(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 103812871 A
(43)申请公布日 2014.05.21

(21)申请号 201410062383.5

(22)申请日 2014.02.24

(71)申请人 北京明朝万达科技有限公司
地址 100088 北京市海淀区知春路太月园3号楼6层

(72)发明人 张帅 咸赫男 喻波 王志华

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04W 12/06(2009.01)

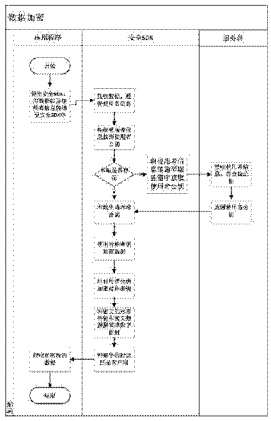
权利要求书2页 说明书7页 附图9页

(54)发明名称

一种基于移动终端应用程序安全应用的开发方法及系统

(57)摘要

本发明公开了一种基于移动终端应用程序安全应用的开发方法及系统，该系统包括：发送终端，安全SDK，服务器，接收终端；该方法包括：发送终端向服务器请求随机数，在接收到请求的随机数后，调用发送终端私钥对该随机数进行签名，并将签名结果和签名公钥证书发送至所述服务器；身份认证成功后，调用安全SDK，使用对称密钥对接收的所述数据信息进行加密，采用所述接收终端公钥对该对称密钥进行加密，将经加密的对称密钥和数据信息发送给接收终端；所述接收终端调用所述安全SDK解密密文数据；通过本发明避免了数据信息安全的相关问题，包括身份认证、数据外泄、设备管控等。



CN 103812871 A

1. 一种基于移动终端应用程序安全应用的开发方法，该方法包括如下步骤：

1）发送终端向服务器请求随机数，在接收到请求的随机数后，调用发送终端私钥对该随机数进行签名，并将签名结果和签名公钥证书发送至所述服务器，该服务器进行证书有效性验证并验签，返回认证结果，如果验证通过，跳至步骤 2）；

2）发送终端调用安全 SDK，并向所述 SDK 发送用户信息及数据信息，所述安全 SDK 根据所述用户信息获取接收终端公钥，然后在本地产生对称密钥，并使用该对称密钥对接收的所述数据信息进行加密，采用所述接收终端公钥对该对称密钥进行加密，将经加密的对称密钥和数据信息拼装成数字信封，最后将该数字信封返回到发送终端；

3）发送终端向接收终端发送上述数字信封；

4）所述接收终端接收到所述数字信封后，调用所述安全 SDK，该安全 SDK 解析所述数字信封，解析出密文对称密钥和密文数据，使用接收终端私钥解密密文对称密钥，使用明文对称密钥解密密文数据。

2. 根据权利要求 1 所述的方法，所述步骤 1）中，发送终端在接收到请求的随机数后，进行枚举设备、打开设备、枚举证书，然后验证 PIN 码，如果验证失败，则结束验证流程，如果验证成功，才继续后续的验证步骤。

3. 根据权利要求 1 所述的方法，所述步骤 2）中所述安全 SDK 根据所述用户信息获取所述接收终端公钥包括：所述安全 SDK 根据所述用户信息在本地查找所述接收终端公钥，如果本地不存在，则将所述用户信息发送到服务器，从所述服务器接收所述接收终端公钥。

4. 根据权利要求 1 所述的方法，所述发送终端和接收终端分别为发送邮件终端和接收邮件终端，所述服务器包括邮件安全管理平台和邮件服务器，所述发送邮件终端通过该邮件服务器向所述接收邮件终端发送邮件。

5. 根据权利要求 4 所述的方法，所述步骤 2）中发送邮件终端调用所述安全 SDK，并向所述安全 SDK 发送明文的 E-mail、邮件接收者列表，所述安全 SDK 根据该邮件接收者列表获取接收邮件终端公钥，并验证该公钥的有效性，验证通过后，对邮件签名。

6. 根据权利要求 5 所述的方法，所述步骤 4）中使用明文对称密钥解密密文数据后，需要验证接收邮件终端公钥的有效性。

7. 一种基于移动终端应用程序安全应用的开发系统，该系统包括：发送终端，安全 SDK，服务器，接收终端；

发送终端向服务器请求随机数，在接收到请求的随机数后，调用发送终端私钥对该随机数进行签名，并将签名结果和签名公钥证书发送至所述服务器，该服务器进行证书有效性验证并验签，返回认证结果；发送终端在身份认证成功后，调用安全 SDK，并向所述 SDK 发送用户信息及数据信息，所述安全 SDK 根据所述用户信息获取接收终端公钥，然后在本地产生对称密钥，并使用该对称密钥对接收的所述数据信息进行加密，采用所述接收终端公钥对该对称密钥进行加密，将经加密的对称密钥和数据信息拼装成数字信封，最后将该数字信封返回到发送终端，发送终端向接收终端发送上述数字信封；所述接收终端接收到所述数字信封后，调用所述安全 SDK，该安全 SDK 解析所述数字信封，解析出密文对称密钥和密文数据，使用接收终端私钥解密密文对称密钥，使用明文对称密钥解密密文数据。

8. 根据权利要求 7 所述的系统，发送终端在接收到请求的随机数后，进行枚举设备、打开设备、枚举证书，然后验证 PIN 码，如果验证失败，则结束验证流程，如果验证成功，才继

续后续的验证步骤。

9. 根据权利要求 7 所述的系统，所述安全 SDK 根据所述用户信息获取所述接收终端公钥包括：所述安全 SDK 根据所述用户信息在本地查找所述接收终端公钥，如果本地不存在，则将所述用户信息发送到服务器，从所述服务器接收所述接收终端公钥。

10. 根据权利要求 7 所述的系统，所述发送终端和接收终端分别为发送邮件终端和接收邮件终端，所述服务器包括邮件安全管理平台和邮件服务器，所述发送邮件终端通过该邮件服务器向所述接收邮件终端发送邮件。

11. 根据权利要求 10 所述的系统，所述发送邮件终端调用所述安全 SDK，并向所述安全 SDK 发送明文的 E-mail、邮件接收者列表，所述安全 SDK 根据该邮件接收者列表获取接收邮件终端公钥，并验证该公钥的有效性，验证通过后，对邮件签名。

12. 根据权利要求 10 所述的系统，所述安全 SDK 使用明文对称密钥解密密文数据后，需要验证接收邮件终端公钥的有效性。

13. 根据权利要求 7 所述的系统，该系统还包括一数据库，用于针对 sqlite3 的页面文件进行加密和解密。14. 根据权利要求 13 所述的系统，该系统还包括一移动管理控制台，提供一个 UI 操作界面，对移动终端行为以及用户进行管控，包括用户管理、策略配置、日志审计。

一种基于移动终端应用程序安全应用的开发方法及系统

技术领域

[0001] 本发明涉及一种移动终端数据安全领域，尤其涉及一种基于移动终端应用程序安全应用的开发方法及系统。

背景技术

[0002] PKI :Public Key Infrastructure，即公钥基础设施，是一种遵循既定标准的密钥管理平台，它能够为所有信息安全应用提供加解密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI 技术是信息安全技术的核心，也是电子商务的关键和基础技术。

[0003] 证书 SDK :Software Development Kit，基于 PKI 体系，一个可以提供安全支撑的开发平台，内部对不同类型，不同介质，不同规范的证书操作进行统一接口封装，用户无需要关心复杂的安全细节，只需调用相应接口得到自己相要的结果数据（如 P1，P7 签验，数据信封，对称加解密，HASH 等等）。本 SDK 要支持跨平台，支持主流的 CSP，P11，国密规范，支持软硬证书。

[0004] HMAC :Hash-based Message Authentication Code，是密钥相关的哈希运算消息认证码，HMAC 运算利用哈希算法，以一个密钥和一个消息为输入，生成一个消息摘要作为输出。

[0005] 随着信息时代的进步和发展，移动智能手机得到了迅速的普及，移动终端应用作为智能手机的核心，不计其数、种类繁多的移动终端应用程序占领了移动应用市场，这些应用满足了用户不同方面的需求。从用户交互形式上可以分为 :用户登录、用户注册、用户认证等，从文本数据信息传输上可以分为 :云电话、邮件、查看文档、文件存储。从信息展示展示上可以分为 :通讯录、邮件、浏览器等应用 ;移动终端应用提供信息展示、传输以及存储的功能，而没有考虑到利用加密技术进行封装，保证数据全生命周期的安全管理。

[0006] 现有使用比较广泛的一些系统都是以口令、域认证以及密码锁作为身份认证，并且对于数据的传输全部采用明文方式 ;数据都是以明文存储到本地 ;

[0007]

	基础方式
身份认证	用户名、口令、图形密码锁
数据传输	明文传输
数据存储	明文存储

[0008] 目前的移动终端应用主要存在的问题 :

[0009] 1. 使用口令或密码锁进行身份认证，密码强度较弱，无法确保身份安全 ;

[0010] 2. 数据传输过程中，明文传输，数据有可能被监听 ;

[0011] 3. 使用移动终端下载查看文件为明文，无法确保数据安全。

[0012] 现有技术中存在基础 SDK，作为移动终端应用的功能支撑，一些开发商将一些基础功能封装到 SDK 中，提供给移动应用开发人员，上层业务逻辑调用基础 SDK 即可快速实现相应的功能，对于移动终端某项应用的功能进行统一的管理、维护，这提高了代码的复用性、工作效率以及降低公司成本。

[0013] 现有的 SDK 针对于用户认证、数据传输、设备管理、第三方应用等功能进行封装，从而对用户的认证提供用户名口令认证方式，针对数据存储提供 SQLite、XML 等技术的封装，对网络提供 Http、TCP 等方式收发高级封装。

[0014] 图 1 是现有技术中邮件 SDK 所具备的功能结构图，图 2 是现有技术中移动终端邮件发送流程图。

[0015] 如图 1 所示，现有的邮件 SDK 包括以下功能组件：口令登录组件，发送邮件组件，创建邮件组件，接收邮件组件，数据库组件，配置组件。

[0016] 现有技术中的邮件系统包括：邮件客户端，邮件 SDK，邮件服务器，邮件发送流程如下：

[0017] 1）邮件客户端的邮件 APP 开始发送邮件；

[0018] 2）邮件 APP 调用 SDK 发送邮件接口；

[0019] 3）邮件 SDK 接收到邮件数据后，将邮件数据传递至邮件服务器；

[0020] 4）邮件服务器接收邮件数据；

[0021] 5）根据接收者地址，邮件服务器将数据发送到邮件接收者处；

[0022] 6）邮件服务器返回结果信息；

[0023] 7）邮件 SDK 将发送结果信息返回；

[0024] 8）邮件客户端接收发送结果信息；

[0025] 9）结束。

[0026] 封装基础应用 SDK 是各个厂商常用的一种方式，如提供邮件移动终端 SDK、通讯录 SDK、网络数据传输 SDK、数据存储 XML、SQLite 等都封装了基础 SDK，为上层应用提供快速开发接口。但大多数的基础 SDK 并未考虑如何保障身份认证本身安全性，如防止回放攻击，防止身份伪装欺骗，在网络传输上过多考虑的是传输效率，或模型轻便，并没有考虑是否存在泄密等安全隐患，文件数据在传输过程中可能被监听；在数据存储方面以明文方式存储到本地可能被窃取，并没有做权限控制与文档生命周期管理；缺乏统一管理、统一保护

发明内容

[0027] 为了解决移动终端应用程序安全应用的开发问题，本发明提出了一种基于移动终端应用程序安全应用的开发方法，该方法包括如下步骤：

[0028] 1）发送终端向服务器请求随机数，在接收到请求的随机数后，调用发送终端私钥对该随机数进行签名，并将签名结果和签名公钥证书发送至所述服务器，该服务器进行证书有效性验证并验签，返回认证结果，如果验证通过，跳至步骤 2）；

[0029] 2）发送终端调用安全 SDK，并向所述 SDK 发送用户信息及数据信息，所述安全 SDK 根据所述用户信息获取接收终端公钥，然后在本地产生对称密钥，并使用该对称密钥对接收的所述数据信息进行加密，采用所述接收终端公钥对该对称密钥进行加密，将经加密的对称密钥和数据信息拼装成数字信封，最后将该数字信封返回到发送终端；

[0030] 3）发送终端向接收终端发送上述数字信封；

[0031] 4)所述接收终端接收到所述数字信封后，调用所述安全 SDK，该安全 SDK 解析所述数字信封，解析出密文对称密钥和密文数据，使用接收终端私钥解密密文对称密钥，使用明文对称密钥解密密文数据，将解密的明文数据信息传递到接收终端的应用层。

[0032] 进一步的，所述步骤 1）中，发送终端在接收到请求的随机数后，进行枚举设备、打开设备、枚举证书，然后验证 PIN 码，如果验证失败，则结束验证流程，如果验证成功，才继续后续的验证步骤。

[0033] 进一步的，所述步骤 2)中所述安全 SDK 根据所述用户信息获取所述接收终端公钥包括：所述安全 SDK 根据所述用户信息在本地查找所述接收终端公钥，如果本地不存在，则将所述用户信息发送到服务器，从所述服务器接收所述接收终端公钥。

[0034] 进一步的，所述发送终端和接收终端分别为发送邮件终端和接收邮件终端，所述服务器包括邮件安全管理平台和邮件服务器，所述发送邮件终端通过该邮件服务器向所述接收邮件终端发送邮件。

[0035] 进一步的，所述步骤 2)中发送邮件终端调用所述安全 SDK，并向所述安全 SDK 发送明文的 E-mail、邮件接收者列表，所述安全 SDK 根据该邮件接收者列表获取接收邮件终端公钥，并验证该公钥的有效性，验证通过后，对邮件签名。

[0036] 进一步的，所述步骤 4）中使用明文对称密钥解密密文数据后，需要验证接收邮件终端公钥的有效性。

[0037] 为了解决移动终端应用程序安全应用的开发问题，本发明还提出了一种基于移动终端应用程序安全应用的开发系统，该系统包括：发送终端，安全 SDK，服务器，接收终端；

[0038] 发送终端向服务器请求随机数，在接收到请求的随机数后，调用发送终端私钥对该随机数进行签名，并将签名结果和签名公钥证书发送至所述服务器，该服务器进行证书有效性验证并验签，返回认证结果；发送终端在身份认证成功后，调用安全 SDK，并向所述 SDK 发送用户信息及数据信息，所述安全 SDK 根据所述用户信息获取接收终端公钥，然后在本地产生对称密钥，并使用该对称密钥对接收的所述数据信息进行加密，采用所述接收终端公钥对该对称密钥进行加密，将经加密的对称密钥和数据信息拼装成数字信封，最后将该数字信封返回到发送终端，发送终端向接收终端发送上述数字信封；所述接收终端接收到所述数字信封后，调用所述安全 SDK，该安全 SDK 解析所述数字信封，解析出密文对称密钥和密文数据，使用接收终端私钥解密密文对称密钥，使用明文对称密钥解密密文数据，将解密的明文数据信息传递到接收终端的应用层。

[0039] 进一步的，发送终端在接收到请求的随机数后，进行枚举设备、打开设备、枚举证书，然后验证 PIN 码，如果验证失败，则结束验证流程，如果验证成功，才继续后续的验证步骤。

[0040] 进一步的，所述安全 SDK 根据所述用户信息获取所述接收终端公钥包括：所述安全 SDK 根据所述用户信息在本地查找所述接收终端公钥，如果本地不存在，则将所述用户信息发送到服务器，从所述服务器接收所述接收终端公钥。

[0041] 进一步的，所述发送终端和接收终端分别为发送邮件终端和接收邮件终端，所述服务器包括邮件安全管理平台和邮件服务器，所述发送邮件终端通过该邮件服务器向所述接收邮件终端发送邮件。

[0042] 进一步的，发送邮件终端调用所述安全 SDK，并向所述安全 SDK 发送明文的 E-mail、邮件接收者列表，所述安全 SDK 根据该邮件接收者列表获取接收邮件终端公钥，用发送邮件终端的私钥对邮件做签名，使用证书设备生产对称密钥，并加密邮件，用接收终端公钥加密对称密钥并与密文邮件封装成数字信封，组装成安全邮件 E-mail，将该安全邮件 E-mail 发送至邮件服务器。

[0043] 进一步的，所述发送邮件终端调用所述安全 SDK，并向所述安全 SDK 发送明文的 E-mail、邮件接收者列表，所述安全 SDK 根据该邮件接收者列表获取接收邮件终端公钥，并验证该公钥的有效性，验证通过后，对邮件签名。

[0044] 进一步的，所述安全 SDK 使用明文对称密钥解密密文数据后，需要验证接收邮件终端公钥的有效性。

[0045] 进一步的，该系统还包括一数据库，用于针对 sqlite3 的页面文件进行加密和解密。

[0046] 进一步的，该系统还包括一移动管理控制台，提供一个 UI 操作界面，对移动终端行为以及用户进行管控，包括用户管理、策略配置、日志审计。

[0047] 通过本发明提出的方案，取得了以下技术效果：

[0048] 第三方应用调用本 SDK 后，可以基本避免数据信息安全的相关问题，包括身份认证、数据外泄、设备管控等。因为用户的身份和硬件设备中的证书是相互绑定的。如果没有此硬件设备，相关的人就不能查看加密数据信息。就算数据信息在传输中被监听截取，但监听者也没有办法对数据信息进行解密，使其得到的数据没有任何意义。

附图说明

[0049] 图 1 是现有技术中邮件 SDK 所具备的功能组件图。

[0050] 图 2 是现有技术中移动终端邮件发送流程图。

[0051] 图 3 是本发明的总体框架图。

[0052] 图 4 是本发明的移动终端身份认证流程图。

[0053] 图 5 是本发明的移动终端数据加密流程图。

[0054] 图 6 是本发明的移动终端数据解密流程图。

[0055] 图 7 是本发明实现移动终端安全发送邮件的总体框架图。

[0056] 图 8 是本发明的移动终端邮件加密流程图。

[0057] 图 9 是本发明的移动终端邮件解密流程图。

具体实施方式

[0058] 本发明的目的在于提供多种安全的身份认证方式，如证书方式认证、动态口令方式认证，完善准入机制，面对数据存储安全，提供安全的 SQLite、XML、配置文件，落地文档加密存储、权限管理，以及生命周期管理等方式，保证移动终端本地数据存储安全；对网络传输提供安全的套接字层，以及多种基于证书的安全代理方式，如安全的 HTTP 加密传输代理、安全的 Socket(TCP / UDP)，从而保护网络传输数据安全，请求数据放篡改、防抵赖。并提供设备管控接口，对设备的 wifi/ 蓝牙进行统一控制。开放一系列底层安全接口，如证书密钥操作，如加解密、签名、验签、P7 封装，PKCS # 11 标准接口，基于这些基础的安全组件，

整合到邮件移动终端、网络应用移动终端、移动办公软件中，确保身份安全与认证过程中的数据安全，并为网络数据以及文件数据从传输到存储提供安全保障，并提供文件安全浏览、权限管理、生命周期管理的能力，基于 PKI 体系的数据加解密技术是目前比较成熟的数据安全保护解决方案，并广泛应用于数据安全领域，将密码学技术整合到数据信息中，那对于数据信息安全行业将是一个质的飞跃。

[0059] 图 3 展示了本发明的总体框架图，整个系统框架具体包括的设备有：

[0060] 安全 SDK：在 PKI 体系下，一个可以进行证书操作的开发平台，支持硬件身份认证证书，提供终端加密、通道管理、证书密钥、身份认证等一系列关于安全的组件，保证数据信息以及身份认证的安全；提供设备管理、流量监控、锁屏控制等一系列终端管控组件，实现对终端设备进行统一管控；MOB 系统支撑组件包括加密 SQLite3、系统配置（XML/Plist）、Key 卡驱动适配器，为上层应用提供快速开发接口；本专利中的 SDK 着重提供身份认证接口和数据信息安全等接口，供上层应用调用。

[0061] 主服务器：支持 Ldap 服务器与 AD 域服务器的账号同步，服务器与安全 SDK 的交互包括：用户认证、策略下发、日志审计；

[0062] 数据库：针对 sqlite3 的页面文件，对页面文件进行加密和解密，解决了当查询数据和更新数据要将整个表进行解密或者将部分字段解密的查询方式，提高运行效率，又屏蔽了对上层实现的安全细节；

[0063] 移动管理控制台：提供一个 UI 操作界面，对移动终端行为以及用户进行管控，包括用户管理、策略配置、日志审计。

[0064] 图 4 展示了移动终端的身份认证流程图。

[0065] 该移动终端的身份认证过程包括：

[0066] 1）移动终端向服务器请求随机数；

[0067] 2）服务器接收请求，并向移动终端返回随机数；

[0068] 3）移动终端枚举设备；

[0069] 4）移动终端打开设备；

[0070] 5）移动终端枚举证书；

[0071] 6）验证 PIN 码，如果验证失败结束验证，如果验证成功调用私钥对随机数进行签名；

[0072] 7）将签名结果和签名公钥证书发送至服务器；

[0073] 8）服务器验证公钥证书有效性，如果验证失败，结束验证；

[0074] 9）如果验证成功，验证签名有效性，验证失败，结束验证；

[0075] 10）签名验证成功，向移动终端返回认证结果；

[0076] 11）移动终端接收验证结果。

[0077] 上述身份认证可以不用公钥证书，可以通过预置密钥和算法的方式进行认证，即挑战 - 响应方式。

[0078] 实施例 1

[0079] 实施例 1 中提供了一种移动终端之间的安全通信方法。

[0080] 如图 5 所示，其展示了本发明移动终端加密数据信息的过程。数据加密过程具体包括以下步骤：移动终端上层应用程序调用安全 SDK 加密数据，传入使用者信息及数据信

息后，安全 SDK 将根据使用者信息查找到使用者的公钥(如果本地不存在，则向服务器请求使用者的公钥)，然后在本地产生对称密钥，使用对称密钥对数据进行加密，用使用者的公钥对对称密钥进行加密，将加密的对称密钥和加密的数据拼装成数字信封，最后将数字信封返回到移动终端上层应用程序。

[0081] 如图 6 所示，其展示了移动终端接收并解密数据信息的过程。数据接收解密过程包括：移动终端上层应用程序调用安全 SDK 解密数据，将密文数据传入安全 SDK，安全 SDK 解析数字信封，解析出当前用户密文对称密钥和密文数据，使用当前用户证书设备私钥解密对称密钥，使用明文对称密钥解密密文数据，将解密的明文数据传递到移动终端的安全应用程序。

[0082] 实施例 2

[0083] 实施例 2 中提供了一种移动终端之间的安全邮件通信方法。

[0084] 所图 7 所示，其展示了移动终端通过 SDK 安全发送邮件的总体框架图。

[0085] 其包括邮件服务器，邮件客户端，安全管理平台和数据库，其中邮件服务器实现邮件的收发，客户端既可以为固定的 PC 客户端，也可以为移动 andriod/IOS 客户端，客户端中集成了基础 SDK，实现邮件的身份认证以及数据加密 / 解密的功能，通过网络通讯获取数据加密的 KEY，客户端通过与安全管理平台通信实现身份认证，策略和加密公钥的获取，安全管理平台包括安全业务处理服务组件和 WEB 服务组件，其又分别包括身份认证组件、证书管理组件、策略管理组件、日志审计组件以及前端控制台、用户信息管理组件，安全管理平台与相关的数据库通信获取数据，数据库与附图 3 中的数据库功能类似。

[0086] 如图 8 所示，其展示了移动终端加密发送邮件的过程，该邮件加密过程包括以下步骤：

[0087] 1）安全邮件移动终端应用程序开始发送邮件；

[0088] 2）安全邮件移动终端应用程序调用 SDK 加密签名接口，传入明文的 E-MAIL、邮件接收者列表；

[0089] 3）安全 SDK 根据邮件接收者列表获取收件人公钥，如果本地没有收件人公钥，则向邮件安全管理平台请求收件人公钥；

[0090] 4）验证收件人公钥的有效性；

[0091] 5）验证通过后，用发件人的私钥对邮件做签名；

[0092] 6）使用发件人证书设备生成对称密钥并加密邮件；

[0093] 7）用收件人公钥和紧急密钥加密对称密钥并和密文邮件封装成数字信封，组装成安全邮件 E-MAIL；

[0094] 8）将安全邮件 E-MAIL 返回给安全邮件移动终端应用程序；

[0095] 9）安全邮件移动终端应用程序接收安全邮件 E-MAIL，将密文的 E-MAIL 发送至邮件服务器；

[0096] 10）邮件服务器接收安全邮件 E-MAIL。

[0097] 如图 9 所示，其展示了安全邮件移动终端接收解密邮件的过程，该过程包括以下步骤：

[0098] 1）安全邮件移动终端应用程序请求接收邮件；

[0099] 2）邮件安全管理平台向安全邮件移动终端应用程序发送邮件；

[0100] 3）安全邮件移动终端应用程序接收安全密文邮件；

[0101] 4）安全邮件移动终端调用 SDK 进行解密，SDK 解析邮件 E-MAIL，解析数字信封；

[0102] 5）SDK 调用收件人私钥解密对称密钥，使用对称密钥解密密文邮件；

[0103] 6）在本地缓存中查找发件人公钥证书；

[0104] 7）如果本地缓存中没有找到，则向邮件服务器请求发件人公钥证书；

[0105] 8）验证发件人公钥证书有效性；

[0106] 9）验证通过后，验证邮件签名；

[0107] 10）向安全邮件移动终端应用程序返回邮件明文和验签结果；

[0108] 11）查看邮件。

[0109] 上述移动终端（安全邮件移动终端）可以为手机，PDA，移动电脑等各种智能移动终端设备。

[0110] 通过本发明的实施例，第三方应用调用本 SDK 后，可以基本避免数据信息安全的相关问题，包括身份认证、数据外泄、设备管控等。因为用户的身份和硬件设备中的证书是相互绑定的。如果没有此硬件设备，相关的人就不能查看加密数据信息。就算数据信息在传输中被监听截取，但监听者也没有办法对数据信息进行解密，使其得到的数据没有任何意义。

[0111] 以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换以及改进等，均应保护在本发明的保护范围之内。

图 1

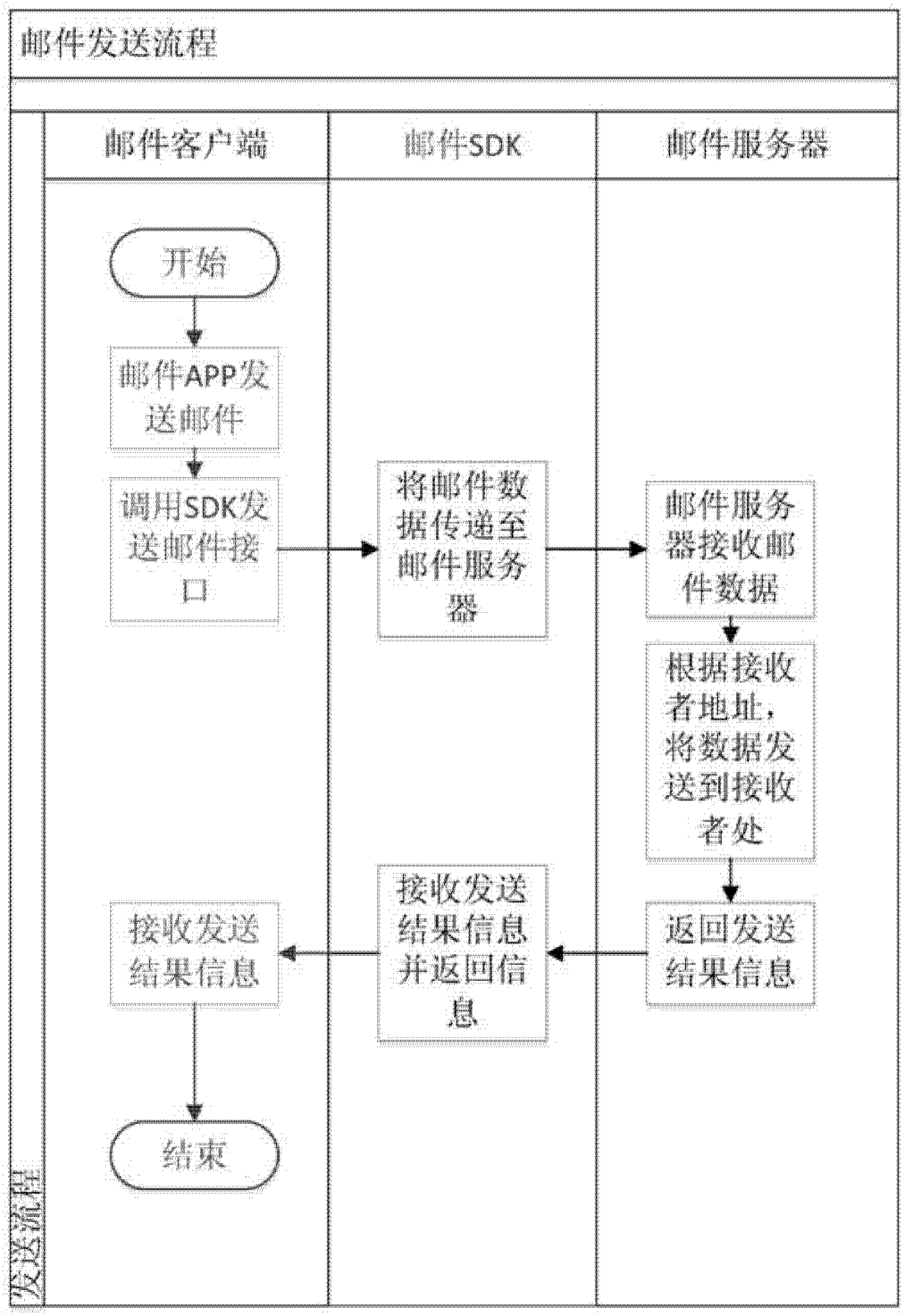

邮件发送流程
邮件客户端
邮件SDK
邮件服务器
开始
邮件APP发送邮件
调用SDK发送邮件接口
将邮件数据传递至邮件服务器
邮件服务器接收邮件数据
根据接收者地址，将数据发送到接收者处
返回发送结果信息
接收发送结果信息并返回信息
接收发送结果信息
结束
发送流程

图 2

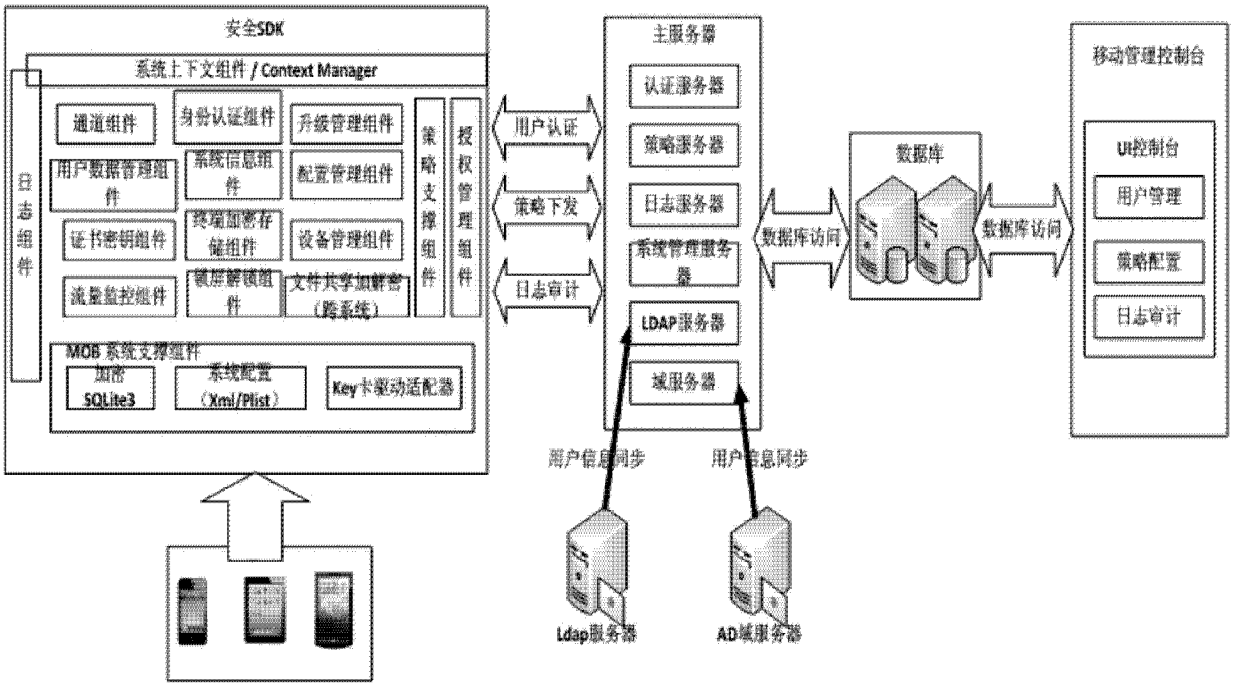

安全SDK
系统上下文组件 / Context Manager
通道组件
身份认证组件
升级管理组件
用户数据管理组件
系统信息组件
配置管理组件
证书密钥组件
终端加密存储组件
设备管理组件
流量监控组件
锁屏解锁组件
文件共享加解密（跨系统）
日志组件
策略支撑组件
授权管理组件
MOB 系统支撑组件
加密 SQLite3
系统配置（Xml/Plist）
Key卡驱动适配器
用户认证
策略下发
日志审计
主服务器
认证服务器
策略服务器
日志服务器
系统管理服务器
LDAP服务器
域服务器
数据库访问
数据库
数据库访问
移动管理控制台
UI控制台
用户管理
策略配置
日志审计
用户信息同步
用户信息同步
Ldap服务器
AD域服务器

图 3

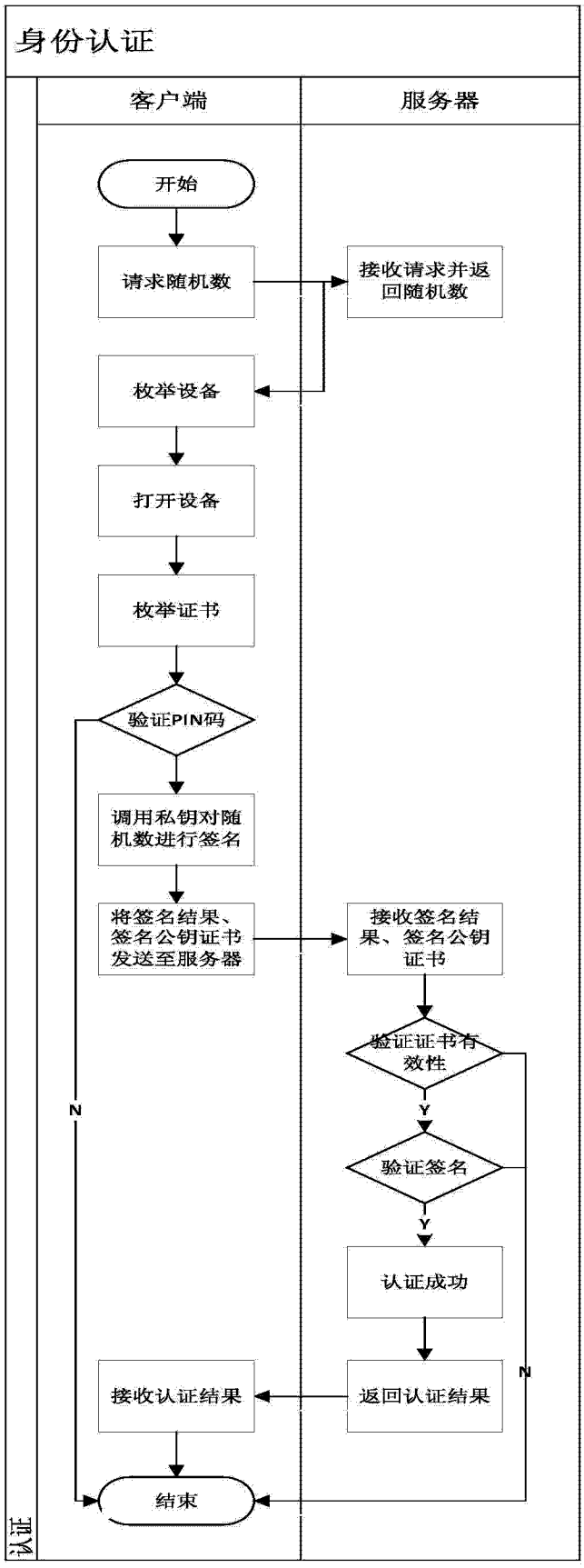

身份认证
客户端
服务器
开始
请求随机数
接收请求并返回随机数
枚举设备
打开设备
枚举证书
验证PIN码
调用私钥对随机数进行签名
将签名结果、签名公钥证书发送至服务器
接收签名结果、签名公钥证书
验证证书有效性
验证签名
认证成功
返回认证结果
接收认证结果
结束
N
Y
Y
N
认证

图 4

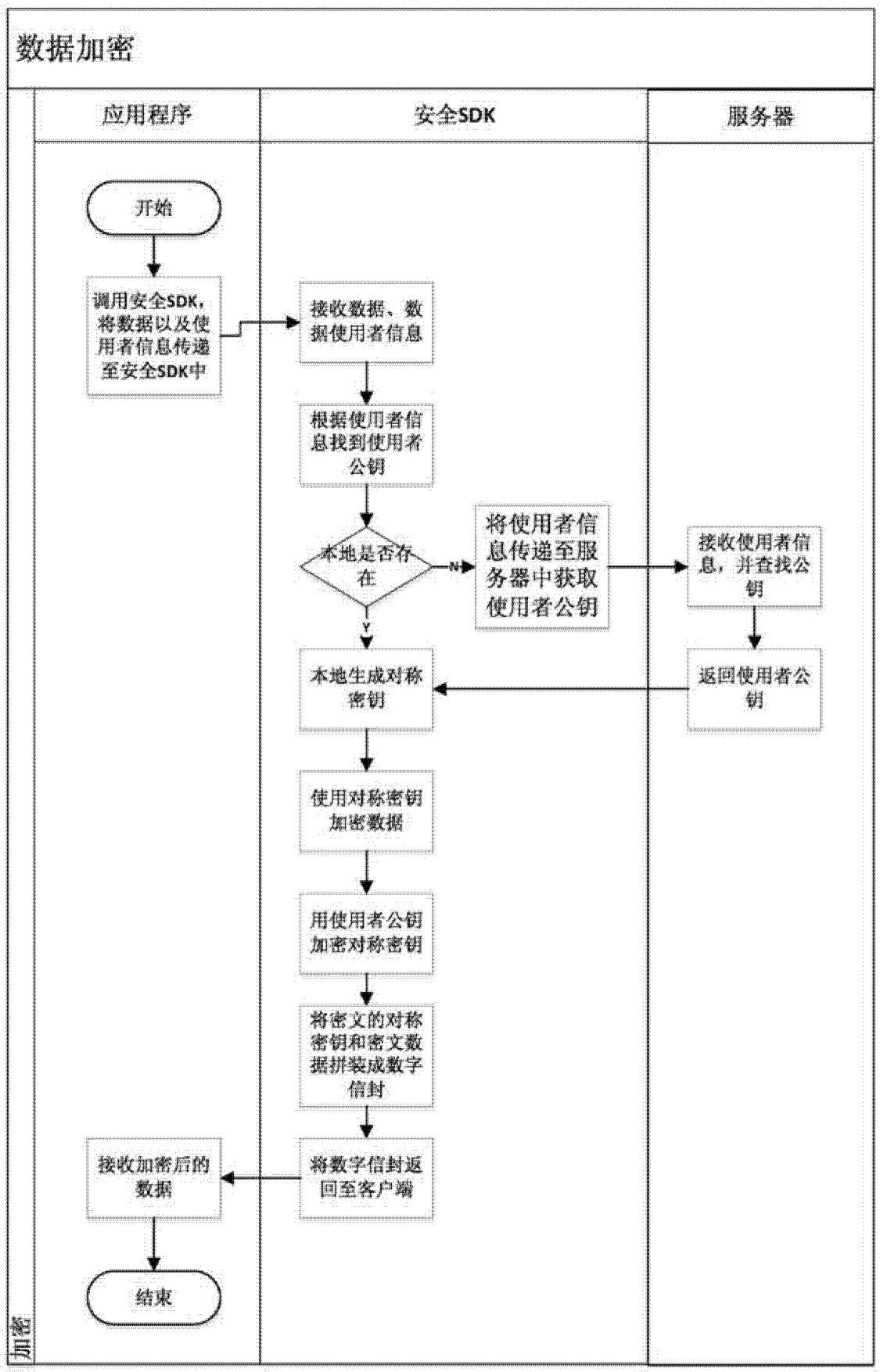

数据加密
应用程序
安全SDK
服务器
开始
调用安全SDK，将数据以及使用者信息传递至安全SDK中
接收数据、数据使用者信息
根据使用者信息找到使用者公钥
本地是否存在
N
将使用者信息传递至服务器中获取使用者公钥
接收使用者信息，并查找公钥
返回使用者公钥
Y
本地生成对称密钥
使用对称密钥加密数据
用使用者公钥加密对称密钥
将密文的对称密钥和密文数据拼装成数字信封
将数字信封返回至客户端
接收加密后的数据
结束
加密

图 5

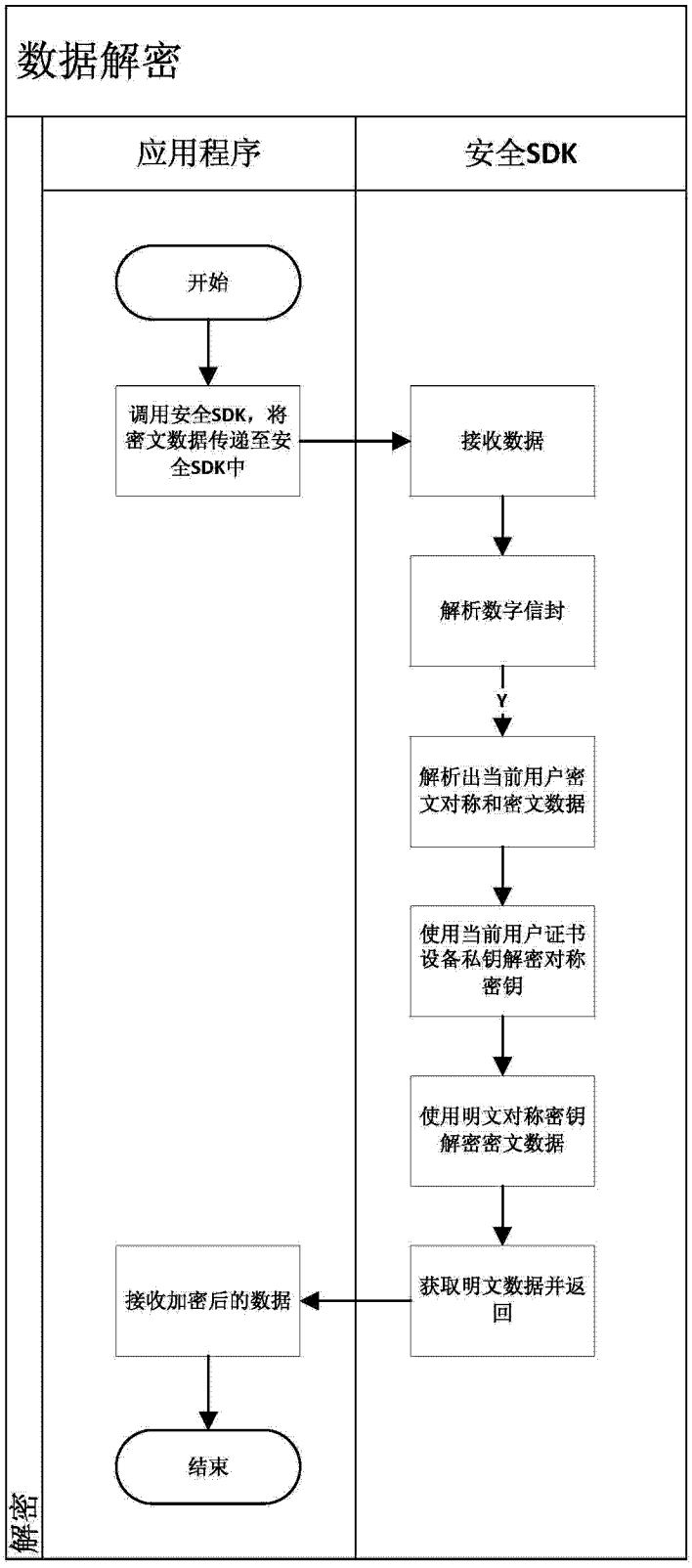

数据解密
应用程序
安全SDK
开始
调用安全SDK，将密文数据传递至安全SDK中
接收数据
解析数字信封
Y
解析出当前用户密文对称和密文数据
使用当前用户证书设备私钥解密对称密钥
使用明文对称密钥解密密文数据
获取明文数据并返回
接收加密后的数据
结束
解密

图 6

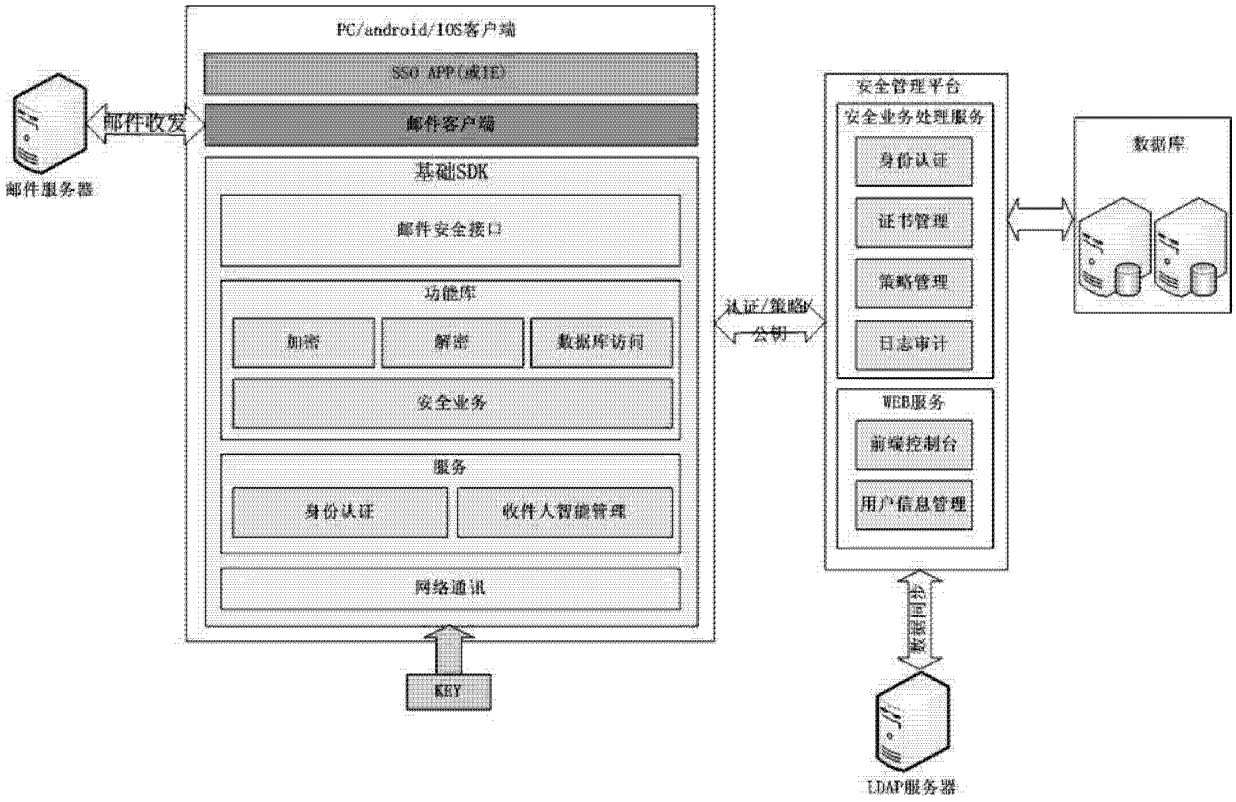

PC/android/IOS客户端
SSO APP(或IE)
邮件客户端
基础SDK
邮件安全接口
功能库
加密
解密
数据库访问
安全业务
服务
身份认证
收件人智能管理
网络通讯
KEY
邮件收发
邮件服务器
认证/策略/公钥
安全管理平台
安全业务处理服务
身份认证
证书管理
策略管理
日志审计
WEB服务
前端控制台
用户信息管理
数据库
LDAP
LDAP服务器

图 7

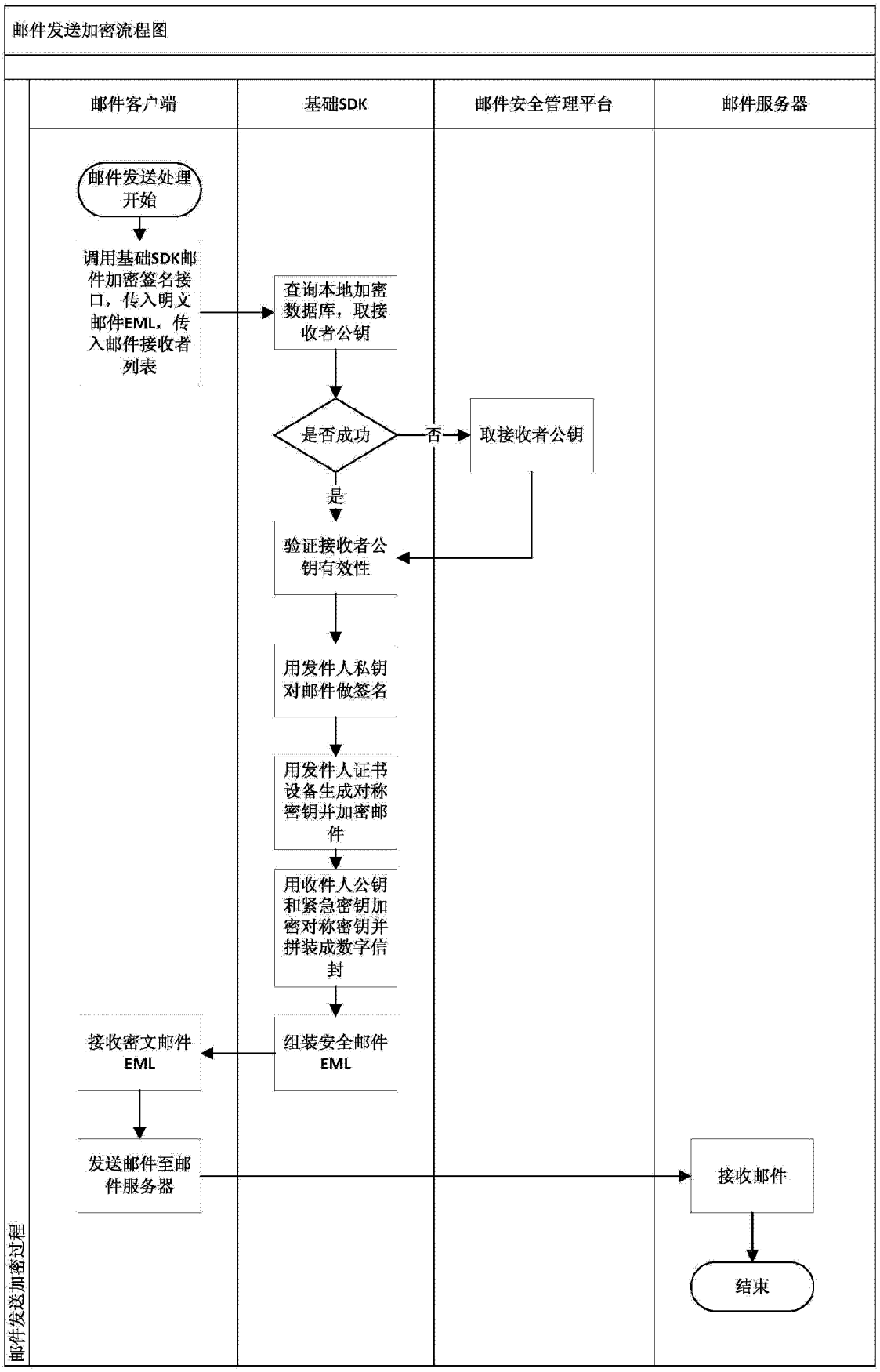

邮件发送加密流程图
邮件客户端
基础SDK
邮件安全管理平台
邮件服务器
邮件发送处理开始
调用基础SDK邮件加密签名接口，传入明文邮件EML，传入邮件接收者列表
查询本地加密数据库，取接收者公钥
是否成功
否
取接收者公钥
是
验证接收者公钥有效性
用发件人私钥对邮件做签名
用发件人证书设备生成对称密钥并加密邮件
用收件人公钥和紧急密钥加密对称密钥并拼装成数字信封
组装安全邮件EML
接收密文邮件EML
发送邮件至邮件服务器
接收邮件
结束
邮件发送加密过程

图 8

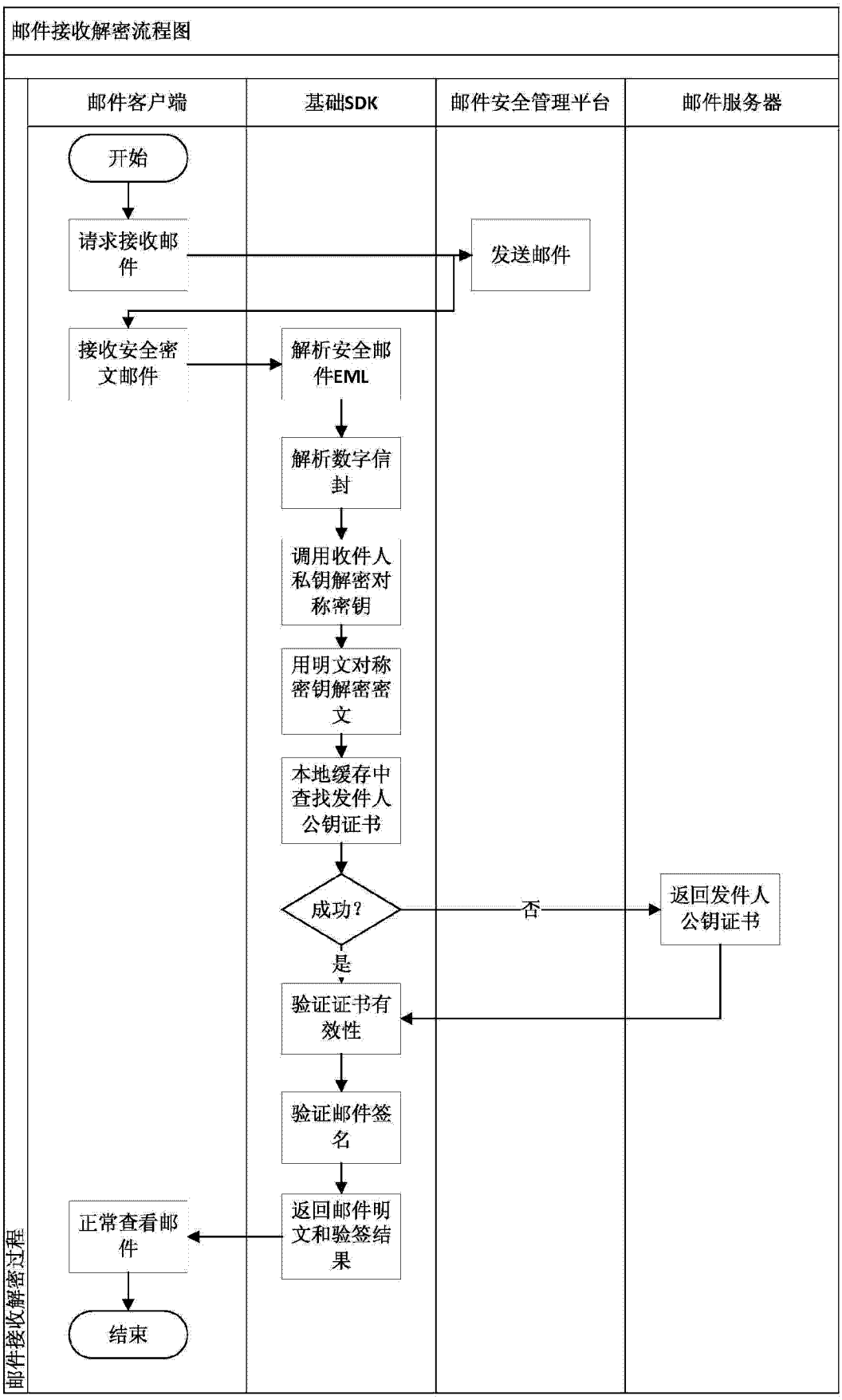

邮件接收解密流程图
邮件客户端
基础SDK
邮件安全管理平台
邮件服务器
开始
请求接收邮件
发送邮件
接收安全密文邮件
解析安全邮件EML
解析数字信封
调用收件人私钥解密对称密钥
用明文对称密钥解密密文
本地缓存中查找发件人公钥证书
成功?
否
返回发件人公钥证书
是
验证证书有效性
验证邮件签名
返回邮件明文和验签结果
正常查看邮件
结束
邮件接收解密过程

图 9