(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103858130 A
(43)申请公布日 2014.06.11

(21)申请号 201380002717.3

(22)申请日 2013.08.23

(85)PCT国际申请进入国家阶段日
2014.03.03

(86)PCT国际申请的申请数据
PCT/CN2013/082182 2013.08.23

(71)申请人 华为终端有限公司
地址 518129 广东省深圳市龙岗区坂田华为基地B区2号楼

(72)发明人 黄曦 吴黄伟

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳

(51)Int.Cl.
G06F 21/51(2013.01)

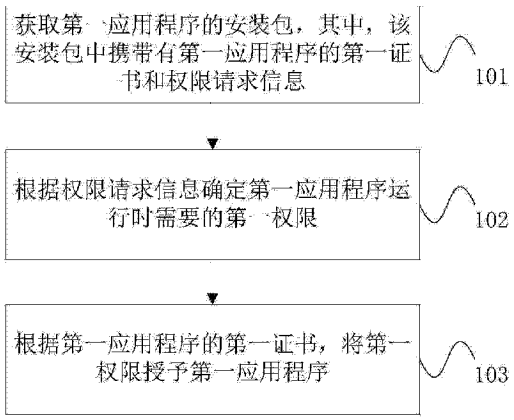
权利要求书5页 说明书18页 附图6页

(54)发明名称

管理权限方法、装置及终端

(57)摘要

本发明实施例提供一种管理权限方法、装置及终端，该管理权限方法包括，通过获取第一应用程序的安装包，该安装包中携带有第一应用程序的第一证书和权限请求信息。接着，根据权限请求信息确定第一应用程序运行时需要的第一权限，其中，第一权限为系统的系统管理员权限，然后，根据第一应用程序的第一证书，将第一权限授予第一应用程序。从而，实现将第一应用程序运行时需要的第一权限授予第一应用程序。



CN 103858130 A

1. 一种管理权限方法，其特征在于，包括：

获取第一应用程序的安装包，所述安装包中携带有所述第一应用程序的第一证书和权限请求信息；

根据所述权限请求信息确定所述第一应用程序运行时需要的第一权限，所述第一权限为系统的系统管理员权限；

根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序。

2. 根据权利要求 1 所述的方法，其特征在于，所述根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序，包括：

确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书中的索引信息在可信证书列表中查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

若确定所述可信证书列表中存储有所述第二证书，则将所述第一权限授予所述第一应用程序；

若确定所述可信证书列表中没有存储所述第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限，或者，提示用户将所述第二证书存储在用户可信证书列表中，并在所述用户将所述第二证书存储在所述用户可信证书列表之后，将所述第一权限授予所述第一应用程序，所述用户可信证书列表中存储有所述用户信任的证书。

3. 根据权利要求 2 所述的方法，其特征在于，所述确定所述可信证书列表中存储有所述第二证书之后，还包括：

确定所述可信证书列表中所述第二证书对应的权限信息是否有所述第一权限；

若是，则将所述第一权限授予所述第一应用程序；

若否，则将所述第二权限授予所述第一应用程序。

4. 根据权利要求 1 所述的方法，其特征在于，所述根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序，包括：

确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书的上级证书中的索引信息查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

若是，则将所述第一权限授予所述第一应用程序；

若否，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限。

5. 根据权利要求 2-4 任一项所述的方法，其特征在于，所述将所述第一权限授予所述第一应用程序之前，还包括：

根据所述第二证书和所述第一应用程序中的签名信息确定所述第一应用程序中的所述安装包是否是完整的；

若不完整，则终止所有操作；

若完整，则将所述第一权限授予所述第一应用程序。

6. 根据权利要求 2-5 任一项所述的方法，其特征在于，所述可信证书列表设置在移动终端或服务器上。

7. 根据权利要求 1-6 任一项所述的方法，其特征在于，所述将所述第一权限授予所述第一应用程序之前，还包括：

在所述系统中设置所述第一权限。

8. 根据权利要求 1-7 任一项所述的方法，其特征在于，所述将所述第一权限授予所述第一应用程序之后，还包括：

接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书的索引、配置于所述第三证书的第三权限以及操作指示，所述操作指示用于删除或者增加所述第三证书对应的所述第三权限，所述第三证书已设置在可信证书列表中；

根据所述更新信息，删除或增加所述可信证书列表中所述第三证书对应的所述第三权限；

若根据所述更新信息，删除所述可信证书列表中所述第三证书对应的所述第三权限，则将所述第三权限不授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序；

若根据所述更新信息，增加所述可信证书列表中所述第三证书对应的所述第三权限，则将所述第三权限授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

9. 根据权利要求 1-7 任一项所述的方法，其特征在于，所述将所述第一权限授予所述第一应用程序之后，还包括：

接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书以及操作指示，所述操作指示用于在可信证书列表中增加或删除所述第三证书；

根据所述更新信息，将所述第三证书增加到所述可信证书列表中，或将所述第三证书从所述可信证书列表中删除；

若将所述第三证书增加到所述可信证书列表，将所述第三证书对应的权限授予所述第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序；

若将所述第三证书从所述可信证书列表中删除，将所述第三证书对应的权限不授予所述第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

10. 一种管理权限装置，其特征在于，包括：

获取模块，用于获取第一应用程序的安装包，所述安装包中携带有所述第一应用程序的第一证书和权限请求信息；

确定模块，用于根据所述权限请求信息确定所述第一应用程序运行时需要的第一权限，所述第一权限为系统的系统管理员权限；

授予模块，用于根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序。

11. 根据权利要求 10 所述的装置，其特征在于，

所述确定模块，具体用于确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书中的索引信息在可信证书列表中查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

所述授予模块，具体用于若确定所述可信证书列表中存储有所述第二证书，则将所述第一权限授予所述第一应用程序；若确定所述可信证书列表中没有存储所述第二证书，则

将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限，或者，提示用户将所述第二证书存储在用户可信证书列表中，并在所述用户将所述第二证书存储在所述用户可信证书列表之后，将所述第一权限授予所述第一应用程序，所述用户可信证书列表中存储有所述用户信任的证书。

12. 根据权利要求 11 所述的装置，其特征在于，所述确定模块，还用于确定所述可信证书列表中所述第二证书对应的权限信息是否有所述第一权限；

所述授予模块，还用于若确定所述可信证书列表中所述第二证书对应的权限信息有所述第一权限，将所述第一权限授予所述第一应用程序；若确定所述可信证书列表中所述第二证书对应的权限信息没有所述第一权限，则将所述第二权限授予所述第一应用程序。

13. 根据权利要求 10 所述的装置，其特征在于，所述确定模块，还用于确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书的上级证书中的索引信息查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

所述授予模块，还用于若确定可信证书列表中存储有所述第二证书，则将所述第一权限授予所述第一应用程序；若确定可信证书列表中没有存储有所述第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限。

14. 根据权利要求 11-13 任一项所述的装置，其特征在于，所述确定模块，还用于根据所述第二证书和所述第一应用程序中的签名信息确定所述第一应用程序中的所述安装包是否是完整的；

所述授予模块，还用于若所述确定模块确定为不完整，则终止所有操作；若所述确定模块确定为完整，则将所述第一权限授予所述第一应用程序。

15. 根据权利要求 11-14 任一项所述的装置，其特征在于，所述可信证书列表设置在移动终端或服务器上。

16. 根据权利要求 10-15 任一项所述的装置，其特征在于，还包括：设置模块，用于在所述系统中设置所述第一权限。

17. 根据权利要求 10-16 任一项所述的装置，其特征在于，还包括：

接收模块，用于接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书的索引、配置于所述第三证书的第三权限以及操作指示，所述操作指示用于指示删除或者增加所述第三证书对应的所述第三权限，所述第三证书已设置在可信证书列表中；

更新模块，用于根据所述更新信息，删除或增加所述可信证书列表中所述第三证书对应的所述第三权限；

处理模块，用于根据所述更新信息，删除所述可信证书列表中所述第三证书对应的所述第三权限，将所述第三权限不授予第二应用程序；根据所述更新信息，增加所述可信证书列表中所述第三证书对应的所述第三权限，将所述第三权限授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

18. 根据权利要求 10-16 任一项所述的装置，其特征在于，接收模块，用于接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书以及操作指示，所述操作指示用于在可信证书列表中增加或删除所述第三证书；

所述更新模块，还用于根据所述更新信息，将所述第三证书增加到所述可信证书列表

中，或将所述第三证书从所述可信证书列表中删除；

所述处理模块，还用于在所述更新模块将所述第三证书增加到所述可信证书列表之后，将所述第三证书对应的权限授予第二应用程序；在所述更新模块将所述第三证书增从所述可信证书列表中删除，将所述第三证书对应的权限不授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

19. 一种终端，其特征在于，包括：接收器以及与所述接收器连接的处理器，其中，

所述接收器，用于获取第一应用程序的安装包，所述安装包中携带有所述第一应用程序的第一证书和权限请求信息；

所述处理器，用于根据所述权限请求信息确定所述第一应用程序运行时需要的第一权限，所述第一权限为系统的系统管理员权限；根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序。

20. 根据权利要求 19 所述的终端，其特征在于，所述处理器，具体用于确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书中的索引信息在可信证书列表中查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；若确定所述可信证书列表中存储有所述第二证书，则将所述第一权限授予所述第一应用程序；若确定所述可信证书列表中没有存储所述第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限，或者，提示用户将所述第二证书存储在用户可信证书列表中，并在所述用户将所述第二证书存储在所述用户可信证书列表之后，将所述第一权限授予所述第一应用程序，所述用户可信证书列表中存储有所述用户信任的证书。

21. 根据权利要求 20 所述的终端，其特征在于，所述处理器，还用于确定所述可信证书列表中所述第二证书对应的权限信息是否有所述第一权限；若确定所述可信证书列表中所述第二证书对应的权限信息有所述第一权限，将所述第一权限授予所述第一应用程序；若确定所述可信证书列表中所述第二证书对应的权限信息没有所述第一权限，则将所述第二权限授予所述第一应用程序。

22. 根据权利要求 19 所述的终端，其特征在于，所述处理器，还用于确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书的上级证书中的索引信息查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；若确定可信证书列表中存储有第二证书，则将所述第一权限授予所述第一应用程序；若确定可信证书列表中没有存储有第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限。

23. 根据权利要求 20 或 21 或 22 所述的终端，其特征在于，所述处理器，还用于根据所述第二证书和所述第一应用程序中的签名信息确定所述第一应用程序中的所述安装包是否是完整的；若所述确定模块确定为不完整，则终止所有操作；若所述确定模块确定为完整，则将所述第一权限授予所述第一应用程序。

24. 根据权利要求 20-23 任一项所述的终端，其特征在于，所述可信证书列表设置在移动终端或服务器上。

25. 根据权利要求 19-24 任一项所述的装置，其特征在于，所述处理器，还用于在所述系统中设置所述第一权限。

26. 根据权利要求 19-25 任一项所述的终端，其特征在于，所述接收器，还用于接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书的索引、配置于所述第三证书的第三权限、以及操作指示，所述操作指示用于指示删除或者增加所述第三证书对应的所述第三权限，所述第三证书已设置在可信证书列表中；

所述处理器，还用于根据所述更新信息，删除或增加所述可信证书列表中所述第三证书对应的所述第三权限；或者，

所述处理器，还用于根据所述更新信息，删除所述可信证书列表中所述第三证书对应的所述第三权限，将所述第三权限不授予第二应用程序；根据所述更新信息，增加所述可信证书列表中所述第三证书对应的所述第三权限，将所述第三权限授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

27. 根据权利要求 19-25 任一项所述的终端，其特征在于，所述接收器，用于接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书以及操作指示，所述操作指示用于在可信证书列表中增加或删除所述第三证书；

所述处理器，还用于根据所述更新信息，将所述第三证书增加到所述可信证书列表中，或将述第三证书从所述可信证书列表中删除；或者，

所述处理器，还用于将所述第三证书增加到所述可信证书列表之后，将所述第三证书对应的权限授予第二应用程序；将所述第三证书从所述可信证书列表中删除，将所述第三证书对应的权限不授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

管理权限方法、装置及终端

技术领域

[0001] 本发明涉及计算机技术，尤其涉及一种管理权限方法、装置及终端。

背景技术

[0002] 在 Android 操作系统中，应用可以申请不同的权限。在应用申请到需要的权限之后，可以调用相应的 API 或应用组件完成相应功能。

[0003] 在现有技术中，需要 ROOT 权限的应用在使用过程中，若未获得 ROOT 权限，将无法正常使用该应用中需要 ROOT 权限的功能；若获取 ROOT 权限，则可以正常运行，即对系统进行控制，如应用权限的管控等。

[0004] 然而，基于安全的考虑，移动终端的开发商没有将 ROOT 权限开放给用户，从而用户在使用没有对用户开放 ROOT 权限的移动终端时，将无法正常使用对应 ROOT 权限的功能，如对移动终端系统的控制或访问。

发明内容

[0005] 本发明实施例提供一种管理权限方法、装置及终端，以实现用户对移动终端系统的控制或访问。

[0006] 本发明第一方面，提供一种管理权限方法，包括：

[0007] 获取第一应用程序的安装包，所述安装包中携带有所述第一应用程序的第一证书和权限请求信息；

[0008] 根据所述权限请求信息确定所述第一应用程序运行时需要的第一权限，所述第一权限为系统的系统管理员权限；

[0009] 根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序。

[0010] 在第一方面的第一种可能的实现方式中，所述根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序，包括：

[0011] 确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书中的索引信息在可信证书列表中查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

[0012] 若确定所述可信证书列表中存储有所述第二证书，则将所述第一权限授予所述第一应用程序；

[0013] 若确定所述可信证书列表中没有存储所述第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限，或者，提示用户将所述第二证书存储在用户可信证书列表中，并在所述用户将所述第二证书存储在所述用户可信证书列表之后，将所述第一权限授予所述第一应用程序，所述用户可信证书列表中存储有所述用户信任的证书。

[0014] 结合第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式

中，所述确定所述可信证书列表中存储有所述第二证书之后，还包括：

[0015] 确定所述可信证书列表中所述第二证书对应的权限信息是否有所述第一权限；

[0016] 若是，则将所述第一权限授予所述第一应用程序；

[0017] 若否，则将所述第二权限授予所述第一应用程序。

[0018] 在第一方面的第三种可能的实现方式中，所述根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序，包括：

[0019] 确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书的上级证书中的索引信息查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

[0020] 若是，则将所述第一权限授予所述第一应用程序；

[0021] 若否，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限。

[0022] 结合第一方面的第一种可能的实现方式或者第一方面的第二种可能的实现方式或第一方面的第三种可能的实现方式中，在第一方面的第四种可能的实现方式中，所述将所述第一权限授予所述第一应用程序之前，还包括：

[0023] 根据所述第二证书和所述第一应用程序中的签名信息确定所述第一应用程序中的所述安装包是否是完整的；

[0024] 若不完整，则终止所有操作；

[0025] 若完整，则将所述第一权限授予所述第一应用程序。

[0026] 结合第一方面的第一种可能的实现方式至第一方面的第四种可能的实现方式中任意一种，在第一方面的第五种可能的实现方式中，所述可信证书列表设置在移动终端或服务器上。

[0027] 结合第一方面至第一方面的第五种可能的实现方式中任意一种，在第一方面的第六种可能的实现方式中，所述将所述第一权限授予所述第一应用程序之前，还包括：

[0028] 在所述系统中设置所述第一权限。

[0029] 结合第一方面至第一方面的第六种可能的实现方式中任意一种，在第一方面的第七种可能的实现方式中，所述将所述第一权限授予所述第一应用程序之后，还包括：

[0030] 接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书的索引、配置于所述第三证书的第三权限以及操作指示，所述操作指示用于删除或者增加所述第三证书对应的所述第三权限，所述第三证书已设置在可信证书列表中；

[0031] 根据所述更新信息，删除或增加所述可信证书列表中所述第三证书对应的所述第三权限；

[0032] 若根据所述更新信息，删除所述可信证书列表中所述第三证书对应的所述第三权限，则将所述第三权限不授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序；

[0033] 若根据所述更新信息，增加所述可信证书列表中所述第三证书对应的所述第三权限，则将所述第三权限授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

[0034] 结合第一方面至第一方面的第六种可能的实现方式中任意一种，在第一方面的第

八种可能的实现方式中，所述将所述第一权限授予所述第一应用程序之后，还包括：

[0035] 接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书以及操作指示，所述操作指示用于在可信证书列表中增加或删除所述第三证书；

[0036] 根据所述更新信息，将所述第三证书增加到所述可信证书列表中，或将所述第三证书从所述可信证书列表中删除；

[0037] 若将所述第三证书增加到所述可信证书列表，将所述第三证书对应的权限授予所述第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序；

[0038] 若将所述第三证书从所述可信证书列表中删除，将所述第三证书对应的权限不授予所述第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

[0039] 本发明第二方面，提供一种管理权限装置，包括：

[0040] 获取模块，用于获取第一应用程序的安装包，所述安装包中携带有所述第一应用程序的第一证书和权限请求信息；

[0041] 确定模块，用于根据所述权限请求信息确定所述第一应用程序运行时需要的第一权限，所述第一权限为系统的系统管理员权限；

[0042] 授予模块，用于根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序。

[0043] 在第二方面的第一种可能的实现方式中，所述确定模块，具体用于确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书中的索引信息在可信证书列表中查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

[0044] 所述授予模块，具体用于若确定所述可信证书列表中存储有所述第二证书，则将所述第一权限授予所述第一应用程序；若确定所述可信证书列表中没有存储所述第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限，或者，提示用户将所述第二证书存储在用户可信证书列表中，并在所述用户将所述第二证书存储在所述用户可信证书列表之后，将所述第一权限授予所述第一应用程序，所述用户可信证书列表中存储有所述用户信任的证书。

[0045] 结合第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，所述确定模块，还用于确定所述可信证书列表中所述第二证书对应的权限信息是否有所述第一权限；

[0046] 所述授予模块，还用于若确定所述可信证书列表中所述第二证书对应的权限信息有所述第一权限，将所述第一权限授予所述第一应用程序；若确定所述可信证书列表中所述第二证书对应的权限信息没有所述第一权限，则将所述第二权限授予所述第一应用程序。

[0047] 在第二方面的第三种可能的实现方式中，所述确定模块，还用于确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书的上级证书中的索引信息查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

[0048] 所述授予模块，还用于若确定可信证书列表中存储有所述第二证书，则将所述第一权限授予所述第一应用程序；若确定可信证书列表中没有存储有所述第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限。

[0049] 结合第二方面的第一种可能的实现方式或者第二方面的第二种可能的实现方式或第二方面的第三种可能的实现方式中，在第二方面的第四种可能的实现方式中，所述确定模块，还用于根据所述第二证书和所述第一应用程序中的签名信息确定所述第一应用程序中的所述安装包是否是完整的；

[0050] 所述授予模块，还用于若所述确定模块确定为不完整，则终止所有操作；若所述确定模块确定为完整，则将所述第一权限授予所述第一应用程序。

[0051] 结合第二方面的第一种可能的实现方式至第二方面的第四种可能的实现方式中任意一种，在第二方面的第五种可能的实现方式中，所述可信证书列表设置在移动终端或服务器上。

[0052] 结合第二方面至第二方面的第五种可能的实现方式中任意一种，在第二方面的第六种可能的实现方式中，还包括：设置模块，用于在所述系统中设置所述第一权限。

[0053] 结合第二方面至第二方面的第六种可能的实现方式中任意一种，在第二方面的第七种可能的实现方式中，还包括：

[0054] 接收模块，用于接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书的索引、配置于所述第三证书的第三权限以及操作指示，所述操作指示用于指示删除或者增加所述第三证书对应的所述第三权限，所述第三证书已设置在可信证书列表中；

[0055] 更新模块，用于根据所述更新信息，删除或增加所述可信证书列表中所述第三证书对应的所述第三权限；

[0056] 处理模块，用于根据所述更新信息，删除所述可信证书列表中所述第三证书对应的所述第三权限，将所述第三权限不授予第二应用程序；根据所述更新信息，增加所述可信证书列表中所述第三证书对应的所述第三权限，将所述第三权限授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

[0057] 结合第二方面至第二方面的第六种可能的实现方式中任意一种，在第二方面的第八种可能的实现方式中，接收模块，用于接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书以及操作指示，所述操作指示用于在可信证书列表中增加或删除所述第三证书；

[0058] 所述更新模块，还用于根据所述更新信息，将所述第三证书增加到所述可信证书列表中，或将所述第三证书从所述可信证书列表中删除；

[0059] 所述处理模块，还用于在所述更新模块将所述第三证书增加到所述可信证书列表之后，将所述第三证书对应的权限授予第二应用程序；在所述更新模块将所述第三证书增从所述可信证书列表中删除，将所述第三证书对应的权限不授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

[0060] 本发明第三方面，提供一种终端，包括：接收器以及与所述接收器连接的处理器，其中，

[0061] 所述接收器，用于获取第一应用程序的安装包，所述安装包中携带有所述第一应用程序的第一证书和权限请求信息；

[0062] 所述处理器，用于根据所述权限请求信息确定所述第一应用程序运行时需要的第一权限，所述第一权限为系统的系统管理员权限；根据所述第一应用程序的所述第一证书，将所述第一权限授予所述第一应用程序。

[0063] 在第三方面的第一种可能的实现方式中，所述处理器，具体用于确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书中的索引信息在可信证书列表中查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；若确定所述可信证书列表中存储有所述第二证书，则将所述第一权限授予所述第一应用程序；若确定所述可信证书列表中没有存储所述第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限，或者，提示用户将所述第二证书存储在用户可信证书列表中，并在所述用户将所述第二证书存储在所述用户可信证书列表之后，将所述第一权限授予所述第一应用程序，所述用户可信证书列表中存储有所述用户信任的证书。

[0064] 结合第三方面的第一种可能的实现方式，在第三方面的第二种可能的实现方式中，所述处理器，还用于确定所述可信证书列表中所述第二证书对应的权限信息是否有所述第一权限；若确定所述可信证书列表中所述第二证书对应的权限信息有所述第一权限，将所述第一权限授予所述第一应用程序；若确定所述可信证书列表中所述第二证书对应的权限信息没有所述第一权限，则将所述第二权限授予所述第一应用程序。

[0065] 在第三方面的第三种可能的实现方式中，所述处理器，还用于确定可信证书列表中是否存储有第二证书，所述第二证书为通过所述第一证书的上级证书中的索引信息查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；若确定可信证书列表中存储有第二证书，则将所述第一权限授予所述第一应用程序；若确定可信证书列表中没有存储有第二证书，则将第二权限授予所述第一应用程序，所述第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限。

[0066] 结合第三方面的第一种可能的实现方式或者第三方面的第二种可能的实现方式或第三方面的第三种可能的实现方式中，在第三方面的第四种可能的实现方式中，所述处理器，还用于根据所述第二证书和所述第一应用程序中的签名信息确定所述第一应用程序中的所述安装包是否是完整的；若所述确定模块确定为不完整，则终止所有操作；若所述确定模块确定为完整，则将所述第一权限授予所述第一应用程序。

[0067] 结合第三方面的第一种可能的实现方式至第三方面的第四种可能的实现方式中任意一种，在第三方面的第五种可能的实现方式中，所述可信证书列表设置在移动终端或服务器上。

[0068] 结合第三方面至第三方面的第五种可能的实现方式中任意一种，在第三方面的第六种可能的实现方式中，所述处理器，还用于在所述系统中设置所述第一权限。

[0069] 结合第三方面至第三方面的第六种可能的实现方式中任意一种，在第三方面的第七种可能的实现方式中，所述接收器，还用于接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书的索引、配置于所述第三证书的第三权限、以及操作指示，所述操作指示用于指示删除或者增加所述第三证书对应的所述第三权限，所述第三证书已设置在可信证书列表中；

[0070] 所述处理器，还用于根据所述更新信息，删除或增加所述可信证书列表中所述第三证书对应的所述第三权限；或者，

[0071] 所述处理器，还用于根据所述更新信息，删除所述可信证书列表中所述第三证书对应的所述第三权限，将所述第三权限不授予第二应用程序；根据所述更新信息，增加所述

可信证书列表中所述第三证书对应的所述第三权限，将所述第三权限授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

[0072] 结合第三方面至第三方面的第六种可能的实现方式中任意一种，在第三方面的第八种可能的实现方式中，所述接收器，用于接收移动终端厂商发送的更新信息，所述更新信息中携带有第三证书以及操作指示，所述操作指示用于在可信证书列表中增加或删除所述第三证书；

[0073] 所述处理器，还用于根据所述更新信息，将所述第三证书增加到所述可信证书列表中，或将述第三证书从所述可信证书列表中删除；或者，

[0074] 所述处理器，还用于将所述第三证书增加到所述可信证书列表之后，将所述第三证书对应的权限授予第二应用程序；将所述第三证书从所述可信证书列表中删除，将所述第三证书对应的权限不授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

[0075] 本发明实施例提供的管理权限方法、装置和终端，通过获取第一应用程序的安装包，该安装包中携带有第一应用程序的第一证书和权限请求信息。根据权限请求信息确定第一应用程序运行时需要的第一权限，其中，第一权限为系统的系统管理员权限，根据第一应用程序的第一证书，将第一权限授予第一应用程序。从而，实现将第一应用程序运行时需要的第一权限授予第一应用程序。这样，可以实现用户对移动终端系统的控制或访问。

附图说明

[0076] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0077] 图 1 为本发明管理权限方法一实施例的流程图；

[0078] 图 2 为本发明管理权限方法另一实施例的流程图；

[0079] 图 3 为本发明管理权限方法再一实施例的流程图；

[0080] 图 4 为本发明管理权限方法中证书吊销列表的示意图；

[0081] 图 5 为本发明管理权限方法再一实施例的流程图；

[0082] 图 6 为本发明管理权限方法再一实施例的流程图；

[0083] 图 7 为本发明管理权限方法再一实施例的流程图；

[0084] 图 8 为本发明管理权限装置一实施例的结构示意图；

[0085] 图 9 为本发明管理权限装置另一实施例的结构示意图；

[0086] 图 10 为本发明终端一实施例的结构示意图。

具体实施方式

[0087] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0088] 本发明实施例提供的管理权限方法可以应用于第三方应用程序安装到移动终端，该移动终端可以为智能手机等。本实施例提供的管理权限的方法可以通过管理权限装置来执行，该管理权限装置可以集成在移动终端上，并且，该管理权限装置可以采用软件和/或硬件的方式来实现。以下对本实施例提供的管理权限方法及装置进行详细地说明。

[0089] 图1为本发明管理权限方法一实施例的流程图，如图1所示，本实施例的方法可以包括：

[0090] 步骤101、获取第一应用程序的安装包，其中，该安装包中携带有第一应用程序的第一证书和权限请求信息。

[0091] 在本实施例中，第一证书可以为第三方应用开发商对第一应用程序进行签名时使用的证书。第一证书可以包括有第一证书的公钥，第一证书的索引，第一证书的所有者信息，以及第一证书的加密算法等。其中，第三方应用开发商可以为除系统开发商和移动终端厂商之外的应用开发商。

[0092] 本实施例中的权限请求信息可以为运行第一应用程序时需要申请的权限信息，一般该权限请求信息设置在安装包的配置文件中，例如，以配置文件为AndroidManifest.xml文件为例，该配置文件至少包括有权限请求信息和第一应用程序的名称。

[0093] 步骤102、根据权限请求信息确定第一应用程序运行时需要的第一权限。

[0094] 在本实施例中，终端可以根据权限请求信息确定第一应用程序运行时需要的权限，也就是说，第一应用程序只有拥有了需要的权限，才能调用相应的API或应用组件，从而完成相应功能，其中，第一应用程序运行时需要的权限可以包括有第一权限和/或第二权限。

[0095] 其中，第一权限为系统的系统管理员权限。该系统的系统管理员权限可以为ROOT_PERMISSION权限。

[0096] 例如，系统的系统管理员权限可以在系统中存储音视频信息、配置信息、或在系统中运行应用程序等。

[0097] 第二权限可以为普通权限，为系统开发商和移动终端厂商对第三方应用程序开放的权限，例如，在Android操作系统中，可以申请134种普通权限，这些普通权限存储在AndroidManifest.xml文件中。

[0098] 步骤103、根据第一应用程序的第一证书，将第一权限授予第一应用程序。

[0099] 在本实施例中，第一证书为对第一应用程序进行签名的证书，根据第一应用程序的第一证书，将第一权限授予第一应用程序的实现方式至少有两种。

[0100] 第一种实现方式，根据第一应用程序的第一证书，确定可信证书列表中存储有第一证书信息，接着，将第一权限授予第一应用程序。

[0101] 具体的，确定可信证书列表中是否存储有第二证书，其中，该第二证书为通过第一证书中的索引信息在可信证书列表中查找到的证书，该可信证书列表中至少存储有允许授予应用程序的证书，移动终端厂商对可信证书列表进行配置，需要说明的是，第二证书为通过第一证书中的索引信息在可信证书列表中查找到得证书，在这种情况下第二证书就是第一证书，第一证书的索引信息没有被篡改。在第一证书的索引信息被篡改后，通过第一证书中的索引信息在可信证书列表中查找到得证书为非第一证书，在这种情况下第二证书不同于第一证书。

[0102] 若确定该可信证书列表中存储有第二证书，则将第一权限授予第一应用程序；

[0103] 若确定可信证书列表中没有存储有第二证书，则将第二权限授予第一应用程序，或者，提示用户将第二证书存储在用户可信证书列表中，并在用户将第二证书存储在用户可信证书列表之后，将第一权限授予第一应用程序，该用户可信证书列表中存储有用户信任的证书。其中，用户可信证书列表可以是用户维护的用户信任的证书，在用户把证书存储在用户可信证书列表之后，就可以把该证书对应的权限授予应用程序。

[0104] 不论是第二证书本身就存储在可信证书列表中，还是提示用户之后，用户将第二证书存储在可信证书列表中，也就是说，在确定该可信证书列表中存储有第二证书之后，进一步的，可以确定可信证书列表中第二证书对应的权限信息是否有第一权限；

[0105] 若是，则将第一权限授予第一应用程序；

[0106] 若否，则将第二权限授予第一应用程序，第二权限为系统开发商和移动终端厂商为第一应用程序开放的权限。

[0107] 第二种实现方式，根据第一应用程序的第一证书，确定可信证书列表中存储有第一证书的上级证书，将第一权限授予第一应用程序。

[0108] 具体的，确定可信证书列表中是否存储有第二证书，该第二证书为通过第一证书的上级证书中的索引信息查找到的证书，所述可信证书列表中至少存储有允许授予应用程序的证书；

[0109] 若是，则将第一权限授予第一应用程序；

[0110] 若否，则将第二权限授予第一应用程序。

[0111] 在本实施例中，通过获取第一应用程序的安装包，该安装包中携带有第一应用程序的第一证书和权限请求信息。根据权限请求信息确定第一应用程序运行时需要的第一权限，其中，第一权限为系统的系统管理员权限，然后，根据第一应用程序的第一证书，将第一权限授予第一应用程序。实现将第一应用程序运行时需要的第一权限授予第一应用程序，这样，可以实现用户对移动终端系统的访问。

[0112] 需要说明的是，在上述实施例中，在步骤 103、将第一权限授予第一应用程序之前，还可以包括：

[0113] 根据第二证书和第一应用程序中的签名信息确定第一应用程序中的安装包是否是完整的。

[0114] 若不完整，则终止所有操作；

[0115] 若完整，则将第一权限授予第一应用程序。

[0116] 举例来讲，通过第一应用程序的第一证书信息，如 CERT.RSA 文件中记录的哈希算法对第一应用程序的安装包中的文件进行哈希计算，得到哈希值 H1，接着，通过第二证书中记录的公钥解密第一应用程序的签名，如 CERT.SF 中的签名信息，得到哈希值 H2，对比 H1 和 H2，若相等，则确定第一应用程序中的安装包是完整的；否则，安装包不完整，终止所有操作；

[0117] 在上述实施例的基础上，可信证书列表可以设置在移动终端或服务器上。

[0118] 进一步的，在上述实施例的基础上，终端还可以接收移动终端厂商发送的更新信息，具体的可以有至少两种适用场景。

[0119] 第一种适用场景，是对可信证书列表中已存储的第三证书中配置的第三权限进行

对应的操作，其中，该第三权限可以为除系统开发商和移动终端厂商之外的应用开发商开发的应用程序，或者，该第三权限也可以为系统开发商和移动终端厂商为应用程序开放的权限。

[0120] 具体的，接收移动终端厂商发送的更新信息，该更新信息中携带有第三证书索引、配置于第三证书的第三权限以及操作指示，其中，该操作指示用于删除或者增加所述第三证书对应的所述第三权限，第三证书已设置在可信证书列表中；

[0121] 根据更新信息对可信证书列表进行更新，删除或增加所述可信证书列表中所述第三证书对应的所述第三权限；

[0122] 若根据所述更新信息，删除所述可信证书列表中所述第三证书对应的第三权限，则将第三权限不授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序；

[0123] 若根据所述更新信息，增加所述可信证书列表中所述第三证书对应的第三权限，则将第三权限授予第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

[0124] 第二种适用场景，是对可信证书列表中已存储的第三证书进行对应的操作。

[0125] 具体的，终端接收移动终端厂商发送的更新信息，该更新信息中携带有第三证书以及操作指示，操作指示用于在可信证书列表中增加或删除所述第三证书，需要说明是的，在可信证书列表中增加第三证书之后，可以相应的增加对应于第三证书的权限；

[0126] 根据所述更新信息，将所述第三证书增加到所述可信证书列表中，或将所述第三证书从所述可信证书列表中删除；

[0127] 若将所述第三证书增加到所述可信证书列表，将第三证书对应的权限授予所述第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序；

[0128] 若将所述第三证书从所述可信证书列表中删除，将第三证书对应的权限不授予所述第二应用程序，所述第二应用程序为通过所述第三证书签名的应用程序。

[0129] 图 2 为本发明管理权限方法另一实施例的流程图，如图 2 所示，本实施例的方法可以包括：

[0130] 步骤 201、获取第一应用程序的安装包。

[0131] 具体的，在移动终端上安装第一应用程序时，可以获取第一应用程序的安装包，并从安装包，即 .apk 文件中获得第一应用程序的第一证书和权限请求信息，例如，该第一证书中可以包括有第一证书的公钥，第一证书的所有者信息，以及第一证书的加密算法等。

[0132] 需要说明的是，第三方应用开发商可以使用第一证书 A 对第一应用程序 S 进行签名，签名方法可以是通用的签名方法，例如，可以首先对第一应用程序的所有内容进行哈希计算以获得哈希值 H，接着，使用对应于第一证书 A 的加密算法，即私钥对哈希值 H 进行加密，也就是对哈希值 H 进行签名，并获得签名值，然后，将第一证书 A 与签名值添加到第一应用程序中，并压缩打包成安装包，即 .apk 文件。

[0133] 步骤 202、确定第一应用程序的安装包中是否存储有第一证书索引信息。

[0134] 需要说明的是，第二证书为通过第一证书中的索引信息在可信证书列表中查找到的证书，在这种情况下，第二证书即为第一证书。

[0135] 具体的，首先确定第一应用程序 S 的第一证书中是否有第一证书索引信息，该第

一证书索引信息为可以唯一标识第一证书的信息，例如，该第一证书索引信息可以是第一证书的公钥信息，也可以是第一证书的编号信息或其他可唯一标识证书的信息，如证书的序列号。

[0136] 若确定第一应用程序的安装包中存储有第一证书索引信息，则执行步骤 203 ；若确定第一应用程序的安装包中没有存储有第一证书索引信息，则执行步骤 206。

[0137] 步骤 203、根据第一证书索引信息，确定设置在移动终端的可信证书列表中是否存储有第二证书。

[0138] 具体的，若确定在移动终端的可信证书列表中存储有第二证书，则执行步骤 204，第二证书即为第一证书。

[0139] 若确定在移动终端的可信证书列表中没有存储有第二证书，则执行步骤 206。

[0140] 进一步的，在上述实施例的基础上，若根据第一证书索引信息，在可信证书列表中没有查找到第二证书，则可以向使用该移动终端的用户发送提示信息，该提示信息可以提示用户将第一应用程序中安装包携带的第一证书添加到用户信任可信证书列表中，并配置携带有该第一证书的第一应用程序需要的权限，如 ROOT_PERMISSION 权限。若用户将该第一证书添加到用户可信证书列表中，则执行步骤 204，若用户拒绝将该第一证书添加到用户信任可信证书列表中，则执行步骤 206。

[0141] 需要说明的是，该可信证书列表可以是由移动终端厂商预置在移动终端中，也可以由用户另外再创建。并且，该可信证书列表可以存放在移动终端的只读内存（Read-OnlyMemory，简称 rom）中，具体实现不做限定，可以是移动终端中的任何可存储介质。进一步的，移动终端厂商还可以对可信证书列表进行加密存储，从而通过加密的方式防止对可信证书列表的篡改。

[0142] 在本实施例中，实现该可信证书列表的具体形式至少有两种，第一种实现方式，将该可信证书列表独立的设置在移动终端中，并通过索引的方法在权限列表中查找与该可信证书列表中存储的证书对应的权限 ；第二种实现方式，将权限列表与可信证书列表并为一个实体，即权限列表在该可信证书列表中存储的每个证书的后面，配置有对应的权限信息。

[0143] 步骤 204、根据第二证书和第一应用程序中的签名信息确定第一应用程序中的安装包是完整的。

[0144] 举例来讲，确定第一应用程序中的安装包是完整的方法可以为，首先通过第一应用程序中的第一证书，如 CERT.RSA 文件中记录的哈希算法对第一应用程序 S 中安装包的文件进行哈希计算，得到哈希值 H1，接着，通过第二证书中存储的公钥解密第一应用程序的签名，如 CERT.SF 中的签名信息，得到哈希值 H2，然后，对比 H1 和 H2，若不相等，则安装包不完整，从而终止任何操作 ；若相等，则安装包完整，从而执行步骤 205。

[0145] 步骤 205、若是完整的，将第一应用程序需要的权限授予第一应用程序。

[0146] 需要说明的是，第一应用程序需要的权限可以包括有第一权限以及第二权限，其中，第一权限为系统的系统管理员权限，例如，系统的系统管理员权限可以在系统中存储音视频信息、配置信息、或在系统中运行应用程序等。第二权限为系统开发商和移动终端厂商共同为第三方应用程序开发的权限。其中，系统的系统管理员权限为 ROOT_PERMISSION 权限。

[0147] 具体的，授予第一权限给第一应用程序的方法可以为，确定可信证书列表中存储

的第二证书对应的权限列表中包括有第一权限，从而将第一权限添加到第一应用程序的权限列表中。同时，还可以将第二权限授予第一应用程序。

[0148] 步骤 206、根据第一应用程序中的第一证书和签名信息确定第一应用程序中的安装包是完整的。

[0149] 举例来讲，确定安装包是完整的方法，可以具体为，首先，使用第一应用程序中记录第一证书信息，如 CERT.RSA 文件中记录的哈希算法对第一应用程序 S 的安装包中的除签名文件之外的所有文件进行哈希计算，得到哈希值 H1，接着，使用第一应用程序的签名 CERT.RSA 文件中的公钥解密签名的数据，例如 CERT.SF 中的签名信息，得到哈希值 H2，然后，对比 H1 和 H2，若相等，则安装包完整，继续后续步骤 207，否则，安装包不完整，终止任何操作。

[0150] 步骤 207、将第一应用程序申请的第二权限授予第一应用程序。

[0151] 本实施例中的，第二权限为系统开发商和移动终端厂商为第一应用程序开放的权限。

[0152] 步骤 208、记录第一应用程序的安装信息，并完成第一程序的安装。

[0153] 在本实施例中，将第一权限和 / 或第二权限授予第一应用程序之后，将关于第一应用程序 S 的信息记录到应用信息记录文件 packages.xml 中，在应用信息记录文件 packages.xml 中记录的信息包括有，第一应用程序 S 的名称，授予第一应用程序 S 的权限信息等。

[0154] 需要说明的是，在上述实施例的基础上，在步骤 201 之前，可以首先在系统中增加第一权限，如，在 Android 系统中增加 ROOT_PERMISSION 权限。

[0155] 进一步的，本实施例的另一种实现方式，与上述如图 2 所示实施例基本类似，区别在于可信证书列表设置在服务器上。

[0156] 需要说明的是，可以将用户可信证书列表设置在移动终端中。

[0157] 图 3 为本发明管理权限方法再一实施例的流程图，图 4 为本发明管理权限方法中证书吊销列表的示意图。如图 3 所示，本实施例的方法可以包括 ：

[0158] 步骤 301、获取第一应用程序的安装包。

[0159] 本实施例中的步骤 301 与图 2 所示步骤 201 的实现原理类似，在此不再赘述。

[0160] 步骤 302、根据第一应用程序中的第一证书和签名信息确定第一应用程序中的安装包是否是完整的。

[0161] 举例来讲，确定第一应用程序中的安装包是完整的方法可以为，首先通过第一应用程序中的第一证书，如 CERT.RSA 文件中记录的哈希算法对第一应用程序 S 中安装包的文件进行哈希计算，得到哈希值 H1，接着，通过第一应用程序中的公钥解密第一应用程序的签名，如 CERT.SF 中的签名信息，得到哈希值 H2，然后，对比 H1 和 H2，若不相等，则安装包不完整，从而终止任何操作 ；若相等，则安装包是完整的。

[0162] 步骤 303、确定第一应用程序是否需要申请第一权限。

[0163] 本实施例的第一应用程序需要申请的权限包括有第一权限以及第二权

[0164] 限，其中，第一权限为系统的系统管理员权限，该系统的系统管理员权限为 ROOT_PERMISSION 权限。例如，系统的系统管理员权限可以在系统中存储音视频信息、配置信息、或在系统中运行应用程序等。第二权限可以为系统开发商和移动终端厂商共同为第三方应

用程序开发的权限。

[0165] 具体的，若第一应用程序需要申请第一权限，则执行步骤 304 ；若第一应用程序不需要申请第一权限，则执行步骤 306。

[0166] 步骤 304、确定可信证书列表中是否存储有第二证书，该第二证书为第一证书的上级证书，其中，可信证书列表设置在移动终端中。

[0167] 在本实施例中，第二证书为第一应用程序中第一证书的上级证书，也就是说，第二证书为通过第一证书的上级证书中的索引信息查找到的证书。

[0168] 另，对于如何确定安装是否完整，可以采用如下方式 ：首先通过对第一证书签名时的哈希算法对第一证书进行哈希计算，得到哈希值 H1，接着，通过第二证书中存储的公钥解密第一证书中的签名，如 CERT.SF 中的签名信息，得到哈希值 H2，然后，对比 H1 和 H2，若相等，则运用第二证书可以确定第一应用程序安装包完整，即确定可信证书列表中存储有与第一证书对应的第二证书，则执行步骤 305。若不相等，则执行步骤 306 ；或者，在确定 H1 和 H2 不相等时，提示用户将该第一证书添加到用户可信证书列表中，若用户将该第一证书添加到用户可信证书列表中，则执行步骤 305，否则，执行步骤 306。

[0169] 进一步的，在对第一证书进行哈希计算，得到哈希值 H1 之前，还可以确定第一证书是否已经被吊销，例如，根据如图 4 所示的证书吊销列表，确定第一证书中是否存储有第一证书，该证书吊销列表存储有已经吊销的证书信息，并且该证书吊销列表设置在移动终端。若确定第一证书存储在证书吊销列表中，例如第一证书编号为 C00001 存储在如图 4 所示的列表中，则确认该第一证书已经被吊销，终止将第一权限授予第一应用程序的操作 ；若确定第一证书没有存储在证书吊销列表中，则确认该第一证书没有被吊销，则可以在对第一证书进行哈希计算，得到哈希值 H1。

[0170] 需要说明的是，移动终端厂商可以使用自己的第二证书为其信任的应用开发商生成一个第二证书的子证书，即第一证书，生成过程为通用的子证书生成过程，例如，对第一证书的信息使用哈希算法得到摘要，使用与第二证书中公钥对应的私钥对第一证书的信息的摘要进行加密，生成签名，存放于第一证书。

[0171] 步骤 305、将第一应用程序需要的权限授予第一应用程序。

[0172] 本实施例中的步骤 305 与图 2 所示步骤 205 的实现原理类似，在此不再赘述。

[0173] 步骤 306、将第一应用程序申请的第二权限授予第一应用程序。

[0174] 步骤 307、记录第一应用程序的安装信息，并完成第一程序的安装。

[0175] 本实施例中的步骤 306、步骤 307 分别与图 2 所示步骤 207、步骤 208 的实现原理类似，在此不再赘述。

[0176] 需要说明的是，在上述实施例的基础上，在步骤 301 之前，可以首先在系统中增加第一权限，如，在 Android 系统中增加 ROOT_PERMISSION 权限。

[0177] 进一步的，本实施例的另一种实现方式，与上述如图 3 所示实施例基本类似，区别在于可信证书列表设置在服务器上。

[0178] 需要说明的是，在步骤 304 中，将第一证书存储在用户可信证书列表中的用户可信证书列表还是如图 2 所示设置在移动终端中。

[0179] 图 5 为本发明管理权限方法再一实施例的流程图，如图 5 所示，本实施例的方法可以包括 ：

[0180] 步骤 501、获取第一应用程序的安装包。

[0181] 步骤 502、根据第一应用程序中的第一证书和签名信息确定第一应用程序中的安装包是完整的。

[0182] 本实施例中的步骤 501、步骤 502 分别与图 3 所示步骤 301、步骤 302 的实现原理类似，在此不再赘述。

[0183] 步骤 503、确定第一应用程序需要申请与系统相同的用户标识。

[0184] 在本实施例中，终端可以解析应用的共享用户标识（sharedUserId）信息，获知第一应用程序需要与系统用户共享用户标识 userId。

[0185] 步骤 504、确定移动终端中是否存储有第二证书，该第二证书为第一证书的上级证书。

[0186] 在本实施例中，若移动终端中存储有第二证书，则执行步骤 505，否则，执行步骤 506。

[0187] 具体的，移动终端厂商可以在移动终端中预先设置第二证书，也可以是安装应用程序在移动终端时，移动终端保存有该应用程序中携带的第二证书，其中，第二证书为第一证书的上级证书。

[0188] 步骤 505、允许第一应用程序与系统共享一个用户标识。

[0189] 具体的，可以在 packages.xml 中记录相应的共享 uid 的信息，记录形式如下：

[0190] <package name="com.M.S"

[0191] codePath="/system/app/S.apk"

[0192] nativeLibraryPath="/data/data/com.M.S/lib"

[0193] flags="1"ft="137c481b198"it="137c481b198"

[0194] ut="137c481b198"version="1"sharedUserId="1000">

[0195] <sigs count="1">

[0196] <cert index="0"/>

[0197] </sigs>

[0198] </package>；

[0199] 步骤 506、根据权限授予规则授予第一应用所申请的权限。

[0200] 具体的，若移动终端中没有存储第二证书，则可以根据第一应用与系统不是共享一个用户标识的权限授予规则授予第一应用所申请的权限；若第一应用程序与系统共享一个用户标识，则可以根据与系统共享一个用户标识的权限授予规则授予第一应用所申请的权限。

[0201] 需要说明的是，如果确定第一应用程序需要申请与系统不是相同的用户标识，则可以将第二权限授予第一应用程序。

[0202] 图 6 为本发明管理权限方法再一实施例的流程图，如图 6 所示，

[0203] 步骤 601、获取第一应用程序的安装包。

[0204] 步骤 602、根据第一应用程序中的第一证书和签名信息确定第一应用程序中的安装包是完整的。

[0205] 本实施例中的步骤 601、步骤 602 分别与图 3 所示步骤 301、步骤 302 的实现原理类似，在此不再赘述。

[0206] 步骤 603、根据第一证书索引信息，确定设置在移动终端的可信证书列表中是否存储有第二证书。

[0207] 本实施例中的步骤 603 与图 2 所示步骤 203 的实现原理类似，在此不再赘述。

[0208] 需要说明的是，若确定在移动终端的可信证书列表中存储有第二证书，则执行步骤 604。

[0209] 若确定在移动终端的可信证书列表中没有存储有第二证书，则执行步骤 605。

[0210] 步骤 604、将第一应用程序需要的权限授予第一应用程序。

[0211] 步骤 605、将第一应用程序申请的第二权限授予第一应用程序。

[0212] 步骤 606、记录第一应用程序的安装信息，并完成第一程序的安装。

[0213] 本实施例中的步骤 604、步骤 605、步骤 606 分别与图 2 所示步骤 205、步骤 207、步骤 208 的实现原理类似，在此不再赘述。

[0214] 需要说明的是，在上述实施例的基础上，在步骤 601 之前，可以首先在系统中增加第一权限，如，在 Android 系统中增加 ROOT_PERMISSION 权限。

[0215] 进一步的，本实施例的另一种实现方式，与上述如图 6 所示实施例基本类似，区别在于可信证书列表设置在服务器上。

[0216] 图 7 为本发明管理权限方法再一实施例的流程图，如图 7 所示，在上述实施例的基础上，在安装完成第一程序之后，还可以包括：

[0217] 步骤 701、接收更新可信证书列表的更新信息。

[0218] 具体的，终端可以接收更新可信证书列表的更新信息有至少两种适用场景。

[0219] 第一适用场景，接收移动终端厂商发送的更新信息，该更新信息中携带有第三证书的索引、配置于第三证书的第三权限以及操作指示，其中，操作指示用于删除或者增加第三证书对应的第三权限，该第三证书已设置在可信证书列表中，其中，该第三权限可以为系统的系统管理员权限，或者，该第三权限也可以为系统开发商和移动终端厂商为应用程序开放的权限。

[0220] 第二适用场景，接收移动终端厂商发送的更新信息，该更新信息中携带有第三证书、以及操作指示，所述操作指示用于在所述可信证书列表中增加或删除所述第三证书，其中，该第三权限可以为系统的系统管理员权限，或者，该第三权限也可以为系统开发商和移动终端厂商为应用程序开放的权限。

[0221] 需要说明的是，移动终端厂商可以通过 OTA 或其他方式将更新消息发送给管理权限装置，并且管理权限装置通过 OTA 或其他方式接收该更新消息，在此不限制管理权限装置获取该更新消息的方式。

[0222] 步骤 702、根据接收到的更新信息，更新可信证书列表。

[0223] 在本实施例中，对应于步骤 701 的适用场景，根据接收到的更新信息，更新可信证书列表具体为：

[0224] 第一适用场景，终端可以根据该更新信息对可信证书列表进行更新，以使删除或增加第三证书对应的第三权限；并根据更新的可信证书列表，将该第三权限不授予或授予第二应用程序，其中，第二应用程序为通过第三证书签名的应用程序。

[0225] 第二适用场景，终端可以根据该更新信息更新可信证书列表，并根据更新的可信证书列表，将第三权限不授予或授予所述第二应用程序，第二应用程序为通过第三证书签

名的应用程序。

[0226] 图 8 为本发明管理权限装置一实施例的结构示意图。如图 8 所示，该管理权限装置可以设置在移动终端，也可以设置独立设置，该管理权限装置包括：获取模块 801、确定模块 802 和授予模块 803。其中，

[0227] 获取模块 801，用于获取第一应用程序的安装包，安装包中携带有第一应用程序的第一证书和权限请求信息；

[0228] 确定模块 802，用于根据权限请求信息确定第一应用程序运行时需要的第一权限，第一权限为系统的系统管理员权限；

[0229] 授予模块 803，用于根据第一应用程序的第一证书，将第一权限授予第一应用程序。

[0230] 在本实施例中，通过获取第一应用程序的安装包，该安装包中携带有第一应用程序的第一证书和权限请求信息。根据权限请求信息确定第一应用程序运行时需要的第一权限，根据第一应用程序的第一证书，将第一权限授予第一应用程序。实现将第一应用程序安装或运行时需要的第一权限授予第一应用程序，这样，可以实现用户对移动终端系统的控制或访问。

[0231] 需要说明的是，第一权限为系统的系统管理员权限。该系统的系统管理员权限为 ROOT_PERMISSION 权限。例如，系统的系统管理员权限可以在系统中存储音视频信息、配置信息、或在系统中运行应用程序等。

[0232] 在上述实施例的基础上，该确定模块 802，具体用于确定可信证书列表中是否存储有第二证书，第二证书为通过第一证书中的索引信息在可信证书列表中查找到的证书，可信证书列表中至少存储有允许授予应用程序的证书；

[0233] 授予模块 803，具体用于若确定可信证书列表中存储有第二证书，则将第一权限授予第一应用程序；若确定可信证书列表中没有存储第二证书，则将第二权限授予第一应用程序，第二权限为系统开发商和移动终端厂商为第一应用程序开放的权限，或者，提示用户将第二证书存储在用户可信证书列表中，并在用户将第二证书存储在用户可信证书列表之后，将第一权限授予第一应用程序，用户可信证书列表中存储有用户信任的证书。

[0234] 进一步的，确定模块 802，还用于确定可信证书列表中第二证书对应的权限信息是否有第一权限；

[0235] 授予模块 803，还用于若确定可信证书列表中第二证书对应的权限信息有第一权限，将第一权限授予第一应用程序；若确定可信证书列表中第二证书对应的权限信息没有第一权限，则将第二权限授予第一应用程序。

[0236] 在上述实施例的基础上，确定模块 802，还用于确定可信证书列表中是否存储有第二证书，第二证书为通过第一证书的上级证书中的索引信息查找到的证书，可信证书列表中至少存储有允许授予应用程序的证书；

[0237] 所述授予模块 803，还用于若确定可信证书列表中存储有第二证书，则将所述第一权限授予所述第一应用程序；若确定可信证书列表中没有存储有第二证书，则将第二权限授予所述第一应用程序，第二权限为所述系统开发商和所述移动终端厂商为所述第一应用程序开放的权限。

[0238] 进一步的，确定模块 802，还用于根据第二证书和第一应用程序中的签名信息确定

第一应用程序中的安装包是否是完整的；

[0239] 授予模块 803，还用于若确定模块 802 确定为不完整，则终止所有操作；若确定模块 802 确定为完整，则将第一权限授予第一应用程序。

[0240] 需要说明的是，可信证书列表设置在移动终端或服务器上。

[0241] 图 9 为本发明管理权限装置另一实施例的结构示意图。如图 9 所示，该管理权限装置，在上述实施例的基础上，该装置还可以包括：设置模块 804，用于在系统中设置第一权限。

[0242] 在上述实施例的基础上，该装置还可以包括：接收模块 805，用于接收移动终端厂商发送的更新信息，更新信息中携带有第三证书的索引、配置于第三证书的第三权限以及操作指示，操作指示用于指示删除或者增加所述第三证书对应的所述第三权限，所述第三证书已设置在所述可信证书列表中；

[0243] 更新模块 806，用于根据更新信息，删除或增加可信证书列表中第三证书对应的第三权限；

[0244] 处理模块 807，用于根据更新信息，删除可信证书列表中第三证书对应的第三权限，将第三权限不授予第二应用程序；根据更新信息，增加可信证书列表中第三证书对应的第三权限，将第三权限授予第二应用程序，第二应用程序为通过第三证书签名的应用程序。

[0245] 可选的，接收模块 805，用于接收移动终端厂商发送的更新信息，更新信息中携带有第三证书以及操作指示，操作指示用于在可信证书列表中增加或删除第三证书；

[0246] 更新模块 806，还用于根据更新信息，将第三证书增加到可信证书列表中，或将第三证书从可信证书列表中删除；

[0247] 处理模块 807，还用于在更新模块将第三证书增加到可信证书列表之后，将第三证书对应的权限授予第二应用程序；在更新模块将第三证书增从可信证书列表中删除，将第三证书对应的权限不授予第二应用程序，第二应用程序为通过第三证书签名的应用程序。

[0248] 从而，实现了不开放第一权限的情况下，实现了将第一应用程序安装或运行时需要的第一权限授予第一应用程序，从而保证了系统的安全稳定。

[0249] 图 10 为本发明终端一实施例的结构示意图。如图 10 所示，该终端，包括：接收器 1001 以及与接收器 1001 连接的处理器 1002，其中，

[0250] 接收器 1001，用于获取第一应用程序的安装包，安装包中携带有第一应用程序的第一证书和权限请求信息；

[0251] 处理器 1002，用于根据权限请求信息确定第一应用程序安装或运行时需要的第一权限，第一权限为系统的系统管理员权限；并根据第一应用程序的第一证书，将第一权限授予第一应用程序，第一证书为对第一应用程序进行签名的证书。

[0252] 在本实施例中，通过获取第一应用程序的安装包，该安装包中携带有第一应用程序的第一证书和权限请求信息。根据权限请求信息确定第一应用程序安装或运行时需要的第一权限，其中，第一权限为第一应用程序无法获得的对系统资源或功能的访问权限，该第一应用程序为除系统开发商和移动终端厂商之外的应用开发商开发的应用程序，根据第一应用程序的第一证书，将第一权限授予第一应用程序。实现将第一应用程序安装或运行时需要的第一权限授予第一应用程序，这样，可以实现用户对移动终端系统的控制或访问。

[0253] 在本实施例中，该处理器 1002，具体用于确定可信证书列表中是否存储有第二证

书，第二证书为通过第一证书中的索引信息在可信证书列表中查找到的证书，可信证书列表中至少存储有允许授予应用程序的证书，移动终端厂商对可信证书列表进行配置；若确定可信证书列表中存储有第二证书，则将第一权限授予第一应用程序；若确定可信证书列表中没有存储第二证书，则将第二权限授予第一应用程序，或者，提示用户将第二证书存储在用户可信证书列表中，并在用户将第二证书存储在用户可信证书列表之后，将第一权限授予第一应用程序，用户可信证书列表中存储有用户信任的证书，第二权限为系统开发商和移动终端厂商为第一应用程序开放的权限。

[0254] 在上述实施例的基础上，处理器 1002，还用于确定可信证书列表中第二证书对应的权限信息是否有第一权限；若确定可信证书列表中第二证书对应的权限信息有第一权限，将第一权限授予第一应用程序；若确定可信证书列表中第二证书对应的权限信息没有第一权限，则将第二权限授予第一应用程序。

[0255] 可选的，在本实施例中，处理器 1002，还用于确定可信证书列表中是否存储有第二证书，第二证书为通过第一证书的上级证书中的索引信息查找到的证书；若确定可信证书列表中存储有第二证书，则将第一权限授予第一应用程序；若确定可信证书列表中没有存储有第二证书，则将第二权限授予第一应用程序。

[0256] 在上述实施例的基础上，处理器 1002，还用于根据第二证书和第一应用程序中的签名信息确定第一应用程序中的安装包是否是完整的；若确定为不完整，则终止所有操作；若确定为完整，则将第一权限授予第一应用程序。

[0257] 进一步的，在上述实施例的基础上，处理器 1002，具体用于通过第一应用程序的第一证书信息对第一应用程序进行哈希计算，获得第一哈希值；通过第二证书中记录的公钥解密对第一应用程序进行哈希计算，获得第二哈希值；若第一哈希值与第二哈希值相等，则安装包是完整的；若第一哈希值与第二哈希值不相等，则安装包是不完整的。

[0258] 在上述实施例的基础上，可信证书列表设置在移动终端或服务器上。

[0259] 在上述实施例的基础上，处理器 1002，还用于在系统中设置第一权限。

[0260] 其中，接收器 1001，还用于接收移动终端厂商发送的更新信息，更新信息中携带有第三证书的索引、配置于第三证书的第三权限、以及操作指示，操作指示用于指示删除或者增加第三证书对应的第三权限，第三证书已设置在可信证书列表中；

[0261] 处理器 1002，还用于根据更新信息，删除或增加可信证书列表中第三证书对应的第三权限；或者，

[0262] 处理器 1002，还用于根据更新信息，删除可信证书列表中第三证书对应的第三权限，将第三权限不授予第二应用程序；根据所述更新信息，增加所述可信证书列表中第三证书对应的第三权限，将第三权限授予第二应用程序，第二应用程序为通过第三证书签名的应用程序。

[0263] 另，接收器 1001，还用于接收移动终端厂商发送的更新信息，更新信息中携带有第三证书以及操作指示，操作指示用于在可信证书列表中增加或删除第三证书；

[0264] 处理器 1002，还用于根据更新信息，将第三证书增加到可信证书列表中，或将第三证书从所述可信证书列表中删除；或者，

[0265] 处理器 1002，还用于将第三证书增加到可信证书列表之后，将第三证书对应的权限授予第二应用程序；将第三证书从可信证书列表中删除，将第三证书对应的权限不授予

第二应用程序，第二应用程序为通过第三证书签名的应用程序。

[0266] 在本实施例中，通过获取第一应用程序的安装包，该安装包中携带有第一应用程序的第一证书和权限请求信息。根据权限请求信息确定第一应用程序安装或运行时需要的第一权限，根据第一应用程序的第一证书，将第一权限授予第一应用程序。

[0267] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0268] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

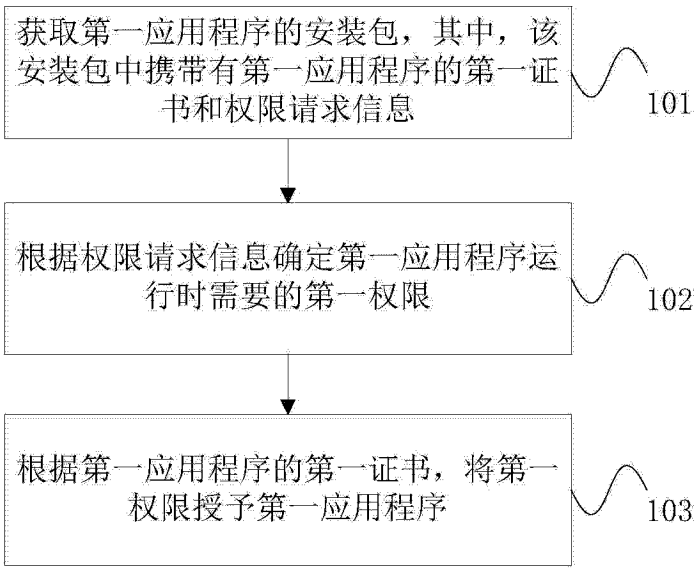

获取第一应用程序的安装包，其中，该安装包中携带有第一应用程序的第一证书和权限请求信息
101
根据权限请求信息确定第一应用程序运行时需要的第一权限
102
根据第一应用程序的第一证书，将第一权限授予第一应用程序
103

图 1

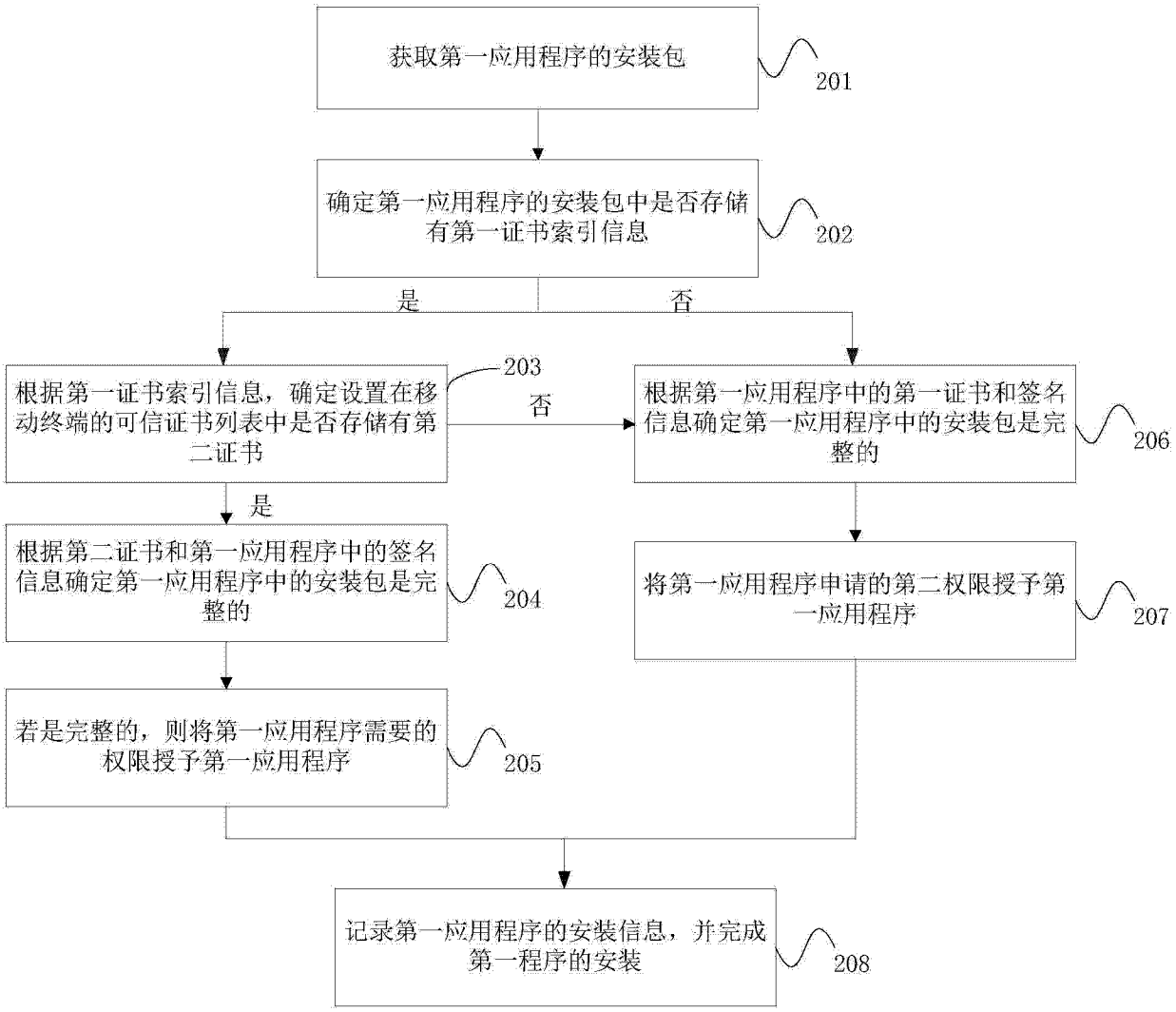

获取第一应用程序的安装包
201
确定第一应用程序的安装包中是否存储有第一证书索引信息
202
是
否
根据第一证书索引信息，确定设置在移动终端的可信证书列表中是否存储有第二证书
203
否
根据第一应用程序中的第一证书和签名信息确定第一应用程序中的安装包是完整的
206
是
根据第二证书和第一应用程序中的签名信息确定第一应用程序中的安装包是完整的
204
将第一应用程序申请的第二权限授予第一应用程序
207
若是完整的，则将第一应用程序需要的权限授予第一应用程序
205
记录第一应用程序的安装信息，并完成第一程序的安装
208

图 2

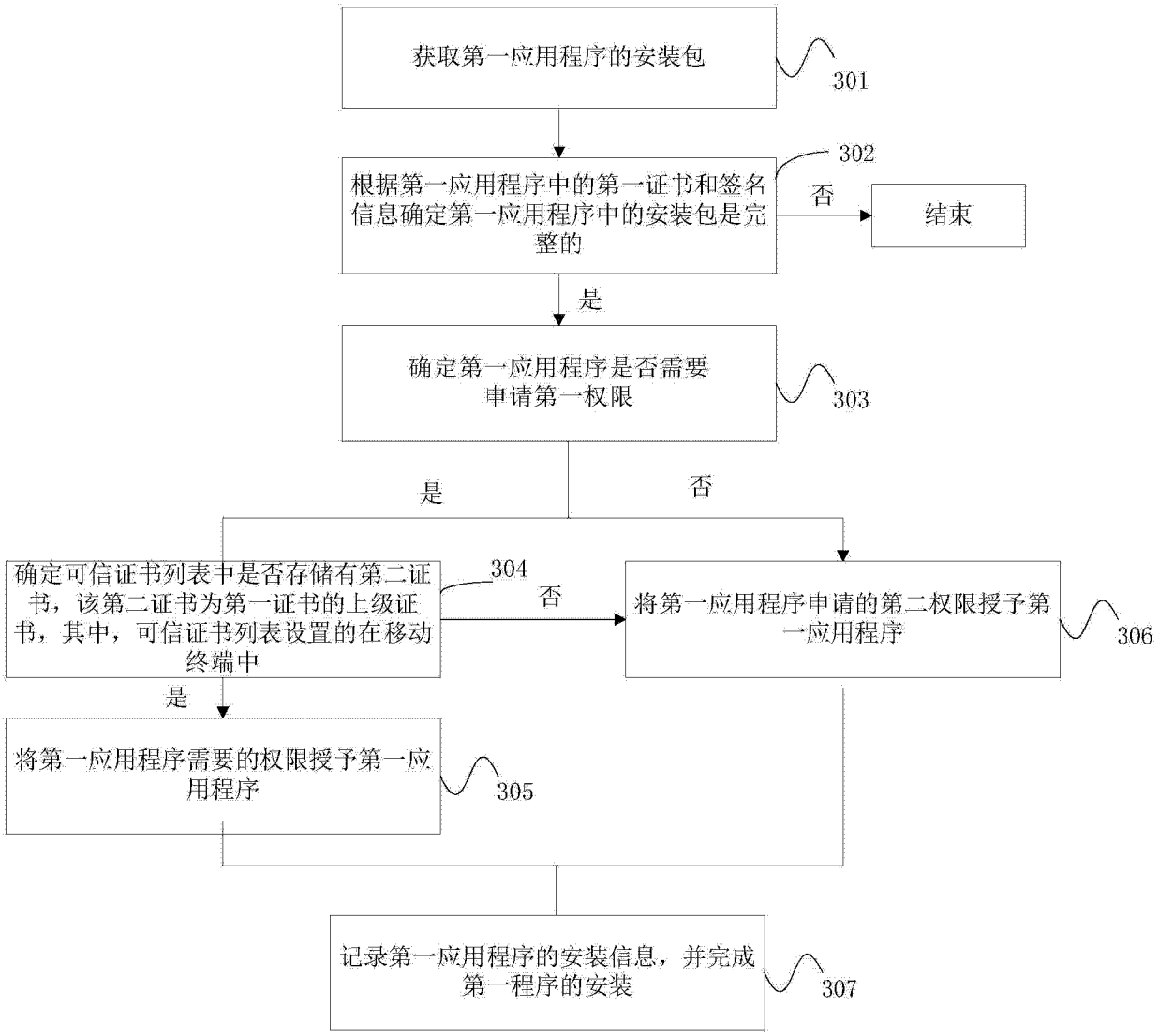


图 3

证书编号	状态	原因	操作时间	证书所有者
C00001	已吊销	业务终止	2013/3/2	M软件公司
D00002	已吊销	证书过期	2013/4/6	X科技公司

图 4

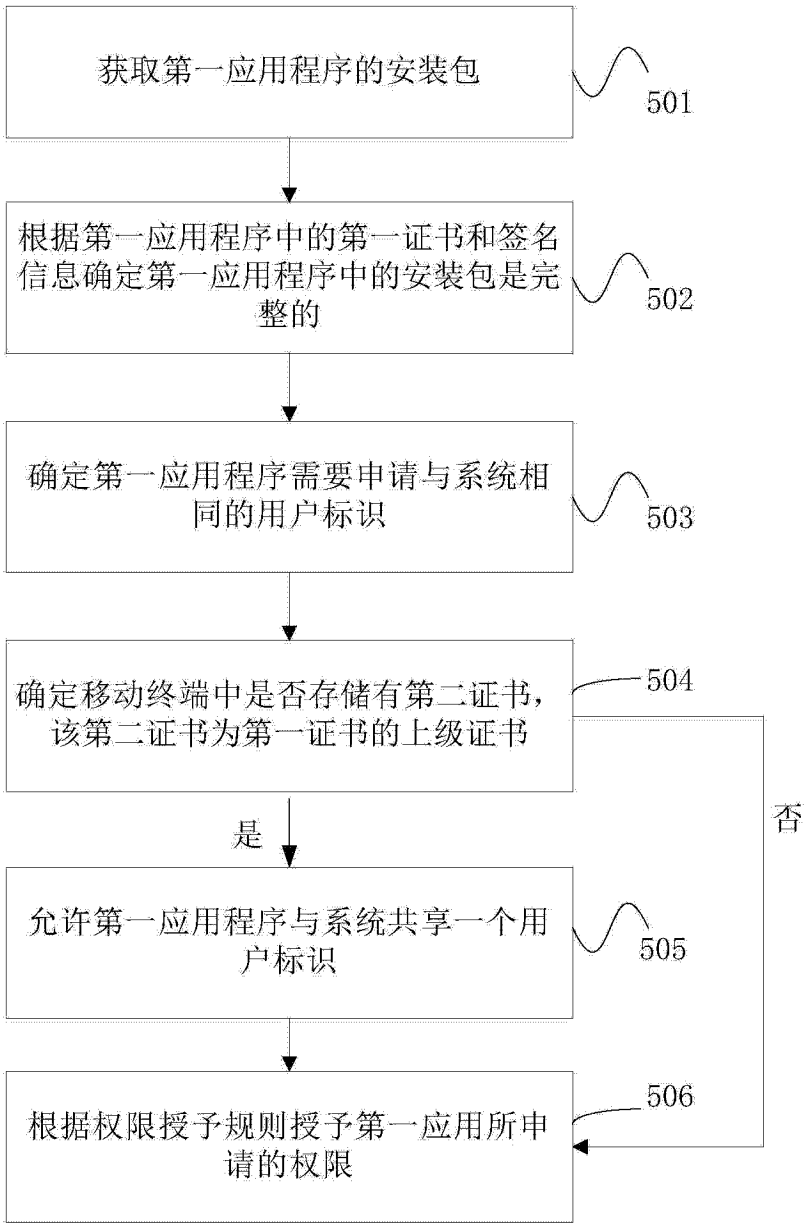

获取第一应用程序的安装包
501
根据第一应用程序中的第一证书和签名信息确定第一应用程序中的安装包是完整的
502
确定第一应用程序需要申请与系统相同的用户标识
503
确定移动终端中是否存储有第二证书，该第二证书为第一证书的上级证书
504
否
是
允许第一应用程序与系统共享一个用户标识
505
根据权限授予规则授予第一应用所申请的权限
506

图 5

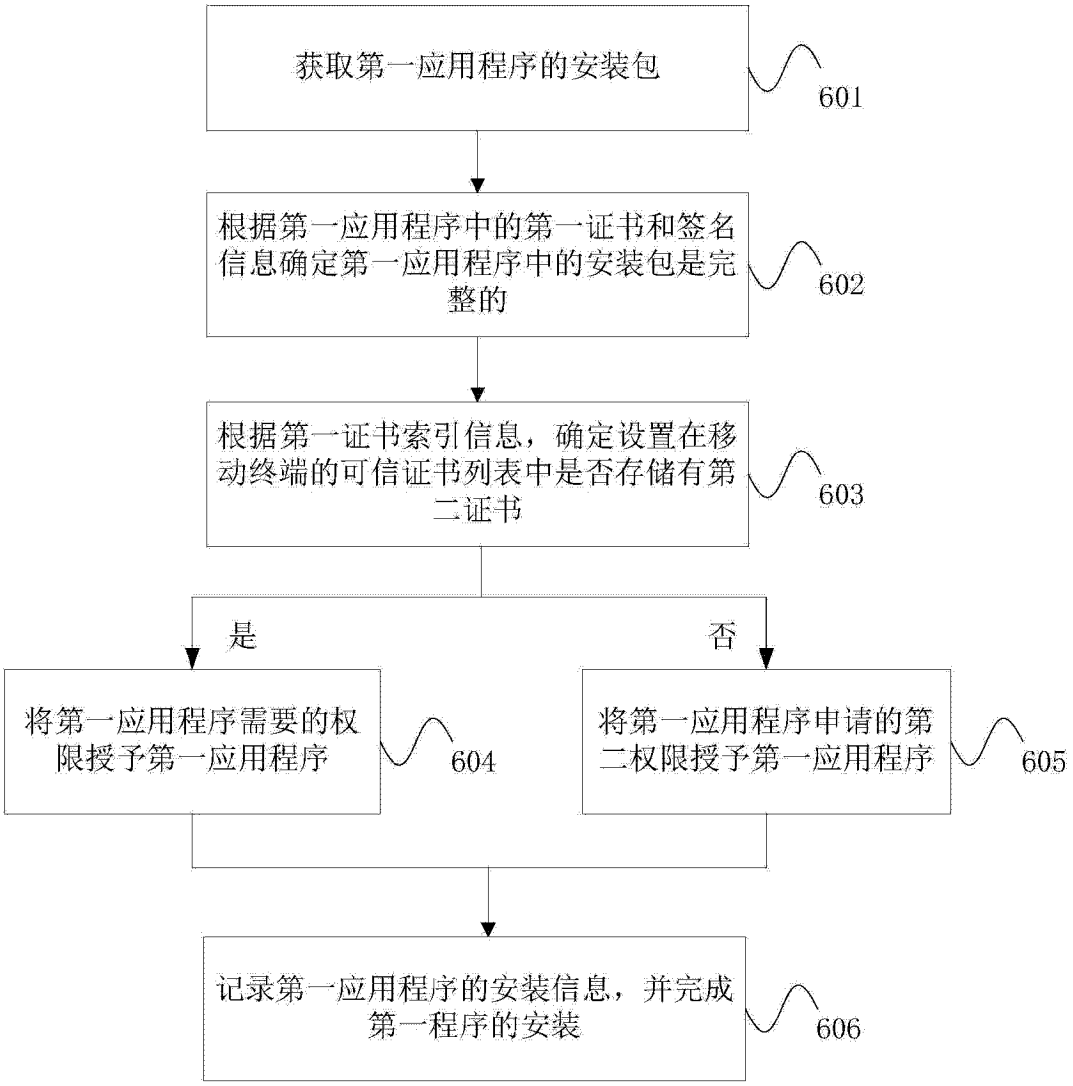

获取第一应用程序的安装包
601
根据第一应用程序中的第一证书和签名信息确定第一应用程序中的安装包是完整的
602
根据第一证书索引信息，确定设置在移动终端的可信证书列表中是否存储有第二证书
603
是
否
将第一应用程序需要的权限授予第一应用程序
604
将第一应用程序申请的第二权限授予第一应用程序
605
记录第一应用程序的安装信息，并完成第一程序的安装
606

图 6

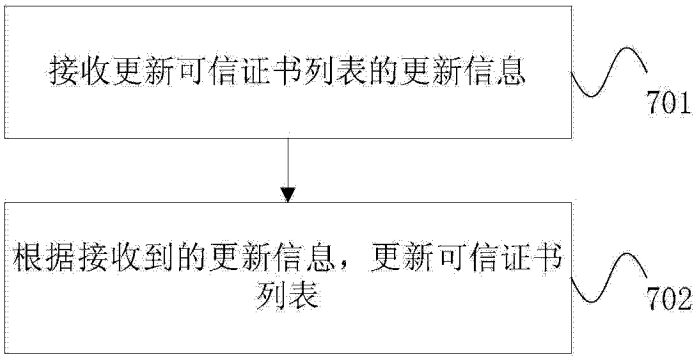

接收更新可信证书列表的更新信息
701
根据接收到的更新信息，更新可信证书列表
702

图 7

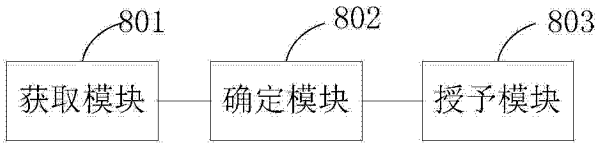

801
802
803
获取模块
确定模块
授予模块

图 8

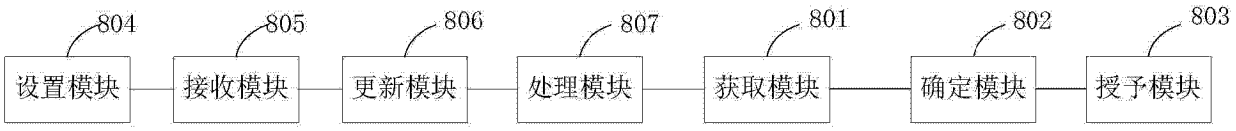

804
805
806
807
801
802
803
设置模块
接收模块
更新模块
处理模块
获取模块
确定模块
授予模块

图 9

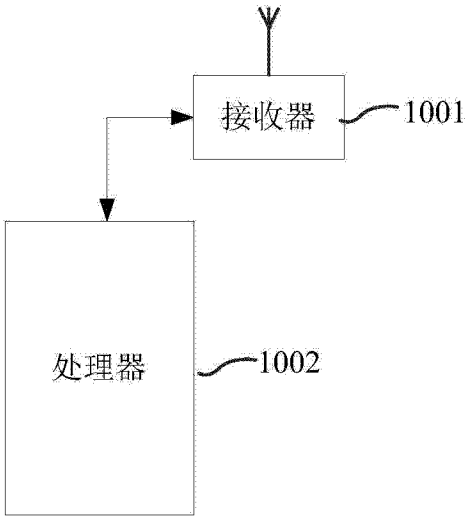

接收器
1001
处理器
1002

图 10