(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 104753676 A
(43)申请公布日 2015.07.01

(21)申请号 201310753081.8

(22)申请日 2013.12.31

(71)申请人 北龙中网(北京)科技有限责任公司
地址 100190 北京市海淀区中关村南四街四号中国科学院软件园1号楼二层

(72)发明人 高宁

(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.
H04L 9/32(2006.01)

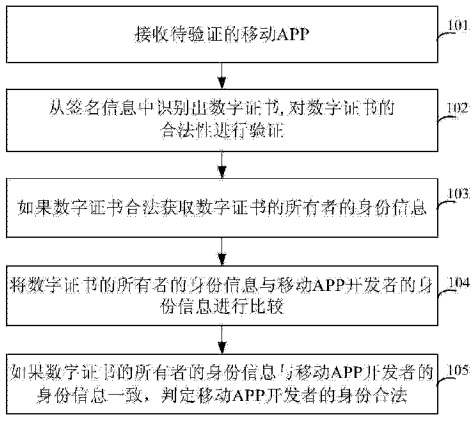
权利要求书2页 说明书11页 附图3页

(54)发明名称

移动APP开发者的身份验证方法及装置

(57)摘要

本发明提供了一种移动APP开发者的身份验证方法及装置。接收待验证的移动APP,移动APP包括签名信息和移动APP开发者的身份信息,签名信息包括用于对移动APP进行数字签名的数字证书和签名数据,数字证书是第三方证书签发机构签发的,从签名信息中识别出数字证书,对数字证书的合法性进行验证,如果数字证书合法,获取数字证书的所有者的身份信息,将所有者的身份信息与开发者的身份信息进行比较,如果所有者的身份信息与开发者的身份信息一致,判定移动APP开发者的身份合法。本发明基于第三方证书签发机构向移动APP开发者签发的数字证书,对开发者的身份进行验证,提高了身份验证效率及可靠性,保证了移动APP的安全性。



CN 104753676 A

1. 一种移动应用程序 APP 开发者的身份验证方法，其特征在于，包括：

接收待验证移动 APP，所述移动 APP 包括签名信息以及所述移动 APP 开发者的身份信息，所述签名信息包括用于对所述移动 APP 进行数字签名的数字证书和签名数据；所述数字证书是由第三方证书签发机构签发的；

从所述签名信息中识别出所述数字证书，对所述数字证书的合法性进行验证；

如果所述数字证书合法，获取所述数字证书的所有者的身份信息；

将所述所有者的身份信息与所述开发者的身份信息进行比较；

如果所述所有者的身份信息与所述开发者的身份信息一致，判定所述开发者的身份合法。

2. 根据权利要求 1 所述的移动 APP 开发者的身份验证方法，其特征在于，所述对所述数字证书的合法性进行验证包括：

判断所述数字证书是否与预存的根证书之间存在对应关系，所述预存的根证书是由所述第三方证书签发机构下发的；

如果判断结果是，判断所述数字证书是否在有效期内；

如果所述数字证书在有效期内，向所述第三方证书签发机构查询所述数字证书是否被吊销；

如果所述数字证书未被吊销，判定所述数字证书合法。

3. 根据权利要求 1 所述的移动 APP 开发者的身份验证方法，其特征在于，所述对所述数字证书的合法性进行验证包括：

向所述第三方证书签发机构发送验证请求，所述验证请求中携带所述数字证书的标识，以使所述第三方证书签发机构对所述数字证书的合法性进行验证；

接收所述第三方证书签发机构返回的验证结果，所述验证结果指示出所述数字证书是否合法。

4. 根据权利要求 2 或 3 所述的移动 APP 开发者的身份验证方法，其特征在于，所述如果所述数字证书合法，获取所述数字证书的所有者的身份信息包括：

从所述数字证书中获取所述所述数字证书的所有者的身份信息；

或者，向所述第三方证书签发机构发送获取请求，以请求从所述第三方证书签发机构获取所述数字证书的所有者的身份信息，所述获取请求携带所述数字证书的标识。

5. 根据权利要求 4 所述的移动 APP 开发者的身份验证方法，其特征在于，所述接收待验证的移动 APP 的设备为移动 APP 市场所在的服务器或者移动终端；

如果所述接收待验证的移动 APP 的设备为所述服务器，则在判定出所述移动 APP 开发者的身份合法后，将所述移动 APP 公布在所述移动 APP 市场上，并将所述移动 APP 标记为可信移动 APP；

或者，如果所述接收待验证的移动 APP 的设备为所述移动终端，则在判定出所述移动 APP 开发者的身份合法后，在所述移动终端上安装所述移动 APP。

6. 一种移动 APP 开发者的身份验证装置，其特征在于，包括：

接收模块，用于接收待验证的移动 APP，所述移动 APP 包括签名信息以及所述移动 APP 开发者的身份信息，所述签名信息包括用于对所述移动 APP 进行数字签名的数字证书和签名数据；所述数字证书是由第三方证书签发机构签发的；

识别验证模块，用于从所述签名信息中识别出所述数字证书并对所述数字证书的合法性进行验证；

获取模块，用于如果所述识别验证模块验证出所述数字证书合法，获取所述数字证书的所有者的身份信息；

比较模块，用于将所述所有者的身份信息与所述开发者的身份信息进行比较；

判定模块，用于如果所述所有者的身份信息与所述开发者的身份信息一致，判定所述开发者的身份合法。

7. 根据权利要求6所述的移动APP开发者的身份验证装置，其特征在于，所述识别验证模块包括：

第一识别单元，用于从所述签名信息中所述识别出所述数字证书；

判断单元，用于判断所述数字证书是否与预存的根证书之间存在对应关 系，以及在所述数字证书与预存的根证书存在对应关系时，判断所述数字证书是否在有效期内；所述预存的根证书是由所述第三方证书签发机构下发的；

查询单元，用于如果所述数字证书在有效期内，向所述第三方证书签发机构查询所述数字证书是否被吊销；

验证单元，用于如果所述数字证书未被吊销，判定所述数字证书合法。

8. 根据权利要求6所述的移动APP开发者的身份验证装置，其特征在于，所述识别验证模块包括：

第二识别单元，用于从所述签名信息中识别出所述数字证书；

发送单元，用于向所述第三方证书签发机构发送验证请求，所述验证请求中携带所述数字证书的标识，以使所述第三方证书签发机构对所述数字证书的合法性进行验证；

接收单元，用于接收所述第三方证书签发机构返回的验证结果，所述验证结果指示出所述数字证书是否合法。

9. 根据权利要求7或8所述的移动APP开发者的身份验证装置，其特征在于，所述获取模块具体用于从所述数字证书中获取所述数字证书的所有者的身份信息，或者向所述第三方证书签发机构发送获取请求，以请求从所述第三方证书签发机构获取所述数字证书的所有者的身份信息，所述获取请求携带所述数字证书的标识。

10. 根据权利要求9所述的移动APP开发者的身份验证装置，其特征在于，所述应用程序开发者的身份验证装置设置在移动APP市场所在的服务器或者移动终端上；

所述应用程序开发者的身份验证装置还包括：执行模块；

如果所述移动APP开发者的身份验证装置设置在所述服务器上，则所述执行模块，用于在所述判定模块判定所述移动APP开发者的身份合法后，将所述移动APP公布在所述移动APP市场上，并所述移动APP标记为可信移动APP；

如果所述移动APP开发者身份验证装置设置在所述移动终端上，则所述执行模块，用于在所述判断模块判断出所述移动APP开发者的身份合法后，在所述移动终端上安装所述移动APP。

移动 APP 开发者的身份验证方法及装置

技术领域

[0001] 本发明涉及通信技术，尤其涉及一种移动 APP 开发者的身份验证方法及装置。

背景技术

[0002] 随着移动互联网技术的快速发展和普及，安装在移动终端上的应用程序(Application，简称 APP)逐渐融入人们日常工作中。在互联网或日常生活中各种应用场景下，都能够获取到对应的大量移动 APP。

[0003] 但是一些非法开发者会对各种移动 APP 进行恶意盗版，为了提高安装在移动终端的各 APP 的安全性，目前多采用人工审核的方式对移动 APP 的开发者进行验证和审核，如果验证出开发者的身份合法后，允许将移动 APP 上传到移动 APP 市场，以供移动终端从移动 APP 市场下载各移动 APP。

[0004] 上述通过人工方式对移动 APP 开发者的身份进行验证，虽然能够提高移动 APP 的安全性，但是移动 APP 开发者身份验证的效率较低、可靠性较差且验证结果不具有通用性，使得移动 APP 的安全性较差。

发明内容

[0005] 本发明提供一种移动 APP 开发者的身份验证方法及装置，以解决现有人工对 APP 开发者的身份进行验证的过程中存在验证效率较低、安全性较差以及验证结果不具有通用性的问题。

[0006] 为了实现上述目的，本发明提供了一种移动 APP 开发者的身份验证方法，包括：

[0007] 接收待验证移动移动 APPAPP，所述 APP 包括签名信息以及所述 APP 开发者的身份信息，所述签名信息包括用于对所述 APP 进行数字签名的数字证书和签名数据；所述数字证书是由第三方证书签发机构签发的；

[0008] 从所述签名信息中识别出所述数字证书并对所述数字证书的合法性进行验证；

[0009] 如果所述数字证书合法，获取所述数字证书的所有者的身份信息；

[0010] 将所述所有者的身份信息与所述开发者的身份信息进行比较；

[0011] 如果所述所有者的身份信息与所述开发者的身份信息一致，判定所述开发者的身份合法。

[0012] 为了实现上述目的，本发明提供了一种移动 APP 开发者的身份验证装置，包括：

[0013] 接收模块，用于接收待验证的移动 APP，所述 APP 包括签名信息以及所述 APP 开发者的身份信息，所述签名信息包括用于对所述 APP 进行数字签名的数字证书和签名数据；所述数字证书是由第三方证书签发机构签发的；

[0014] 识别验证模块，用于从所述签名信息中识别出所述数字证书并对所述数字证书的合法性进行验证；

[0015] 获取模块，用于如果所述识别验证模块验证出所述数字证书合法，获取所述数字证书的所有者的身份信息；

[0016] 比较模块，用于将所述所有者的身份信息与所述开发者的身份信息进行比较；

[0017] 判定模块，用于如果所述所有者的身份信息与所述开发者的身份信息一致，判定所述开发者的身份合法。

[0018] 本发明提供的一种移动 APP 开发者的身份验证方法及装置，接收待验证的移动 APP，移动 APP 包括签名信息以及 APP 开发者的身份信息，签名信息包括用于对移动 APP 进行数字签名的数字证书和签名数据，数字证书是由第三方证书签发机构签发的，从签名信息中识别出数字证书并对数字证书的合法性进行验证，如果数字证书合法，获取数字证书的所有者的身份信息，将所有者的身份信息与开发者的身份信息进行比较，如果所有者的身份信息与开发者的身份信息一致，判定 APP 开发者的身份合法。本实施例中通过第三方证书签发机构向 APP 的开发者签发数字证书，开发者基于数字证书开发 APP，APP 市场的服务器或者移动终端在接收到开发者开发的 APP 后，基于数字证书对 APP 开发者的身份进行验证，不仅提高了身份验证效率，而且可靠性较高，保证了 APP 来源的安全性。本发明中基于数字证书对开发者身份进行验证，使得验证结果具有通用性。

附图说明

[0019] 图 1 为本发明实施例提供的一种移动 APP 开发者的身份验证方法的流程示意图；

[0020] 图 2 为本发明实施例提供的另一种移动 APP 开发者的身份验证方法的的流程示意图；

[0021] 图 3 为本发明实施例提供的一种移动 APP 开发者的身份验证装置的结构示意图；

[0022] 图 4 为本发明实施例提供的一种识别验证模块的结构示意图；

[0023] 图 5 为本发明实施例提供的另一种识别验证模块的结构示意图；

[0024] 图 6 为本发明实施例提供的一种移动 APP 开发者的身份验证系统的结构示意图。

具体实施方式

[0025] 下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

[0026] 图 1 为本发明实施例提供的一种移动 APP 开发者的身份验证方法的流程示意图。如图 1 所示，该移动 APP 开发者的身份验证方法包括以下步骤：

[0027] 101、接收待验证的移动 APP。

[0028] 其中所述移动 APP 包括签名信息以及所述移动 APP 开发者的身份信息，所述签名信息包括用于对所述移动 APP 进行数字签名的数字证书以及签名数据；所述数字证书是由第三方证书签发机构签发的。

[0029] 具体地第三方证书签发机构可以向移动 APP 开发者签发数字证书，该开发者在开发完移动 APP 时，采用上述数字证书对该移动 APP 进行数字签名，可以生成该移动 APP 的签名数据，然后将用于对移动 APP 进行数字签名的数字证书以及生成的签名数据携带在签名信息中，并将签名信息携带在移动 APP 中。本实施例中通过该签名信息可以指示出对该移动 APP 进行数字签名的数字证书。进一步地移动 APP 开发者通过终端将自身的身份信息携带在移动 APP 中。

[0030] 一般接收待验证的移动 APP 的设备可以为移动 APP 市场所在的服务器或者移动终端。例如，在开发者试图将待验证的移动 APP 发布到移动 APP 市场上，则移动 APP 市场所在

的服务器可以接收开发者通过网络上传的待验证的移动 APP。

[0031] 进一步地，接收待验证的移动 APP 的设备还可以为移动终端，当移动终端对应的用户试图安装一个移动 APP 时，移动终端可以接收到一个待验证的移动 APP，其中该待验证的移动 APP 可以为移动终端从移动 APP 市场中下载得到，也可以为移动终端从互联网的相关网站下载得到。

[0032] 102、从签名信息中识别出数字证书，对数字证书的合法性进行验证。

[0033] 由于移动 APP 携带有签名信息，签名信息包括用于对移动 APP 进行数字签名的数字证书，在接收到待验证的移动 APP 后，从该签名信息中可以识别出数字证书，并且对数字证书的合法性进行验证。

[0034] 本实施例中在移动终端或者移动 APP 市场所在的服务器中预先存储有可信的第三方证书签发机构下发的根证书。在识别出数字证书后，可以查询数字证书是否与预存的根证书之间存在对应关系，一般每个数字证书与对应的根证书之间存在上下级关系。即本实施例中查询对移动 APP 进行数字签名的数字证书对应的根证书是否存在与预存的根证书中。

[0035] 如果判断出数字证书与预存的一个根证书之间存在上下级关系，说明数字证书对应的根证书存在于预存的根证书中，进一步地判断该数字证书是否在有效期内。一般数字证书的有效期存储在数字证书中，从数字证书中可以得到数字证书的有效期，然后就可以根据有效期判断当前数字证书是否处于有效期内。当判断出该数字证书在有效期内之后，向第三方证书签发机构查询数字证书是否被吊销，接收第三方证书签发机构的查询结果，如果该查询结果指示出该数字证书未被吊销，说明该数字证书合法。

[0036] 可选地，如果移动终端或者移动 APP 市场所在的服务器中未存储有可信的第三方证书签发机构下发的根证书时，在识别出数字证书后，向第三方证书签发机构发送验证请求，其中验证请求中携带该数字证书的标识，以使第三方证书签发机构对数字证书的合法性进行验证。其中，数字证书的标识可以为数字证书的序列号。在第三方证书对数字证书验证完成后，生成该数字证书的验证结果，其中，验证结果指示出数字证书是否合法。从第三方证书签发机构处接收该验证结果，通过该验证结果确定数字证书是否合法。

[0037] 其中，第三方证书签发机构接收到验证请求后，可以查询自身是否存储有数字证书的标识即数字证书的序列号，如果查询到数字证书的标识，说明该数字证书是由自身签发的，然后进一步地验证该数字证书证书是否在有效期内，如果该数字证书在有效期内，判断该数字证书是否被吊销，如果该数字证书未被吊销确定该数字合法，并生成一个数字证书证书的验证结果。

[0038] 103、如果数字证书合法获取数字证书的所有者的身份信息。

[0039] 一般在数字证书中预先存储有该数字证书所有者的身份信息。可选地，如果数字证书中未存储有数字证书所有者的身份信息，向第三方证书签发机构发送获取请求，以请求从第三方证书签发机构中获取数字证书的所有者的身份信息。其中获取请求包括数字证书的标识，例如，数字证书的序列号。

[0040] 104、将数字证书的所有者的身份信息与移动 APP 开发者的身份信息进行比较。

[0041] 从待验证的移动 APP 中获取到移动 APP 开发者的身份信息，将的数字证书的所有者的身份信息与移动 APP 开发者的身份信息进行比较，判断移动 APP 开发者的身份是否合

法。

[0042] 105、如果数字证书的所有者的身份信息与移动 APP 开发者的身份信息一致，判定移动 APP 开发者的身份合法。

[0043] 当数字证书的所有者的身份信息与移动 APP 开发者的身份信息一致，判断出该移动 APP 开发者的身份合法。

[0044] 本实施例中，接收待验证的移动 APP 的设备包括移动 APP 市场所在的服务器和移动终端。对于所述服务器，在判断出移动 APP 开发者的身份合法后，该服务器将待验证的移动 APP 公布在移动 APP 市场上，以供移动终端下载该移动 APP。而且可以将该移动 APP 标记为可信移动 APP。对于移动终端，在判断出移动 APP 开发者的身份合法后，该移动终端安装该移动 APP 以供用户使用该移动 APP。

[0045] 本实施例提供的移动 APP 开发者的身份验证方法，接收待验证的移动 APP，移动 APP 包括签名信息以及移动 APP 开发者的身份信息，签名信息包括用于对移动 APP 进行数字签名的数字证书和签名数据，数字证书是由第三方证书签发机构签发的，从签名信息中识别出数字证书并对数字证书的合法性进行验证，如果数字证书合法，获取数字证书的所有者的身份信息，将所有者的身份信息与开发者的身份信息进行比较，如果所有者的身份信息与开发者的身份信息一致，判定移动 APP 开发者的身份合法。本实施例中通过第三方证书签发机构向移动 APP 的开发者签发数字证书，开发者基于数字证书开发移动 APP，移动 APP 市场的服务器或者移动终端在接收到开发者开发的移动 APP 后，基于数字证书对移动 APP 开发者的身份进行验证，不仅提高了身份验证效率而且可靠性较高，保证了移动 APP 来源的安全性。本实施例中基于数字证书对开发者身份进行验证，使得验证结果具有通用性。

[0046] 图 2 为本发明实施例提供的另一种移动 APP 开发者的身份验证方法的流程示意图。如图 2 所示，该移动 APP 开发者的身份验证方法包括以下步骤：

[0047] 201、第三方证书签发机构接收移动 APP 开发者通过终端发送的用于获取数字证书的获取请求。

[0048] 其中所述获取请求中包括移动 APP 开发者的身份信息。本实施例中移动 APP 开发者的身份信息包括移动 APP 开发者名称、移动 APP 开发者的地址信息、移动 APP 开发者的所属机构、移动 APP 开发者的工商或组织机构信息、移动 APP 开发者的联系方式等信息。

[0049] 202、第三方证书签发机构通过对移动 APP 开发者身份信息的验证后，向移动 APP 开发者下发数字证书。

[0050] 具体地，第三方证书签发机构具有与外部系统交互的接口，例如工商接口、组织机构接口、备案接口、域名接口、身份证接口等。第三方证书签发结构通过这些接口与外部系统进行交互，对移动 APP 开发者的身份信息进行验证或者审核。

[0051] 203、移动 APP 开发者通过所在终端上开发待验证移动 APP，基于数字证书生成用于对待验证移动 APP 进行数字签名的签名信息添加在待验证移动 APP 中。

[0052] 移动 APP 开发者在接收到数字证书后，可以基于数字证书通过终端开发移动 APP，并且在开发移动 APP 的过程中，采用数字证书对该移动 APP 进行数字签名，生成该移动 APP 的签名数据，然后将用于对移动 APP 进行数字签名的数字证书以及签名数据携带在签名信息中，并将该签名信息携带在移动 APP 中。本实施例中通过该签名信息可以指示出对移动 APP 进行数字签名的数字证书。

[0053] 204、移动 APP 开发者通过所在的终端将自身的身份信息添加到经过数字签名后的待验证移动 APP 中。

[0054] 205、移动 APP 开发者通过所在的终端将携带有签名信息和开发者身份信息的待验证移动 APP 上传到移动 APP 市场所在的服务器上。

[0055] 移动 APP 开发者在完成待验证移动 APP 的开发后，向移动 APP 市场所在的服务器上传该携带有签名信息和开发者身份信息的待验证移动 APP，以使服务器将该移动 APP 公布在移动 APP 市场上以供移动终端下载。

[0056] 206、所述服务器从待验证移动 APP 携带的签名信息中识别出该移动 APP 对应的数字证书并对该数字证书的合法性进行验证。

[0057] 移动 APP 市场所在的服务器从待验证移动 APP 携带的签名信息中，识别出该移动 APP 对应的数字证书。在识别出待验证移动 APP 对应的数字证书后，服务器可以查询数字证书是否与预存的根证书之间存在对应关系，一般每个数字证书与对应的根证书之间存在上下级关系。即本实施例中查询对待验证移动 APP 进行数字签名的数字证书对应的根证书是否存在与预存的根证书中。

[0058] 如果判断出待验证移动 APP 对应的数字证书与预存的一个根证书之间存在上下级关系，说明待验证移动 APP 对应的数字证书对应的根证书存在于预存的根证书中。服务器判断该数字证书是否在有效期内。一般数字证书的有效期存储在数字证书中，服务器从待验证移动 APP 对应的数字证书中可以得到数字证书的有效期，然后服务器就可以根据有效期判断当前数字证书是否处于有效期内。当判断出待验证移动 APP 对应的数字证书在有效期内之后，服务器向第三方证书签发机构查询待验证移动 APP 对应的数字证书是否被吊销，接收第三方证书签发机构的查询结果，如果该查询结果指示出该数字证书未被吊销，说明待验证移动 APP 对应的数字证书合法。

[0059] 207、如果待验证移动 APP 对应的数字证书合法，所述服务器获取该数字证书的所有者的身份信息。

[0060] 一般在数字证书中预先存储有该数字证书所有者的身份信息。可选地，如果数字证书中未存储有数字证书所有者的身份信息，向第三方证书签发机构发送获取请求，以请求从第三方证书签发机构中获取数字证书的所有者的身份信息。其中获取请求包括数字证书的标识，例如，数字证书的序列号。

[0061] 208、所述服务器将待验证移动 APP 对应的数字证书的所有者的身份信息与待验证移动 APP 开发者的身份信息进行比较。

[0062] 209、如果待验证移动 APP 对应的数字证书的所有者的身份信息与待验证移动 APP 开发者的身份信息一致，所述服务器判定待验证移动 APP 开发者的身份合法。

[0063] 210、所述服务器将待验证移动 APP 公布在移动 APP 市场上，并将待验证移动 APP 标记为可信移动 APP。

[0064] 服务器将待验证移动 APP 公布在移动 APP 市场上，以供移动终端下载合法来源的移动 APP，并将该移动 APP 标记为可信移动 APP。进一步服务器在公布的移动 APP 下添加该移动 APP 的描述信息以及基本验证信息。而如果判断出待验证移动 APP 开发者的身份不合法，所述服务器将拒绝将待验证移动 APP 公布在移动 APP 市场上，从而保证了移动 APP 市场上的移动 APP 来源的安全性。

[0065] 211、移动终端向所述服务器发送用于请求下载待安装移动 APP 的下载请求。

[0066] 具体地，当移动终端对应的用户试图从移动 APP 市场中下载一个待安装移动 APP 时，可以通过该移动终端向移动 APP 市场所在的服务器，发送一个用于请求下载待安装移动 APP 的下载请求。其中，该下载请求中携带待安装的移动 APP 的标识。服务器通过该标识将对应的待安装移动 APP 下发给移动终端。

[0067] 212、移动终端接收待安装的移动 APP，判断待安装移动 APP 是否为可信移动 APP。

[0068] 本实施例中，由于步骤 210 中当移动 APP 市场所在的服务器判断出移动 APP 开发者的身份合法后，可以将该移动 APP 标记为可信移动 APP。相应地，移动终端在接收到待安装移动 APP 后，可以识别该移动 APP 是否为可信移动 APP，如果判断出待安装移动 APP 并非可信移动 APP 时，执行步骤 213 ；如果判断出待安装移动 APP 为可信移动 APP 时，执行步骤 217。

[0069] 213、移动终端从待安装移动 APP 携带的签名信息中识别出该移动 APP 对应的数字证书并对该数字证书的合法性进行验证。

[0070] 本实施例中，待安装移动 APP 携带该待安装移动 APP 的签名信息以及该移动 APP 开发者的身份信息。其中签名信息包括用于对该移动 APP 进行数字签名的数字证书和签名数据。

[0071] 214、如果待安装移动 APP 对应的数字证书合法，移动终端获取该数字证书的所有者的身份信息。

[0072] 215、移动终端将待安装移动 APP 对应的数字证书的所有者的身份信息与待安装移动 APP 开发者的身份信息进行比较。

[0073] 216、如果待安装移动 APP 对应的数字证书的所有者的身份信息与待安装移动 APP 开发者的身份信息一致，移动终端判定待安装移动 APP 开发者的身份合法。

[0074] 当判断出待安装移动 APP 对应的数字证书的所有者的身份信息与待安装移动 APP 开发者的身份信息一致时，执行步骤 217。

[0075] 其中移动终端执行的步骤 213 ～ 216 类似于服务器执行的步骤 206 ～ 209，此处不再赘述。

[0076] 217、移动终端安装待安装移动 APP。

[0077] 在判断出该待下载移动 APP 开发者的身份合法后，移动终端将在自身安装该移动 APP 以供用户使用该移动 APP。进一步地，在判断出该待安装移动 APP 开发者的身份不合法后，移动终端可以向用户发出提醒信息，提醒用户该移动 APP 存在风险。

[0078] 进一步地，第三方证书签发机构可以接收移动终端对应的用户通过移动终端或者其他终端发送的查询请求，以获取移动 APP 开发者详细的身份信息以及身份信息的验证信息。

[0079] 本实施例中通过第三方证书签发机构向移动 APP 的开发者签发数字证书，开发者在开发移动 APP 的过程中，基于数字证书对移动 APP 开发者的身份信息进行数字签名，当移动 APP 市场的服务器接收到开发者开发的移动 APP 后，基于数字证书对移动 APP 开发者的身份信息进行验证，在身份验证合法后才能将移动 APP 公布到移动 APP 市场上，在移动终端试图安装该移动 APP 时，移动终端再次基于数字证书对移动 APP 开发者的身份进行验证，不仅提高了身份验证的可靠性，增强了对移动 APP 来源的安全性。本实施例中基于数字证书

对开发者身份进行验证，使得验证结果具有通用性。

[0080] 此处需要说明，由于移动终端不仅可以从移动 APP 市场中获取到待安装移动 APP，还可以通过其他途径获取到待安装移动 APP，如互联网相关网站。当移动终端通过其他途径获取待安装移动 APP 时，移动终端需要将执行步骤 213 ～ 216 的过程，以确保待安装移动 APP 的开发者的身份合法。

[0081] 图 3 为本发明实施例提供的一种移动 APP 开发者的身份验证装置的结构示意图。如图 3 所示，该装置包括 :接收模块 31、识别验证模块 32、获取模块 33、比较模块 34 和判定模块 35。

[0082] 第三方证书签发机构可以向移动 APP 开发者签发数字证书，该开发者在开发完移动 APP 时，采用上述数字证书对该移动 APP 进行数字签名，生成该移动 APP 的签名数据，然后将用于对移动 APP 进行数字签名的数字证书以及签名数据携带在签名信息中，并将该签名信息携带在移动 APP 中。本实施例中通过该签名信息可以指示出对该移动 APP 进行数字签名的数字证书。进一步地，移动 APP 开发者通过终端将自身的身份信息携带在移动 APP 中。其中，移动 APP 开发者的数字证书是由第三方证书签发机构签发的。

[0083] 一般接收待验证的移动 APP 的设备可以为移动 APP 市场所在的服务器或者移动终端。例如，在开发者试图将待验证的移动 APP 发布到移动 APP 市场上，则移动 APP 市场所在的服务器可以接收开发者通过网络上传的待验证的移动 APP。当移动终端对应的用户试图安装一个移动 APP 时，移动终端可以接收到一个待验证的移动 APP，其中该待验证的移动 APP 可以为移动终端从移动 APP 市场中下载得到，也可以为移动终端从互联网的相关网站下载得到。

[0084] 本实施例中该移动 APP 开发者的身份验证装置可以设置在移动 APP 市场所在的服务器，也可以设置在移动终端上。

[0085] 移动 APP 开发者的身份验证装置中的接收模块 31 接收待验证的移动 APP，由于移动 APP 携带有签名信息，而且签名信息中包括用于对移动 APP 进行数字签名的数字证书，在接收到待验证的移动 APP 后，识别验证模块 32 从待验证移动 APP 携带的签名信息中识别出该移动 APP 对应的数字证书，并对该数字证书的合法性进行验证。

[0086] 本实施例中在移动终端或者移动 APP 市场所在的服务器中预先存储有可信的第三方证书签发机构下发的根证书。在识别出数字证书后，识别验证模块 32 可以查询数字证书是否与预存的根证书之间存在对应关系，一般每个数字证书与对应的根证书之间存在上下级关系。即本实施例中识别验证模块 32 查询对移动 APP 进行数字签名的数字证书对应的根证书是否存在与预存的根证书中。

[0087] 如果判断出数字证书与预存的一个根证书之间存在上下级关系，说明数字证书对应的根证书存在于预存的根证书中。识别验证模块 32 判断该数字证书是否在有效期内。一般数字证书的有效期存储在数字证书中，识别验证模块 32 从数字证书中可以得到数字证书的有效期，然后就可以根据有效期判断当前数字证书是否处于有效期内。当判断出该数字证书在有效期内之后，识别验证模块 32 向第三方证书签发机构查询数字证书是否被吊销，接收第三方证书签发机构的查询结果，如果该查询结果指示出该数字证书未被吊销，说明该数字证书合法。

[0088] 可选地，如果移动终端或者移动 APP 市场所在的服务器中未存储有可信的第三方

证书签发机构下发的根证书时，在识别出数字证书后，识别验证模块 32 向第三方证书签发机构发送验证请求，其中验证请求中携带该数字证书的标识，以使第三方证书签发机构对数字证书的合法性进行验证。其中，数字证书的标识可以为数字证书的序列号。在第三方证书对数字证书验证完成后，生成该数字证书的验证结果，其中验证结果指示出数字证书是否合法。识别验证模块 32 从第三方证书签发机构处接收该验证结果，通过该验证结果确定数字证书是否合法。其中，关于第三方证书签发机构对数字证书合法性的验证过程，参见上述实施例中相关内容的记载，此处不再赘述

[0089] 识别验证模块 32 与获取模块 33 连接，在识别验证模块 32 验证出数字证书合法后，获取模块 33 获取数字证书的所有者的身份信息。

[0090] 一般在数字证书中预先存储有该数字证书所有者的身份信息。可选地，如果数字证书中未存储有数字证书所有者的身份信息，获取模块 33 向第三方证书签发机构发送获取请求，以请求从第三方证书签发机构中获取数字证书的所有者的身份信息。其中获取请求包括数字证书的标识，例如，数字证书的序列号。

[0091] 获取模块 33 与比较模块 34 连接，比较模块 34 将数字证书的所有者的身份信息与开发者的身份信息进行比较，以判断移动 APP 开发者的身份是否合法。

[0092] 具体地，比较模块 34 从待验证的移动 APP 中获取到移动 APP 开发者的身份信息，将的数字证书的所有者的身份信息与移动 APP 开发者的身份信息进行比较。比较莫 34 与判定模块 35 连接，在比较模块 34 比较出数字证书的所有者的身份信息与移动 APP 开发者的身份信息一致，判定模块 35 判断出该移动 APP 开发者的身份合法。

[0093] 本实施例提供的移动 APP 开发者的身份验证装置，接收待验证的移动 APP，移动 APP 包括签名信息以及移动APP 开发者的身份信息，签名信息包括用于对移动APP 进行数字签名的数字证书和签名数据，数字证书是由第三方证书签发机构签发的，从签名信息中识别出数字证书，对数字证书的合法性进行验证，如果数字证书合法，获取数字证书的所有者的身份信息，将所有者的身份信息与开发者的身份信息进行比较，如果所有者的身份信息与开发者的身份信息一致，判定移动 APP 开发者的身份合法。本实施例中通过第三方证书签发机构向移动 APP 的开发者签发数字证书，开发者基于数字证书开发移动 APP，移动 APP 市场的服务器或者移动终端在接收到开发者开发的移动 APP 后，基于数字证书对移动 APP 开发者的身份进行验证，不仅提高了身份验证效率而且可靠性较高，保证了移动 APP 来源的安全性。本实施例中基于数字证书对开发者身份进行验证，使得验证结果具有通用性。

[0094] 进一步地，本实施例中，接收待验证的移动APP 的设备包括移动 APP 市场所在的服务器和移动终端。该移动 APP 开发者的身份验证装置还包括执行模块 36。

[0095] 对于所述服务器，在判定模块 35 判断出移动 APP 开发者的身份合法后，则执行模块 36 将待验证的移动 APP 公布在移动 APP 市场上，以供移动终端下载该移动 APP。而且可以将该移动 APP 标记为可信移动 APP。对于移动终端，在判定模块 35 判断出移动 APP 开发者的身份合法后，则执行模块 36 将移动 APP 按照在移动终端上，以供用户使用该移动 APP。

[0096] 图 4 为本发明实施例提供的一种识别验证模块的结构示意图。如图 4 所示，该识别验证模块 32 包括 :第一识别单元 321、判断单元 322、查询单元 323 和验证单元 324。

[0097] 如果在移动终端或者移动 APP 市场所在的服务器中预先存储有可信的第三方证书签发机构下发的根证书。

[0098] 与接收模块 31 连接到第一识别单元 321 用于从待验证移动 APP 携带的签名信息中识别出待验证移动 APP 对应的数字证书。

[0099] 与第一识别单元 321 连接的判断单元 322 用于判断数字证书是否与预存的根证书之间存在对应关系，以及在数字证书与预存的根证书存在对应关系时，判断数字证书是否在有效期内。

[0100] 其中，预存的根证书是由第三方证书签发机构下发的。

[0101] 一般数字证书的有效期存储在数字证书中，判断单元 322 从数字证书中可以得到数字证书的有效期，根据有效期判断当前数字证书是否处于有效期内。

[0102] 与判断单元 322 连接的查询单元 323 用于在判断单元 322 判断出数字证书在有效期内，向第三方证书签发机构查询数字证书是否被吊销。

[0103] 分别与查询单元 323 和获取模块 33 连接的验证单元 324 用于在查询单元 323 查询出数字证书未被吊销之后，判定数字证书为合法的数字证书。

[0104] 图 5 为本发明实施例提供的另一种识别验证模块的结构示意图。如图 5 所示，该识别验证模块 32 包括 ：第二识别单元 325、发送单元 326 和接收单元 327。

[0105] 如果在移动终端或者移动 APP 市场所在的服务器中未预先存储有可信的第三方证书签发机构下发的根证书。

[0106] 与接收模块 31 连接的第二识别单元 325 用于从待验证移动 APP 携带的签名信息中识别出该移动 APP 对应的数字证书。

[0107] 与第二识别单元 325 连接的发送单元 326 用于向第三方证书签发机构发送验证请求，以使第三方证书签发机构对数字证书的合法性进行验证。

[0108] 其中验证请求中携带数字证书的标识，如数字证书的序列号。

[0109] 与获取模块 33 连接的接收单元 327 用于接收第三方证书签发机构返回的验证结果，其中验证结果指示出数字证书是否合法。

[0110] 本实施例中通过该验证结果确定数字证书是否合法。

[0111] 图 6 为本发明实施例提供的一种移动 APP 开发者身份验证的系统结构示意图。如图 6 所示，该系统包括 ：第三方证书签发机构 1、终端 2、服务器 3、移动终端 4 和其他终端 5。其中，终端 2 为移动 APP 开发者所在的终端，服务器 3 为移动 APP 市场所在的服务器。其中，服务器 3 和移动终端 4 中分别设置有移动 APP 开发者的身份验证装置。

[0112] 第三方证书签发机构 1 接收移动 APP 开发者通过终端 2 发送的用于获取数字证书的获取请求。其中所述获取请求中包括移动 APP 开发者的身份信息。本实施例中移动 APP 开发者的身份信息包括移动 APP 开发者名称、移动 APP 开发者的地址信息、移动 APP 开发者的所属机构、移动 APP 开发者的工商或组织机构信息、移动 APP 开发者的联系方式等信息。

[0113] 第三方证书签发机构 1 通过对移动 APP 开发者身份信息的验证后，向移动 APP 开发者下发数字证书。具体地，第三方证书签发机构 1 具有与外部系统交互的接口，例如工商接口、组织机构接口、备案接口、域名接口、身份证接口等。第三方证书签发结构通过这些接口与外部系统进行交互，对移动 APP 开发者的身份信息进行验证或者审核。

[0114] 移动 APP 开发者通过所在终端 2 在开发的待验证移动 APP，基于数字证书生成用于对待验证移动 APP 进行数字签名的签名信息添加在待验证移动 APP 中。移动 APP 开发者在接收到数字证书后，可以基于数字证书通过终端 2 开发移动 APP，并且在开发移动 APP 的过

程中，采用数字证书对该移动 APP 进行数字签名，得到该数字证书的签名信息。该签名信息可以指示出对移动 APP 进行数字签名的数字证书。也就是说，基于数字证书为待验证移动 APP 生成一个签名信息，通过该签名信息可以指示出该移动 APP 开发者对应的数字证书。

[0115] 移动 APP 开发者通过所在的终端 2 将自身的身份信息添加到经过数字签名后的待验证移动 APP 中。移动 APP 开发者在完成待验证移动 APP 的开发后，通过终端 2 向移动 APP 市场所在的服务器 3 上传该携带有签名信息和开发者身份信息的待验证移动 APP，以使服务器 3 将该移动 APP 公布在移动 APP 市场上以供移动终端 4 下载。

[0116] 移动 APP 市场所在的服务器 3 从待验证移动 APP 携带的签名信息中，识别出该移动 APP 对应的数字证书。在识别出待验证移动 APP 对应的数字证书后，服务器 3 可以查询数字证书是否与预存的根证书之间存在对应关系，一般每个数字证书与对应的根证书之间存在上下级关系。即本实施例中查询对待验证移动 APP 进行数字签名的数字证书对应的根证书是否存在与预存的根证书中。

[0117] 如果判断出待验证移动 APP 对应的数字证书与预存的一个根证书之间存在上下级关系，说明待验证移动 APP 对应的数字证书对应的根证书存在于预存的根证书中。服务器 3 判断该数字证书是否在有效期内。一般数字证书的有效期存储在数字证书中，服务器 3 从待验证移动 APP 对应的数字证书中可以得到数字证书的有效期，服务器 3 根据有效期判断当前数字证书是否处于有效期内。当判断出待验证移动 APP 对应的数字证书在有效期内之后，服务器 3 向第三方证书签发机构 1 查询待验证移动 APP 对应的数字证书是否被吊销，接收第三方证书签发机构 1 的查询结果，如果该查询结果指示出该数字证书未被吊销，说明待验证移动 APP 对应的数字证书合法。

[0118] 如果待验证移动 APP 对应的数字证书合法，服务器 3 获取该数字证书的所有者的身份信息。一般在数字证书中预先存储有该数字证书所有者的身份信息。可选地，如果数字证书中未存储有数字证书所有者的身份信息，服务器 3 向第三方证书签发机构 1 发送获取请求，以请求从第三方证书签发机构 1 中获取数字证书的所有者的身份信息。其中获取请求包括数字证书的标识，例如，数字证书的序列号。

[0119] 服务器 3 将待验证移动 APP 对应的数字证书的所有者的身份信息与待验证移动 APP 开发者的身份信息进行比较。如果待验证移动 APP 对应的数字证书的所有者的身份信息与待验证移动 APP 开发者的身份信息一致，服务器 3 判定待验证移动 APP 开发者的身份合法。服务器 3 将待验证移动 APP 公布在移动 APP 市场上，并将待验证移动 APP 标记为可信移动 APP。服务器 3 还可以在公布的移动 APP 下添加该移动 APP 的描述信息以及基本验证信息。而如果判断出待验证移动 APP 开发者的身份不合法，服务器 3 将拒绝将待验证移动 APP 公布在移动 APP 市场上，从而保证了移动 APP 市场上的移动 APP 来源的安全性。

[0120] 当移动终端 4 对应的用户试图从移动 APP 市场中下载一个待安装移动 APP 时，可以通过该移动终端 4 向移动 APP 市场所在的服务器 3，发送一个用于请求下载待安装移动 APP 的下载请求。其中，该下载请求中携带待安装的移动 APP 的标识。服务器 3 通过该标识将对应的待安装移动 APP 下发给移动终端 4。

[0121] 本实施例中，由于当移动 APP 市场所在的服务器 3 判断出移动 APP 开发者的身份合法后，可以将该移动 APP 标记为可信移动 APP。相应地，移动终端 4 在接收到待安装移动 APP 后，可以识别该移动 APP 是否为可信移动 APP，如果判断出待安装移动 APP 并非可信移

动 APP 时，移动终端 4 识别出待安装移动 APP 对应的数字证书并对该数字证书的合法性进行验证。待安装移动 APP 携带该移动 APP 的签名信息以及该待安装移动 APP 开发者的身份信息，其中签名信息包括用于对该移动 APP 进行数字签名的数字证书和签名数据，以及如果待安装移动 APP 对应的数字证书合法，移动终端 4 获取该数字证书的所有者的身份信息。

[0122] 移动终端 4 将待安装移动 APP 对应的数字证书的所有者的身份信息与待安装移动 APP 开发者的身份信息进行比较。如果待安装移动 APP 对应的数字证书的所有者的身份信息与待安装移动 APP 开发者的身份信息一致，移动终端 4 判定待安装移动 APP 开发者的身份合法。移动终端 4 上述验证过程，类似为服务器 3 的验证过程，此处不再赘述。

[0123] 在判断出该待下载移动 APP 开发者的身份合法后，移动终端 4 将在自身安装该移动 APP 以供用户使用该移动 APP。进一步地，在判断出该待安装移动 APP 开发者的身份不合法后，移动终端 4 可以向用户发出提醒信息，提醒用户该移动 APP 存在风险。

[0124] 进一步地，第三方证书签发机构 1 可以接收移动终端 4 对应的用户通过移动终端 4 或者其他终端 5 发送的查询请求，以获取移动 APP 开发者详细的身份信息以及身份信息的验证信息。

[0125] 本实施例中通过第三方证书签发机构向移动 APP 的开发者签发数字证书，开发者在开发移动 APP 的过程中，基于数字证书对移动 APP 开发者的身份信息进行数字签名，当移动 APP 市场的服务器接收到开发者开发的移动 APP 后，基于数字证书对移动 APP 开发者的身份信息进行验证，在身份验证合法后才能将移动 APP 公布到移动 APP 市场上，在移动终端试图安装该移动 APP 时，移动终端 4 再次基于数字证书对移动 APP 开发者的身份进行验证，不仅提高了身份验证的可靠性，增强了对移动 APP 来源的安全性。

[0126] 此处需要说明，由于移动终端 4 不仅可以从移动 APP 市场中获取到待安装移动 APP，还可以通过其他途径获取到待安装移动 APP，如互联网相关网站。当移动终端 4 通过其他途径获取待安装移动 APP 时，移动终端 4 需要将上验证过程，以确保待安装移动 APP 的开发者的身份合法。

[0127] 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。

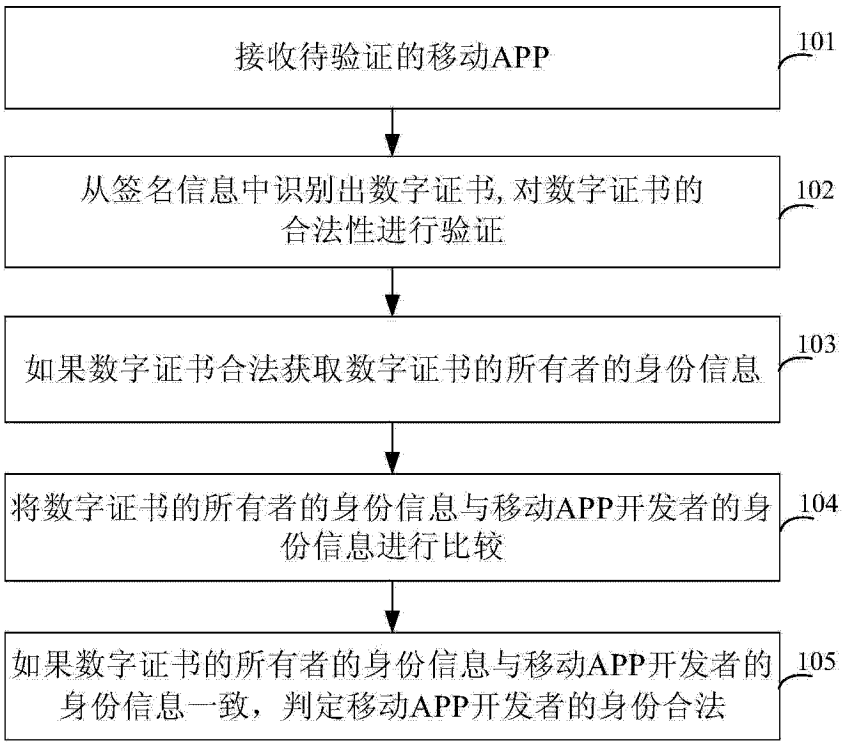

接收待验证的移动APP
101
从签名信息中识别出数字证书，对数字证书的合法性进行验证
102
如果数字证书合法获取数字证书的所有者的身份信息
103
将数字证书的所有者的身份信息与移动APP开发者的身份信息进行比较
104
如果数字证书的所有者的身份信息与移动APP开发者的身份信息一致，判定移动APP开发者的身份合法
105

图 1

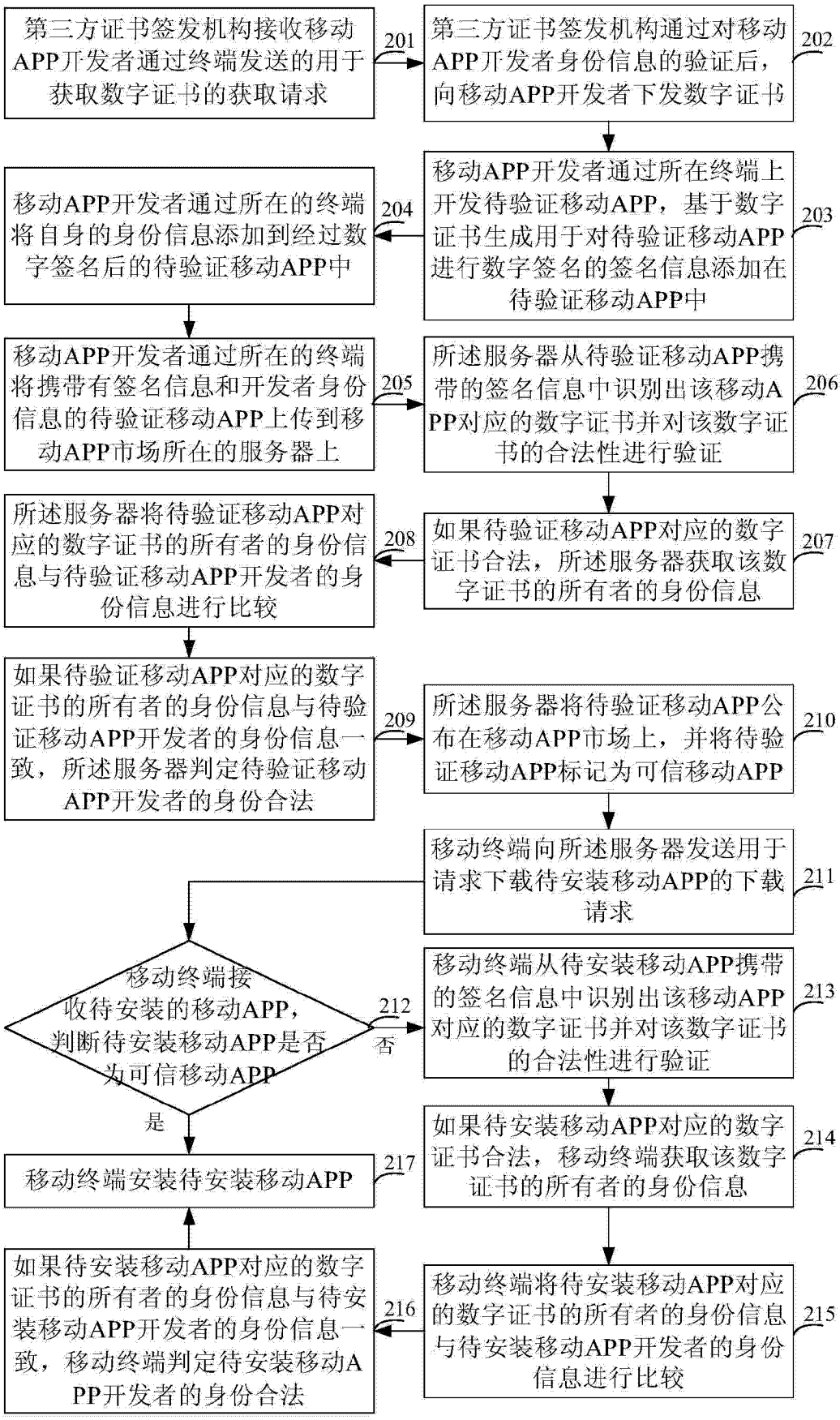

第三方证书签发机构接收移动APP开发者通过终端发送的用于获取数字证书的获取请求
201
第三方证书签发机构通过对移动APP开发者身份信息的验证后，向移动APP开发者下发数字证书
202
移动APP开发者通过所在终端上开发待验证移动APP，基于数字证书生成用于对待验证移动APP进行数字签名的签名信息添加在待验证移动APP中
203
移动APP开发者通过所在的终端将自身的身份信息添加到经过数字签名后的待验证移动APP中
204
移动APP开发者通过所在的终端将携带有签名信息和开发者身份信息的待验证移动APP上传到移动APP市场所在的服务器上
205
所述服务器从待验证移动APP携带的签名信息中识别出该移动APP对应的数字证书并对该数字证书的合法性进行验证
206
如果待验证移动APP对应的数字证书合法，所述服务器获取该数字证书的所有者的身份信息
207
所述服务器将待验证移动APP对应的数字证书的所有者的身份信息与待验证移动APP开发者的身份信息进行比较
208
如果待验证移动APP对应的数字证书的所有者的身份信息与待验证移动APP开发者的身份信息一致，所述服务器判定待验证移动APP开发者的身份合法
209
所述服务器将待验证移动APP公布在移动APP市场上，并将待验证移动APP标记为可信移动APP
210
移动终端向所述服务器发送用于请求下载待安装移动APP的下载请求
211
移动终端接收待安装的移动APP，判断待安装移动APP是否为可信移动APP
212
否
是
移动终端从待安装移动APP携带的签名信息中识别出该移动APP对应的数字证书并对该数字证书的合法性进行验证
213
如果待安装移动APP对应的数字证书合法，移动终端获取该数字证书的所有者的身份信息
214
移动终端将待安装移动APP对应的数字证书的所有者的身份信息与待安装移动APP开发者的身份信息进行比较
215
如果待安装移动APP对应的数字证书的所有者的身份信息与待安装移动APP开发者的身份信息一致，移动终端判定待安装移动APP开发者的身份合法
216
移动终端安装待安装移动APP
217

图 2

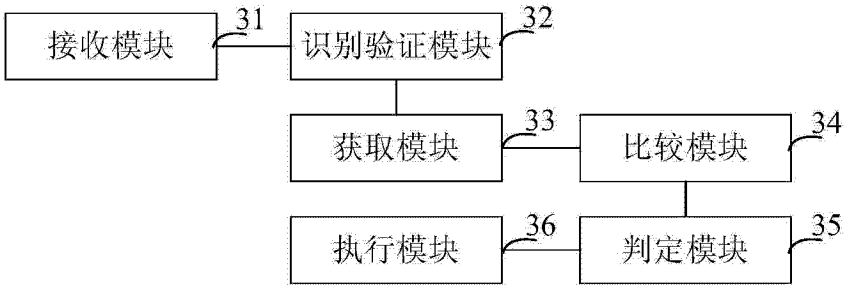

接收模块
31
识别验证模块
32
获取模块
33
比较模块
34
执行模块
36
判定模块
35

图 3

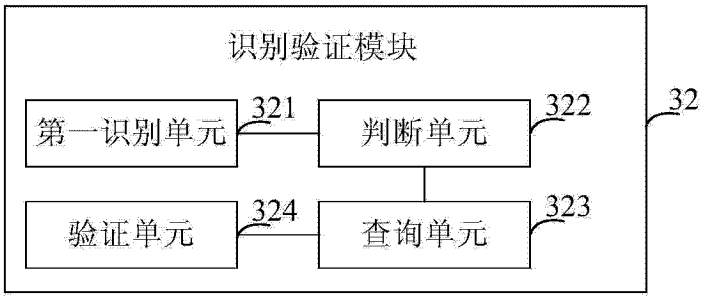

识别验证模块
第一识别单元
321
判断单元
322
32
验证单元
324
查询单元
323

图 4

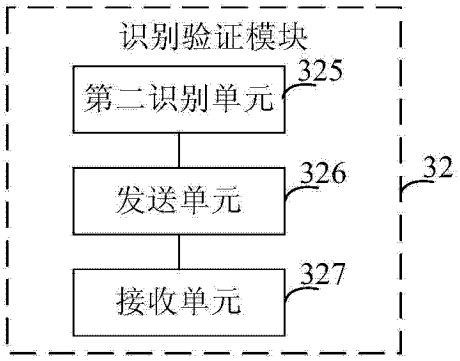

识别验证模块
第二识别单元
325
发送单元
326
32
接收单元
327

图 5

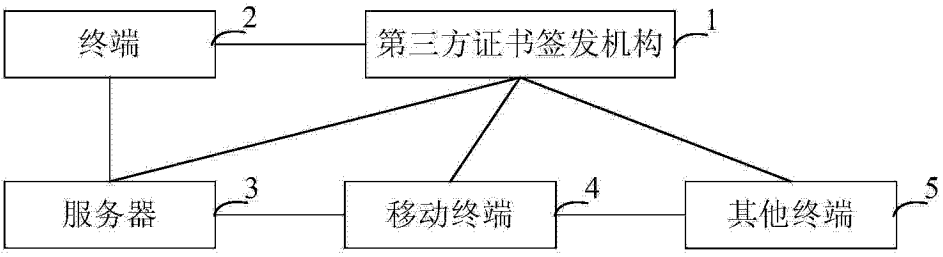

终端
2
第三方证书签发机构
1
服务器
3
移动终端
4
其他终端
5

图 6