国北京市朝阳区慧忠路 5 号远大中心 B 座 1802、1803、1805, Beijing 100101 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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))。

(54) **Title**: METHOD AND DEVICE FOR TERMINAL VERIFICATION

(54) **发明名称** : 终端验证方法及装置

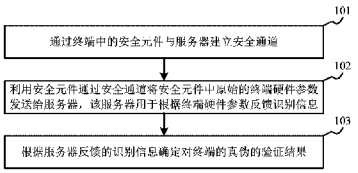

图1 /FIG. 1

101 Establishing a secure channel with a server by means of a security component in the terminal
102 Sending original terminal hardware parameters of the security component to the server through the secure channel by means of the security component, the server being used for feeding back identifying information according to the terminal hardware parameters
103 Determining authenticity verification result of the terminal according to the identifying information fed back by the server

(57) **Abstract**: A method and device for terminal verification are provided, and relate to the technical field of computer technology. The method comprises: establishing a secure channel with a server by means of a security component in the terminal (101); sending original terminal hardware parameters of the security component to the server through the secure channel by means of the security component, the server being used for feeding back identifying information according to the terminal hardware parameters (102); determining authenticity verification result of the terminal according to the identifying information fed back by the server (103). The device includes: channel establishing module (310), parameter sending module (320) and result determination module (330). The method and device solve the problem that the verification application can not identify authenticity of the terminal because of the terminal performance degradation, and achieve the effect of improving the accuracy of authenticity verification of the terminal.

(57) **摘要**: 一种终端验证方法及装置，属于计算机技术领域。所述方法包括：通过终端中的安全元件与服务器建立安全通道（101）；利用所述安全元件通过所述安全通道将所述安全元件中原始的终端硬件参数发送给所述服务器，所述服务器用于根据所述终端硬件参数反馈识别信息（102）；根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果（103）。所述装置包括：通道建立模块（310）、参数发送模块（320）和结果确定模块（330）。该方法和装置解决了终端性能下降导致验证应用程序无法识别终端的真伪的问题，达到了提高验证终端的真伪的准确性的效果。

WO 2016/065749 A1

终端验证方法及装置

本申请基于申请号为201410602394.8 、申请日为2014 年10 月31 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本公开涉及计算机技术领域，特别涉及一种终端验证方法及装置。

背景技术

随着用户更换终端的速度的提高，一些厂家会从用户废弃的终端中提取零件，将提取出的零件组装成一个终端进行销售。由于组装得到的终端的性能不稳定，因此，用户需要对购买的终端进行验证，以识别终端的真伪。

若终端中安装了验证应用程序，则终端可以运行验证应用程序，通过验证应用程序从终端的CPU（Central Processing Unit，中央处理单元）中读取终端硬件参数，该终端硬件参数包括型号、序列号、IMEI（International Mobile Equipment Identity，移动设备国际身份码）号、内存、CPU 参数和摄像头参数等；将终端硬件参数与公开的正版终端的基准硬件参数进行比较，计算终端硬件参数的评分；根据评分确定终端的真伪。

公开人在实现本公开的过程中，发现相关技术中至少存在以下缺陷：当终端由于使用时间较长导致性能下降时，终端硬件参数的评分会下降，使得验证应用程序无法识别终端的真伪。

发明内容

为解决终端性能下降导致验证应用程序无法识别终端的真伪的问题，本公开提供了一种终端验证方法及装置。

根据本公开实施例的第一方面，提供一种终端验证方法，包括：

通过终端中的安全元件与服务器建立安全通道；

利用所述安全元件通过所述安全通道将所述安全元件中原始的终端硬件参数发送给所述服务器，所述服务器用于根据所述终端硬件参数反馈识别信息；

根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果。

可选的，所述终端硬件参数是在首次启动所述终端之前写入所述安全元件的且所述终端硬件参数处于禁止编辑状态。

可选的，所述根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果，包括：

若所述识别信息是所述终端硬件参数，则将所述终端硬件参数与基准硬件参数进行比

较，根据比较结果确定对所述终端的真伪的验证结果；

若所述识别信息是所述服务器将所述终端硬件参数与基准硬件参数进行比较后生成的比较结果，则根据所述比较结果确定对所述终端的真伪的验证结果。

可选的，所述通过终端中的安全元件与服务器建立安全通道，包括：

通过所述安全元件向所述服务器发送安全通道建立请求；

通过所述安全元件接收所述服务器根据所述安全通道建立请求发送的选择命令，对所述选择命令进行响应，所述选择命令用于指示所述服务器将要与所述安全元件进行通信；

通过所述安全元件与所述服务器进行相互验证；

在相互验证通过后，通过所述安全元件建立所述安全通道。

可选的，所述通过所述安全元件与所述服务器进行相互验证，包括：

通过所述安全元件接收所述服务器发送的第一验证信息，所述第一验证信息包括初始化更新命令和第一键值；

在通过所述安全元件对所述第一键值的验证通过后，生成第二验证信息发送给所述服务器，所述第二验证信息包括卡片密文和根据所述初始化更新命令生成的第二键值；

通过所述安全元件接收所述服务器发送的外部认证命令，所述外部认证命令中携带有主机密文，所述主机密文是所述服务器对所述卡片密文和所述第二键值的验证通过后生成并发送的；

在通过所述安全元件对所述主机密文的验证通过后，确定与所述服务器之间的相互验证通过。

根据本公开实施例的第二方面，提供一种终端验证装置，包括：

通道建立模块，被配置为通过终端中的安全元件与服务器建立安全通道；

参数发送模块，被配置为利用所述安全元件通过所述通道建立模块建立的所述安全通道将所述安全元件中原始的终端硬件参数发送给所述服务器，所述服务器用于根据所述终端硬件参数反馈识别信息；

结果确定模块，被配置为根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果。

可选的，所述终端硬件参数是在首次启动所述终端之前写入所述安全元件的且所述终端硬件参数处于禁止编辑状态。

可选的，所述结果确定模块，包括：

第一确定子模块，被配置为在所述识别信息是所述终端硬件参数时，将所述终端硬件参数与基准硬件参数进行比较，根据比较结果确定对所述终端的真伪的验证结果；

第二确定子模块，被配置为在所述识别信息是所述服务器将所述终端硬件参数与基准硬件参数进行比较后生成的比较结果时，根据所述比较结果确定对所述终端的真伪的验证结果。

可选的，所述通道建立模块，包括：

请求发送子模块，被配置为通过所述安全元件向所述服务器发送安全通道建立请求；

命令响应子模块，被配置为通过所述安全元件接收所述服务器根据所述请求发送子模块发送的所述安全通道建立请求发送的选择命令，对所述选择命令进行响应，所述选择命令用于指示所述服务器将要与所述安全元件进行通信；

信息验证子模块，被配置为通过所述安全元件与所述服务器进行相互验证；

通道建立子模块，被配置为在所述信息验证子模块确定相互验证通过后，通过所述安全元件建立所述安全通道。

可选的，所述信息验证子模块，包括：

信息接收子模块，被配置为通过所述安全元件接收所述服务器发送的第一验证信息，所述第一验证信息包括初始化更新命令和第一键值；

信息发送子模块，被配置为在通过所述安全元件对所述信息接收子模块接收到的所述第一键值的验证通过后，生成第二验证信息发送给所述服务器，所述第二验证信息包括卡片密文和根据所述初始化更新命令生成的第二键值；

命令接收子模块，被配置为通过所述安全元件接收所述服务器发送的外部认证命令，所述外部认证命令中携带有主机密文，所述主机密文是所述服务器对所述信息发送子模块发送的所述卡片密文和所述第二键值的验证通过后生成并发送的；

验证确定子模块，被配置为在通过所述安全元件对所述命令接收子模块接收到的所述主机密文的验证通过后，确定与所述服务器之间的相互验证通过。

根据本公开实施例的第三方面，提供一种终端验证装置，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

通过终端中的安全元件与服务器建立安全通道；

利用所述安全元件通过所述安全通道将所述安全元件中原始的终端硬件参数发送给所述服务器，所述服务器用于根据所述终端硬件参数反馈识别信息；

根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果。

本公开的实施例提供的技术方案可以包括以下有益效果：

通过终端中的安全元件与服务器建立安全通道；利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，服务器用于根据终端硬件参数反馈识别信息；根据服务器反馈的识别信息确定对终端的真伪的验证结果，由于终端硬件参数是初始写入安全元件的参数，不会随着终端性能的下降而变化，保证了终端硬件参数的准确性，解决了终端性能下降导致验证应用程序无法识别终端的真伪的问题，达到了提高验证终端的真伪的准确性的效果。并且，可以直接读取硬件参数来识别终端的真伪，而不需要计算终端硬件参数的评分，简化了识别终端的真伪的操作，提高了对终端的验证效率。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性的，并不能限制本公开。

附图说明

此处的附图被并入说明书中并构成本公开说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

图 1 是根据一示例性实施例示出的一种终端验证方法的流程图。

图 2 是根据另一示例性实施例示出的一种终端验证方法的流程图。

图 3 是根据一示例性实施例示出的一种终端验证装置的框图。

图 4 是根据一示例性实施例示出的一种终端验证装置的框图。

图 5 是根据一示例性实施例示出的一种用于终端验证的装置的框图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

图 1 是根据一示例性实施例示出的一种终端验证方法的流程图，该终端验证方法应用于终端中，如图 1 所示，该终端验证方法包括以下步骤。

在步骤 101 中，通过终端中的安全元件与服务器建立安全通道。

安全元件（Secure Element）是安装在终端中的元件。由于终端没有读取安全元件中的数据的权限，因此，终端可以通过服务器与安全元件建立安全通道，再通过服务器获取安全元件中的数据。其中，安全通道是安全元件与服务器之间建立的通道，供安全元件与服务器之间进行数据通信。

在步骤 102 中，利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，该服务器用于根据终端硬件参数反馈识别信息。

终端硬件参数是指终端的硬件参数，用于识别终端的真伪。

本实施例中，可以预先将终端硬件参数存储在安全元件中，在安全元件与服务器之间建立了安全通道后，安全元件通过安全通道将终端硬件参数发送给服务器。由于服务器获取的终端硬件参数是原始存储在安全元件中的，而不是对终端的性能进行实时检测获取到的，因此，终端硬件参数不会随着终端性能的下降而变化，保证了终端硬件参数的准确性。

在步骤 103 中，根据服务器反馈的识别信息确定对终端的真伪的验证结果。

终端可以直接根据识别信息对终端的真伪进行识别，而不是对终端硬件参数进行评分，可以简化识别终端的真伪的操作，从而提高了对终端的验证效率。

综上所述，本公开提供的终端验证方法，通过终端中的安全元件与服务器建立安全通道；利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，服务器

用于根据终端硬件参数反馈识别信息；根据服务器反馈的识别信息确定对终端的真伪的验证结果，由于终端硬件参数是初始写入安全元件的参数，不会随着终端性能的下降而变化，保证了终端硬件参数的准确性，解决了终端性能下降导致验证应用程序无法识别终端的真伪的问题，达到了提高验证终端的真伪的准确性的效果。并且，可以直接读取硬件参数来识别终端的真伪，而不需要计算终端硬件参数的评分，简化了识别终端的真伪的操作，提高了对终端的验证效率。

图 2 是根据另一示例性实施例示出的一种终端验证方法的流程图，该终端验证方法应用于终端中，如图 2 所示，该终端验证方法包括如下步骤。

在步骤 201 中，通过终端中的安全元件与服务器建立安全通道。

安全元件是安装在终端中的元件。其中，安全元件可以内置于终端的芯片中，也可以内置于配件中，通过配件安装在终端中。比如，安全元件可以内置于 SIM（Subscriber Identity Module，客户识别模块）卡中，或，安全元件可以内置于 Micro SD（Micro Secure Digital Memory Card，微型安全数码卡）中。当然，安全元件还可以内置于其它配件中，本实施例不对包含安全元件的配件作限定。

由于终端没有读取安全元件中的数据的权限，因此，终端可以通过服务器与安全元件建立安全通道，再通过服务器获取安全元件中的数据。其中，安全通道是安全元件与服务器之间建立的通道，供安全元件与服务器之间进行数据通信。

其中，通过终端中的安全元件与服务器建立安全通道，包括：

1）通过安全元件向服务器发送安全通道建立请求；

2）通过安全元件接收服务器根据安全通道建立请求发送的选择命令，对选择命令进行响应，选择命令用于指示服务器将要与安全元件进行通信；

3）通过安全元件与服务器进行相互验证；

4）在相互验证通过后，通过安全元件建立安全通道。

若用户需要验证终端的真伪，可以启动终端中安装的预定应用程序，终端通过该预定应用程序向安全元件发送安全通道建立命令，安全元件在安全通道建立命令的指示下，触发安全通道的建立过程。

在建立安全通道时，安全元件可以获取自身的安全元件标识，将安全元件标识携带在安全通道建立请求中发送给服务器，该安全通道建立请求用于指示安全元件请求建立安全通道。服务器从接收到安全通道建立请求中读取安全元件标识，将安全元件标识添加到选择命令（SELECT 命令）中发送给安全元件标识，该选择命令用于指示服务器将要与安全元件进行通信。安全元件标识在接收到选择命令后，确定服务器将要与自身进行通信，向服务器发送准备完毕的响应。服务器在接收到响应后，触发与安全元件之间的相互验证过程，在相互验证通过后，安全元件与服务器之间建立安全通道。其中，相互验证用于保证安全元件与服务器的安全性。

可选的，通过安全元件与服务器进行相互验证，包括：

1）通过安全元件接收服务器发送的第一验证信息，第一验证信息包括初始化更新命令和第一键值；

2）在通过安全元件对第一键值的验证通过后，生成第二验证信息发送给服务器，第二验证信息包括卡片密文和根据初始化更新命令生成的第二键值；

3）通过安全元件接收服务器发送的外部认证命令，外部认证命令中携带有主机密文，主机密文是服务器对卡片密文和第二键值的验证通过后生成并发送的；

4）在通过安全元件对主机密文的验证通过后，确定与服务器之间的相互验证通过。

在相互验证过程中，服务器在接收到响应后，生成第一随机数添加到初始化更新命令中，再根据时间戳、生成的第二随机数和固定字符串生成第一键值，将初始化更新命令和第一键值添加到第一验证信息中发送给安全元件。其中，第一键值可以是 host challenge key。

安全元件在接收到第一验证信息后，对第一键值进行验证，在对第一键值的验证通过后，根据初始化更新命令中的第一随机数生成卡片密文（card 密文），再根据时间戳、生成的卡片随机数和固定字符串生成第二键值，将卡片密文和第二键值添加到第二验证信息中发送给服务器。其中，第二键值可以是 card challenge key。

服务器在接收到第二验证信息后，对第二键值和卡片密文进行验证，在对第二键值和卡片密文的验证都通过后，生成主机密文（host 密文），将主机密文添加到外部认证命令中发送给安全元件。

安全元件从外部认证命令中读取主机密文，对主机密文进行验证，在对主机密文的验证通过后，确定与服务器之间的相互验证通过。

需要说明的是，安全元件需要通过密钥对第一验证信息进行验证、生成第二验证信息以及对主机密文进行验证，该密钥可以是一个，也可以是多个，其是在首次启动终端之前设置的，无法被修改，因此，可以保证相互验证的准确性。

在步骤 202 中，利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，该服务器用于根据终端硬件参数反馈识别信息。

终端硬件参数是指终端的硬件参数，用于识别终端的真伪。其中，可以预先将终端硬件参数存储在安全元件中，在安全元件与服务器之间建立了安全通道后，安全元件通过安全通道将终端硬件参数发送给服务器。由于服务器获取的终端硬件参数是原始存储在安全元件中的，而不是对终端的性能进行实时检测获取到的，因此，终端硬件参数不会随着终端性能的下降而变化，保证了终端硬件参数的准确性。

本实施例中，终端硬件参数是在首次启动终端之前写入安全元件的且终端硬件参数处于禁止编辑状态。

在实际实现时，终端硬件参数可以是厂家在终端出厂时设置的，且同一批次终端的终端硬件参数相同。由于安全元件中的终端硬件参数是在首次启动终端之前写入的且处于禁

止编辑状态，因此，在用户启动终端后，终端无法对安全元件中的终端硬件参数进行修改，避免了终端恶意修改安全元件中的终端硬件参数，从而无法识别终端的真伪的问题，达到了提高验证终端的准确性的效果。

在步骤 203 中，若识别信息是终端硬件参数，则将终端硬件参数与基准硬件参数进行比较，根据比较结果确定对终端的真伪的验证结果；若识别信息是服务器将终端硬件参数与基准硬件参数进行比较后生成的比较结果，则根据比较结果确定对终端的真伪的验证结果。

服务器接收到终端硬件参数后，可以根据终端硬件参数生成识别信息，将识别信息发送给安全元件，安全元件再根据识别信息验证终端的真伪。本实施例中，根据服务器反馈的识别信息确定对终端的真伪的验证结果，包括：

1）若识别信息是终端硬件参数，则将终端硬件参数与基准硬件参数进行比较，根据比较结果确定对终端的真伪的验证结果；

2）若识别信息是服务器将终端硬件参数与基准硬件参数进行比较后生成的比较结果，则根据比较结果确定对终端的真伪的验证结果。

当服务器中未存储正版终端的基准硬件参数且终端中存储有该基准硬件参数时，服务器可以将接收到的终端硬件参数作为识别信息发送给终端，终端将终端硬件参数与基准硬件参数进行比较，将比较结果作为验证结果。

当服务器中存储有正版终端的基准硬件参数时，服务器可以将接收到的终端硬件参数与基准硬件参数进行比较，将比较结果发送给终端，终端将比较结果作为验证结果。通常，服务器的处理能力比终端的处理能力强，因此，通过服务器比较终端硬件参数和基准硬件参数的速度较快，可以提高对终端的验证效率。

假设终端硬件参数包括型号、序列号、IMEI 号和内存，则可以将终端硬件参数中的型号、序列号、IMEI 号、内存分别与基准硬件参数中的型号、序列号、IMEI 号、内存进行比较，若终端硬件参数中的型号、序列号、IMEI 号、内存分别与基准硬件参数中的型号、序列号、IMEI 号、内存相同，则得到终端硬件参数与基准硬件参数相同的比较结果，再根据该比较结果确定终端是正版终端。

本实施例中，终端可以直接根据识别信息对终端的真伪进行识别，而不是对终端硬件参数进行评分，可以简化识别终端的真伪的操作，从而提高了对终端的验证效率。

需要说明的是，安全元件是终端中已经安装的元件，终端可以直接根据已有的安全元件对终端进行验证，而不需要在终端中安装验证应用程序或额外的元件，可以节省对终端的验证成本。

综上所述，本公开提供的终端验证方法，通过终端中的安全元件与服务器建立安全通道；利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，服务器用于根据终端硬件参数反馈识别信息；根据服务器反馈的识别信息确定对终端的真伪的验证结果，由于终端硬件参数是初始写入安全元件的参数，不会随着终端性能的下降而变化，

保证了终端硬件参数的准确性，解决了终端性能下降导致验证应用程序无法识别终端的真伪的问题，达到了提高验证终端的真伪的准确性的效果。并且，可以直接读取硬件参数来识别终端的真伪，而不需要计算终端硬件参数的评分，简化了识别终端的真伪的操作，提高了对终端的验证效率。

另外，终端硬件参数是在首次启动终端之前写入安全元件的且终端硬件参数处于禁止编辑状态，使得终端启动后，无法对安全元件中的终端硬件参数进行修改，解决了终端的 CPU 中存储的终端硬件参数会被恶意修改，导致验证应用程序无法识别终端的真伪的问题，达到了提高验证终端的真伪的准确性的效果。

图 3 是根据一示例性实施例示出的一种终端验证装置的框图，该终端验证装置应用于终端中，如图 3 所示，该终端验证装置包括：通道建立模块 310、参数发送模块 320 和结果确定模块 330。

该通道建立模块 310，被配置为通过终端中的安全元件与服务器建立安全通道；

该参数发送模块 320，被配置为利用安全元件通过通道建立模块 310 建立的安全通道将安全元件中原始的终端硬件参数发送给服务器，服务器用于根据终端硬件参数反馈识别信息；

该结果确定模块 330，被配置为根据服务器反馈的识别信息确定对终端的真伪的验证结果。

综上所述，本公开提供的终端验证装置，通过终端中的安全元件与服务器建立安全通道；利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，服务器用于根据终端硬件参数反馈识别信息；根据服务器反馈的识别信息确定对终端的真伪的验证结果，由于终端硬件参数是初始写入安全元件的参数，不会随着终端性能的下降而变化，保证了终端硬件参数的准确性，解决了终端性能下降导致验证应用程序无法识别终端的真伪的问题，达到了提高验证终端的真伪的准确性的效果。并且，可以直接读取硬件参数来识别终端的真伪，而不需要计算终端硬件参数的评分，简化了识别终端的真伪的操作，提高了对终端的验证效率。

图 4 是根据一示例性实施例示出的一种终端验证装置的框图，该终端验证装置应用于终端中，如图 4 所示，该终端验证装置包括：通道建立模块 410、参数发送模块 420 和结果确定模块 430。

该通道建立模块 410，被配置为通过终端中的安全元件与服务器建立安全通道；

该参数发送模块 420，被配置为利用安全元件通过通道建立模块 410 建立的安全通道将安全元件中原始的终端硬件参数发送给服务器，服务器用于根据终端硬件参数反馈识别信息；

该结果确定模块 430，被配置为根据服务器反馈的识别信息确定对终端的真伪的验证

结果。

可选的，终端硬件参数是在首次启动终端之前写入安全元件的且终端硬件参数处于禁止编辑状态。

可选的，结果确定模块 430，包括：第一确定子模块 431 或第二确定子模块 432；

该第一确定子模块 431，被配置为在识别信息是终端硬件参数时，将终端硬件参数与基准硬件参数进行比较，根据比较结果确定对终端的真伪的验证结果；

该第二确定子模块 432，被配置为在识别信息是服务器将终端硬件参数与基准硬件参数进行比较后生成的比较结果时，根据比较结果确定对终端的真伪的验证结果。

可选的，通道建立模块 410，包括：请求发送子模块 411、命令响应子模块 412、信息验证子模块 413 和通道建立子模块 414；

该请求发送子模块 411，被配置为通过安全元件向服务器发送安全通道建立请求；

该命令响应子模块 412，被配置为通过安全元件接收服务器根据请求发送子模块 411 发送的安全通道建立请求发送的选择命令，对选择命令进行响应，选择命令用于指示服务器将要与安全元件进行通信；

该信息验证子模块 413，被配置为通过安全元件与服务器进行相互验证；

该通道建立子模块 414，被配置为在信息验证子模块 413 确定相互验证通过后，通过安全元件建立安全通道。

可选的，信息验证子模块 413，包括：信息接收子模块 4131、信息发送子模块 4132、命令接收子模块 4133 和验证确定子模块 4134；

该信息接收子模块 4131，被配置为通过安全元件接收服务器发送的第一验证信息，第一验证信息包括初始化更新命令和第一键值；

该信息发送子模块 4132，被配置为在通过安全元件对信息接收子模块 4131 接收到的第一键值的验证通过后，生成第二验证信息发送给服务器，第二验证信息包括卡片密文和根据初始化更新命令生成的第二键值；

该命令接收子模块 4133，被配置为通过安全元件接收服务器发送的外部认证命令，外部认证命令中携带有主机密文，主机密文是服务器对信息发送子模块 4132 发送的卡片密文和第二键值的验证通过后生成并发送的；

该验证确定子模块 4134，被配置为在通过安全元件对命令接收子模块 4133 接收到的主机密文的验证通过后，确定与服务器之间的相互验证通过。

综上所述，本公开提供的终端验证装置，通过终端中的安全元件与服务器建立安全通道；利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，服务器用于根据终端硬件参数反馈识别信息；根据服务器反馈的识别信息确定对终端的真伪的验证结果，由于终端硬件参数是初始写入安全元件的参数，不会随着终端性能的下降而变化，保证了终端硬件参数的准确性，解决了终端性能下降导致验证应用程序无法识别终端的真伪的问题，达到了提高验证终端的真伪的准确性的效果。并且，可以直接读取硬件参数来

识别终端的真伪，而不需要计算终端硬件参数的评分，简化了识别终端的真伪的操作，提高了对终端的验证效率。

另外，终端硬件参数是在首次启动终端之前写入安全元件的且终端硬件参数处于禁止编辑状态，使得终端启动后，无法对安全元件中的终端硬件参数进行修改，解决了终端的CPU 中存储的终端硬件参数会被恶意修改，导致验证应用程序无法识别终端的真伪的问题，达到了提高验证终端的真伪的准确性的效果。

关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

图 5 是根据一示例性实施例示出的一种用于终端验证装置 500 的框图。例如，装置 500 可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

参照图 5，装置 500 可以包括以下一个或多个组件：处理组件 502，存储器 504，电源组件 506，多媒体组件 508，音频组件 510，输入/输出（I/ O）的接口 512，传感器组件 514，以及通信组件 516。

处理组件 502 通常控制装置 500 的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理组件 502 可以包括一个或多个处理器 518 来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件 502 可以包括一个或多个模块，便于处理组件 502 和其他组件之间的交互。例如，处理组件 502 可以包括多媒体模块，以方便多媒体组件 508 和处理组件 502 之间的交互。

存储器 504 被配置为存储各种类型的数据以支持在装置 500 的操作。这些数据的示例包括用于在装置 500 上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器 504 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁存储器，快闪存储器，磁盘或光盘。

电源组件 506 为装置 500 的各种组件提供电力。电源组件 506 可以包括电源管理系统，一个或多个电源，及其他与为装置 500 生成、管理和分配电力相关联的组件。

多媒体组件 508 包括在所述装置 500 和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器（LCD）和触摸面板（TP）。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件 508 包括一个前置摄像头和/或后置摄像头。当装置 500 处于操作模式，如拍摄模式或视频模式时，前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前

置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

音频组件 510 被配置为输出和/或输入音频信号。例如，音频组件 510 包括一个麦克风（MIC），当装置 500 处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 504 或经由通信组件 516 发送。在一些实施例中，音频组件 510 还包括一个扬声器，用于输出音频信号。

I/ O 接口 512 为处理组件 502 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

传感器组件 514 包括一个或多个传感器，用于为装置 500 提供各个方面的状态评估。例如，传感器组件 514 可以检测到装置 500 的打开/关闭状态，组件的相对定位，例如所述组件为装置 500 的显示器和小键盘，传感器组件 514 还可以检测装置 500 或装置 500 一个组件的位置改变，用户与装置 500 接触的存在或不存在，装置 500 方位或加速/减速和装置 500 的温度变化。传感器组件 514 可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 514 还可以包括光传感器，如 CMOS 或 CCD 图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件 514 还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

通信组件 516 被配置为便于装置 500 和其他设备之间有线或无线方式的通信。装置 500 可以接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信组件 516 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件 516 还包括近场通信（NFC）模块，以促进短程通信。例如，在 NFC 模块可基于射频识别（RFID）技术，红外数据协会（IrDA）技术，超宽带（UWB）技术，蓝牙（BT）技术和其他技术来实现。

在示例性实施例中，装置 500 可以被一个或多个应用专用集成电路（ASIC）、数字信号处理器（DSP）、数字信号处理设备（DSPD）、可编程逻辑器件（PLD）、现场可编程门阵列（FPGA）、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。

在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器 504，上述指令可由装置 500 的处理器 518 执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器（RAM）、CD-ROM、磁带、软盘和光数据存储设备等。

本领域技术人员在考虑说明书及实践这里的公开的后，将容易想到本的其它实施方案。本申请旨在涵盖本的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。

说明书和实施例仅被视为示例性的，本的真正范围和精神由下面的权利要求指出。

应当理解的是，本并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本的范围仅由所附的权利要求来限制。

权利要求

1、一种终端验证方法，其特征在于，包括：

通过终端中的安全元件与服务器建立安全通道；

利用所述安全元件通过所述安全通道将所述安全元件中原始的终端硬件参数发送给所述服务器，所述服务器用于根据所述终端硬件参数反馈识别信息；

根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果。

2、根据权利要求 1 所述的方法，其特征在于，所述终端硬件参数是在首次启动所述终端之前写入所述安全元件的且所述终端硬件参数处于禁止编辑状态。

3、根据权利要求 1 所述的方法，其特征在于，所述根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果，包括：

若所述识别信息是所述终端硬件参数，则将所述终端硬件参数与基准硬件参数进行比较，根据比较结果确定对所述终端的真伪的验证结果；

若所述识别信息是所述服务器将所述终端硬件参数与基准硬件参数进行比较后生成的比较结果，则根据所述比较结果确定对所述终端的真伪的验证结果。

4、根据权利要求 1 至 3 任一项所述的方法，其特征在于，所述通过终端中的安全元件与服务器建立安全通道，包括：

通过所述安全元件向所述服务器发送安全通道建立请求；

通过所述安全元件接收所述服务器根据所述安全通道建立请求发送的选择命令，对所述选择命令进行响应，所述选择命令用于指示所述服务器将要与所述安全元件进行通信；

通过所述安全元件与所述服务器进行相互验证；

在相互验证通过后，通过所述安全元件建立所述安全通道。

5、根据权利要求 4 所述的方法，其特征在于，所述通过所述安全元件与所述服务器进行相互验证，包括：

通过所述安全元件接收所述服务器发送的第一验证信息，所述第一验证信息包括初始化更新命令和第一键值；

在通过所述安全元件对所述第一键值的验证通过后，生成第二验证信息发送给所述服务器，所述第二验证信息包括卡片密文和根据所述初始化更新命令生成的第二键值；

通过所述安全元件接收所述服务器发送的外部认证命令，所述外部认证命令中携带有主机密文，所述主机密文是所述服务器对所述卡片密文和所述第二键值的验证通过后生成并发送的；

在通过所述安全元件对所述主机密文的验证通过后，确定与所述服务器之间的相互验

证通过。

6、一种终端验证装置，其特征在于，包括：

通道建立模块，被配置为通过终端中的安全元件与服务器建立安全通道；

参数发送模块，被配置为利用所述安全元件通过所述通道建立模块建立的所述安全通道将所述安全元件中原始的终端硬件参数发送给所述服务器，所述服务器用于根据所述终端硬件参数反馈识别信息；

结果确定模块，被配置为根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果。

7、根据权利要求 6 所述的装置，其特征在于，所述终端硬件参数是在首次启动所述终端之前写入所述安全元件的且所述终端硬件参数处于禁止编辑状态。

8、根据权利要求 6 所述的装置，其特征在于，所述结果确定模块，包括：

第一确定子模块，被配置为在所述识别信息是所述终端硬件参数时，将所述终端硬件参数与基准硬件参数进行比较，根据比较结果确定对所述终端的真伪的验证结果；

第二确定子模块，被配置为在所述识别信息是所述服务器将所述终端硬件参数与基准硬件参数进行比较后生成的比较结果时，根据所述比较结果确定对所述终端的真伪的验证结果。

9、根据权利要求 6 至 8 任一项所述的装置，其特征在于，所述通道建立模块，包括：

请求发送子模块，被配置为通过所述安全元件向所述服务器发送安全通道建立请求；

命令响应子模块，被配置为通过所述安全元件接收所述服务器根据所述请求发送子模块发送的所述安全通道建立请求发送的选择命令，对所述选择命令进行响应，所述选择命令用于指示所述服务器将要与所述安全元件进行通信；

信息验证子模块，被配置为通过所述安全元件与所述服务器进行相互验证；

通道建立子模块，被配置为在所述信息验证子模块确定相互验证通过后，通过所述安全元件建立所述安全通道。

10、根据权利要求 9 所述的装置，其特征在于，所述信息验证子模块，包括：

信息接收子模块，被配置为通过所述安全元件接收所述服务器发送的第一验证信息，所述第一验证信息包括初始化更新命令和第一键值；

信息发送子模块，被配置为在通过所述安全元件对所述信息接收子模块接收到的所述第一键值的验证通过后，生成第二验证信息发送给所述服务器，所述第二验证信息包括卡片密文和根据所述初始化更新命令生成的第二键值；

命令接收子模块，被配置为通过所述安全元件接收所述服务器发送的外部认证命令，所述外部认证命令中携带有主机密文，所述主机密文是所述服务器对所述信息发送子模块发送的所述卡片密文和所述第二键值的验证通过后生成并发送的；

验证确定子模块，被配置为在通过所述安全元件对所述命令接收子模块接收到的所述主机密文的验证通过后，确定与所述服务器之间的相互验证通过。

11、一种终端验证装置，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

通过终端中的安全元件与服务器建立安全通道；

利用所述安全元件通过所述安全通道将所述安全元件中原始的终端硬件参数发送给所述服务器，所述服务器用于根据所述终端硬件参数反馈识别信息；

根据所述服务器反馈的所述识别信息确定对所述终端的真伪的验证结果。

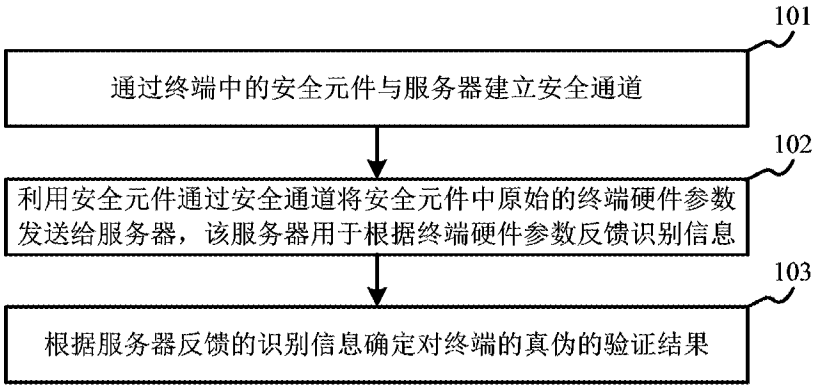
101
通过终端中的安全元件与服务器建立安全通道
102
利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，该服务器用于根据终端硬件参数反馈识别信息
103
根据服务器反馈的识别信息确定对终端的真伪的验证结果

图1

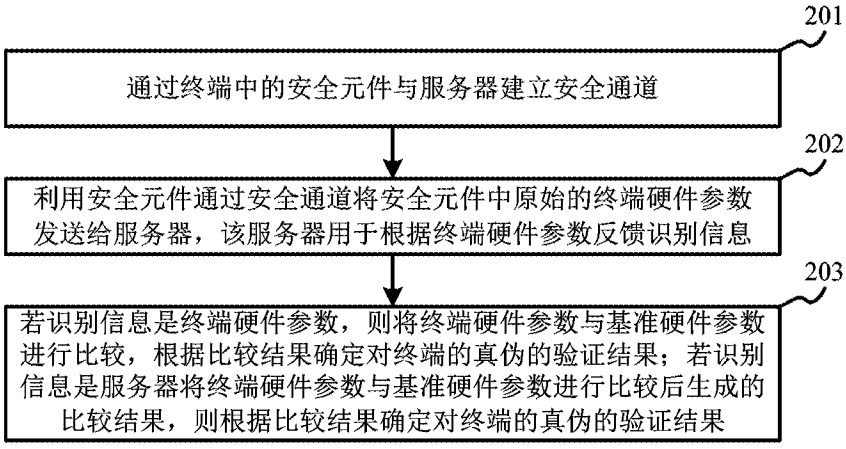
201
通过终端中的安全元件与服务器建立安全通道
202
利用安全元件通过安全通道将安全元件中原始的终端硬件参数发送给服务器，该服务器用于根据终端硬件参数反馈识别信息
203
若识别信息是终端硬件参数，则将终端硬件参数与基准硬件参数进行比较，根据比较结果确定对终端的真伪的验证结果；若识别信息是服务器将终端硬件参数与基准硬件参数进行比较后生成的比较结果，则根据比较结果确定对终端的真伪的验证结果

图2

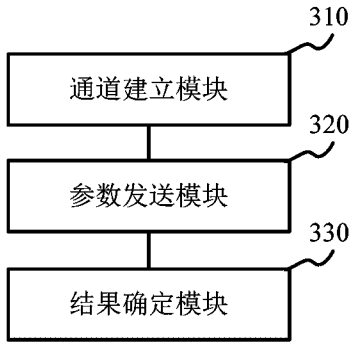
310
通道建立模块
320
参数发送模块
330
结果确定模块

图3

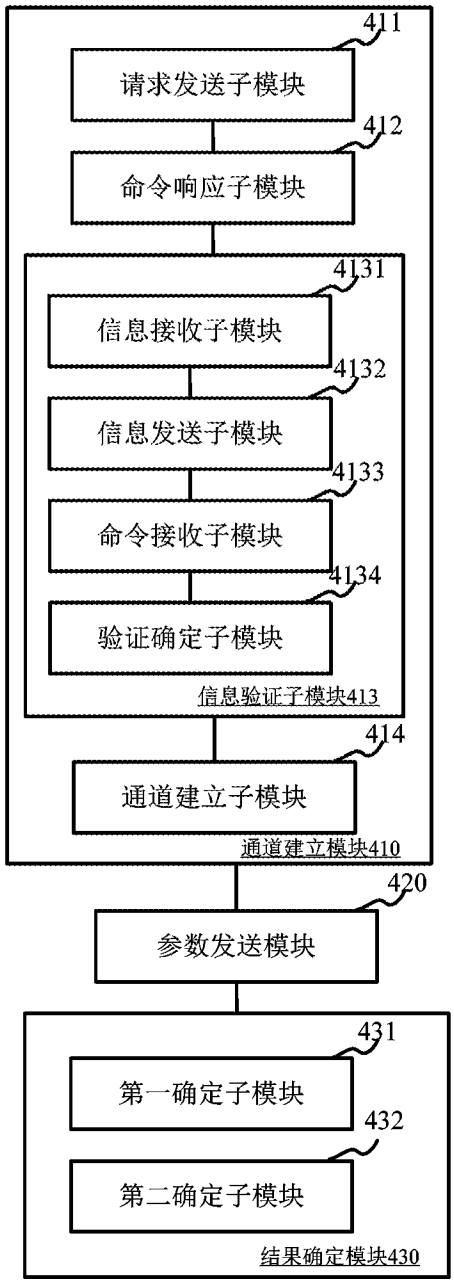
411
请求发送子模块
412
命令响应子模块
4131
信息接收子模块
4132
信息发送子模块
4133
命令接收子模块
4134
验证确定子模块
信息验证子模块413
414
通道建立子模块
通道建立模块410
420
参数发送模块
431
第一确定子模块
432
第二确定子模块
结果确定模块430

图4

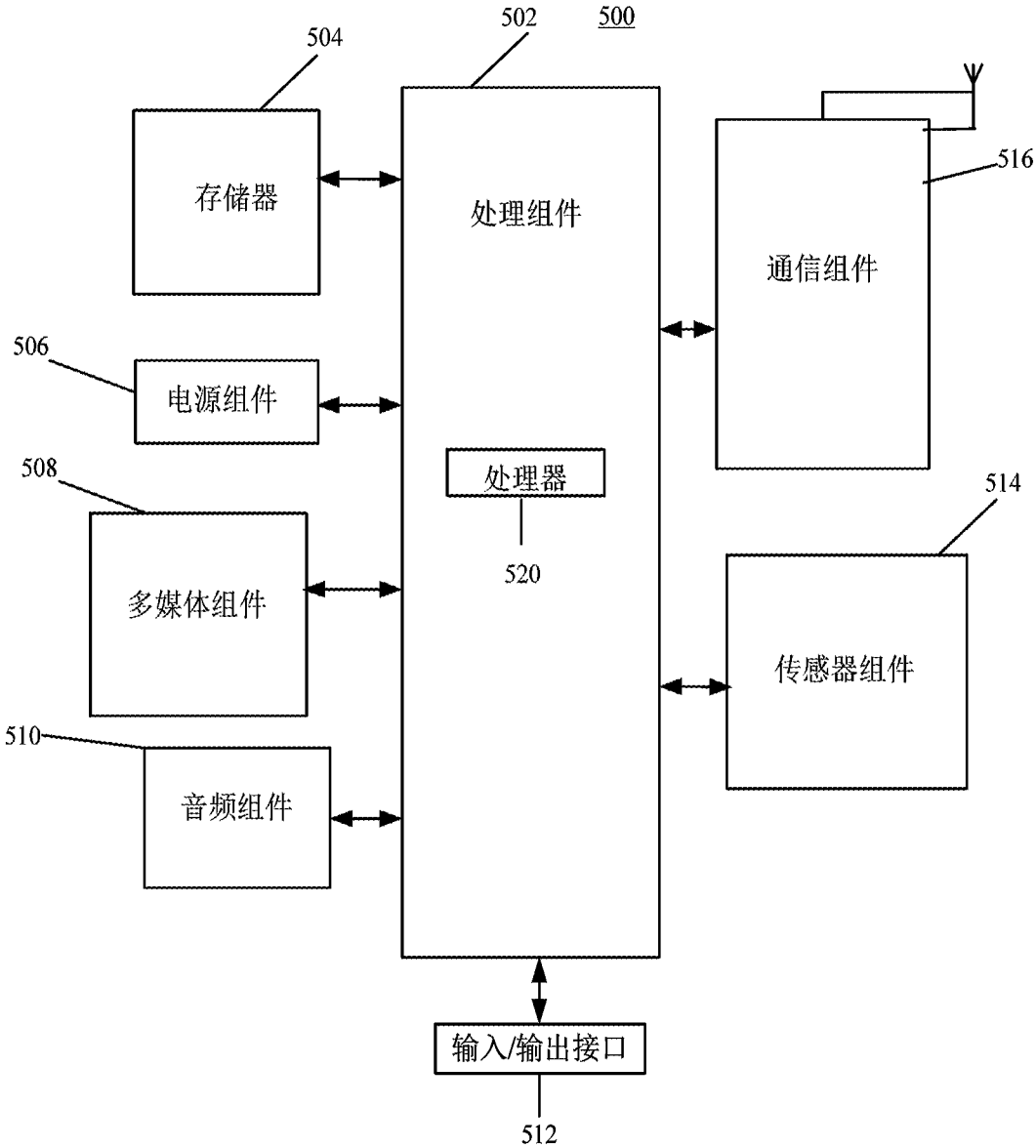
500
502
504
存储器
处理组件
通信组件
516
506
电源组件
处理器
520
508
多媒体组件
514
传感器组件
510
音频组件
输入/输出接口
512

图5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/071248

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44 (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; H04L

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, CNKI, WPI, EPODOC: safe, channel, accuracy, true and false, terminal, verificat+, feedback, hardware, parameter, identify, information

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103646044 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 19 March 2014 (19.03.2014), description, paragraphs 56-87, and figure 1	1-4, 6-9, 11
A	CN 103841239 A (BEIJING ANTUTU TECHNOLOGY CO., LTD.), 04 June 2014 (04.06.2014), the whole document	1-11
A	CN 1697424 A (ZHU, Wenhe), 16 November 2005 (16.11.2005), the whole document	1-11
A	US 2014115340 A1 (SAMSUNG ELECTRONICS CO., LTD.), 24 April 2014 (24.04.2014), the whole document	1-11

☐ 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
07 July 2015 (07.07.2015)	**28 July 2015 (28.07.2015)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **ZHANG, Qian** Telephone No.: (86-10) **62413681**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/071248

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103646044 A	19 March 2014	None	
CN 103841239 A	04 June 2014	None	
CN 1697424 A	16 November 2005	None	
US 2014115340 A1	24 April 2014	KR 20140050322 A	29 April 2014

国际检索报告

国际申请号
PCT/CN2015/071248

A. 主题的分类

G06F 21/44(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; H04L

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,CNKI,WPI,EPODOC:终端，验证，鉴别，安全，通道，硬件，参数，准确性，反馈，识别，真伪，terminal, verificat+,feedback,hardware,parameter,identify,information

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 103646044 A (北京奇虎科技有限公司 等) 2014年 3月 19日 (2014-03-19) 说明书第56-87段，附图1	1-4，6-9，11
A	CN 103841239 A (北京安兔兔科技有限公司) 2014年 6月 4日 (2014-06-04) 全文	1-11
A	CN 1697424 A (朱文和) 2005年 11月 16日 (2005-11-16) 全文	1-11
A	US 2014115340 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2014年 4月 24日 (2014-04-24) 全文	1-11

☐ 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
2015年 7月 7日	2015年 7月 28日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国	张千
传真号 (86-10)62019451	电话号码 (86-10)62413681

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/071248

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 103646044 A	2014年 3月 19日	无	
CN 103841239 A	2014年 6月 4日	无	
CN 1697424 A	2005年 11月 16日	无	
US 2014115340 A1	2014年 4月 24日	KR 20140050322 A	2014年 4月 29日