

(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
2018 年 5 月 24 日 (24.05.2018)



(10) 国际公布号
WO 2018/090934 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/111151

(22) 国际申请日: 2017 年 11 月 15 日 (15.11.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611021781.8 2016 年 11 月 15 日 (15.11.2016) 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: 祝铨(ZHU, Li); 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: 北京三高永信知识产权代理有限公司(BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国北京市海淀区学院路蓟门里和景园 A 座 1 单元 102 室, Beijing 100088 (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: EVENT REPORTING METHOD AND APPARATUS

(54) 发明名称: 事件上报方法及装置

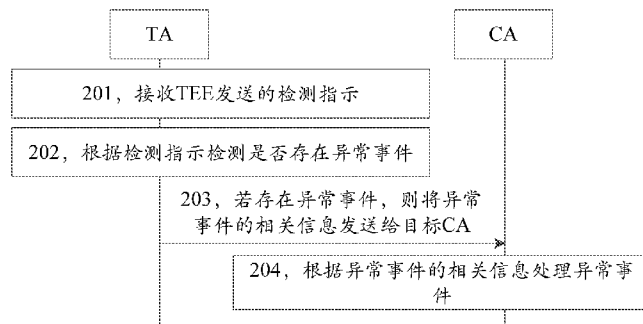


图 2

201 RECEIVING A DETECTION INDICATION SENT BY A TEE
202 DETECTING, ACCORDING TO THE DETECTION INDICATION, WHETHER THERE IS AN EXCEPTIONAL EVENT
203 IF THERE IS AN EXCEPTIONAL EVENT, THEN SENDING RELATED INFORMATION ABOUT THE EXCEPTIONAL EVENT TO A TARGET CA
204 DEALING WITH THE EXCEPTIONAL EVENT ACCORDING TO THE RELATED INFORMATION ABOUT THE EXCEPTIONAL EVENT

(57) Abstract: Disclosed are an event reporting method and apparatus, falling within the technical field of communications. The method comprises: a trusted application (TA) receiving a detection indication sent by a trusted execution environment (TEE), wherein the detection indication is sent by the TEE after monitoring a pre-set event, the pre-set event is an event set according to the requirement, provided by a target object, for detecting an exceptional event, and the target object is a target client application (CA) or a communication processor (CP); the TA detecting, according to the detection indication, whether there is an exceptional event; and if there is an exceptional event, then the TA sending related information about the exceptional event to the target object, so that the target object deals with the exceptional event according to the related information about the exceptional event. When a TA detects that there is an exceptional event, the present invention actively sends related information about the exceptional event to a target object, thus solving

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))。

the problem in the existing solution that an exceptional event is untimely reported and improving the timeliness of the TA reporting the exceptional event to a CA or a CP.

(57) 摘要: 本发明公开了一种事件上报方法及装置, 属于通信技术领域。所述方法包括: 可信应用TA接收可信执行环境TEE发送的检测指示, 检测指示由TEE在监测到预设事件后发送, 预设事件是根据目标对象提供的检测异常事件的需求所设定的事件, 目标对象为目标客户应用CA或通信处理器CP; TA根据检测指示检测是否存在异常事件; 若存在异常事件, 则TA将异常事件的相关信息发送给目标对象, 以使得目标对象根据异常事件的相关信息处理异常事件。本发明通过TA在检测到存在异常事件的情况下, 主动将异常事件的相关信息发送给目标对象, 解决了现有方案中异常事件上报不及时的问题, 提高了TA向CA或CP上报异常事件的及时性。

事件上报方法及装置

本申请要求于 2016 年 11 月 15 日提交国家知识产权局、申请号为 201611021781.8、发明名称为“事件上报方法及装置”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

本发明涉及通信技术领域,特别涉及一种事件上报方法及装置。

背景技术

随着移动网络和智能终端的高速发展以及消费电子产品智能化的普及,移动应用的种类和数量越来越多。当前的移动应用已经不仅限于对智能终端的基本功能、娱乐功能方面的扩展,它所涉及的领域逐渐扩大到各行各业,例如:移动支付相关的金融应用、内容版权保护应用以及云计算下瘦终端的安全应用等,这些行业应用都需要更高安全级别的终端运行环境。

然而,智能终端的操作系统本身的设计主要侧重于功能性方面要求,并非从安全性角度出发,同时加上整个系统的开放性、庞大性、复杂性而无法杜绝相应的系统漏洞,致使一些利用这些漏洞的恶意程序不断出现,从而造成应用程序处于危险之中。虽然可以利用一些软件防护手段,如防火墙、杀毒软件等进行相应的保护,但由于新型病毒程序的层出不穷以及经常性的系统更新升级,导致无法做到软件上的完全保护。

基于这些问题,业界进行了深入的研究工作,提出一种新型解决思路,即把同一硬件设备划为两种相互独立且硬件上隔离的执行环境:富执行环境(Rich Execution Environment, REE)和可信执行环境(Trusted Execution Environment, TEE)。富执行环境也称为普通执行环境。平台上的软硬件资源可以分别标识为两种执行环境状态,标识为安全执行状态的软硬件资源只能由可信执行环境所访问,而标识为普通执行状态的软硬件资源则可以为两种执行环境所访问。REE 运行目前常用的移动操作系统如 Android 等,TEE 运行一个功能简单、代码量小、封闭且可人为审核控制的安全操作系统。安全性要求较高的应用部署在安全操作系统中,并为部署在移动操作系统中的普通应用提供安全服务。当普通应用调用相应的安全应用执行时,硬件设备由 REE 切换到 TEE 执行,此时整个硬件设备处于可信状态,设备与外界的交互都得到控制,保证都是真实可信的行为。

TEE 的软硬件执行环境和 REE 类似,通过芯片的特有技术(如 ARM 的 Trustzone 技术,或者 Intel 多 CPU 技术),实现 TEE 和 REE 的物理运行环境的隔离,从而保障在 TEE 中的应用程序的安全性。TEE 使用的外设都需要具备安全属性,这样才可以避免 TEE 访问外设的时候造成的安全数据泄漏风险。

TEE 中运行的应用称为可信应用(Trusted Application, TA),REE 中运行的应用称为客户应用(Client Application, CA)。客户应用也称为普通应用。目前而言,TA 主要实现的功能包括加解密、认证和数据存储等,其作用是作为 CA 的安全扩展功能。例如,TA 存储密钥和证书用以完成数据的加解密和认证操作。又例如,TA 存储诸如指纹数据、银行账户等

关键数据。随着 TA 的功能的增强, TA 内部通常也会管理和校验安全数据的有效性, 包括数据的正确性、完整性、时效性等。

在现有技术中, 当 TA 检测到某些异常事件(例如 TA 存储的证书已过期)发生时, TA 保存异常事件的相关数据, 等待 REE 查询后再上报给相应的 CA。在一个示例中, CA 采用定时轮询方式查询是否存在异常事件。CA 启动定时器, 当定时器超时时向 TA 发送查询请求, 如果 TA 之前检测到有异常事件发生, 则将保存的异常事件的相关数据发送给 CA。CA 接收到异常事件的相关数据之后, 处理该异常事件。上述现有技术提供的事件上报方式, TA 并不能够及时地向 CA 上报异常事件。

10 发明内容

本发明实施例提供了一种事件上报方法及装置, 用以解决现有方案中异常事件上报不及时的问题。

一方面, 本发明实施例提供了一种事件上报方法, 该方法包括: TA 接收 TEE 发送的检测指示, 该检测指示由 TEE 在监测到预设事件后发送, 预设事件是根据目标对象提供的检测异常事件的需求所设定的事件, 目标对象为目标 CA 或通信处理器 (Communication Processor, CP); TA 根据检测指示检测是否存在异常事件; 若存在异常事件, 则 TA 将异常事件的相关信息发送给目标对象; 目标对象根据异常事件的相关信息处理异常事件。

本发明实施例提供的方案中, 通过 TA 在检测到存在异常事件的情况下, 主动将异常事件的相关信息发送给目标对象, 解决了现有方案中异常事件上报不及时的问题, 提高了 TA 向 CA 或者 CP 上报异常事件的及时性。

在一个可能的设计中, 目标对象为目标 CA, TA 将异常事件的相关信息发送给目标对象, 包括: TA 向可信区域驱动 (TZ Driver) 发送目标 CA 的应用标识和异常事件的相关信息。TZ Driver 用于根据目标 CA 的应用标识向目标 CA 发送异常事件的相关信息。相应地, 目标 CA 从 TZ Driver 接收异常事件的相关信息。

通过上述方式, 实现了 TA 通过 TZ Driver 向目标 CA 定向上报异常事件。

在另一个可能的设计中, 目标对象为目标 CA, TA 将异常事件的相关信息发送给目标对象, 包括: TA 向 TZ Driver 发送异常事件的相关信息。TZ Driver 用于采用广播方式向包括目标 CA 在内的多个 CA 发送异常事件的相关信息。相应地, 目标 CA 接收由 TZ Driver 采用广播方式发送的异常事件的相关信息。

通过上述方式, 实现了 TA 通过 TZ Driver 向目标 CA 广播上报异常事件, 可以实现一个异常事件发送给多个目标 CA 的功能。另外, 采用广播方式上报异常事件, 可以避免异常事件在上报过程中被非法软件截取而导致目标 CA 无法接收到异常事件的情况发生, 确保异常事件能够成功上报给目标 CA。

在又一个可能的设计中, 目标对象为目标 CA, TA 将异常事件的相关信息发送给目标对象, 包括: TA 将异常事件的相关信息写入安全共享内存, 并向 CP 发送安全中断。安全共享内存是指物理属性在内存管理单元 (Memory Management Unit, MMU) 中被设置为安全打开状态的共享内存。安全中断用于触发 CP 在处于安全模式的情况下从安全共享内存中读取异常事件的相关信息, 并采用广播方式向包括目标 CA 在内的多个 CA 发送异常事件的相关信息。相应地, CA 接收由 CP 采用广播方式发送的异常事件的相关信息。

通过上述方式，实现了TA通过CP向目标CA广播上报异常事件，可以实现一个异常事件发送给多个目标CA的功能。另外，采用广播方式上报异常事件，可以避免异常事件在上报过程中被非法软件截取而导致目标CA无法接收到异常事件的情况发生，确保异常事件能够成功上报给目标CA。另外，TA通过将异常事件的相关信息安全地发送给CP，而不需
5 要经过REE，避免非法程序或外部物理攻击造成数据在传输过程中被泄漏或破坏。TA和CP之间的数据可以明文传输，提高效率的同时也没有降低安全性。

在又一个可能的设计中，目标对象为CP，TA将异常事件的相关信息发送给目标对象，包括：TA将异常事件的相关信息写入安全共享内存，并向CP发送安全中断，该安全中断用于触发CP在处于安全模式的情况下从安全共享内存中读取异常事件的相关信息，并根据
10 异常事件的相关信息处理该异常事件。

通过上述方式，实现了TA主动向CP上报异常事件，且能够确保将异常事件的相关信息安全地发送给CP。

另一方面，本发明实施例提供一种事件上报装置，该装置具有实现上述方法示例中TA侧行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述
15 硬件或软件包括一个或多个与上述功能相对应的模块。

又一方面，本发明实施例提供一种事件上报装置，该装置具有实现上述方法示例中CA侧行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。

再一方面，本发明实施例提供一种终端，该终端具有TEE和REE，终端的结构中包括
20 处理器，所述处理器被配置为支持终端执行上述方法中相应的功能。可选地，终端的结构中还包括通信接口，所述通信接口用于支持终端与其他设备之间的通信。进一步的，终端还可以包括存储器，所述存储器用于与处理器耦合，其保存终端必要的程序指令和数据。

再一方面，本发明实施例提供一种计算机存储介质，用于储存为上述用于终端所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

相较于现有技术，本发明实施例的方案中，通过TA在检测到存在异常事件的情况下，
25 主动将异常事件的相关信息发送给目标对象，解决了现有方案中异常事件上报不及时的问题，提高了TA向CA或CP上报异常事件的及时性。

附图说明

30 图1是本发明实施例可能适用的一种终端的结构示意图；
图2是本发明实施例提供的一种事件上报方法的流程图；
图3A是本发明实施例提供的另一种事件上报方法的流程图；
图3B是本发明实施例提供的另一种事件上报方法的流程图；
图4A是本发明实施例提供的另一种事件上报方法的流程图；
35 图4B是本发明实施例提供的另一种事件上报方法的流程图；
图5A是本发明实施例提供的另一种事件上报方法的流程图；
图5B示例性示出了一种AP、CP和共享内存之间的连接关系的示意图；
图5C是本发明实施例提供的另一种事件上报方法的流程图；
图6是本发明实施例提供的另一种事件上报方法的流程图；

图 7 是本发明实施例提供的另一种事件上报方法的流程图；

图 8 是本发明实施例提供的另一种事件上报方法的流程图；

图 9 是本发明实施例提供的一种事件上报装置的框图；

图 10 是本发明实施例提供的另一种事件上报装置的框图；

5 图 11 是本发明实施例提供的一种终端的框图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

10 图 1 示出了本发明实施例可能适用的一种终端的结构示意图。如图 1 所示，该终端包括应用处理器 (Application Processor, AP)。AP 可以是中央处理器 (Central Processing Unit, CPU)，AP 也可以包括 CPU 及 CPU 外围硬件。

在本发明实施例中，终端部署有 TEE 和 REE。TA 和 CA 均可在 AP 中运行。

15 如图 1 所示，终端还包括传声器、屏幕以及 CP 等外设，运行在 AP 上的 TA 或 CA 可以通过与外设之间的接口访问外设。需要说明的是，当 TA 访问外设时，会触发外设进入安全模式，在这种情况下，外设只能被 TA 所访问，而不能被 CA 所访问。

此外，终端还包括一些必要的 TEE 硬件和 REE 硬件等，图中未示出。

20 终端可以包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其他处理设备，以及各种形式的用户设备 (User Equipment, UE)，移动台 (Mobile Station, MS)，终端设备 (terminal device) 等等。为方便描述，上面提到的设备统称为终端。

在现有技术中，TA 并不能够及时地向 CA 上报异常事件。有鉴于此，本发明实施例提供了一种事件上报方法，和基于这个方法的装置和终端。本发明实施例提供的技术方案，核心思想是 TA 在检测到异常事件时，主动向 CA 上报异常事件，以提高及时性。

25 下面将基于上面所述的本发明实施例涉及的共性方面，对本发明实施例进一步详细说明。

图 2 是本发明实施例提供的一种事件上报方法的流程图，该方法可以包括如下几个步骤。

步骤 201，TA 接收 TEE 发送的检测指示。

30 检测指示由 TEE 在监测到预设事件后发送。预设事件是根据目标对象提供的检测异常事件的需求所设定的事件。例如，预设事件可以是硬件或者软件发送的中断，也可以是定时器超时。目标对象可以是目标 CA 或 CP。在本实施例中，主要以目标对象为目标 CA 为例进行说明。检测指示用于指示 TA 检测是否存在异常事件。可选地，检测指示中携带有所需检测的异常事件的相关信息，以便 TA 据此确定所需检测的异常事件。

35 另外，当 TEE 中存在多个不同的 TA 且该多个不同的 TA 分别用于检测不同的异常事件时，TEE 根据监测到的预设事件的类型，向该预设事件的类型对应的 TA 发送检测指示。其中，预设事件的类型和 TA 之间的对应关系可预先在 TEE 中配置。

步骤 202，TA 根据检测指示检测是否存在异常事件。

TA 接收到 TEE 发送的检测指示之后，根据该检测指示检测是否存在异常事件。例如，

TA 根据检测指示中携带有所需检测的异常事件的相关信息，确定所需检测的异常事件，而后检测是否存在该异常事件。

异常事件是指与正常工作状态不相符的事件。在本发明实施例中，对异常事件的类型不作限定，例如异常事件可以是安全存储区域的数据被非法修改、安全存储区域的数据出错、证书已过期，等等。

步骤 203，若存在异常事件，则 TA 将异常事件的相关信息发送给目标 CA。

相应地，目标 CA 接收 TA 发送的异常事件的相关信息。

在本发明实施例中，当 TA 检测到存在异常事件时，TA 主动将异常事件的相关信息发送给目标 CA，从而提高了事件上报的及时性。目标 CA 是与异常事件相关的 CA，也即上述提供检测异常事件的需求并用于处理该异常事件的 CA。目标 CA 可以是一个 CA，也可以是多个 CA。可选地，异常事件的相关信息包括异常事件的类型或者其它用于描述异常事件的信息。

另外，当 TA 检测到不存在异常事件时，TA 向 TEE 发送用于指示不存在异常事件的检测结果。

步骤 204，目标 CA 根据异常事件的相关信息处理异常事件。

目标 CA 接收到 TA 发送的异常事件的相关信息之后，据此处理异常事件。针对不同类型的异常事件，目标 CA 所采取的处理方式也有所不同，有关内容可参见下文示例性实施例。

可选地，当目标对象为 CP 时，若存在异常事件，则 TA 将异常事件的相关信息发送给 CP。相应地，CP 接收 TA 发送的异常事件的相关信息，根据异常事件的相关信息处理该异常事件。CP 对异常事件所做的处理是与通信功能相关的处理，例如关闭通信业务。

综上所述，本实施例提供的方法，通过 TA 在检测到存在异常事件的情况下，主动将异常事件的相关信息发送给目标对象，解决了现有方案中异常事件上报不及时的问题，提高了 TA 向 CA 或 CP 上报异常事件的及时性。

在本发明实施例中，提供了 TA 向 CA 主动上报异常事件的 3 种不同实现方式。在下面图 3A 所示实施例中，介绍 TA 通过 TZ Driver 向目标 CA 定向上报异常事件。在下面图 4A 所示实施例中，介绍 TA 通过 TZ Driver 向目标 CA 广播上报异常事件。在下面图 5A 所示实施例中，介绍 TA 通过 CP 向目标 CA 广播上报异常事件。

图 3A 是本发明实施例提供的另一种事件上报方法的流程图。图 3A 所示的方法中，与图 2 所示方法相同或类似的内容可以参考图 2 中的详细描述，此处不作赘述。该方法可以包括如下几个步骤。

步骤 301，TEE 在监测到预设事件后，向 TA 发送检测指示。

相应地，TA 接收 TEE 发送的检测指示。

步骤 302，TA 根据检测指示检测是否存在异常事件。

步骤 303，若存在异常事件，则 TA 向 TZ Driver 发送目标 CA 的应用标识和异常事件的相关信息。

相应地，TZ Driver 接收 TA 发送的目标 CA 的应用标识和异常事件的相关信息。

TZ Driver 用于实现 REE 和 TEE 之间的数据通信功能，因此 TA 可通过 TZ Driver 向目

标 CA 上报异常事件。在本实施例中, TA 向 TZ Driver 发送目标 CA 的应用标识和异常事件的相关信息。目标 CA 是与异常事件相关的 CA。目标 CA 的应用标识用于唯一标识目标 CA。

步骤 304, TZ Driver 根据目标 CA 的应用标识向目标 CA 发送异常事件的相关信息。

相应地, 目标 CA 从 TZ Driver 接收异常事件的相关信息。

5 步骤 305, 目标 CA 根据异常事件的相关信息处理异常事件。

在一个示例中, 如图 3B 所示, 通过回调方式向目标 CA 发送异常事件的相关信息, 相应的步骤流程如下:

步骤 31, 目标 CA 调用注册接口, 向 TZ Driver 发送注册请求。

相应地, TZ Driver 接收目标 CA 发送的注册请求。

10 注册请求用于请求注册回调函数。注册请求中携带有目标 CA 的应用标识。可选地, 注册请求中还携带异常事件的类型。

步骤 32, TZ Driver 根据目标 CA 的应用标识注册回调函数。

可选地, 当注册请求中还携带有异常事件的类型时, TZ Driver 记录异常事件的类型与回调函数之间的处理关系。

15 步骤 33, TEE 在监测到预设事件后, 向 TA 发送检测指示。

相应地, TA 接收 TEE 发送的检测指示。

步骤 34, TA 根据检测指示检测是否存在异常事件。

步骤 35, 若存在异常事件, 则 TA 向 TZ Driver 发送目标 CA 的应用标识和异常事件的相关信息。

20 相应地, TZ Driver 接收 TA 发送的目标 CA 的应用标识和异常事件的相关信息。

步骤 36, TZ Driver 根据目标 CA 的应用标识, 查询对应的回调函数。

步骤 37, TZ Driver 调用查询到的回调函数, 通过该回调函数向目标 CA 发送异常事件的相关信息。

相应地, 目标 CA 从 TZ Driver 接收异常事件的相关信息。

25 步骤 38, 目标 CA 根据异常事件的相关信息处理异常事件。

综上所述, 本实施例提供的方法, 实现了 TA 通过 TZ Driver 向目标 CA 定向上报异常事件。

30 图 4A 是本发明实施例提供的另一种事件上报方法的流程图。图 4A 所示的方法中, 与图 2 所示方法相同或类似的内容可以参考图 2 中的详细描述, 此处不作赘述。该方法可以包括如下几个步骤。

步骤 401, TEE 在监测到预设事件后, 向 TA 发送检测指示。

相应地, TA 接收 TEE 发送的检测指示。

步骤 402, TA 根据检测指示检测是否存在异常事件。

35 步骤 403, 若存在异常事件, 则 TA 向 TZ Driver 发送异常事件的相关信息。

相应地, TZ Driver 接收 TA 发送的异常事件的相关信息。

在本实施例中, 由于通过 TZ Driver 向目标 CA 广播上报异常事件, 因此 TA 仅需将异常事件的相关信息发送给 TZ Driver 即可, 而无需将目标 CA 的应用标识发送给 TZ Driver。

步骤 404, TZ Driver 采用广播方式向包括目标 CA 在内的多个 CA 发送异常事件的相关

信息。

相应地，目标 CA 接收由 TZ Driver 采用广播方式发送的异常事件的相关信息。

目标 CA 是与异常事件相关的 CA。在本实施例中，由于采用广播上报方式，因此可以实现一个异常事件发送给多个目标 CA 的功能。

5 步骤 405，目标 CA 根据异常事件的相关信息处理异常事件。

在一个示例中，如图 4B 所示，由 TZ Driver 通过广播方式向包括目标 CA 在内的多个 CA 发送异常事件的相关信息，相应的步骤流程如下：

步骤 41，TEE 在监测到预设事件后，向 TA 发送检测指示。

相应地，TA 接收 TEE 发送的检测指示。

10 步骤 42，TA 根据检测指示检测是否存在异常事件。

步骤 43，若存在异常事件，则 TA 向 TZ Driver 发送异常事件的相关信息。

相应地，TZ Driver 接收 TA 发送的异常事件的相关信息。

步骤 44，TZ Driver 将异常事件的相关信息转换为 AT (Attention) 命令。

15 步骤 45，TZ Driver 通过 AT 发送接口将 AT 命令发送给无线接口层 (Radio Interface Layer, RIL)。

相应地，RIL 接收 TZ Driver 发送的 AT 命令。

步骤 46，RIL 解析 AT 命令得到异常事件的相关信息。

步骤 47，RIL 将异常事件的相关信息发送给 REE 中运行的操作系统框架 (Framework)。

相应地，Framework 接收 RIL 发送的异常事件的相关信息。

20 步骤 48，Framework 向包括目标 CA 在内的多个 CA 广播异常事件的相关信息。

相应地，目标 CA 接收由 Framework 采用广播方式发送的异常事件的相关信息。

步骤 49，目标 CA 根据异常事件的相关信息处理异常事件。

25 综上所述，本实施例提供的方法，实现了 TA 通过 TZ Driver 向目标 CA 广播上报异常事件，可以实现一个异常事件发送给多个目标 CA 的功能。另外，采用广播方式上报异常事件，可以避免异常事件在上报过程中被非法软件截取而导致目标 CA 无法接收到异常事件的情况发生，确保异常事件能够成功上报给目标 CA。

30 图 5A 是本发明实施例提供的另一种事件上报方法的流程图。图 5A 所示的方法中，与图 2 所示方法相同或类似的内容可以参考图 2 中的详细描述，此处不作赘述。该方法可以包括如下几个步骤。

步骤 501，TEE 在监测到预设事件后，向 TA 发送检测指示。

相应地，TA 接收 TEE 发送的检测指示。

步骤 502，TA 根据检测指示检测是否存在异常事件。

步骤 503，若存在异常事件，则 TA 将异常事件的相关信息写入安全共享内存。

35 安全共享内存是指物理属性在 MMU 中被设置为安全打开状态的共享内存。当共享内存的物理属性为安全打开状态时，只有在 TA 驱动下的 AP 或处于安全模式的 CP 才可以通
过总线 (Bus) 对该共享内存进行访问。也就是说，只有 AP 运行的 TEE 和 TA 能够访问该
共享内存，AP 运行的 REE 和 CA 是不能访问该共享内存的。这样，AP 运行的 REE 和 CA
就没有办法访问该共享内存的数据，也就保证了内存数据对 REE 和 CA 的安全隔离。当共

享内存的物理属性为非安全打开状态（即普通状态）时，AP 运行的 REE 和 CA 也可以访问该共享内存。

示例性地，如图 5B 所示，其示出了一种 AP、CP 和共享内存之间的连接关系的示意图。其中，MMU、AP 和 CP 之间通过总线两两连接，共享内存通过 MMU 与总线连接。处于安全模式的 CP 和在 TA 驱动下的 AP 均可以访问物理属性为安全打开状态的共享内存。具体地，可以在 MMU 中设置共享内存的物理属性为安全打开状态。

可选地，CP 为通信调制解调器（Modem）、蓝牙处理器、无线保真（Wireless Fidelity, Wi-Fi）处理器或语音处理器。通信调制解调器可以是 2G、3G、4G 或下一代通信系统的无线通信调制解调器，语音处理器可以为包括可实现语音功能的编解码器（Codec）或语音压缩等功能的高保真（High Fidelity, Hi-Fi）处理器。可以理解的是，CP 和 AP 也可以集成在一个处理器内。本文中的 CP 和 AP 可以分别是一个独立的处理器，也可以是一个处理器内的部分功能电路。

步骤 504，TA 向 CP 发送安全中断。

相应地，CP 接收 TA 发送的安全中断。

TA 将异常事件的相关信息写入安全共享内存之后，还需要通过中断触发 CP 处理。该中断为安全中断，也即该中断会触发 CP 进入安全模式，然后由安全模式的中断处理程序接管后完成后续的数据处理流程。安全中断用于触发 CP 在处于安全模式的情况下从安全共享内存中读取异常事件的相关信息，并采用广播方式向包括目标 CA 在内的多个 CA 发送异常事件的相关信息。

TA 可以通过 AP 与 CP 之间的进程间通信（Inter-Process Communication, IPC）机制向 CP 发送安全中断。

步骤 505，CP 在处于安全模式的情况下从安全共享内存中读取异常事件的相关信息。

CP 在接收到 TA 发送的安全中断之后，如果 CP 的工作模式已经处于安全模式，则 CP 直接从安全共享内存中读取异常事件的相关信息，CP 的工作模式不会切换；如果 CP 的工作模式处于非安全模式，则 CP 从非安全模式切换至安全模式，然后从安全共享内存中读取异常事件的相关信息。

可选地，上述步骤 505 之后还包括如下步骤 506：

步骤 506，CP 根据异常事件的相关信息处理该异常事件。

CP 对异常事件所做的处理与目标 CA 对异常事件所做的处理有所不同，CP 对异常事件所做的处理是与通信功能相关的处理，例如关闭通信业务。在实际应用中，可根据异常事件的具体类型，设定 CP 对异常事件所做的处理以及目标 CA 对异常事件所做的处理。CP 在处理完成之后执行下述步骤 507。

步骤 507，CP 采用广播方式向包括目标 CA 在内的多个 CA 发送异常事件的相关信息。

相应地，目标 CA 接收由 CP 采用广播方式发送的异常事件的相关信息。

目标 CA 是与异常事件相关的 CA。在本实施例，由于采用广播上报方式，因此可以实现一个异常事件发送给多个目标 CA 的功能。

步骤 508，目标 CA 根据异常事件的相关信息处理异常事件。

在一个示例中，如图 5C 所示，由 CP 通过广播方式向包括目标 CA 在内的多个 CA 发送异常事件的相关信息，相应的步骤流程如下：

步骤 51, TEE 在监测到预设事件后, 向 TA 发送检测指示。

相应地, TA 接收 TEE 发送的检测指示。

步骤 52, TA 根据检测指示检测是否存在异常事件。

步骤 53, 若存在异常事件, 则 TA 将异常事件的相关信息写入安全共享内存。

5 步骤 54, TA 向 CP 发送安全中断。

相应地, CP 接收 TA 发送的安全中断。

步骤 55, CP 在处于安全模式的情况下从安全共享内存中读取异常事件的相关信息。

步骤 56, CP 根据异常事件的相关信息处理该异常事件。

步骤 57, CP 将异常事件的相关信息转换为 AT 命令。

10 步骤 58, CP 通过 AT 发送接口将 AT 命令发送给 RIL。

相应地, RIL 接收 CP 发送的 AT 命令。

步骤 59, RIL 解析 AT 命令得到异常事件的相关信息。

步骤 60, RIL 将异常事件的相关信息发送给 REE 中运行的 Framework。

相应地, Framework 接收 RIL 发送的异常事件的相关信息。

15 步骤 61, Framework 向包括目标 CA 在内的多个 CA 广播异常事件的相关信息。

相应地, 目标 CA 接收由 Framework 采用广播方式发送的异常事件的相关信息。

步骤 62, 目标 CA 根据异常事件的相关信息处理异常事件。

综上所述, 本实施例提供的方法, 实现了 TA 通过 CP 向目标 CA 广播上报异常事件, 可以实现一个异常事件发送给多个目标 CA 的功能。另外, 采用广播方式上报异常事件, 可以避免异常事件在上报过程中被非法软件截取而导致目标 CA 无法接收到异常事件的情况发生, 确保异常事件能够成功上报给目标 CA。

20 另外, TA 通过将异常事件的相关信息安全地发送给 CP, 而不需要经过 REE, 避免非法程序或外部物理攻击造成数据在传输过程中被泄漏或破坏。TA 和 CP 之间的数据可以明文传输, 提高效率的同时也没有降低安全性。

25 需要补充说明的是, 当目标对象为 CP 时, TA 可采用如下方式将异常事件的相关信息发送给 CP。TA 将异常事件的相关信息写入安全共享内存, 并向 CP 发送安全中断, 该安全中断用于触发 CP 在处于安全模式的情况下从安全共享内存中读取异常事件的相关信息, 并根据异常事件的相关信息处理该异常事件。

30 通过上述方式, 实现了 TA 主动向 CP 上报异常事件, 且能够确保将异常事件的相关信息安全地发送给 CP。

下面, 通过几个具体的例子对本发明实施例提供的技术方案进行介绍说明。

35 图 6 是本发明实施例提供的另一种事件上报方法的流程图。在图 6 所示实施例中, TA 实现数据安全存储监测。该方法可以包括如下几个步骤:

步骤 601, TEE 监测到安全存储区域被访问。

步骤 602, TEE 向 TA 发送检测指示。

相应地, TA 接收 TEE 发送的检测指示。

步骤 603, TA 对安全存储区域的数据进行检查, 检测数据是否被破坏。若是, 则执行

下述步骤 605；若否，则执行下述步骤 604。

例如，TA 检查安全存储区域的数据是否被非法修改或者数据内容是否出错等。

步骤 604，TA 向 TEE 发送用于指示安全存储区域的数据未被破坏的检测结果。

相应地，TEE 接收 TA 发送的用于指示安全存储区域的数据未被破坏的检测结果。

5 步骤 605，TA 向 TEE 发送异常事件的相关信息。

例如，异常事件的相关信息包括：用于指示安全存储区域的数据被破坏的检测结果，以及被破坏的数据类型等信息。

相应地，TEE 接收 TA 发送的异常事件的相关信息，并执行下述步骤 606。

步骤 606，TEE 向 TZ Driver 发送异常事件的相关信息。

10 相应地，TZ Driver 接收 TEE 发送的异常事件的相关信息。

步骤 607，TZ Driver 向目标 CA 发送异常事件的相关信息。

TZ Driver 可以通过上文介绍的定向方式或者广播方式向目标 CA 发送异常事件的相关信息。

相应地，目标 CA 接收 TZ Driver 发送的异常事件的相关信息。

15 步骤 608，目标 CA 根据异常事件的相关信息处理异常事件。

例如，目标 CA 执行对安全存储区域的数据的保护性流程，比如通知用户关键数据被破坏，或者重新更新关键数据内容等。

图 7 是本发明实施例提供的另一种事件上报方法的流程图。在图 7 所示实施例中，TA 实现证书有效期监测。应用和服务端之间的数据交互会使用证书方式，证书一般都有有效期，证书的有效期过期需要服务器重新签发证书，使用过期的证书进行交互会存在安全风险和隐患。通过本实施例提供的方法，TA 可以定时查询存储在 TEE 中的证书的有效期，如果证书的有效期过期，主动通知相应的 CA 触发重新颁发证书的流程。该方法可以包括如下几个步骤：

25 步骤 701，TEE 在监测到定时器超时，向 TA 发送检测指示。

相应地，TA 接收 TEE 发送的检测指示。

步骤 702，TA 检测证书的有效期是否过期。若是，则执行下述步骤 705 和 706；若否，则执行下述步骤 703。

步骤 703，TA 向 TEE 发送用于指示重启定时器的信息。

30 相应地，TEE 接收 TA 发送的用于指示重启定时器的信息，并执行下述步骤 704。

步骤 704，TEE 重启定时器。

步骤 705，TA 删除证书内容。

步骤 706，TA 向 TEE 发送用于指示证书已过期的信息。

相应地，TEE 接收 TA 发送的用于指示证书已过期的信息，并执行下述步骤 707。

35 步骤 707，TEE 向 TZ Driver 发送异常事件的相关信息。

例如，异常事件的相关信息包括：用于指示证书已过期的信息，以及已过期的证书的标识等信息。

相应地，TZ Driver 接收 TEE 发送的异常事件的相关信息。

步骤 708，TZ Driver 向目标 CA 发送异常事件的相关信息。

TZ Driver 可以通过上文介绍的定向方式或者广播方式向目标 CA 发送异常事件的相关信息。

相应地，目标 CA 接收 TZ Driver 发送的异常事件的相关信息。

步骤 709，目标 CA 根据异常事件的相关信息处理异常事件。

5 例如，目标 CA 执行向服务器请求重新签发证书的流程。

图 8 是本发明实施例提供的另一种事件上报方法的流程图。在图 8 所示实施例中，TA 实现通信业务有效性控制。通信业务可以是语音业务、漫游业务、数据业务等。通信业务的有效性控制在 TA 比 REE 侧具备更高的安全性，并且 TA 可以直接控制 Modem 关闭相关业务。Modem 关闭业务之后可以产生一个 AT 命令，通过 RIL 通知给 Framework 进行广播，提示用户当前通信业务已失去有效性，节省用户的通信资费或者避免非法软件造成通信资费的上升。该方法可以包括如下几个步骤：

步骤 801，TEE 在监测到定时器超时，向 TA 发送检测指示。

相应地，TA 接收 TEE 发送的检测指示。

15 步骤 802，TA 检测通信业务是否已失去有效性。若是，则执行下述步骤 805；若否，则执行下述步骤 803。

其中，TA 检测通信业务是否已失去有效性可以是检测语音业务的累计时长是否已超过第一预设时长，也可以是检测漫游业务的累计时长是否已超过第二预设时长，还可以是检测数据业务的累计流量是否已超过预设流量，等等。

20 步骤 803，TA 向 TEE 发送用于指示重启定时器的信息。

相应地，TEE 接收 TA 发送的用于指示重启定时器的信息，并执行下述步骤 804。

步骤 804，TEE 重启定时器。

步骤 805，TA 向 Modem 发送异常事件的相关信息。

25 例如，异常事件的相关信息包括：用于指示通信业务已失去有效性的检测结果，以及已失去有效性的通信业务的业务标识。

相应地，Modem 接收 TA 发送的异常事件的相关信息。

步骤 806，Modem 关闭已失去有效性的通信业务。

步骤 807，Modem 将异常事件的相关信息转换为 AT 命令，并通过 AT 发送接口向 RIL 发送 AT 命令。

30 相应地，RIL 接收 Modem 发送的 AT 命令。

步骤 808，RIL 解析 AT 命令得到异常事件的相关信息，并且通知 Framework 进行广播。

在上述各个方法实施例中，从多侧交互的角度对本发明技术方案进行了介绍说明。有关 TA 侧的步骤可以单独实现成为 TA 侧的事件上报方法，有关 CA 侧的步骤可以单独实现成为 CA 侧的事件上报方法。

下述为本发明装置实施例，可以用于执行本发明方法实施例。对于本发明装置实施例中未披露的细节，请参照本发明方法实施例。

图 9 是本发明实施例提供的一种事件上报装置的框图。该装置具有实现上述方法示例

中 TA 侧的各个步骤的功能，所述功能可以通过硬件实现，也可通过硬件执行相应的软件实现。该装置可以包括：接收单元 910、检测单元 920 和发送单元 930。

接收单元 910，用于接收 TEE 发送的检测指示，所述检测指示由所述 TEE 在监测到预设事件后发送，所述预设事件是根据目标对象提供的检测异常事件的需求所设定的事件，
5 所述目标对象为目标客户应用 CA 或通信处理器 CP。

检测单元 920，用于根据所述检测指示检测是否存在所述异常事件。

发送单元 930，用于当存在所述异常事件时，将所述异常事件的相关信息发送给所述目标对象，以使得所述目标对象根据所述异常事件的相关信息处理所述异常事件。

在一个示例中，所述目标对象为所述目标 CA；所述发送单元 930，用于向 TZ Driver
10 发送所述目标 CA 的应用标识和所述异常事件的相关信息。其中，所述 TZ Driver 用于根据所述目标 CA 的应用标识向所述目标 CA 发送所述异常事件的相关信息。

在另一示例中，所述目标对象为所述目标 CA；所述发送单元 930，用于向 TZ Driver 发送所述异常事件的相关信息。其中，所述 TZ Driver 用于采用广播方式向包括所述目标 CA 在内的多个 CA 发送所述异常事件的相关信息。

15 在又一示例中，所述目标对象为所述目标 CA；所述发送单元 930，用于将所述异常事件的相关信息写入安全共享内存，并向 CP 发送安全中断。其中，所述安全共享内存是指物理属性在 MMU 中被设置为安全打开状态的共享内存，所述安全中断用于触发所述 CP 在处于安全模式的情况下从所述安全共享内存中读取所述异常事件的相关信息，并采用广播方式向包括所述目标 CA 在内的多个 CA 发送所述异常事件的相关信息。

20 综上所述，本实施例提供的装置，通过 TA 在检测到存在异常事件的情况下，主动将异常事件的相关信息发送给目标对象，解决了现有方案中异常事件上报不及时的问题，提高了 TA 向 CA 或 CP 上报异常事件的及时性。

图 10 是本发明实施例提供的另一种事件上报装置的框图。该装置具有实现上述方法示
25 例中 CA 侧的各个步骤的功能，所述功能可以通过硬件实现，也可通过硬件执行相应的软件实现。该装置可以包括：接收单元 1010 和处理单元 1020。

接收单元 1010，用于接收 TA 发送的异常事件的相关信息，所述异常事件的相关信息由所述 TA 在接收到 TEE 发送的检测指示并根据所述检测指示检测到存在所述异常事件时主动向 CA 发送。

30 处理单元 1020，用于根据所述异常事件的相关信息处理所述异常事件。

在一个示例中，所述接收单元 1010，用于从 TZ Driver 接收所述异常事件的相关信息。其中，所述 TZ Driver 用于从所述 TA 接收所述 CA 的应用标识和所述异常事件的相关信息，并根据所述 CA 的应用标识向所述 CA 发送所述异常事件的相关信息。

在另一示例中，所述接收单元 1010，用于接收由 TZ Driver 采用广播方式发送的所述异常
35 事件的相关信息。其中，所述 TZ Driver 用于从所述 TA 接收所述异常事件的相关信息，并采用所述广播方式向包括所述 CA 在内的多个 CA 发送所述异常事件的相关信息。

在又一示例中，所述接收单元 1010，用于接收由 CP 采用广播方式发送的所述异常事件的相关信息。其中，所述 CP 用于在接收到所述 TA 发送的安全中断之后，在所述 CP 处于安全模式的情况下从安全共享内存中读取由所述 TA 写入的所述异常事件的相关信息，并

采用所述广播方式向包括所述 CA 在内的多个 CA 发送所述异常事件的相关信息,所述安全共享内存是指物理属性在 MMU 中被设置为安全打开状态的共享内存。

综上所述,本实施例提供的装置,通过 TA 在检测到存在异常事件的情况下,主动将异常事件的相关信息发送给 CA,解决了现有方案中异常事件上报不及时的问题,提高了 TA 向 CA 上报异常事件的及时性。

本发明一示例性实施例还提供了一种终端,该终端部署有 TEE 和 REE。TEE 包括如图 9 所示实施例或者基于图 9 所示实施例提供的可选实施例所提供的事件上报装置。REE 包括如图 10 所示实施例或者基于图 10 所示实施例提供的可选实施例所提供的事件上报装置。

需要说明的是:上述实施例提供的装置在实现其功能时,仅以上述各功能模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能模块完成,即将设备的内部结构划分成不同的功能模块,以完成以上描述的全部或者部分功能。另外,上述实施例提供的装置与方法实施例属于同一构思,其具体实现过程详见方法实施例,这里不再赘述。

上述主要从终端的角度对本发明实施例提供的方案进行了介绍。可以理解的是,终端为了实现上述功能,其包含了执行各个功能相应的硬件结构和/或软件模块。结合本发明中所公开的实施例描述的各示例的模块及算法步骤,本发明实施例能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行,取决于技术方案的特定应用和设计约束条件。本领域技术人员可以对每个特定的应用来使用不同的方法来实现所描述的功能,但是这种实现不应认为超出本发明实施例的技术方案的范围。

图 11 是本发明实施例提供的一种终端的框图。该终端用于实现上述方法示例的功能。终端 1100 可以包括:处理器 1101。

处理器 1101 用于实现终端 1100 的各项功能。所述处理器 1101 还用于执行上述方法实施例中的各个步骤,或者本发明所描述的技术方案的其它步骤。

可选地,终端 1100 还包括通信接口 1102。通信接口 1102 用于支持终端 1100 与其他设备之间的通信。

进一步地,终端 1100 还可以包括存储器 1103,存储器 1103 用于存储终端 1100 的程序代码和数据。

此外,终端 1100 还可以包括总线 1104。所述存储器 1103 和所述通信接口 1102 通过总线 1104 与所述处理器 1101 相连。

可以理解的是,图 11 仅仅示出了终端 1100 的简化设计。在实际应用中,终端 1100 可以包含任意数量的通信接口,处理器,存储器等,而所有可以实现本发明实施例的设备都在本发明实施例的保护范围之内。

应当理解的是,在本文中提及的“多个”是指两个或两个以上。“和/或”,描述关联对象的关联关系,表示可以存在三种关系,例如,A 和/或 B,可以表示:单独存在 A,同时存

在 A 和 B，单独存在 B 这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

5 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1、一种事件上报方法，其特征在于，所述方法包括：

可信应用 TA 接收可信执行环境 TEE 发送的检测指示，所述检测指示由所述 TEE 在监
5 测到预设事件后发送，所述预设事件是根据目标对象提供的检测异常事件的需求所设定的
事件，所述目标对象为目标客户应用 CA 或通信处理器 CP；

所述 TA 根据所述检测指示检测是否存在所述异常事件；

若存在所述异常事件，则所述 TA 将所述异常事件的相关信息发送给所述目标对象，以
使得所述目标对象根据所述异常事件的相关信息处理所述异常事件。

10

2、根据权利要求 1 所述的方法，其特征在于，所述目标对象为所述目标 CA，所述 TA
将所述异常事件的相关信息发送给所述目标对象，包括：

所述 TA 向可信区域驱动 TZ Driver 发送所述目标 CA 的应用标识和所述异常事件的相
关信息；

15

其中，所述 TZ Driver 用于根据所述目标 CA 的应用标识向所述目标 CA 发送所述异常
事件的相关信息。

3、根据权利要求 1 所述的方法，其特征在于，所述目标对象为所述目标 CA，所述 TA
将所述异常事件的相关信息发送给所述目标对象，包括：

20

所述 TA 向 TZ Driver 发送所述异常事件的相关信息；

其中，所述 TZ Driver 用于采用广播方式向包括所述目标 CA 在内的多个 CA 发送所述
异常事件的相关信息。

4、根据权利要求 1 所述的方法，其特征在于，所述目标对象为所述目标 CA，所述 TA
25 将所述异常事件的相关信息发送给所述目标对象，包括：

所述 TA 将所述异常事件的相关信息写入安全共享内存，并向 CP 发送安全中断；

30

其中，所述安全共享内存是指物理属性在内存管理单元 MMU 中被设置为安全打开状
态的共享内存，所述安全中断用于触发所述 CP 在处于安全模式的情况下从所述安全共享内
存中读取所述异常事件的相关信息，并采用广播方式向包括所述目标 CA 在内的多个 CA 发
送所述异常事件的相关信息。

5、一种事件上报方法，其特征在于，所述方法包括：

35

客户应用 CA 接收可信应用 TA 发送的异常事件的相关信息，所述异常事件的相关信息
由所述 TA 在接收到可信执行环境 TEE 发送的检测指示并根据所述检测指示检测到存在所
述异常事件时主动向所述 CA 发送；

所述 CA 根据所述异常事件的相关信息处理所述异常事件。

6、根据权利要求 5 所述的方法，其特征在于，所述 CA 接收可信应用 TA 发送的异常
事件的相关信息，包括：

所述 CA 从可信区域驱动 TZ Driver 接收所述异常事件的相关信息；

其中，所述 TZ Driver 用于从所述 TA 接收所述 CA 的应用标识和所述异常事件的相关信息，并根据所述 CA 的应用标识向所述 CA 发送所述异常事件的相关信息。

5 7、根据权利要求 5 所述的方法，其特征在于，所述 CA 接收可信应用 TA 发送的异常事件的相关信息，包括：

所述 CA 接收由 TZ Driver 采用广播方式发送的所述异常事件的相关信息；

其中，所述 TZ Driver 用于从所述 TA 接收所述异常事件的相关信息，并采用所述广播方式向包括所述 CA 在内的多个 CA 发送所述异常事件的相关信息。

10

8、根据权利要求 5 所述的方法，其特征在于，所述 CA 接收可信应用 TA 发送的异常事件的相关信息，包括：

所述 CA 接收由通信处理器 CP 采用广播方式发送的所述异常事件的相关信息；

15 其中，所述 CP 用于在接收到所述 TA 发送的安全中断之后，在所述 CP 处于安全模式的情况下从安全共享内存中读取由所述 TA 写入的所述异常事件的相关信息，并采用所述广播方式向包括所述 CA 在内的多个 CA 发送所述异常事件的相关信息，所述安全共享内存是指物理属性在内存管理单元 MMU 中被设置为安全打开状态的共享内存。

9、一种事件上报装置，其特征在于，所述装置包括：

20 接收单元，用于接收可信执行环境 TEE 发送的检测指示，所述检测指示由所述 TEE 在监测到预设事件后发送，所述预设事件是根据目标对象提供的检测异常事件的需求所设定的事件，所述目标对象为目标客户应用 CA 或通信处理器 CP；

检测单元，用于根据所述检测指示检测是否存在所述异常事件；

25 发送单元，用于当存在所述异常事件时，将所述异常事件的相关信息发送给所述目标对象，以使得所述目标对象根据所述异常事件的相关信息处理所述异常事件。

10、根据权利要求 9 所述的装置，其特征在于，所述目标对象为所述目标 CA；

所述发送单元，用于向可信区域驱动 TZ Driver 发送所述目标 CA 的应用标识和所述异常事件的相关信息；

30 其中，所述 TZ Driver 用于根据所述目标 CA 的应用标识向所述目标 CA 发送所述异常事件的相关信息。

11、根据权利要求 9 所述的装置，其特征在于，所述目标对象为所述目标 CA；

所述发送单元，用于向 TZ Driver 发送所述异常事件的相关信息；

35 其中，所述 TZ Driver 用于采用广播方式向包括所述目标 CA 在内的多个 CA 发送所述异常事件的相关信息。

12、根据权利要求 9 所述的装置，其特征在于，所述目标对象为所述目标 CA；

所述发送单元，用于将所述异常事件的相关信息写入安全共享内存，并向通信处理器

CP 发送安全中断；

其中，所述安全共享内存是指物理属性在内存管理单元 MMU 中被设置为安全打开状态的共享内存，所述安全中断用于触发所述 CP 在处于安全模式的情况下从所述安全共享内存中读取所述异常事件的相关信息，并采用广播方式向包括所述目标 CA 在内的多个 CA 发送所述异常事件的相关信息。

13、一种事件上报装置，其特征在于，所述装置包括：

接收单元，用于接收可信应用 TA 发送的异常事件的相关信息，所述异常事件的相关信息由所述 TA 在接收到可信执行环境 TEE 发送的检测指示并根据所述检测指示检测到存在所述异常事件时主动向客户应用 CA 发送；

处理单元，用于根据所述异常事件的相关信息处理所述异常事件。

14、根据权利要求 13 所述的装置，其特征在于，

所述接收单元，用于从可信区域驱动 TZ Driver 接收所述异常事件的相关信息；

其中，所述 TZ Driver 用于从所述 TA 接收所述 CA 的应用标识和所述异常事件的相关信息，并根据所述 CA 的应用标识向所述 CA 发送所述异常事件的相关信息。

15、根据权利要求 13 所述的装置，其特征在于，

所述接收单元，用于接收由 TZ Driver 采用广播方式发送的所述异常事件的相关信息；

其中，所述 TZ Driver 用于从所述 TA 接收所述异常事件的相关信息，并采用所述广播方式向包括所述 CA 在内的多个 CA 发送所述异常事件的相关信息。

16、根据权利要求 13 所述的装置，其特征在于，

所述接收单元，用于接收由通信处理器 CP 采用广播方式发送的所述异常事件的相关信息；

其中，所述 CP 用于在接收到所述 TA 发送的安全中断之后，在所述 CP 处于安全模式的情况下从安全共享内存中读取由所述 TA 写入的所述异常事件的相关信息，并采用所述广播方式向包括所述 CA 在内的多个 CA 发送所述异常事件的相关信息，所述安全共享内存是指物理属性在内存管理单元 MMU 中被设置为安全打开状态的共享内存。

17、一种计算机可读存储介质，包括指令，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求 1-4 任意一项所述的方法。

18、一种计算机可读存储介质，包括指令，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求 5-8 任意一项所述的方法。

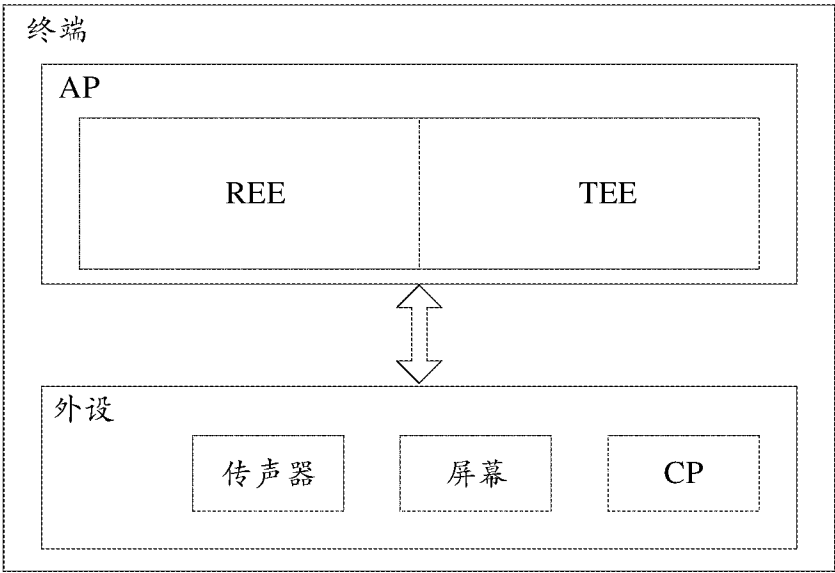


图 1

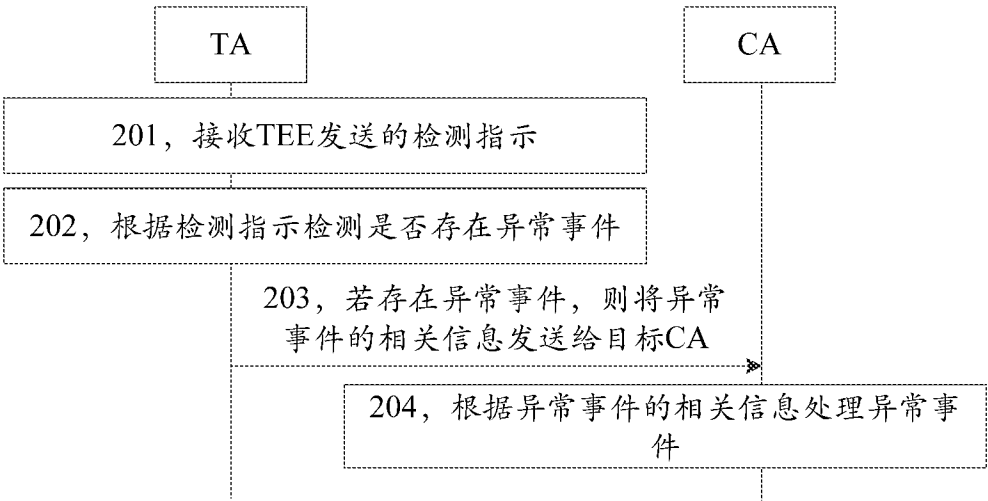


图 2

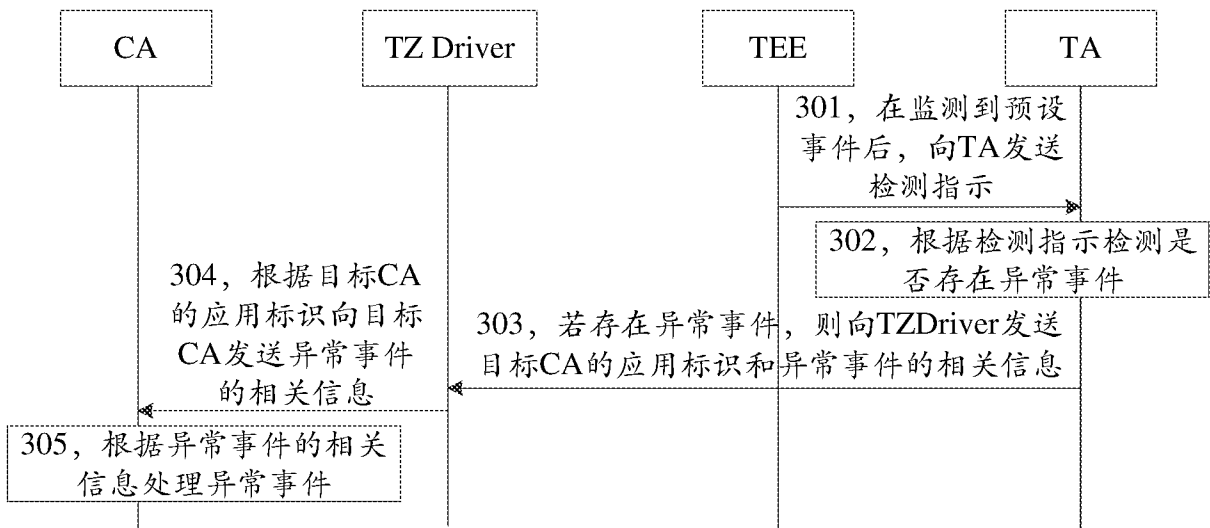


图 3A

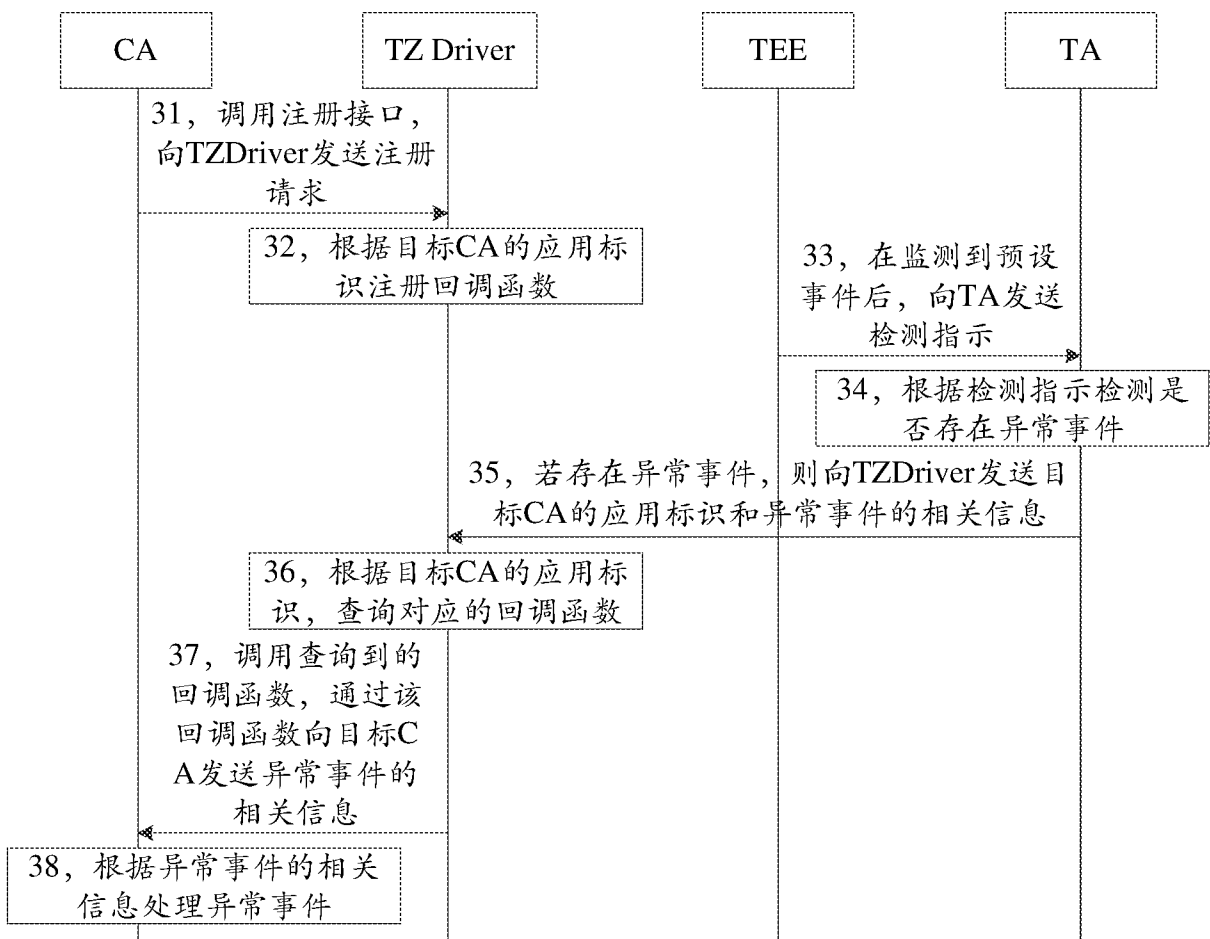


图 3B

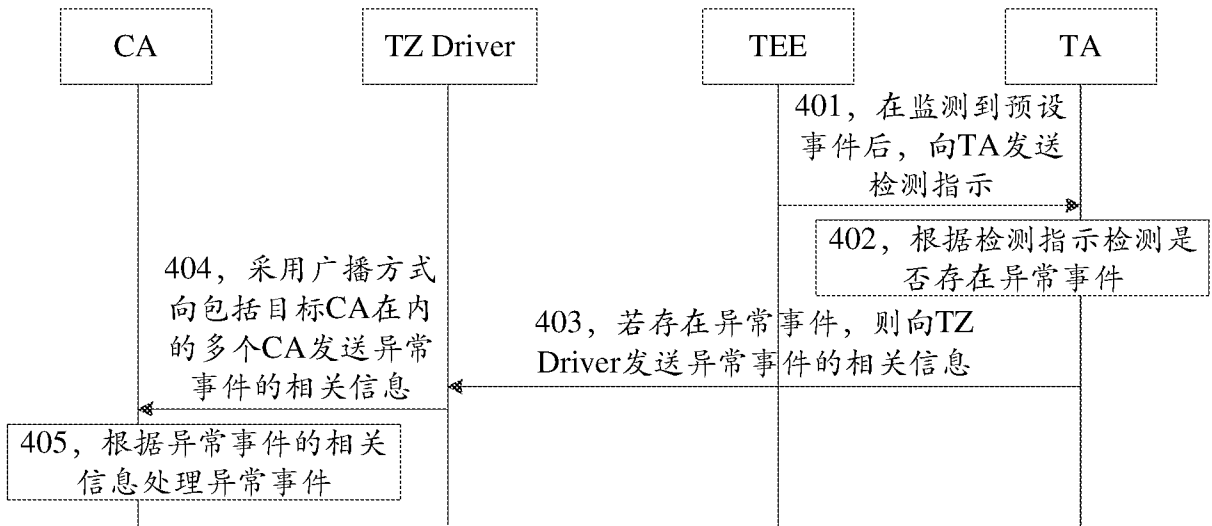


图 4A

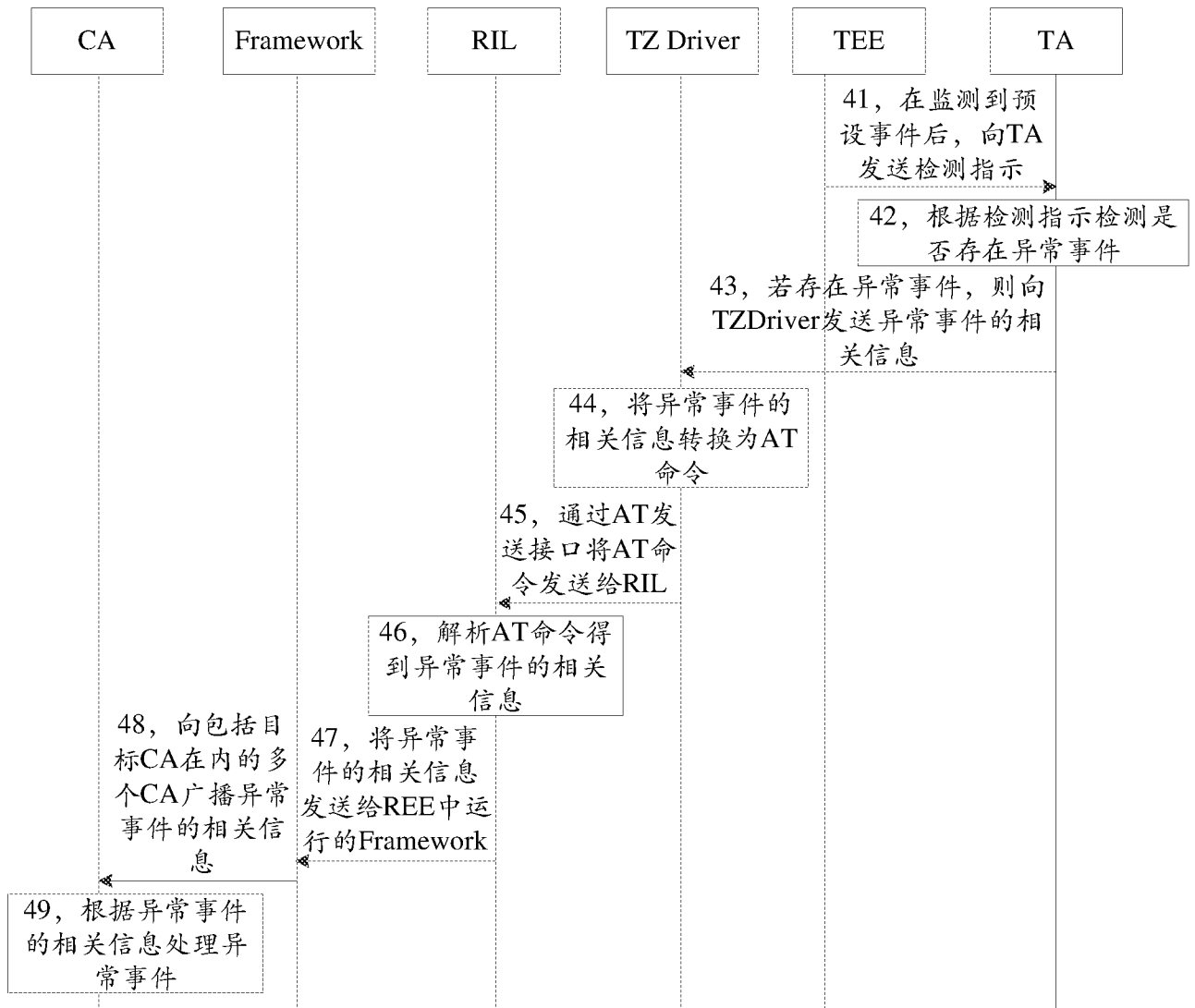


图 4B

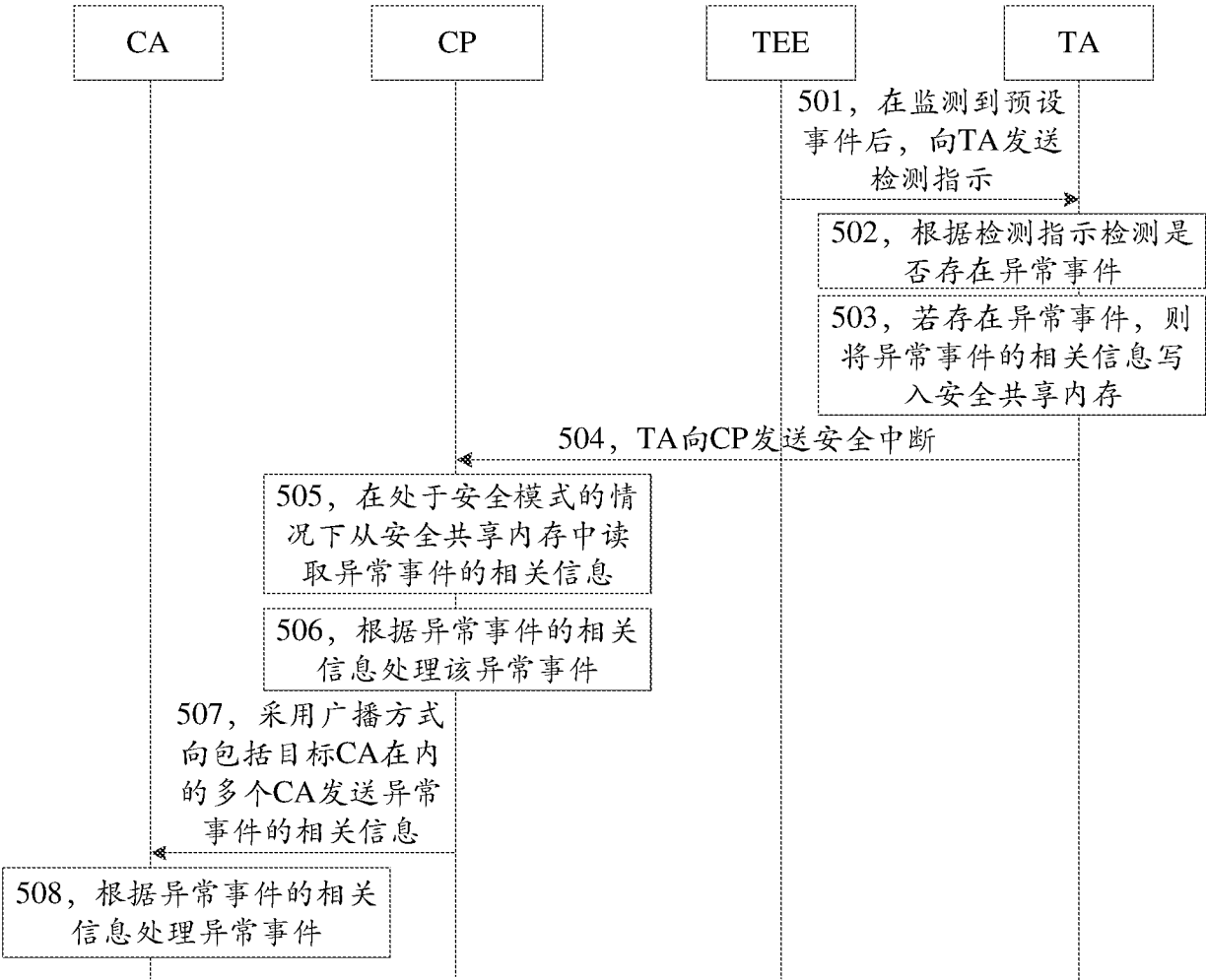


图 5A

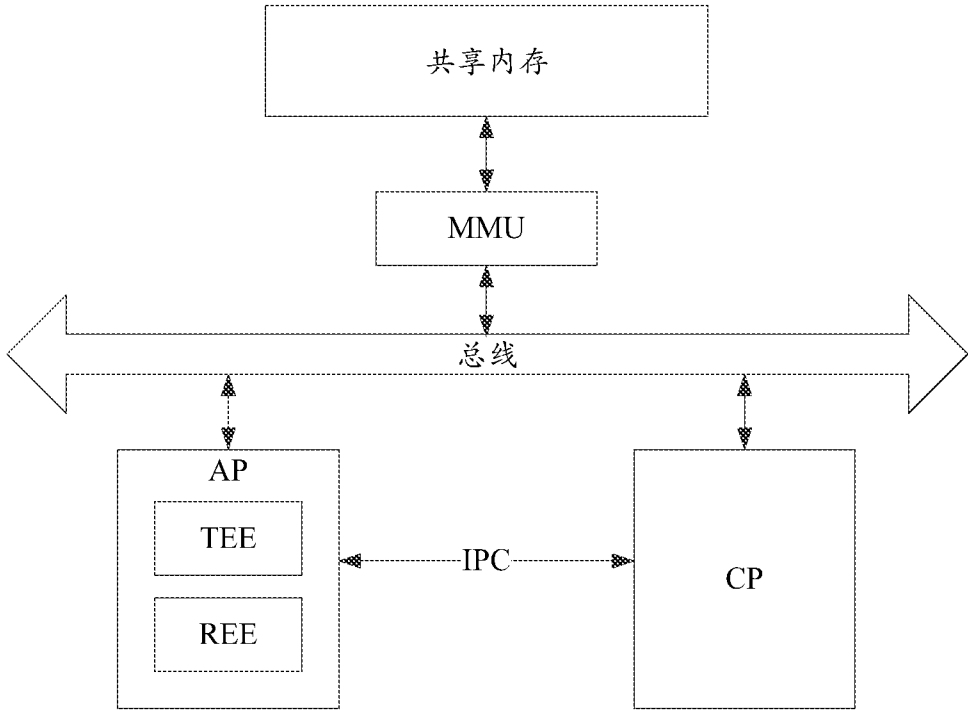


图 5B

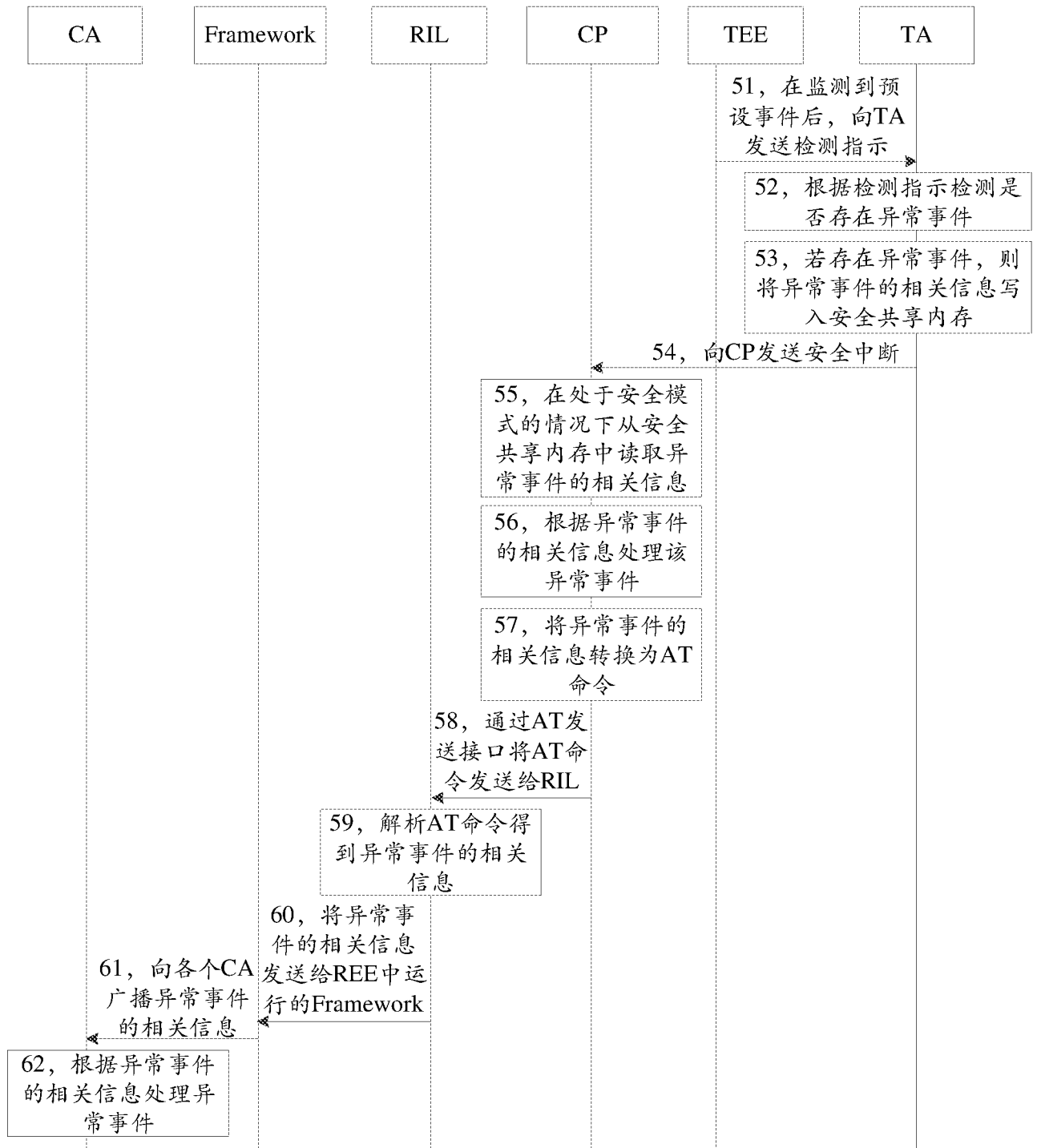


图 5C

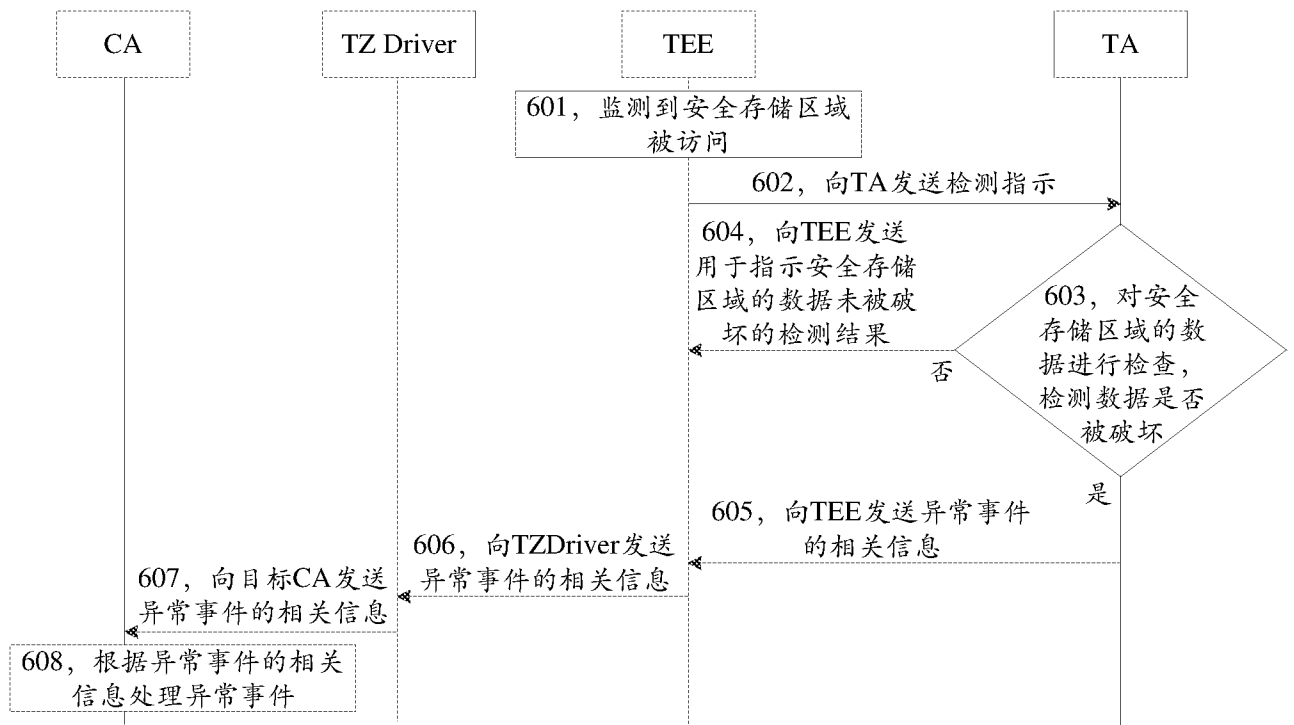


图 6

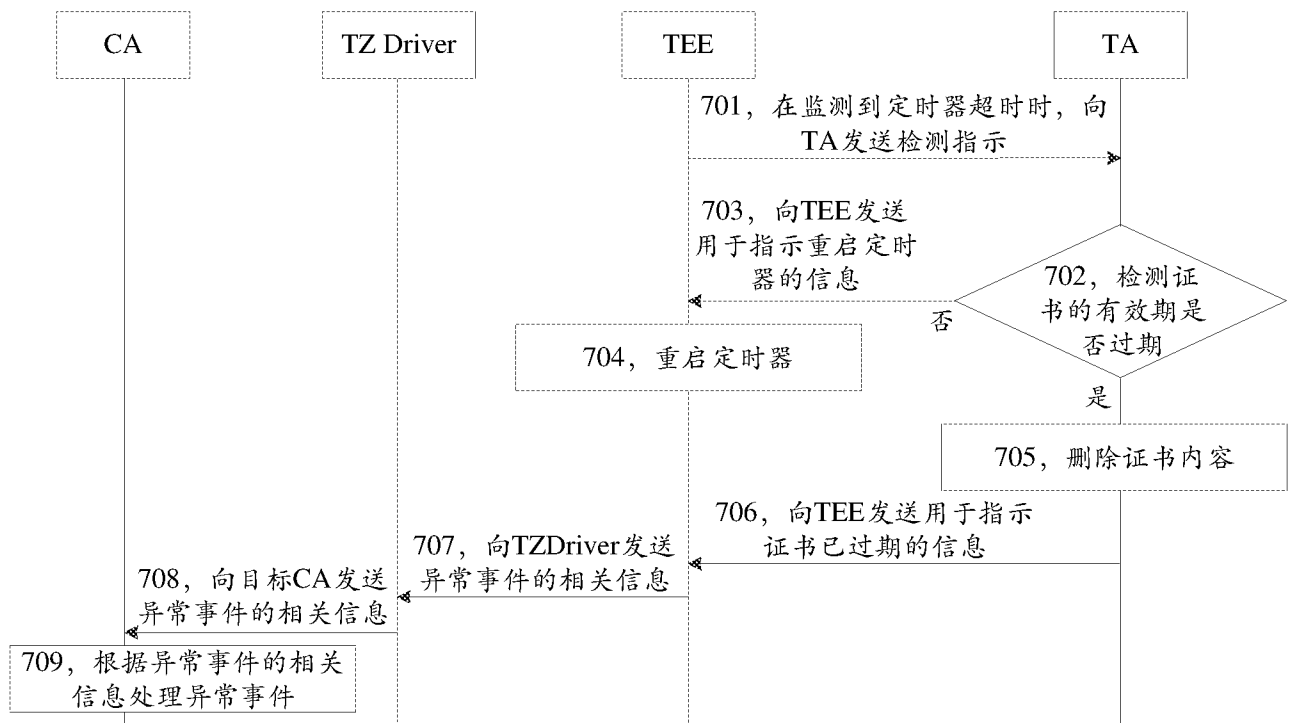


图 7

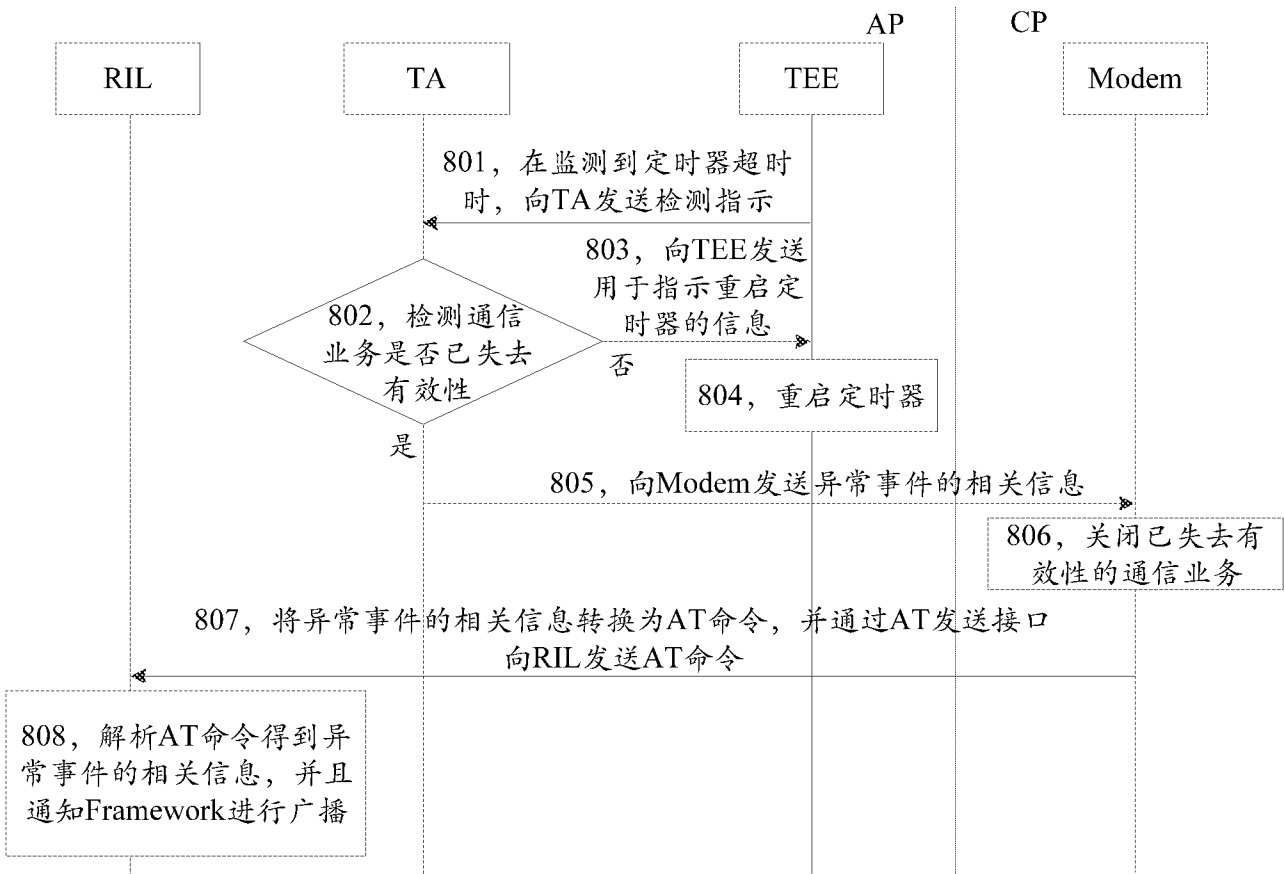


图 8



图 9

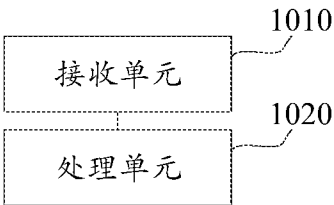


图 10

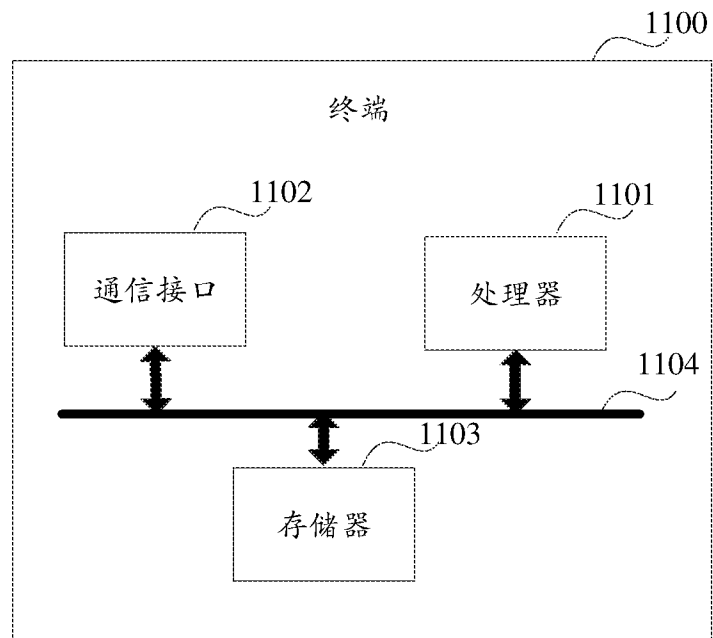


图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/111151

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

H04L; H04W

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)

CPRSABS; CNTXT; CNKI; VEN: 可信, 执行, 环境, 可信应用, 客户应用, 异常, 事件, 发送, 接收, trust, execution, environment, trusted, application), client, application, abnormality, affair, event, send, receive

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106603498 A (HUAWEI TECHNOLOGIES CO., LTD.), 26 April 2017 (26.04.2017), claims 1-16, and description, paragraphs [0230]-[0236]	1-18
A	WO 2016105651 A1 (INTEL CORPORATION), 30 June 2016 (30.06.2016), entire document	1-18
A	CN 105978917 A (HENGBAO CO., LTD.), 28 September 2016 (28.09.2016), entire document	1-18

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 17 January 2018	Date of mailing of the international search report 01 February 2018
Name and mailing address of the ISA 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 CHENG, Dong Telephone No. (86-10) 62411276

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/111151

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106603498 A	26 April 2017	None	
WO 2016105651 A1	30 June 2016	CN 107003889 A	01 August 2017
		US 9444627 B2	13 September 2016
		US 2016191246 A1	30 June 2016
		EP 3238370 A1	01 November 2017
CN 105978917 A	28 September 2016	None	

国际检索报告

国际申请号

PCT/CN2017/111151

A. 主题的分类

H04L 29/06 (2006.01) 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)

H04L; H04W

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))

CPRSABS; CNTXT; CNKI; VEN: 可信, 执行, 环境, 可信应用, 客户应用, 异常, 事件, 发送, 接收, trust, execution, environment, trusted, application), client, application, abnormality, affair, event, send, receive

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
PX	CN 106603498 A (华为技术有限公司) 2017年 4月 26日 (2017 - 04 - 26) 权利要求1-16, 说明书第【0230】-【0236】段	1-18
A	WO 2016105651 A1 (英特尔公司) 2016年 6月 30日 (2016 - 06 - 30) 全文	1-18
A	CN 105978917 A (恒宝股份有限公司) 2016年 9月 28日 (2016 - 09 - 28) 全文	1-18

☐ 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

2018年 1月 17日

国际检索报告邮寄日期

2018年 2月 1日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

程东

传真号 (86-10) 62019451

电话号码 (86-10) 62411276

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/111151

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	106603498	A	2017年 4月 26日	无			
WO	2016105651	A1	2016年 6月 30日	CN	107003889	A	2017年 8月 1日
				US	9444627	B2	2016年 9月 13日
				US	2016191246	A1	2016年 6月 30日
				EP	3238370	A1	2017年 11月 1日
CN	105978917	A	2016年 9月 28日	无			