(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108235767 B
(45)授权公告日 2021.10.26

(21)申请号 201680057108.1
(22)申请日 2016.12.30
(65)同一申请的已公布的文献号
申请公布号 CN 108235767 A
(43)申请公布日 2018.06.29
(66)本国优先权数据
201610953093.9 2016.11.03 CN
(85)PCT国际申请进入国家阶段日
2018.04.04
(86)PCT国际申请的申请数据
PCT/CN2016/113961 2016.12.30
(87)PCT国际申请的公布数据
WO2018/082189 ZH 2018.05.11
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 吴波
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 冯艳莲
(51)Int.Cl.
G06F 21/74(2013.01)
G06Q 20/38(2012.01)
(56)对比文件
US 2014157363 A1,2014.06.05
杨波等.基于TrustZone 的可信移动终端云服务安全接入方案.《软件学报》.2016,第27卷(第6期),全文.
Jaewon Choi et al..Isolated Mini-domain for Trusted Cloud Computing.《2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing》.2013,全文.
审查员 李莎

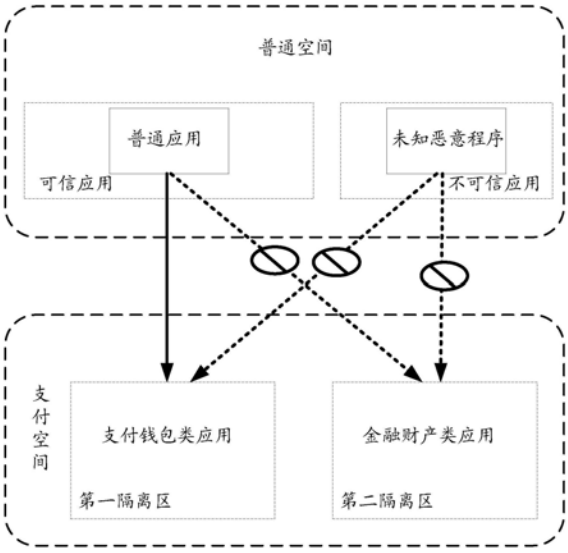
权利要求书3页 说明书11页 附图13页

(54)发明名称

一种支付应用的隔离方法、装置及终端

(57)摘要

一种支付应用的隔离方法、装置及终端。在该支付应用的隔离方法中,获取用户选择的、待添加到隔离区的支付应用;若待添加的所述支付应用具有添加到第一隔离区的属性,则将待添加的所述支付应用添加到第一隔离区;若待添加的所述支付应用具有添加到第二隔离区的属性,则将待添加的所述支付应用添加到第二隔离区;其中,添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用调用的属性,添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性,能够兼顾用户使用支付应用的方便性和支付应用的安全性。



CN 108235767 B

1.一种支付应用的隔离方法,其特征在于,应用于终端,所述方法包括:

获取用户选择的、待添加到隔离区的支付应用;

若待添加的所述支付应用具有添加到第一隔离区的属性,则将待添加的所述支付应用添加到第一隔离区;

若待添加的所述支付应用具有添加到第二隔离区的属性,则将待添加的所述支付应用添加到第二隔离区;

其中,添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用调用的属性,添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性,所述可信应用为安装在所述终端上的应用,所述安装在所述第二隔离区之外的应用为安装在所述终端上的应用;

其中,所述终端中创建有终端主用户和终端子用户,所述终端子用户为终端主用户的隐藏用户;

所述将待添加的所述支付应用添加到第二隔离区,包括:

将待添加的所述支付应用添加到所述终端子用户中,所述第二隔离区属于所述终端子用户;

其中,添加到第一隔离区内的支付应用为支付钱包类应用,添加到第二隔离区内的支付应用为金融财产类应用。

2.如权利要求1所述的方法,其特征在于,将待添加的所述支付应用添加到所述终端子用户中之后,所述方法还包括:

删除所述终端子用户的非必要进程。

3.如权利要求1所述的方法,其特征在于,所述终端中创建有终端主用户和终端子用户;

所述将待添加的所述支付应用添加到第一隔离区,包括:

将待添加的所述支付应用添加到所述终端主用户,所述第一隔离区属于所述终端主用户

将待添加的所述支付应用添加到所述终端主用户之后,所述方法还包括:

在终端主用户的显示界面上,以不同于普通应用显示方式的显示方式显示添加到所述第一隔离区的支付应用。

4.如权利要求1至3任一项所述的方法,其特征在于,将待添加的所述支付应用添加到第一隔离区之后,所述方法还包括:

若检测到未知恶意程序访问添加到所述第一隔离区内的支付应用,则拦截所述未知恶意程序的访问,并显示提示信息,所述提示信息用于提示存在未知恶意程序。

5.如权利要求1至3任一项所述的方法,其特征在于,添加到第一隔离区和第二隔离区内的支付应用为支付专区内预先创建的支付应用;

所述获取用户选择的、待添加到隔离区的支付应用之后,所述方法还包括:

确定支付专区内存在与待添加的所述支付应用相同的支付应用。

6.一种支付应用的隔离装置,其特征在于,应用于终端,包括:

获取单元,用于获取用户选择的、待添加到隔离区的支付应用;

处理单元,用于若确定所述获取单元获取的待添加的所述支付应用具有添加到第一隔

离区的属性，则将待添加的所述支付应用添加到第一隔离区；若确定所述获取单元获取的待添加的所述支付应用具有添加到第二隔离区的属性，则将待添加的所述支付应用添加到第二隔离区；

其中，添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用调用的属性，添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性，所述可信应用为安装在所述终端上的应用，所述安装在所述第二隔离区之外的应用为安装在所述终端上的应用；

其中，所述终端中创建有终端主用户和终端子用户，所述终端子用户为终端主用户的隐藏用户；

所述处理单元采用如下方式将待添加的所述支付应用添加到第二隔离区：

将待添加的所述支付应用添加到所述终端子用户中，所述第二隔离区属于所述终端子用户；

其中，添加到第一隔离区内的支付应用为支付钱包类应用，添加到第二隔离区内的支付应用为金融财产类应用。

7.如权利要求6所述的装置，其特征在于，所述处理单元还用于：

将待添加的所述支付应用添加到所述终端子用户中之后，删除所述终端子用户的非必要进程。

8.如权利要求6所述的装置，其特征在于，所述终端中创建有终端主用户和终端子用户，所述终端子用户为终端主用户的隐藏用户；

所述处理单元采用如下方式将待添加的所述支付应用添加到第一隔离区：

将待添加的所述支付应用添加到所述终端主用户，所述第一隔离区属于所述终端主用户；

所述终端中包括的显示单元，用于在所述处理单元将待添加的所述支付应用添加到所述终端主用户之后，在终端主用户的显示界面上，以不同于普通应用显示方式的显示方式显示添加到所述第一隔离区的支付应用。

9.如权利要求6至8任一项所述的装置，其特征在于，所述处理单元，还用于：

将待添加的所述支付应用添加到第一隔离区之后，若检测到未知恶意程序访问添加到所述第一隔离区内的支付应用，则拦截所述未知恶意程序的访问；

所述装置中包括的显示单元，用于显示提示信息，所述提示信息用于提示存在未知恶意程序。

10.如权利要求6至8任一项所述的装置，其特征在于，添加到第一隔离区和第二隔离区内的支付应用为支付专区内预先创建的支付应用；

所述获取单元，还用于：

获取用户选择的、待添加到隔离区的支付应用之后，确定支付专区内存在与待添加的所述支付应用相同的支付应用。

11.一种终端，其特征在于，包括处理器、存储器、显示设备和输入设备；

所述输入设备、所述显示设备、所述存储器均通过总线与所述处理器连接，其中，

所述输入设备，用于获取用户选择支付应用的输入指令；

所述存储器，用于存储所述处理器执行的程序代码；

所述处理器，用于调用所述存储器存储的程序代码，通过所述输入设备获取的输入指令获取用户选择的、待添加到隔离区的支付应用，并执行如下功能：

若确定待添加的所述支付应用具有添加到第一隔离区的属性，则将待添加的所述支付应用添加到第一隔离区；若确定待添加的所述支付应用具有添加到第二隔离区的属性，则将待添加的所述支付应用添加到第二隔离区；其中，添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用调用的属性，添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性；

所述显示设备，用于在所述处理器的控制下显示待添加的所述支付应用的应用图标，所述可信应用为安装在所述终端上的应用，所述安装在所述第二隔离区之外的应用为安装在所述终端上的应用；

其中，所述终端中创建有终端主用户和终端子用户，所述终端子用户为终端主用户的隐藏用户；

所述处理器采用如下方式将待添加的所述支付应用添加到第二隔离区：

将待添加的所述支付应用添加到所述终端子用户中，所述第二隔离区属于所述终端子用户；

其中，添加到第一隔离区内的支付应用为支付钱包类应用，添加到第二隔离区内的支付应用为金融财产类应用。

12.如权利要求11所述的终端，其特征在于，所述处理器还用于：

将待添加的所述支付应用添加到所述终端子用户中之后，删除所述终端子用户的非必要进程。

13.如权利要求11所述的终端，其特征在于，所述终端中创建有终端主用户和终端子用户，所述终端子用户为终端主用户的隐藏用户；

所述处理器采用如下方式将待添加的所述支付应用添加到第一隔离区：

将待添加的所述支付应用添加到所述终端主用户中，所述第一隔离区属于所述终端主用户；

所述处理器还用于：

在将待添加的所述支付应用添加到所述终端主用户之后，控制所述显示设备在终端主用户的显示界面上，以不同于普通应用显示方式的显示方式显示添加到所述第一隔离区的支付应用。

14.如权利要求11至13任一项所述的终端，其特征在于，所述处理器，还用于：

将待添加的所述支付应用添加到第一隔离区之后，若检测到未知恶意程序访问添加到所述第一隔离区内的支付应用，则拦截所述未知恶意程序的访问；

所述显示设备，还用于显示提示信息，所述提示信息用于提示存在未知恶意程序。

15.如权利要求11至13任一项所述的终端，其特征在于，添加到第一隔离区和第二隔离区内的支付应用为支付专区内预先创建的支付应用；

所述处理器，还用于：

通过输入设备获取用户选择的、待添加到隔离区的支付应用之后，确定支付专区内存在与待添加的所述支付应用相同的支付应用。

一种支付应用的隔离方法、装置及终端

[0001] 本申请要求2016年11月03日提交、申请号为201610953093.9、发明名称为“一种移动终端上支付应用的保护方法和设备”的专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及通信技术领域，尤其涉及一种支付应用的隔离方法、装置及终端。

背景技术

[0003] 随着通信技术的发展，终端能够实现的功能越来越强大，使用范围和环境也越来越多样化，例如目前在终端中使用各种各样的支付财产类应用实现移动支付的功能越来越普及。

[0004] 终端使用支付应用实现移动支付功能，方便了用户进行财产的支付，但是会面临财产被盗取的风险。例如，盗取财产的未知恶意应用通过访问终端上安装的支付财产类应用，可盗取用户的财产。目前，为了避免用户财产被盗取，提高终端上安装的支付应用的使用安全性，一般是将支付应用安装于一个独立空间，该独立空间内的支付应用和独立空间外的应用完全隔离，使得空间外盗取财产的未知恶意应用无法访问独立空间内的支付财产类应用。

[0005] 然而，安装在终端上的支付应用，不可避免的会被终端上安装的一些普通应用调用，被普通应用调用的支付应用通常是用户使用频率较高的应用，这些使用频率较高的应用若安装在独立空间内，则会给用户的使用带来极大的不便。

发明内容

[0006] 本申请实施例提供一种支付应用的隔离方法、装置及终端，以在保证支付应用使用安全性的前提下，兼顾用户使用的方便性。

[0007] 第一方面，提供一种支付应用的隔离方法，终端获取用户选择的、待添加到隔离区的支付应用。若待添加的所述支付应用具有添加到第一隔离区的属性，则将待添加的所述支付应用添加到第一隔离区。若待添加的所述支付应用具有添加到第二隔离区的属性，则将待添加的所述支付应用添加到第二隔离区。其中，添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用调用的属性，添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性，不允许任何其它应用调用。

[0008] 本申请实施例中将待添加到隔离区的支付应用，按照支付应用具备添加到第一隔离区或第二隔离区的属性，将具有能够被安装在所述第一隔离区之外的可信应用调用的支付应用添加到第一隔离区内，以在提供安全保护的前提下方便可信应用调用。将具有与安装在所述第二隔离区之外的应用完全隔离的支付应用添加到第二隔离区内，以提供高安全级别的安全保护。通过上述方法能够兼顾用户使用支付应用的方便性和支付应用的安全性。

[0009] 其中，添加到第一隔离区内的支付应用可为支付钱包类应用，添加到第二隔离区内的支付应用可为金融财产类应用。

[0010] 一种可能的设计中，预先创建支付专区，在预先创建的支付专区内包括添加到第一隔离区和第二隔离区内的支付应用。获取用户选择的、待添加到隔离区的支付应用之后，确定支付专区内存在与待添加的所述支付应用相同的支付应用，以便能够确定待添加的支付应用添加到第一隔离区或第二隔离区的属性信息。

[0011] 另一种可能的设计中，将第一隔离区和第二隔离区创建到不同的终端用户中，例如将第一隔离区安装到终端主用户中，而将第二隔离区安装到终端子用户中，并将安装了第二隔离区的终端子用户设置为隐藏用户，以便进一步提高安全性。

[0012] 又一种可能的设计中，将待添加到第二隔离区的支付应用添加到所述终端子用户中后，可删除创建第二隔离区的终端子用户的非必要进程，通过对非必要进程进行裁剪，以在保证安全的同时，减轻资源和内存消耗。

[0013] 又一种可能的设计中，将待添加到第一隔离区的支付应用添加到所述终端主用户之后，在终端主用户的显示界面上，以不同于普通应用显示方式的显示方式显示添加到所述第一隔离区的支付应用，以方便用户能够确定进行安全保护的支付应用。

[0014] 又一种可能的设计中，将待添加的所述支付应用添加到第一隔离区之后，若检测到未知恶意程序访问添加到所述第一隔离区内的支付应用，则拦截所述未知恶意程序的访问，并显示提示信息，所述提示信息用于提示存在未知恶意程序。

[0015] 第二方面，提供一种支付应用的隔离装置，该支付应用的隔离装置具有实现上述第一方面涉及的支付应用隔离方法的功能。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。

[0016] 一种可能的设计中，支付应用的隔离装置包括获取单元和处理单元，其中，获取单元和处理单元的功能与可以和各方法步骤相对应，在此不予赘述。

[0017] 第三方面，提供一种终端，该终端包括处理器、存储器、显示设备和输入设备；所述输入设备、所述显示设备、所述存储器可通过总线与所述处理器连接，其中，所述存储器，用于存储所述处理器执行的程序代码。用户通过所述输入设备选择在所述终端上待添加的支付应用。所述处理器，用于调用所述存储器存储的程序代码，通过所述输入设备获取用户选择的、待添加到隔离区的支付应用，控制显示设备显示支付应用的应用图标，并完成如第一方面中所涉及的任意一种支付应用隔离方法。所述显示设备用于在所述处理器的控制下显示支付应用。

[0018] 本申请实施例提供的支付应用的隔离方法、装置及终端，将具有能够被安装在所述第一隔离区之外的可信应用调用的支付应用添加到第一隔离区内，以在提供安全保护的前提下方便可信应用调用。将具有与安装在所述第二隔离区之外的应用完全隔离的支付应用添加到第二隔离区内，以提供高安全级别的安全保护。通过上述方法能够兼顾用户使用支付应用的方便性和支付应用的安全性。

附图说明

[0019] 图1为本申请实施例提供的终端的一种结构示意图；

[0020] 图2A至图2B为本申请实施例提供的隔离支付应用的交互示意图；

[0021] 图3为本申请实施例提供的支付应用的隔离方法的实现流程图；

[0022] 图4A至图4E为本申请实施例提供的将支付应用添加到不同安全级别的隔离区内的过程示意图；

[0023] 图5为本申请实施例提供的添加支付应用的流程示意图；

[0024] 图6为本申请实施例提供的终端主用户中支付应用的显示示意图；

[0025] 图7为本申请实施例提供的隔离后的支付应用的另一交互示意图；

[0026] 图8为本申请实施例提供的支付应用的隔离装置的结构示意图。

具体实施方式

[0027] 本申请实施例提供的支付应用的隔离方法，可应用于终端。需要理解的是，本申请实施例中涉及的终端，还可称之为移动终端(Mobile Terminal)、移动台(Mobile Station，MS)、用户设备(User Equipment，UE)等。该终端，可以是向用户提供语音和/或数据连通性的设备，具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备，比如：该终端可以是移动电话(或称为“蜂窝”电话)、具有移动终端的计算机等，还可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置，当然也可以是可穿戴设备(如智能手表、智能手环等)、平板电脑、个人电脑(Personal Computer，PC)、个人数字助理(Personal Digital Assistant，PDA)、POS(销售终端，Point of Sales)等。

[0028] 图1所示为本申请实施例涉及的终端100的一种可选的硬件结构示意图。

[0029] 如图1所示，终端100内部可包括处理器101，分别与处理器101连接的存储器102、显示设备103和输入设备104。其中，存储器102可用于存储程序和数据，包括本申请实施例中涉及的支付应用的程序，处理器101通过运行存储在存储器102的程序从而执行终端100的各种功能应用以及数据处理，例如执行终端100的支付应用的隔离功能。

[0030] 下面结合图1对终端100的各个构成部件进行具体的介绍：

[0031] 处理器101是终端100的控制中心，利用各种接口和线路连接整个终端的各个部分，通过运行或执行存储在存储器102内的程序(或称为“模块”)，以及调用存储在存储器102内的数据，执行终端100的各种功能和处理数据，从而对终端100进行整体监控。

[0032] 可选的，处理器101可包括至少一个处理单元；可选地，处理器101可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器101中。

[0033] 存储器102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(比如：安卓操作系统，简称“安卓系统”，其中，操作系统也可简称为“系统”)、至少一个功能所需的应用程序(比如声音播放功能、图象播放功能等)，以及本申请实施例涉及的至少一个支付应用的程序等。存储数据区可存储根据终端100的使用所创建的数据，包括本申请实施例中涉及的支付应用的相关设置信息或使用情况信息等。此外，存储器102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。

[0034] 输入设备104可用于接收输入的数字或字符信息，以及产生与终端100的用户设置以及功能控制有关的键信号输入的输入指令，包括本申请实施例中涉及的用户选择在终端

上添加的支付应用的输入指令。具体地，输入设备104可包括触控面板1041以及其他输入设备1042。触控面板1041，也称为触摸屏，可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触控面板1041上或在触控面板1041附近的操作)，并根据预先设定的程式驱动相应的连接装置。可选的，触控面板1041可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给处理器101，并能接收处理器101发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触控面板1041。除了触控面板1041，输入设备104还可以包括其他输入设备1042。具体地，其他输入设备1042可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0035] 显示设备103可用于显示由用户输入的信息或提供给用户的信息以及终端100的各种菜单，包括本申请实施例中涉及的支付应用的信息。显示设备103可包括显示面板1031，可选的，可以采用液晶显示器(Liquid Crystal Display，LCD)、有机发光二极管(Organic Light-Emitting Diode，OLED)等形式来配置显示面板1031。进一步的，触控面板1041可覆盖显示面板1031，当触控面板1041检测到在其上或附近的触摸操作后，传送给处理器101以确定触摸事件的类型，随后处理器101根据触摸事件的类型在显示面板1031上提供相应的视觉输出。虽然在图1中，触控面板1041与显示面板1031是作为两个独立的部件来实现终端100的输入和输入功能，但是在某些实施例中，可以将触控面板1041与显示面板1031集成而实现终端100的输入和输出功能。

[0036] 本领域技术人员可以理解，图1中示出的终端100的内部结构并不构成对终端的限定，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。例如终端100还可包括提供用户与终端100之间音频接口的音频电路、扬声器和麦克风等。当终端100采用无线方式与外界通信时，还可包括射频(Radio Frequency，RF)电路和连接的天线，无线保真(Wireless Fidelity，WiFi)模块和连接的天线等。此外，终端100还包括传感器以及为其供电的电源等，在此不再一一列举。

[0037] 本申请实施例中，处理器101通过运行存储器102中存储的操作系统，调用存储器102中存储的程序，通过所述输入设备104获取的输入指令获取用户选择的、待添加到隔离区的支付应用，控制显示设备103显示支付应用以及其他应用的应用图标，并执行如下功能：若确定待添加的所述支付应用具有添加到第一隔离区的属性，则将待添加的所述支付应用添加到第一隔离区；若确定待添加的所述支付应用具有添加到第二隔离区的属性，则将待添加的所述支付应用添加到第二隔离区；其中，添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用调用的属性，添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性，以在保证支付应用使用安全性的前提下，兼顾用户使用的方便性。

[0038] 本申请实施例中涉及的应用指的是安装在终端上的应用程序，支付应用指的是安装在终端上能够执行财产支付的应用程序。可信应用是指可以访问第一隔离区内的支付应用的应用程序。该可以访问第一隔离区内的支付应用的应用程序可采用预定义的方式设定，具体的预定义方式不限定，例如可以是预定义通过终端上安装的具有安全防护功能的

应用程序验证之后的应用程序为可信应用，也可是预定义终端上已安装或其它应用市场上的具有设定功能属性的应用程序为可信应用。

[0039] 本申请实施例中终端的处理器可将安装在终端上的应用划分为支付应用和普通应用，并将支付应用安装在支付空间，普通应用安装在普通空间，其中，支付空间和普通空间可理解为是终端上被逻辑划分的两个独立的逻辑单元，如图2A所示。本申请实施例中涉及的支付应用指的是安装在终端上的能够执行财产支付的应用程序。本申请实施例涉及的普通应用指的是安装在终端上的非支付应用。安装在终端上的支付应用可包括支付钱包类应用和金融财产类应用。支付钱包类应用的使用场景一般是通过被普通应用程序调用实现支付，例如支付宝、淘宝、京东钱包、微信等可以认为是支付钱包类应用。金融财产类应用相对支付钱包类应用而言，一般不会被普通应用程序调用，例如中国工商银行、招商银行、农业银行、中国银行等银行的应用，以及证券、理财等的应用可以认为是金融财产类应用。

[0040] 本申请实施例中，为兼顾用户使用支付应用的方便性和支付应用的安全性，终端的处理器可在终端上设置不同的隔离区，不同的隔离区提供不同安全级别的隔离效果。安全级别低的隔离区内添加的支付应用能够与其它应用之间进行交互，安全级别高的隔离区内添加的支付应用与其他应用不能交互。例如，对支付应用进行隔离保护的隔离区包括第一隔离区和第二隔离区。添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用(诸如普通应用)调用的属性，添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性，不允许任何其它应用调用。例如，图2A中终端的处理器可将支付钱包类应用添加至第一隔离区，将金融财产类应用添加至第二隔离区。第一隔离区内的支付钱包类应用能够被可信应用调用与访问，而不能被不可信的应用(诸如未知恶意程序)调用与访问，第二隔离区内的金融财产类应用不能被任何应用程序(普通应用和未知恶意程序)调用与访问，进而能够兼顾用户使用支付应用的方便性和支付应用的安全性。本申请实施例中可由按照在终端上具有安全防护功能的应用程序识别普通应用和未知恶意程序，例如通过终端上安装的手机卫士识别普通应用和未知恶意程序。图2B是图2A的一个示例性说明，图2B中被添加到第一隔离区的支付宝和微信，能够被添加到普通空间的淘宝和京东等可信应用调用与访问，被添加到第二隔离区的招商银行和同花顺，不能够被添加安装在第二隔离区以外的其它应用调用与访问，例如不能被添加到普通空间内的应用调用与访问。

[0041] 图3所示为本申请实施例提供的支付应用的隔离方法的实现流程图。

[0042] S101：获取用户选择的、待添加到隔离区的支付应用。

[0043] 本申请实施例中待添加到隔离区的支付应用是由用户选择的。一种实施方式中，待添加到隔离区的支付应用是由用户确定并选择的，用户通过终端的显示设备输入选择指令后，终端即可确定该应用为待添加到隔离区的支付应用。另一种实施方式中，待添加到隔离区的支付应用是由终端确定的，用户通过终端的输入设备输入选择指令后，终端根据用户输入的选择指令，确定用户选择的支付应用是否为待添加到隔离区的支付应用。

[0044] 本申请实施例中用户可通过终端的输入设备输入选择待添加到隔离区的支付应用的选择指令可有多种实现方式，例如用户通过在终端的触摸屏进行点击等选取操作，由触摸屏感应该选取操作后确定用户选择的待添加到隔离区的支付应用。终端的处理器通过触摸屏可获取用户选择的、待添加到隔离区的支付应用。

[0045] 本申请实施例中终端的处理器可预定义添加到不同隔离区的支付应用。例如若终端的处理器将支付应用划分为支付钱包类应用和金融财产类应用，对支付应用进行隔离保护的隔离区包括第一隔离区和第二隔离区。添加到所述第一隔离区内的支付应用能够被可信应用调用，添加到所述第二隔离区内的支付应用与安装在所述第二隔离区之外的应用完全隔离。例如，添加到第一隔离区内的支付应用为支付钱包类应用，添加到第二隔离区内的支付应用为金融财产类应用。

[0046] 本申请实施例中终端的处理器获取用户选择的、待添加到隔离区的支付应用后，可根据该待添加的支付应用具备的属性信息，将支付应用添加到与第一隔离区或第二隔离区内。其中，支付应用具备的属性信息主要是指支付应用添加到第一隔离区或第二隔离区的属性信息。添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用调用的属性，添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性。

[0047] S102：若待添加的所述支付应用具有添加到第一隔离区的属性，则将待添加的所述支付应用添加到第一隔离区。

[0048] S103：若待添加的所述支付应用具有添加到第二隔离区的属性，则将待添加的所述支付应用添加到第二隔离区。

[0049] 下面将结合实际应用，首先介绍本申请实施例提供的将支付应用添加到不同安全级别的隔离区内的具体实现过程。

[0050] 本申请实施例中，终端上可安装支付空间的应用(APP)，该支付空间中设置有不同安全级别隔离区。在终端显示界面上显示该支付空间的应用图标，用户通过在终端显示界面上通过诸如点击等操作选择支付空间的应用图标，可启动支付空间并进入支付空间。例如图4A中用户在终端显示界面上选择支付空间的应用图标后，可进入图4B所示的名称为支付保护中心的支付空间中。本申请实施例中以将支付空间命名为支付保护中心为例进行说明，当然具体的命名名称不限定。本申请实施例以下涉及的支付保护中心可以理解为是支付空间。在图4B所示的支付空间内可显示用于提示用户添加支付应用到支付保护中心中的图标，用户选择该添加图标后，可选择添加的支付应用到支付保护中心中。一种可能的实施方式中，用户可选择终端本地已安装的支付类应用到支付保护中心中，例如图4C中用户选择已通过安全检测的本地支付类应用添加到支付保护中心中，图4C中被用户选中的待添加到支付保护中心中的支付应用显示图标上面以“√”形式表示。另一种可能的实施方式中，本申请实施例中用户可选择在支付专区内下载正版的支付应用添加到支付保护中心中。其中，所述支付专区可以理解为是提供添加到第一隔离区和第二隔离区内的支付应用的应用商店。

[0051] 一种可能的实施方式中，本申请实施例中终端的处理器可预先创建支付专区，在预先创建的支付专区内包括待添加到第一隔离区和第二隔离区内的支付应用。通过所述支付专区可下载获取到添加到第一隔离区和第二隔离区内的支付应用。该支付专区可以通过云端建立，并在支付空间内提供接入支付专区的入口链接。例如图4D中显示的名称为“添加更多正版应用”的图标的应用程序可认为是提供接入支付专区的入口链接。用户采用上述实施例的方式启动支付空间后，用户通过点击所述入口链接可接入支付专区，如图4E所示。本申请实施例中图4E所示的支付专区所显示的支付应用仅是进行示意性说明，该支付专区

内未完全显示出待添加到第一隔离区和第二隔离区的支付应用。用户可通过支付专区上所显示的“搜索正版应用”搜索查询其它未显示的支付应用。用户在支付专区内选择需要添加到第一隔离区或第二隔离区内的支付应用。

[0052] 本申请实施例中用户选择完待添加到隔离区内的之后应用后，终端的处理器可直接将待添加的支付应用添加到第一隔离区或第二隔离区内。

[0053] 本申请实施例中在支付专区内的支付应用具有添加到第一隔离区或第二隔离区的属性信息。用户在支付专区内下载获取到的支付应用可直接添加到第一隔离区或第二隔离区内。

[0054] 需要说明的是，本申请实施例中添加到隔离区内的支付应用中并不限定一定来自支付专区，例如可以是终端上未创建隔离区之前已安装的支付应用，当终端创建隔离区后，可在显示设备显示提示信息，以提示用户是否将已安装的支付应用添加到创建的隔离区内。本申请实施例一种可能的实施方式中，用户向隔离区内添加非支付专区内的支付应用，可与支付专区内的支付应用完全一致，即终端的处理器通过输入设备获取用户选择的、待添加到隔离区的支付应用之后，需确定支付专区内存在与待添加的所述支付应用相同的支付应用，以便终端的处理器在添加支付应用到隔离区时，可确定支付应用是否具有添加到第一隔离区或第二隔离区的属性信息。

[0055] 需要说明的是，本发明实施例中所述支付应用相同是指具有主体功能相同的支付应用，并不限定诸如版本信息等属性信息相同，例如不同版本的同一支付应用可以理解为是相同的支付应用。

[0056] 本申请实施例中对终端的处理器确定支付应用是否具有添加到第一隔离区或第二隔离区的属性信息的具体实现过程不作限定。例如，一种可能的实施方式中，可采用预定义的方式，预先对添加到第一隔离区内的支付应用添加第一标签，预先对添加到第二隔离区内的支付应用添加第二标签。终端的处理器通过输入设备获取到待添加的支付应用后，可通过解析该待添加的支付应用的标签是第一标签还是第二标签，将该待添加的支付应用添加到第一隔离区或第二隔离区。若该待添加的支付应用的标签是第一标签，则将该待添加的支付应用添加到第一隔离区。若该待添加的支付应用的标签是第二标签，则将该待添加的支付应用添加到第二隔离区。另一种可能的实施方式中，可采用诸如语义分析的方式确定该待添加的支付应用的属性信息。例如，若通过语义分析，确定该待添加的支付应用具有支付功能，并具有被其它应用调用的通信接口，则可认为该待添加的支付应用是需要与其它应用经常进行交互的，故可将该添加的支付应用添加到第一隔离区。若通过语义分析，确定该待添加的支付应用仅具有支付功能，则可认为该待添加的支付应用是不需要与其它应用经常进行交互的，故可将该添加的支付应用添加到第二隔离区。

[0057] 本申请实施例其次对支付应用添加到第一隔离区和第二隔离区后，对支付应用的安全保护过程进行说明。

[0058] 一种可能的实施方式中，本申请实施例中可采用多终端用户的创建方式，将第一隔离区和第二隔离区创建到不同的终端用户中，例如将第一隔离区安装到终端主用户中，而将第二隔离区安装到终端子用户中，并将安装了第二隔离区的终端子用户设置为隐藏用户，以便进一步提高安全性。所述隐藏用户是指在终端主用户的显示界面上不显示的终端子用户，例如该隐藏用户可以理解为是终端在访客模式下未呈现给访客的终端中创建的用

户。

[0059] 本申请实施例中,可在首次启动支付空间时,创建第二隔离区所在的终端子用户,以对第二隔离区内的支付应用进行隔离保护。创建第二隔离区所在的终端子用户时,可采用包管理服务(Package manager service,PMS)、用户管理服务(user manager service,UMS)和活动管理服务(activity manager service,AMS)等服务体系创建。其中,PMS负责终端子用户中安装的支付应用的管理、添加和删除,并向支付空间、终端操作系统和桌面(Launcher)等提供功能。UMS和AMS负责终端子用户的创建、删除、开始和停止,也会被支付空间、终端操作系统和Launcher等应用层模块调用。其中,采用PMS、UMS和AMS创建终端子用户的具体实施过程可参阅目前通用的创建技术,本申请实施例在此不再详述。

[0060] 本申请实施例中第二隔离区所在的终端子用户为隐藏用户,添加到该隐藏用户下的支付应用运行在独立的用户空间内,不能被终端主用户的应用程序发现,也无从调用,且数据与终端主用户中运行的应用程序的数据分离,以使第二隔离区内的支付应用处于完全隔离状态,提高安全性。

[0061] 一种可能的实施方式中,本申请实施例中可删除终端子用户的非必要进程,通过对非必要进程进行裁剪,以在保证安全的同时,减轻资源和内存消耗。其中,非必要进程是指除去系统核心进程之外的进程,核心进程是指维持系统运转的最小系统的进程集合,包括任务调度、内存管理、进程通信、数据管理、文件系统等。例如裁剪后的终端子用户中仅含20+个进程,如theme、chrome等,使得资源占用从80M将为20M。

[0062] 本申请实施例创建了第二隔离区的终端子用户后,可通过诸如白名单方式,添加支付应用到第一隔离区和第二隔离区。例如,参阅图5所示,在白名单中包括添加到第二隔离区的支付应用,在用户选择了待添加的支付应用(终端的处理器确定待添加的应用)时,判断待添加的支付应用是否属于白名单中包括添加到第二隔离区的支付应用,若是,则将该待添加的支付应用添加到第二隔离区,若否,则将该待添加的支付应用添加到第一隔离区。当然也可在白名单中包括添加到第一隔离区的支付应用,具体实施过程与白名单中包括添加到第二隔离区的支付应用的实施过程类似,在此不再赘述。

[0063] 一种可能的实施方式中,本申请实施例中终端的处理器可使用Intent Firewall(操作系统中进程通信的防火墙,该操作系统可以是Android操作系统)对添加到第一隔离区内的支付应用进行隔离保护。本申请实施例中,可使用Intent Firewall中的活动(Activity)、服务(Service)、广播(Broadcast)和内容提供器(Content Provider)四大组件,对调用第一隔离区内支付应用的应用程序进行管控和拦截,仅允许符合调用策略的可信应用调用第一隔离区内的支付应用。其中,应用Intent Firewall中的Activity、Service、Broadcast和Content Provider四大组件进行管控和拦截的具体实施过程,可参阅目前通用的拦截技术,本申请实施例在此不再详述。在检测到未知恶意程序访问添加到所述第一隔离区内的支付应用时,拦截所述未知恶意程序的访问,并显示提示信息,所述提示信息用于提示存在未知恶意程序。

[0064] 本申请实施例中,若终端中创建有终端主用户和终端子用户,所述终端子用户为终端主用户的隐藏用户。若待添加的支付应用具备添加到第一隔离区的属性,则终端的处理器可将待添加到第一隔离区的支付应用添加到所述终端主用户中。若待添加的支付应用具备添加到第二隔离区的属性,则终端的处理器可将待添加到第二隔离区的支付应用添加

到所述终端子用户中。

[0065] 采用多终端用户的创建方式，将第一隔离区和第二隔离区创建到不同的终端用户中，并将支付应用添加到第一隔离区和第二隔离区后，由于第一隔离区属于终端主用户，故添加到第一隔离区内的支付应用，在终端的显示设备显示的终端主用户的显示界面上中正常显示。由于第二隔离区属于终端子用户，并且该终端子用户为隐藏用户，故添加到第二隔离区内的支付应用在终端显示设备显示的终端主用户的显示界面上，并不显示。

[0066] 可选的，本申请实施例中针对添加到第一隔离区的支付应用，可在终端主用户的显示界面上，以不同于普通应用显示方式的显示方式显示该添加到第一隔离区的支付应用，例如，在终端主用户的显示界面上显示的该添加到第一隔离区的支付应用的应用图标上添加标记，或者以不同的灰度显示该添加到第一隔离区的支付应用的应用图标。例如，图6中将添加到终端主用户的支付应用的显示图标中添加标记，以使用户能够获知该支付应用是添加到隔离区内的。

[0067] 本申请实施例中，通过将不同隔离类型的支付应用添加到不同安全级别的第一隔离区和第二隔离区内，添加到所述第一隔离区内的支付应用能够被可信应用调用，添加到所述第二隔离区内的支付应用与安装在所述第二隔离区之外的应用完全隔离，能够兼顾用户使用支付应用的方便性和支付应用的安全性。

[0068] 采用本申请实施例提供的支付应用隔离方法，添加到支付空间内第一隔离区的支付应用能够被可信应用调用，该添加到支付空间内第一隔离区的支付应用和终端主用户中的普通应用之间能够进行交互，并能够访问普通应用数据，例如图7中，将支付钱包类应用添加到创建在终端主用户中的第一隔离区后，该支付钱包类应用基于Intent Firewall中的Activity、Service、Broadcast和Content Provider四大组件对未知恶意程序进行管控和拦截，未知恶意程序不能够访问该支付钱包类应用，但是该支付钱包类应用能够被终端主用户中的普通应用调用，支付钱包类应用与终端主用户中的普通用户之间可以进行交互，并均能够访问普通应用数据。添加到支付空间内第二隔离区的支付应用，与安装在第二隔离区之外的任何应用完全隔离，不能进行交互，该第二隔离区的支付应用仅能够访问该第二隔离区内对应的支付应用的数据。例如图7中，将金融财产类应用添加到创建在终端子用户中的第二隔离区后，该金融财产类应用与第一隔离区内的支付钱包类应用、终端主用户中的普通应用以及未知恶意程序等之间均不存在数据交互，该金融财产类应用仅能够访问该第二隔离区内对应的支付应用的数据。

[0069] 需要说明的是，本申请实施例图7中将添加到创建在终端子用户中的第二隔离区中的金融财产类应用，以显示终端子用户的方式在支付空间内为例进行说明的，实际应用中为了进一步提高安全性，该终端子用户可以为隐藏用户，在终端显示设备的显示界面上并不显示。

[0070] 本申请实施例中，用户若需要访问创建在终端子用户中的第二隔离区内的支付应用，则需要采用诸如账号认证方式登录终端子用户，然后进入支付空间，进入第二隔离区，选择待访问的支付应用并访问支付应用。

[0071] 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。结合本申请中所公开的实施例描述的各示例的单元及算法步骤，本申请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申请实施例的技术方案的范围。

[0072] 本申请实施例可以根据上述方法示例对终端进行功能单元的划分，例如，可以对应各个功能划分各个功能单元，也可以将两个或两个以上的功能集成在一个处理单元中。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。需要说明的是，本申请实施例中对单元的划分是示意性的，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。

[0073] 在采用集成的单元的情况下，图8示出了本申请实施例提供的一种支付应用的隔离装置的结构示意图。参阅图8所示，支付应用的隔离装置100包括获取单元101和处理单元102。其中，获取单元101，用于获取用户选择的、待添加到隔离区的支付应用。

[0074] 处理单元102，用于若确定所述获取单元101获取的待添加的所述支付应用具有添加到第一隔离区的属性，则将待添加的所述支付应用添加到第一隔离区；若确定所述获取单元101获取的待添加的所述支付应用具有添加到第二隔离区的属性，则将待添加的所述支付应用添加到第二隔离区。

[0075] 其中，添加到第一隔离区内的支付应用具有能够被安装在所述第一隔离区之外的可信应用调用的属性，添加到第二隔离区内的支付应用具有与安装在所述第二隔离区之外的应用完全隔离的属性。

[0076] 其中，所述终端中创建有终端主用户和终端子用户，所述终端子用户为终端主用户的隐藏用户。所述处理单元102可将待添加的所述支付应用添加到所述终端子用户中，所述第二隔离区属于所述终端子用户，以进一步提高第二隔离区内支付应用的安全性。

[0077] 其中，所述处理单元102还用于：将待添加的所述支付应用添加到第二隔离区所在的终端子用户中之后，删除所述终端子用户的非必要进程，以在保证安全的同时，减轻资源和内存消耗。

[0078] 其中，所述终端中创建有终端主用户和终端子用户，所述终端子用户为终端主用户的隐藏用户。所述处理单元102可将待添加的所述支付应用添加到所述终端主用户，所述第一隔离区属于所述终端主用户。所述终端中包括的显示单元103，用于在所述处理单元102将待添加的所述支付应用添加到所述终端主用户之后，在终端主用户的显示界面上，以不同于普通应用显示方式的显示方式显示添加到所述第一隔离区的支付应用。

[0079] 所述处理单元102，还用于：将待添加的所述支付应用添加到第一隔离区之后，若检测到未知恶意程序访问添加到所述第一隔离区内的支付应用，则拦截所述未知恶意程序的访问。所述装置中包括的显示单元103，用于显示提示信息，所述提示信息用于提示存在未知恶意程序。

[0080] 其中，添加到第一隔离区和第二隔离区内的支付应用为支付专区内预先创建的支付应用。所述获取单元101，还用于：获取用户选择的、待添加到隔离区的支付应用之后，确定支付专区内存在与待添加的所述支付应用相同的支付应用，以便能够确定添加到隔离区的支付应用的隔离类型。

[0081] 本申请实施例提供的支付应用的隔离装置100具有实现上述方法实施例中涉及的支付应用隔离方法过程中的所有功能，其具体实现过程可参阅上述实施例及附图的相关描

述,在此不再赘述。

[0082] 需要说明的是,本申请实施例中附图中涉及的各附图仅是进行示意性说明,并不限定实际实施过程中终端的形态,例如图4A至图4E以及图6中仅是对终端显示界面上显示的支付应用进行示意性说明,省略了终端的机壳等部分,实际实施过程中该显示界面是显示在具有终端机壳等实体结构上的,并且终端显示界面上显示的具体内容以及应用名称都不限定。

[0083] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令处理器完成,所述的程序可以存储于计算机可读存储介质中,所述存储介质是非短暂性(英文:non-transitory)介质,例如随机存取存储器,只读存储器,快闪存储器,硬盘,固态硬盘,磁带(英文:magnetic tape),软盘(英文:floppy disk),光盘(英文:optical disc)及其任意组合。

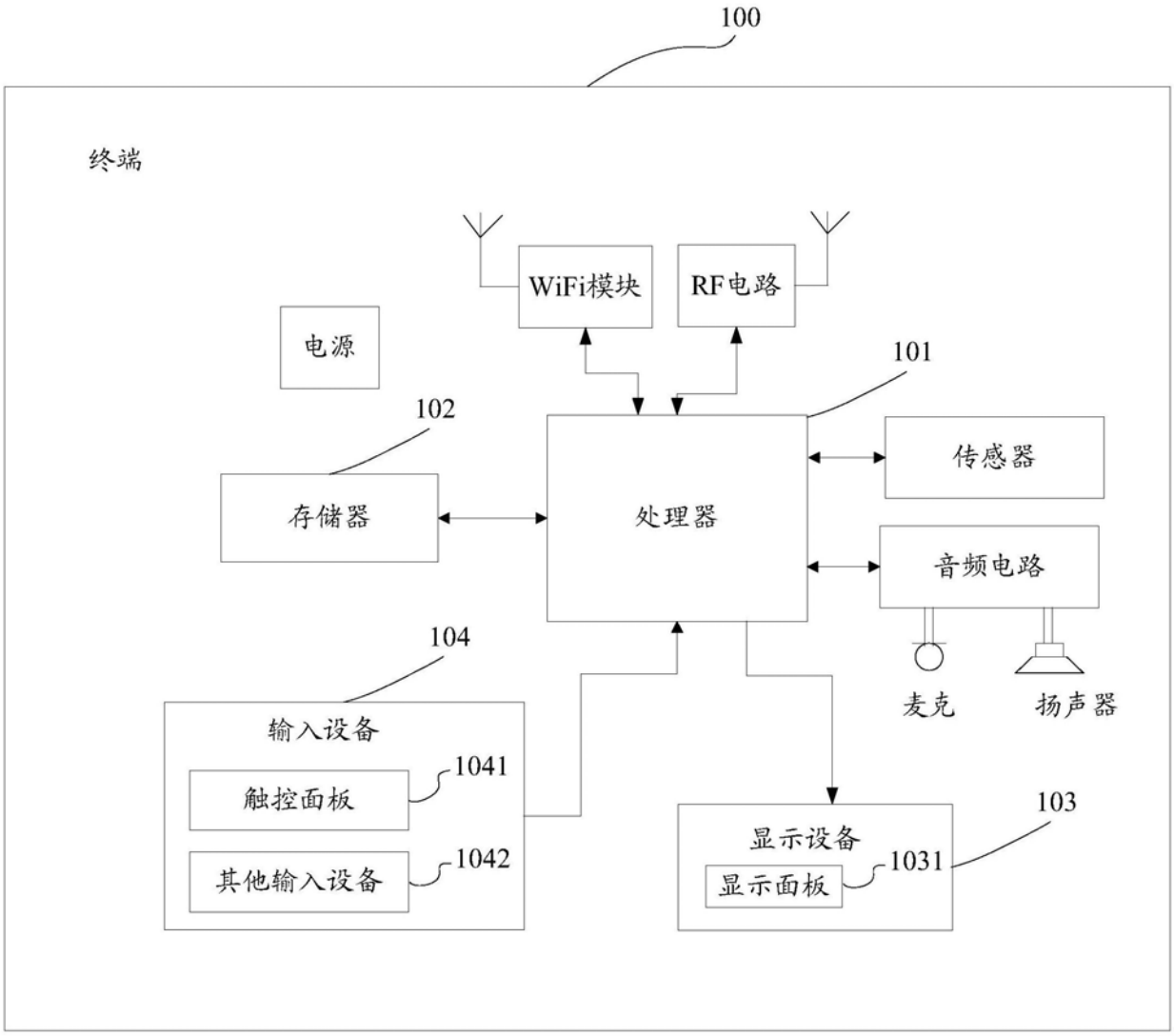

100
终端
WiFi模块
RF电路
电源
101
102
传感器
存储器
处理器
音频电路
104
麦克
扬声器
输入设备
1041
触控面板
1042
其他输入设备
显示设备
103
1031
显示面板

图1

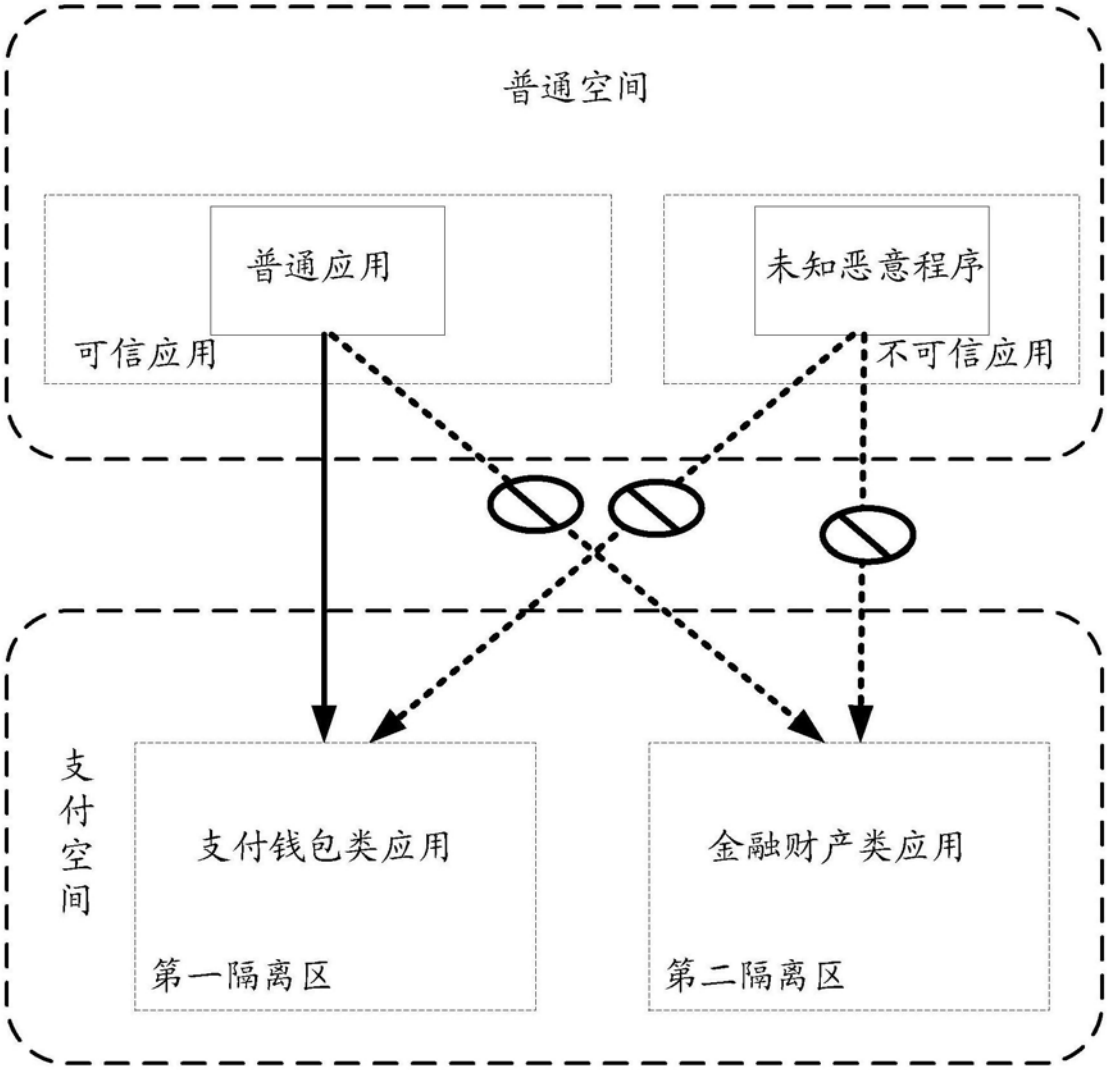

普通空间
普通应用
可信应用
未知恶意程序
不可信应用
支付空间
支付钱包类应用
第一隔离区
金融财产类应用
第二隔离区

图2A

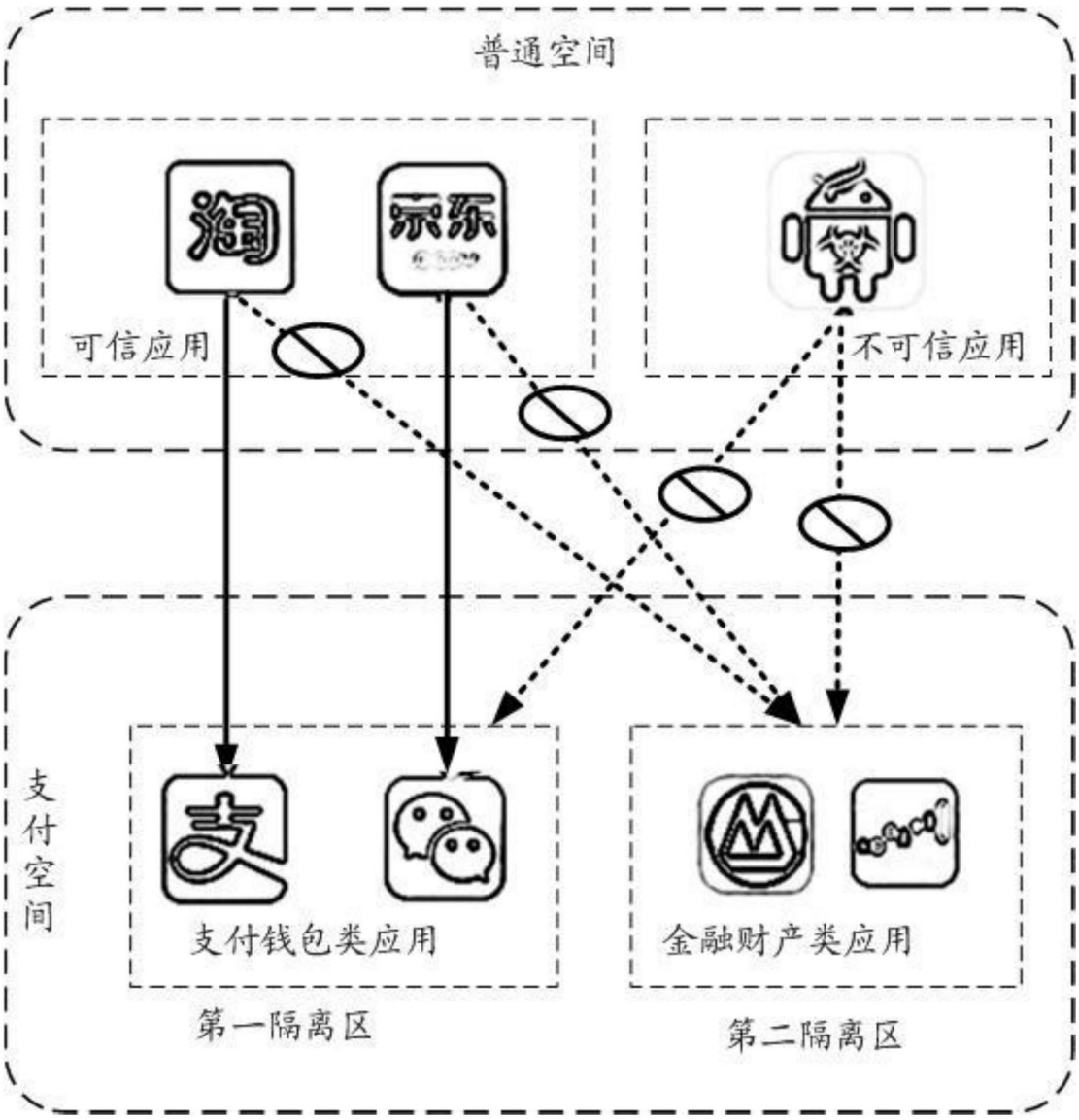


图2B

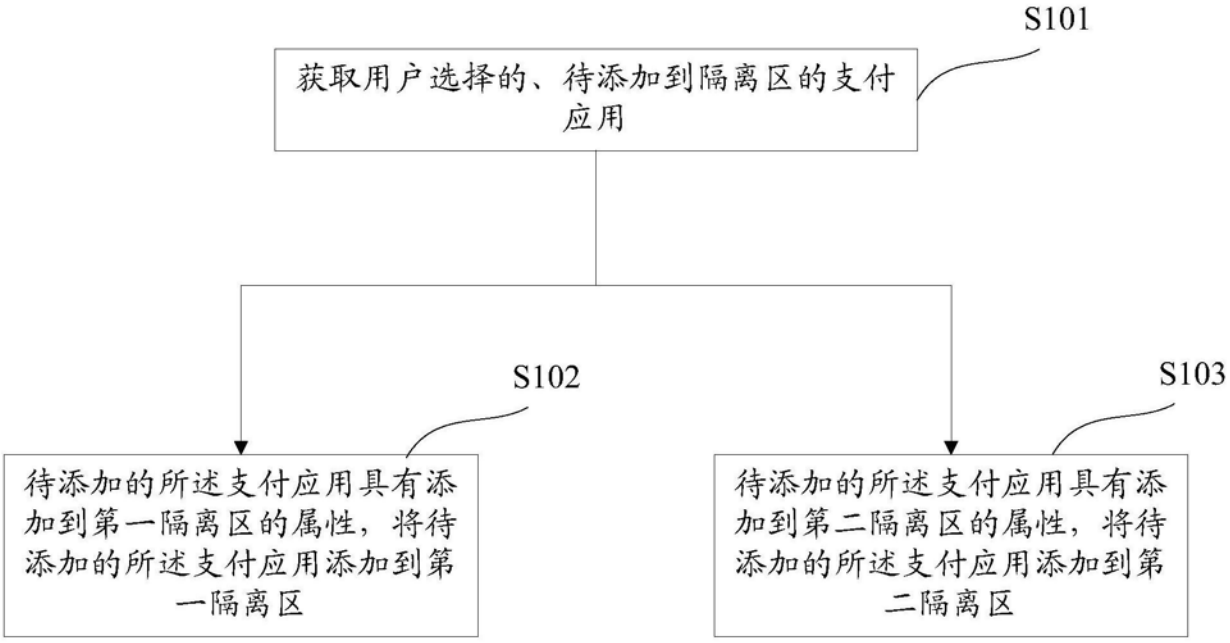

S101
获取用户选择的、待添加到隔离区的支付应用
S102
S103
待添加的所述支付应用具有添加到第一隔离区的属性，将待添加的所述支付应用添加到第一隔离区
待添加的所述支付应用具有添加到第二隔离区的属性，将待添加的所述支付应用添加到第二隔离区

图3


CMCC
08:08
08:08
AM
Beijing
Tuesday, January 12
Wednesday
Thursday
Friday
12°
20°/ 10°
26°/ 10°
20°/ 10°
18°/ 12°
支付空间

图4A

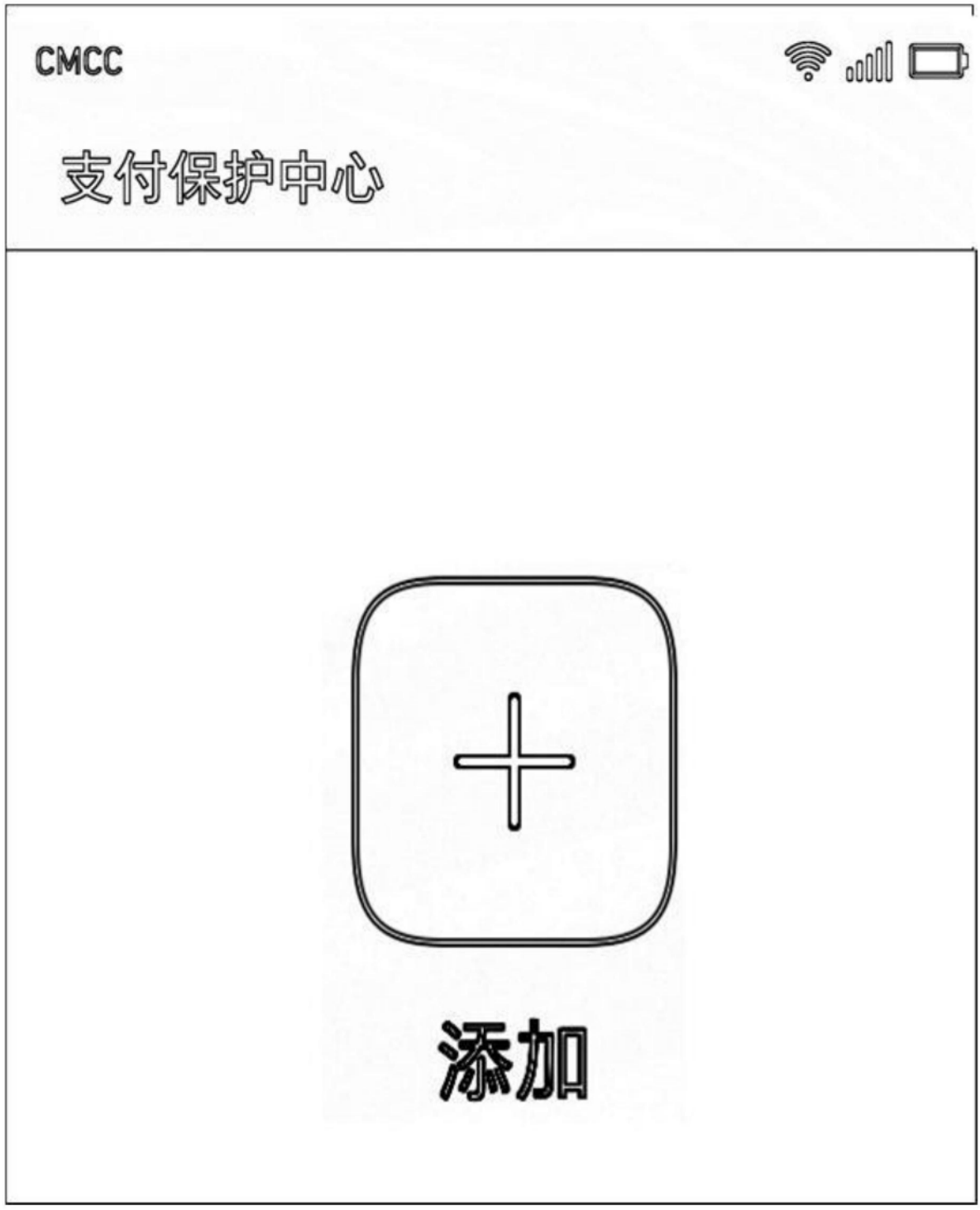


图4B

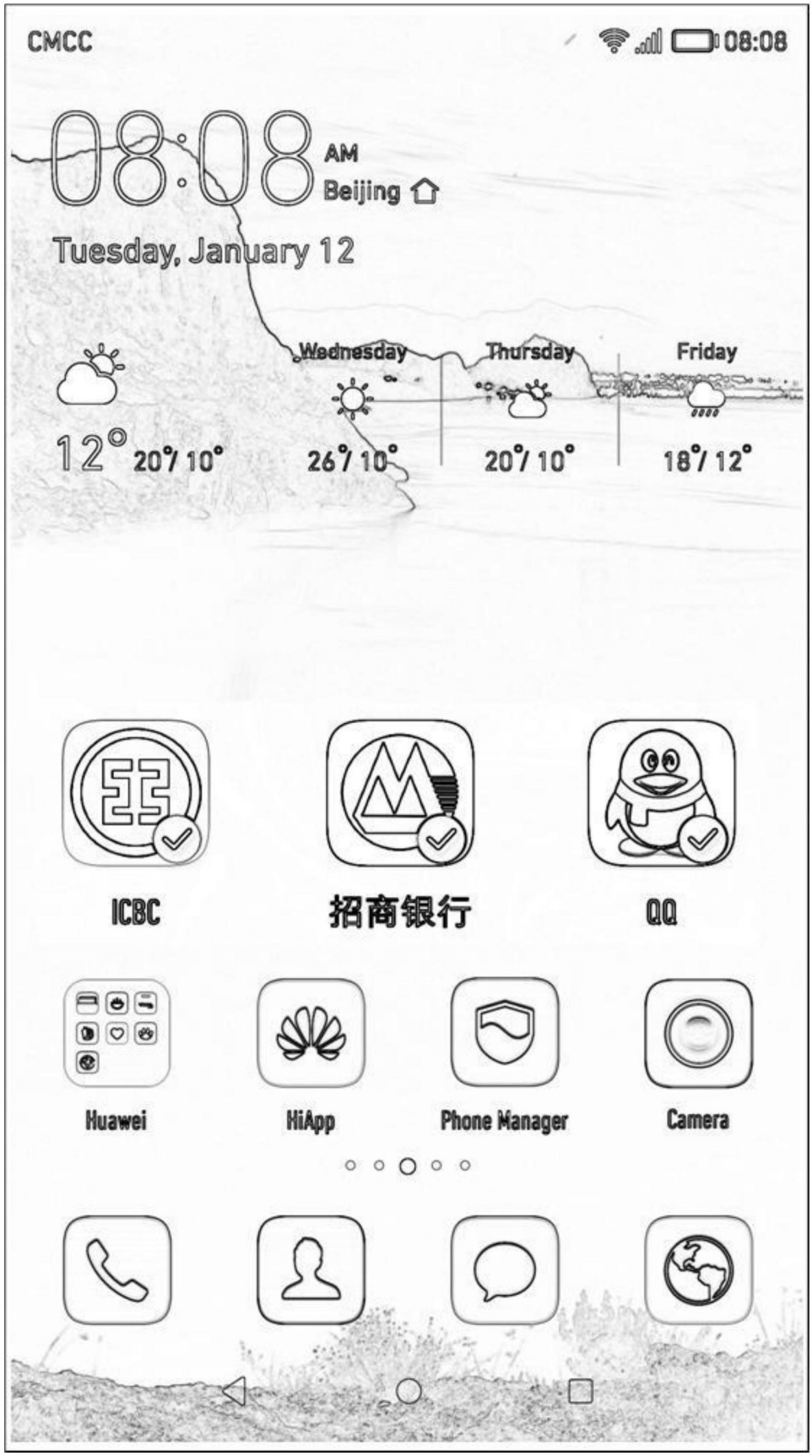

CMCC
08:08
08:08
AM
Beijing
Tuesday, January 12
Wednesday
Thursday
Friday
12° 20°/ 10°
26°/ 10°
20°/ 10°
18°/ 12°
ICBC
招商银行
QQ
Huawei
HiApp
Phone Manager
Camera

图4C


CMCC
08:08
添加（9/36）
本地支付类应用（已通过安全检测）
ICBC
招商银行
QQ
大智慧
农业银行
中国银行
彩票宝
双色球
京东钱包
微信
浦发银行
香港银行
E-Bank
城市银行
中国邮政
手机银行
添加更多正版应用

图4D


CMCC
08:08
添加正版应用（0/120）
搜索正版应用
支付专区
E-Bank
21.2M
E-Bank,您的贴身管家
下载
城市银行
21.2M
城市银行，您的贴身管家
下载
邮政银行
21.2M
城市银行，您的贴身管家
下载
香港银行
21.2M
城市银行，您的贴身管家
下载
浦发银行
21.2M
城市银行，您的贴身管家
下载
浦发银行
SPD BANK

图4E

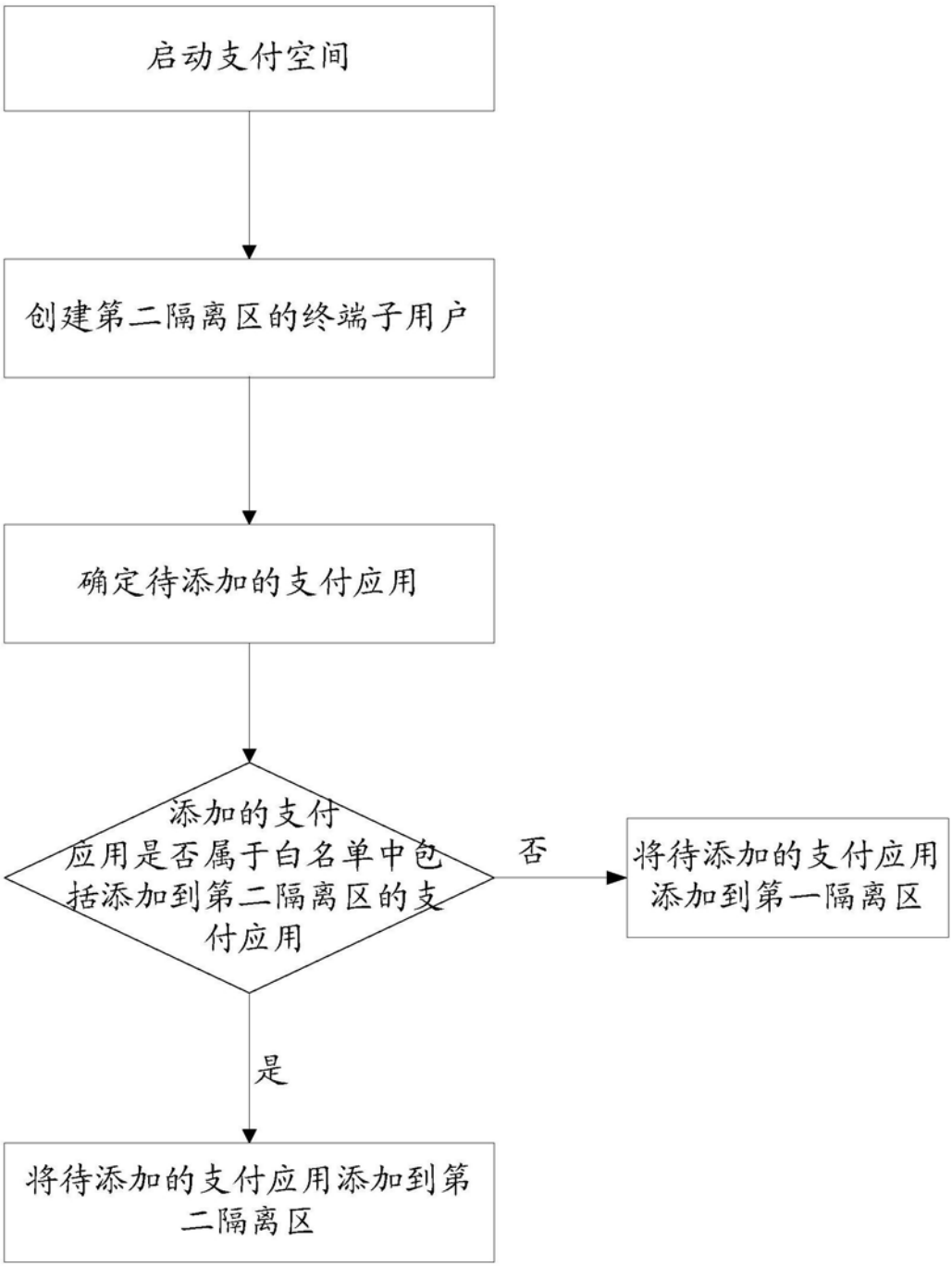

启动支付空间
创建第二隔离区的终端子用户
确定待添加的支付应用
添加的支付应用是否属于白名单中包括添加到第二隔离区的支付应用
否
将待添加的支付应用添加到第一隔离区
是
将待添加的支付应用添加到第二隔离区

图5


CMCC
08:08
支付保护中心
支付环环境安全
支付保护中
ICBC
招商银行
QQ
大智慧
农业银行
手机银
中国银行
彩票宝
双色球
Bank
E-Bank
城市银行
中国邮政
手机银行
京东钱包
京东钱包
添加

图6

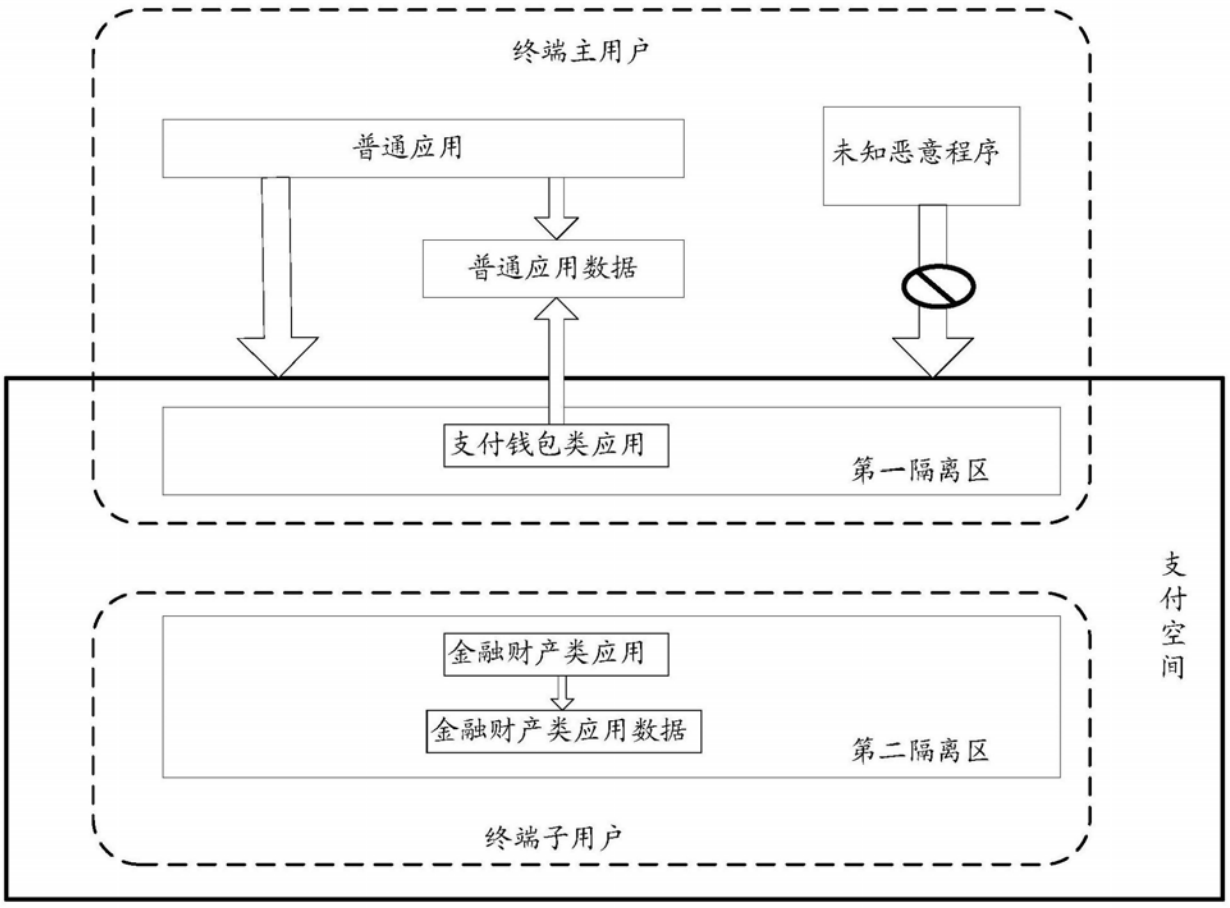

终端主用户
普通应用
普通应用数据
未知恶意程序
支付钱包类应用
第一隔离区
支付空间
金融财产类应用
金融财产类应用数据
第二隔离区
终端子用户

图7

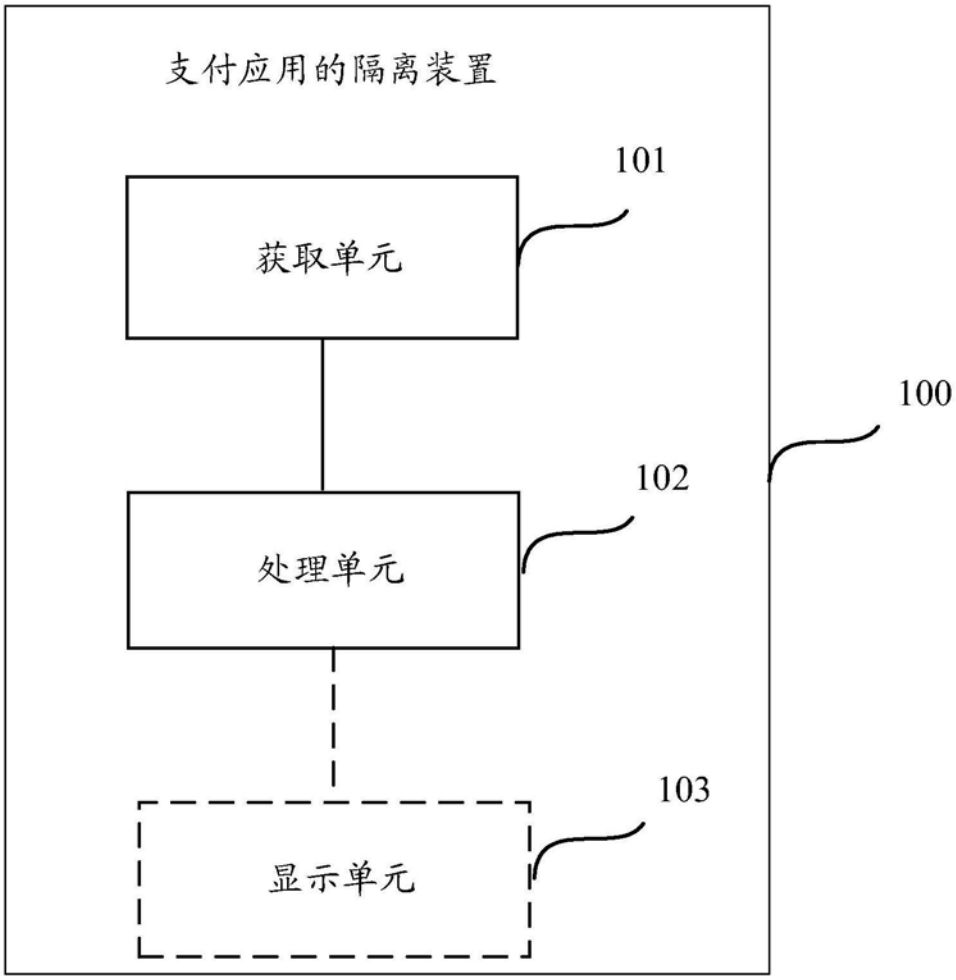


图8