(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 105260663 B
(45)授权公告日 2017.12.01

(21)申请号 201510586671.5

(22)申请日 2015.09.15

(65)同一申请的已公布的文献号
申请公布号 CN 105260663 A

(43)申请公布日 2016.01.20

(73)专利权人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 田琛 王雅哲 徐震 蔡智强

(74)专利代理机构 北京科迪生专利代理有限责任公司 11251
代理人 成金玉 孟卜娟

(51)Int.Cl.
G06F 21/60(2013.01)

(56)对比文件
CN 104091135 A,2014.10.08,
CN 104143065 A,2014.11.12,
CN 104318182 A,2015.01.28,
CN 104581214 A,2015.04.29,
CN 104392188 A,2015.03.04,
CN 104683336 A,2015.06.03,
王熙友.ARMTrustZone安全隔离技术研究与应用.《中国优秀硕士学位论文全文数据库信息科技辑(月刊)》.2014,(第01期),I136-387.

审查员 简文雨

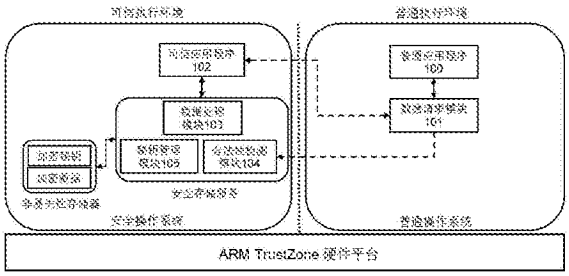
权利要求书3页 说明书8页 附图6页

(54)发明名称

一种基于TrustZone技术的安全存储服务系统及方法

(57)摘要

一种基于TrustZone技术的安全存储服务系统及方法,包括数据请求模块、普通应用程序、安全存储服务、可信应用程序;数据请求模块负责普通应用程序与可信应用程序间数据安全存储服务请求的封装与调用,为普通应用程序提供统一的数据存储、数据加载和数据销毁的服务请求接口;安全存储服务包括合法性检测模块、数据处理模块和秘钥管理模块。本发明目的在于为支持TrustZone技术的终端设备上的应用程序提供统一的数据安全存储接口,既解决应用程序敏感数据的安全存储问题,又保证应用程序开发的便捷性。



CN 105260663 B

1.一种基于TrustZone技术的安全存储服务系统，包括可信执行环境和普通执行环境，可信执行环境提供安全操作系统运行，由安全操作系统负责加载并运行可信应用程序；普通执行环境提供普通操作系统运行，普通操作系统调用普通应用程序运行，其特征在于：

在普通执行环境中增加数据请求模块，数据请求模块负责普通应用程序与可信应用程序间数据安全存储服务请求的封装与调用，为普通应用程序提供统一的数据安全存储服务请求接口，数据安全存储服务请求接口包括数据存储请求接口、数据加载请求接口和数据销毁请求接口；

在可信执行环境中增加安全存储服务，实现将数据安全存储作为服务运行于可信执行环境的安全操作系统中；所述安全存储服务功能分为数据存储、数据加载和数据销毁；所述数据存储实现对敏感数据加密和签名，并将加密数据和签名数据存储在可信执行环境的非易失存储器中；数据加载实现从可信执行环境的非易失存储器中加载加密数据并解密出敏感数据；数据销毁实现从可信执行环境的非易失存储器中移除存储的加密数据；所述安全存储服务由合法性检测模块、数据处理模块和秘钥管理模块构成；所述合法性检测模块在普通应用程序发起数据安全存储服务请求时，对普通应用程序进程做运行时检测，保证数据安全存储服务请求的合法性；数据处理模块为可信应用程序提供统一的数据安全存储远程调用接口，所述数据安全存储远程调用接口包括数据存储调用接口、数据加载调用接口和数据销毁调用接口；所述远程调用是指可信执行环境中可信应用程序之间的远程通信方式，可信应用程序向数据处理模块发送远程调用后，由安全操作系统负责将该远程调用路由到对应的数据安全存储远程调用接口，执行相应的数据安全存储操作，并将操作结果返回至可信应用程序；秘钥管理模块为数据处理模块处理加解密数据提供相关秘钥生成、秘钥加载和秘钥销毁功能。

2.根据权利要求1所述的基于TrustZone技术的安全存储服务系统，其特征在于：在普通应用程序中提取特征信息，所述特征信息是一段可以唯一标记普通应用程序的信息；特征信息被第三方CA证书签名并存储在可信应用程序中，用于普通应用程序的合法性检测。

3.根据权利要求1所述的基于TrustZone技术的安全存储服务系统，其特征在于：所述数据请求模块为数据存储请求接口、数据加载请求接口和数据销毁请求接口定义了唯一的调用请求号；可信应用程序接收到数据请求模块的调用请求后，根据调用请求号向数据处理模块发起远程调用，执行相应的安全存储服务操作。

4.根据权利要求1所述的基于TrustZone技术的安全存储服务系统，其特征在于：在数据请求模块的数据存储请求接口、数据加载请求接口和数据销毁请求接口的第一条指令前插入软件中断指令SWI，并定义新的软件中断号；当普通应用程序调用数据请求模块接口向可信应用程序发送数据安全存储服务请求时，将触发SWI软件中断异常，普通操作系统捕获SWI软件中断并将普通应用程序的进程异常信息发送给可信执行环境的TrustZone监视器；TrustZone监视器捕获进程异常信息后，调用合法性检测模块对普通应用程序的进程做合法性检测。

5.根据权利要求1所述的基于TrustZone技术的安全存储服务系统，其特征在于：所述合法性检测模块的实现过程为：获取普通应用程序的进程异常信息和可信应用程序标示符后，从可信应用程序中加载普通应用程序的特征信息签名，并根据捕获的普通应用程序进程异常信息和特征信息签名对普通应用程序进行合法性检测，最后依据检测结果为当前普

通应用程序进程设置检测状态标志位。

6.一种基于TrustZone技术的安全存储服务方法，其特征在于实现步骤如下：

(1)为普通应用程序实现数据请求模块，同时为普通应用程序提取特征信息，使用第三方CA证书对特征信息签名，并将特征信息签名值存储到对应的可信应用程序中，普通应用程序通过调用数据请求模块的数据安全存储服务请求接口向可信应用程序发送服务请求；

(2)普通应用程序调用数据请求模块接口时，普通操作系统利用软件中断异常机制捕获其进程异常信息及请求的可信应用程序标示符，并将进程异常信息和可信应用程序标示符发送给可信执行环境的TrustZone监视器，由TrustZone监视器调用安全存储服务的合法性检测模块完成对普通应用程序进程的合法性检测；

(3)合法性检测模块获取普通应用程序的进程异常信息和可信应用程序标示符后，从可信应用程序中加载普通应用程序的特征信息签名，并根据捕获的普通应用程序进程信息和特征信息签名对普通应用程序进行合法性检测，最后依据检测结果为普通应用程序进程设置检测状态标志位；

(4)可信应用程序接收普通应用程序的数据安全存储服务请求后，对普通应用程序请求的原始数据完成数据预处理操作，并通过远程调用数据处理模块执行相应的数据安全存储操作；

(5)安全操作系统负责处理可信应用程序向数据处理模块发起的远程调用，安全操作系统将远程调用路由到数据处理模块并执行相应的数据安全存储远程调用接口，数据安全存储远程调用接口在执行前需要检测普通应用程序进程的检测状态标志位，若检测失败，则拒绝可信应用程序发起的远程调用；若检测通过，则数据安全存储远程调用接口将协同秘钥管理模块为可信应用程序执行相应的数据安全存储操作。

7.根据权利要求6所述的一种基于TrustZone技术的安全存储服务方法，其特征在于：所述步骤(2)中，普通应用程序调用数据请求模块接口时，为了使普通操作系统捕获普通应用程序进程的软件中断异常，需要在代码层面上对数据请求模块接口进行特殊处理：在每个请求接口的第一条代码指令前插入软件中断指令SWI，并定义新软件中断号；同时在保证对操作系统最小修改的前提下，为普通操作系统添加新软件中断号的中断处理逻辑，用于捕获普通应用程序的进程异常信息并向可信执行环境发送进程异常信息。

8.根据权利要求6所述的一种基于TrustZone技术的安全存储服务方法，其特征在于：所述步骤(3)中，合法性检测先通过普通应用程序的进程异常信息计算运行时的特征信息；再使用第三方CA证书公钥验签存储在可信应用程序中的特征信息签名，获得合法的特征信息；最后对运行时的特征信息和验签后获取的特征信息进行比较，并根据比较结果判定普通应用程序进程的合法性。

9.根据权利要求6所述的一种基于TrustZone技术的安全存储服务方法，其特征在于：所述步骤(4)中，所述数据预处理操作是指可信应用程序向数据处理模块发起远程调用前，对普通应用程序请求的原始数据进行一些必要的处理操作，包括普通应用程序从远程服务器下载一份机密文件，机密文件内容实际由可信应用程序和远程服务器的共享密钥加密，当可信应用程序接收到普通应用程序存储文件的调用请求后，首先需要使用可信应用程序和远程服务器的共享密钥对加密的文件内容进行解密，然后再通过远程调用数据处理模块对解密后的文件内容执行安全存储操作。

10.根据权利要求6所述的一种基于TrustZone技术的安全存储服务方法，其特征在于：所述步骤(5)中，数据安全存储远程调用接口包括：数据存储调用接口、数据加载调用接口和数据销毁调用接口；数据安全存储远程调用接口在执行前，需要判断由合法性检测模块设定的检测状态标志位，来决定是否为可信应用程序执行相应的数据安全存储操作，所述数据安全存储操作包括：数据存储操作、数据加载操作和数据销毁操作。

一种基于TrustZone技术的安全存储服务系统及方法

技术领域

[0001] 本发明涉及一种基于TrustZone技术的安全存储服务系统及方法，属于移动终端设备的数据安全存储领域。

背景技术

[0002] 随着移动互联网技术和移动智能终端的快速发展，移动终端处理的业务从传统的通信、娱乐领域延伸到移动办公、移动支付等高安全、高敏感业务领域。移动终端需要处理越来越多的敏感数据，包括用户账户信息、个人隐私信息、支付订单信息、企业私密文件等。如何有效得保障移动终端上敏感数据的安全性成为了移动终端设备开展高安全、高敏感业务面临的一大难题。

[0003] 通常的解决方案是通过高强度密码算法对敏感数据加密，将加密数据存储在移动操作系统的文件系统上，并利用操作系统的权限控制机制来限制加密数据文件的访问，从而实现敏感数据的安全存储。但是由于传统移动终端操作系统的复杂性和开放性使其无法创造安全的运行环境，操作系统自身以及应用程序很容易遭受恶意攻击。当恶意应用攻击合法应用后，以合法应用的身份访问存储在文件系统上的加密数据，并通过相应解密逻辑获取敏感数据，导致敏感数据遭受窃取。同时部分移动终端设备用户为了获得更好的体验对设备进行刷机，当恶意应用获取移动操作系统的最高权限后，系统中所有对敏感数据的保护将无安全性可言。此外，将敏感数据加密存储在普通文件系统中也存在遭受非法破坏导致拒绝服务攻击的风险。因此传统的解决方案安全性不够高，难以真正有效地解决应用程序敏感数据的安全存储问题。

[0004] 为了从根本上解决移动终端应用程序敏感数据的安全存储问题，必须从底层硬件架构、操作系统等多个环节设计软硬件结合的整体解决方案。ARM TrustZone硬件隔离技术和可信执行环境(TEE)概念的提出为解决这个问题带来新的思路。基于ARM TrustZone技术构建的可信执行环境可以将涉及敏感数据的应用程序分成普通应用程序和可信应用程序，普通应用程序运行在普通执行环境中(如传统linux系统、安卓操作系统等)处理大部分非敏感业务。可信应用程序运行在可信执行环境中处理敏感业务。普通执行环境与可信执行环境相互隔离，保证了可信应用程序处理敏感数据的安全性。

[0005] 虽然TrustZone技术为应用程序处理敏感数据提供了安全隔离的运行时环境和物理环境，但是TrustZone技术并没有定义关于数据安全存储的技术标准，基于TrustZone技术实现数据安全存储仍面临以下几个问题：如何为可信应用程序开发和普通应用程序开发提供统一的安全存储接口；如何对发送数据安全存储请求的普通应用程序做合法性检测。

发明内容

[0006] 本发明的技术解决问题：克服现有技术的不足，提供一种基于TrustZone技术的安全存储服务系统及方法，防止敏感数据泄露，从而有效地保证数据安全性，具有数据存储高安全性、程序开发接口统一等优势。

[0007] 本发明技术解决方案为:一种基于TrustZone技术的安全存储服务系统及方法,下面简要介绍下本方案的基本思想,本发明在吸取已有解决方案优点的基础之上,提出了自己的设计思想,具体来说,本发明的系统包括下列几个方面:

[0008] 方面一,将安全存储服务以后台服务的形式运行于可信执行环境的安全操作系统中。所述安全存储服务是指在可信执行环境初始化完成后,由安全操作系统负责静态加载并在后台运行的可信应用程序。按照功能分类将安全存储服务分为数据存储、数据加载和数据销毁三类功能。数据存储功能实现对敏感数据的加密和签名,并将加密数据和签名数据存储在可信执行环境的非易失存储器中;数据加载功能实现从可信执行环境的非易失存储器中加载加密数据并解密出敏感数据;数据销毁功能实现从可信执行环境的非易失存储器中移除加密数据和签名数据。

[0009] 安全存储服务的数据处理模块为可信应用程序提供统一的数据安全存储远程调用接口,包括数据存储调用接口、数据加载调用接口和数据销毁调用接口。所述远程调用是指可信执行环境中可信应用程序之间的远程通信方式,可信应用程序向数据处理模块发送远程调用,安全操作系统将远程调用路由到对应的数据安全存储远程调用接口,执行相应的数据安全存储操作,并将操作结果返回至可信应用程序。

[0010] 方面二,为普通应用程序提供数据请求模块。所述数据请求模块是由一系列数据安全存储服务请求接口构成的共享库,包括数据存储请求接口、数据加载请求接口和数据销毁请求接口。每个调用请求接口定义相应的调用请求号。普通应用程序调用数据请求模块接口后,最终通过TrustZone可信执行环境通信代理向可信应用程序发送数据安全存储服务请求。可信应用程序接收到服务请求后,根据调用请求号向安全存储服务发起远程调用,执行相应的数据安全存储操作。

[0011] 方面三,基于TrustZone技术的可信执行环境并未对普通执行环境发起的调用请求定义相关的验证标准,普通执行环境的恶意程序可能通过攻击合法普通应用程序伪造调用请求或者直接伪装成合法的普通应用程序向可信应用程序发起调用请求,从而存在敏感数据泄露的风险。基于此问题,本发明一个重要方面在于保证对操作系统最小修改的前提下,实现在可信执行环境中对发送数据安全存储服务请求的普通应用程序做运行时的合法性检测。其具体实现依赖于安全存储服务的合法性检测模块、数据请求模块在代码实现上的特殊处理及普通应用程序的特征信息提取与存储。

[0012] 一种基于TrustZone技术的安全存储服务实现方法,实现步骤如下:

[0013] (1)为普通应用程序实现数据请求模块,同时为普通应用程序提取特征信息,使用第三方CA证书对特征信息签名,并将特征信息签名值存储到对应的可信应用程序中。普通应用程序通过调用数据请求模块的数据安全存储服务请求接口向可信应用程序发送服务请求;

[0014] (2)普通应用程序调用数据请求模块接口时,普通操作系统利用软件中断异常机制捕获其进程信息及请求的可信应用程序标示符,并将进程异常信息和可信应用程序标示符发送给可信执行环境的TrustZone监视器,由TrustZone监视器调用安全存储服务的合法性检测模块完成对普通应用程序进程的合法性检测。

[0015] (3)合法性检测模块获取普通应用程序的进程异常信息和可信应用程序标示符后,从可信应用程序中加载普通应用程序的特征信息签名,并根据捕获的普通应用程序进

程信息和特征信息签名对普通应用程序进行合法性检测，最后依据检测结果为当前普通应用程序进程设置检测状态标志位。

[0016] (4)可信应用程序接收普通应用程序的数据安全存储服务请求后，对普通应用程序请求的原始数据完成数据预处理操作，并通过远程调用方式请求数据处理模块执行相应的数据安全存储操作。

[0017] (5)安全操作系统负责处理可信应用程序向数据处理模块发起的远程调用，安全操作系统将远程调用路由到数据处理模块并执行相应的数据安全存储远程调用接口。数据安全存储远程调用接口在执行前需要检测普通应用程序进程的检测状态标志位。若检测失败，则拒绝可信应用程序发起的远程调用；若检测通过，则数据安全存储远程调用接口将协同秘钥管理模块为可信应用程序执行相应的数据安全存储操作。

[0018] 所述步骤(1)中，数据安全存储服务请求接口包括：数据存储请求接口、数据加载请求接口和数据销毁请求接口。数据请求模块为每个模块接口定义了唯一的调用请求号。

[0019] 所述步骤(1)中，普通应用程序的特征信息是一段可以唯一标记普通应用程序的信息；特征信息被第三方CA证书签名并存储在可信应用程序中用于普通应用程序的合法性检测。

[0020] 所述步骤(2)中，普通应用程序调用数据请求模块接口时，为了使普通操作系统捕获其进程的软件中断异常，需要在代码层面上对数据请求模块接口进行特殊处理：在每个请求接口的第一条代码指令前插入软件中断指令SWI，并定义新软件中断号；同时在保证对操作系统最小修改的前提下，为普通操作系统添加新软件中断号的中断处理逻辑，用于捕获普通应用程序的进程异常信息并向可信执行环境发送进程异常信息。

[0021] 所述步骤(3)中，合法性检测通过普通应用程序的进程异常信息计算运行时的特征值并与存储在可信应用程序中的特征值进行比较，再根据比较结果判定普通应用程序进程的合法性。

[0022] 所述步骤(4)中，数据预处理操作是指可信应用程序向安全存储服务发起远程调用前，对普通应用程序请求的原始数据进行一些必要的处理操作。例如，普通应用程序从远程服务器下载一份机密文件，机密文件内容实际由可信应用程序和远程服务器的共享密钥加密，当可信应用程序接收到普通应用程序存储文件的调用请求后，首先需要使用可信应用程序和远程服务器的共享密钥对加密的文件内容进行解密，然后再通过远程调用数据处理模块对解密后的文件内容执行安全存储操作。

[0023] 所述步骤(5)中，数据安全存储远程调用接口包括：数据存储调用接口、数据加载调用接口和数据销毁调用接口。数据安全存储远程调用接口在执行前，需要判断由合法性检测模块设定的检测状态标志位，来决定是否为可信应用程序执行相应的数据安全存储操作。所述数据安全存储操作包括：数据存储操作、数据加载操作和数据销毁操作。

[0024] 本发明与现有技术相比，具有以下优点：

[0025] (1)利用TrustZone隔离技术将数据安全存储做为敏感业务隔离在可信执行环境的安全操作系统中，并以服务的形式为可信应用程序提供统一的远程调用接口，即使普通操作系统遭受攻击，仍然可以保证安全存储服务的安全性。

[0026] (2)在普通操作系统中，通过数据请求模块为普通应用程序提供统一的数据安全存储服务请求接口；并且在传统TrustZone隔离技术的基础上，结合普通操作系统的软件中

断机制和安全存储服务的合法性检测模块对发送数据安全存储服务请求的普通应用程序的进程进行合法性检测。

[0027] (3)安全存储服务存储的敏感数据是经过加密和可信应用程序证书签名认证后存放在可信执行环境中的非易失性存储器中，既保证了敏感数据与普通操作系统隔离，也保证了敏感数据在可信应用程序之间的隔离。

[0028] (4)安全存储服务存取敏感数据时的加解密秘钥由安全存储服务统一管理并存储在可信执行环境中的非易失性存储器中，既保证了数据秘钥与普通操作系统隔离，也实现了加解密操作对应用程序的透明性。

[0029] 综上所述，本发明相比较传统的数据加密存储方式，不仅提高了数据存储的安全性，同时也为应用程序开发提供了统一的程序调用接口。

附图说明

[0030] 图1为本发明的整体框架示意图；

[0031] 图2为本发明的数据请求模块实现流程图；

[0032] 图3为本发明的普通应用程序特征信息提取及存储流程图；

[0033] 图4为本发明的数据存储操作流程图；

[0034] 图5为本发明的数据加载操作流程图；

[0035] 图6为本发明的数据销毁操作流程图。

具体实施方式

[0036] 本发明利用ARM TrustZone硬件隔离技术和可信执行环境(TEE)作为基础平台，实现可以有效提供数据安全存储服务，基础平台上的普通应用程序和可信应用程序通过调用安全存储服务系统提供的统一接口实现敏感数据的安全存储、安全加载和安全销毁；同时保证对操作系统最小修改的前提下，在可信执行环境中对发起数据安全存储服务请求的普通应用程序做运行时的合法性检测，拒绝非法普通应用程序发起的或者合法普通应用程序遭受恶意攻击后发起的服务请求，防止敏感数据泄露，从而有效地保证数据安全性。基于此，本发明基于TrustZone技术的安全存储服务系统及方法具有数据存储安全性高、程序开发接口统一等优势。

[0037] 为使本发明的目的、优点以及技术方案更加清楚明白，以下通过具体实施，并结合附图，对本发明进一步详细说明。

[0038] 对于图1从整体上描述了该方案实施的总体架构，主要包括以下四部分的内容。

[0039] 一、基于普通执行环境的数据请求模块的实现方法

[0040] 依据可信执行环境(TEE)的客户端API为普通应用程序100实现数据请求模块101，数据处理模块提供三类数据存储服务请求接口：数据存储请求接口NS_ReqStoreData、数据加载请求接口NS_ReqLoadData和数据销毁请求接口NS_ReqDestroyData；普通应用程序100通过调用数据请求模块101接口向可信应用程序102发送数据安全存储服务请求。

[0041] 为了使可信执行环境能够在普通应用程序发送数据安全存储服务请求时对其进程进行合法性检测，需要对普通操作系统和数据请求模块作特别处理；下面结合图2具体描述数据请求模块接口的处理过程：

[0042] (11)在每个数据请求模块101接口的第一条指令前插入软件中断指令SWI,并定义新的软件中断号;

[0043] (12)当普通应用程序100调用数据请求模块接口时,触发SWI软件中断异常;

[0044] (13)普通操作系统捕获SWI软件中断,进入管理模式;

[0045] (14)普通操作系统的软件中断处理程序完成新软件中断号的处理逻辑:

[0046] a)通过LR_svc寄存器计算数据请求模块接口被调用时的指令地址$Addr_{ins}$=LR_svc-4;从参数寄存器R0中获取可信应用程序标示符UUID;

[0047] b)获取当前普通应用程序的进程代码段基地址TextBase和代码段大小TextSize;

[0048] c)将接口被调用时指令地址$Addr_{ins}$、进程代码段基地址TextBase、进程代码段大小TextSize和可信应用程序标示符UUID封装成普通应用程序100的进程异常信息,通过执行SMC指令将进程异常信息发送给可信执行环境,并由合法性检测模块104完成对普通应用程序进程的合法性检测。

[0049] (15)普通操作系统恢复普通应用程序的软件中断异常,并通过TrustZone可信执行环境通信代理向可信应用程序102发送数据安全存储服务请求。

[0050] 二、普通应用程序特征信息提取及存储的实现方法

[0051] 为了实现可信执行环境中的合法性检测模块104对普通应用程序100进行合法性检测,需要为合法性检测模块提供普通应用程序的特征信息作为检验参照,特征信息是一段可以唯一标记普通应用程序的信息。下面结合图3描述本发明中对普通应用程序特征信息提取和存储的实现步骤:

[0052] (21)在普通应用程序100发布前,开发人员读取普通应用程序二进制文件信息获取代码段大小$Size_{text}$;使用哈希算法对普通应用程序代码段二进制信息进行哈希运算,生成代码段哈希值H_{text}=Hash(Text),其中Text代表普通应用程序代码段;将代码段大小$Size_{text}$和代码段哈希值H_{text}做为普通应用程序的特征信息$SpecInfo_{app}=(Size_{text}||H_{text})$;

[0053] (22)使用可信第三方CA证书签名普通应用程序的特征信息$SpecInfo_{app}$,生成特征信息签名$Sign_{app}=Sign(Size_{text}||H_{text})$;

[0054] (23)将特征信息签名$Sign_{app}$存储到可信应用程序102的特定数据段中。所述可信应用程序是指接受普通应用程序数据存储调用请求的可信应用程序。

[0055] 三、基于可信执行环境的合法性检测模块的实现方法

[0056] 当普通应用程序100调用数据请求模块101接口向可信应用程序102发送数据存储调用请求时,将触发软件中断异常,普通操作系统将普通应用程序的进程异常信息发送给可信执行环境的TrustZone监视器;TrustZone监视器捕获进程异常信息后,调用安全存储服务的合法性检测模块104对普通应用程序100的进程异常信息进行合法性检验。

[0057] 合法性检测的具体实现步骤如下:

[0058] (31)合法性检测模块104通过步骤(14)获取普通应用程序100的进程异常信息(包括接口调用指令地址$Addr_{ins}$、进程代码段基地址TextBase、进程代码段大小TextSize与可信应用程序标示符UUID),并根据可信应用程序标示符UUID从对应的可信应用程序102的特定数据段加载普通应用程序特征信息签名$Sign_{app}$;

[0059] (32)合法性检测模块104使用步骤(21)中的哈希算法对进程内存地址TextBase到

TextBase+TextSize之间的代码段数据进行哈希运算，计算普通应用程序100进程的代码段哈希值H'text＝Hash(Text)，得到普通应用程序的进程特征信息SpecInfo'$_{app}$＝(TextSize||H'text)；其中Text表示普通应用程序进程的代码段；

[0060] (33)合法性检测模块104使用第三方可信CA证书公钥对步骤(31)获取的特征信息签名Sign$_{app}$进行验签，得到普通应用程序100的特征信息SpecInfo$_{app}$＝(Size$_{text}$||H$_{text}$)；

[0061] (34)合法性检测模块104比较特征信息SpecInfo$_{app}$和SpecInfo'$_{app}$是否相等。如果相等，并且满足TextBase<Addr$_{ins}$<TextBase+TextSize，则判定当前普通应用程序100进程是合法的，并将检测状态标志位置1；否则判定当前普通应用程序进程是非法的，则将检测状态标志位置0；其中检测状态标志位表示当前普通应用程序进程是否通过合法性检测，如果检测标志位为1，则表示通过检测；否则表示未通过检测。

[0062] 四、基于可信执行环境的数据处理模块和秘钥管理模块的实现方法

[0063] 同样依据可信执行环境(TEE)的内部API为安全存储服务实现数据处理模块103，数据处理模块提供三类数据存储操作接口：数据存储操作接口SE_StoreData、数据加载操作接口SE_LoadData和数据销毁操作接口SE_DestroyData；可信应用程序102通过远程调用数据处理模块101的各接口完成普通应用程序100的数据安全存储服务请求。

[0064] (41)结合图4具体描述数据存储调用接口的具体实现步骤

[0065] a)可信应用程序102向数据处理模块103发起数据存储操作的远程调用，请求参数中包括可信应用程序标示符UUID、待处理的敏感数据DATA$_{ta}$和密码算法标示符ID$_{algo}$；

[0066] b)数据处理模块103接收到可信应用程序102的数据存储调用请求后，通过判断(34)步骤中合法性检测模块104设定的检测状态标志位来决定远程调用是否可以被接受处理。若检测状态标志位为0，则拒绝远程调用；若检测状态标志位为1，则处理远程调用；

[0067] c)合法性检测通过后，数据处理模块103根据密码算法标示符ID$_{algo}$向秘钥管理模块105发起秘钥生成请求；

[0068] d)秘钥管理模块105收到秘钥生成请求后，首先根据密码算法标示符ID$_{algo}$调用秘钥生成器生成对称密码算法的随机秘钥KEY$_{algo}$＝KeyGenerator(ID$_{algo}$)；其次加载可信应用程序的证书公钥KEY$_{ta}$对密码算法标示符ID$_{algo}$和随机秘钥KEY$_{algo}$加密，生成秘钥加密数据EKEY$_{ta}$＝AsymEncrypt(KEY$_{ta}$,(IDalgo||KEY$_{algo}$))；接着加载可信应用程序102的证书私钥PKEY$_{ta}$对秘钥加密数据EKEY$_{ta}$签名，产生秘钥签名数据SKEYta＝Sign(PKEY$_{ta}$,EKEY$_{ta}$)；最后以可信应用程序标示符UUID为索引将秘钥加密数据EKEY$_{ta}$和秘钥签名数据SKEY$_{ta}$按照特定的组织方式存储到可信执行环境中的非易失性存储器上，并向数据处理模块103返回生成的随机秘钥KEY$_{algo}$。其中，KeyGenerator是对称密钥生成器算法；AsymEncrypt是公钥加密算法；Sign是公钥签名算法；

[0069] e)秘钥成功生成后，数据处理模块103首先根据密码算法标示符ID$_{algo}$调用对应的对称密码加密算法并使用随机秘钥KEY$_{algo}$对敏感数据DATA$_{ta}$进行加密，生成加密数据EDATA$_{ta}$＝SymEncrypt(KEY$_{algo}$,DATA$_{ta}$)；其次使用哈希算法对加密数据计算哈希值HDATA$_{ta}$＝Hash(EDATA$_{ta}$)；接着使用可信应用程序102的证书私钥PKEYta对哈希值签名，生成签名数据SDATA$_{ta}$＝Sign(PKEY$_{ta}$,HDATA$_{ta}$)；最后数据处理模块103以可信应用程序标示符UUID为索引将加密数据EDATA$_{ta}$和签名数据SDATA$_{ta}$按照特定的组织方式存储到可信执行环境中的非易失性存储器上，并向可信应用程序返回数据存储结果。其中，SymEncrypt是对称加密算

法;Hash是哈希算法;Sign是公钥签名算法。

[0070] (42)结合图5具体描述数据加载调用接口的具体实现步骤

[0071] a)可信应用程序102向数据处理模块103发起数据加载操作的远程调用,请求参数中包括可信应用程序标示符UUID;

[0072] b)数据处理模块103接收到可信应用程序102的数据加载调用请求后,按照(41-b)步骤对调用请求进行合法性检测;

[0073] c)合法性检测通过后,数据处理模块103根据可信应用程序标示符UUID向秘钥管理模块104发起秘钥加载请求;

[0074] d)秘钥管理模块收到秘钥加载请求后,首先以可信应用程序标示符UUID为索引从可信执行环境中加载秘钥加密数据$EKEY_{ta}$和秘钥签名数据$SKEY_{ta}$;其次加载可信应用程序102的证书公钥KEY_{ta}对秘钥签名数据$SKEY_{ta}$验签,得到秘钥加密数据$EKEY'_{ta}=Verify(KEY_{ta},SKEY_{ta})$;接着判断$EKEY_{ta}$和$EKEY'_{ta}$是否相等,若不相等,则拒绝处理秘钥加载操作并向数据处理模块103返回秘钥加载失败结果;若相等,则加载可信应用程序102的证书私钥$PKEY_{ta}$对秘钥加密数据$EKEY'_{ta}$解密,获得密码算法标示符和随机秘钥,即$(ID_{algo}||KEY_{algo})=AsymDecrypt(PKEY_{ta},EKEY'_{ta})$;最后秘钥管理模块105返回秘钥加载成功结果并向数据处理模块发送密码算法标示符ID_{algo}和随机秘钥KEY_{algo}。其中,AsymDecrypt是公钥解密算法;Verify是公钥验签算法;

[0075] e)秘钥成功加载后,数据处理模块103首先以可信应用程序标示符UUID为索引从可信执行环境中加载加密数据$EDATA_{ta}$和签名数据$SDATA_{ta}$;其次加载可信应用程序102的证书公钥KEY_{ta}对签名数据$SDATA_{ta}$验签,得到加密数据的哈希值$HDATA'_{ta}=Verify(KEY_{ta},SDATA_{ta})$;接着使用(41-e)步骤中的哈希算法对加密数据$EDATA_{ta}$计算哈希值$HDATA_{ta}=Hash(EDATA_{ta})$,并判断$HDATA'_{ta}$和$HDATA_{ta}$是否相等,若不相等,则拒绝处理数据加载操作;若相等,则根据密码算法标示符ID_{algo}调用对应的对称密码解密算法并使用随机秘钥对加密数据进行解密,获得敏感数据$DATA_{ta}=SymDecrypt(KEY_{algo},EDATA_{ta})$;最后数据处理模块103向可信应用程序102返回数据加载成功结果并发送敏感数据$DATA_{ta}$。其中,Verify是公钥验签算法。Hash是哈希算法,SymDecrypt是对称解密算法。

[0076] (43)结合图6具体描述数据销毁调用接口的具体实现步骤

[0077] a)可信应用程序102向数据处理模块103发起数据销毁操作的远程调用,请求参数中包括可信应用程序标示符UUID;

[0078] b)数据处理模块103接收到可信应用程序102的数据销毁调用请求后,按照(41-b)步骤对调用请求进行合法性检测;

[0079] c)合法性检测通过后,数据处理模块103首先以可信应用程序标示符UUID为索引从可信执行环境中加载加密数据$EDATA_{ta}$和签名数据$SDATA_{ta}$;其次加载可信应用程序102的证书公钥KEY_{ta}对签名数据$SDATA_{ta}$验签,得到加密数据$EDATA_{ta}$的哈希值$HDATA'_{ta}=Verify(KEY_{ta},SDATA_{ta})$;最后使用(41-e)步骤中的哈希算法对加密数据$EDATA_{ta}$计算哈希值$HDATA_{ta}=Hash(EDATA_{ta})$,并判断$HDATA'_{ta}$和$HDATA_{ta}$是否相等,若不相等,则拒绝处理数据销毁操作;若相等,则以可信应用程序标示符UUID为索引从可信执行环境中安全地清除加密数据$EDATA_{ta}$和签名数据$SDATA_{ta}$,并向秘钥管理模块105发起秘钥销毁请求;

[0080] d)秘钥管理模块105收到秘钥销毁请求后,以可信应用程序标示符UUID为索引从

可信执行环境中安全地清除秘钥加密数据$EKEY_{ta}$和秘钥签名数据$SKEY_{ta}$；

[0081] e)数据处理模块103成功销毁加密数据和签名数据后，向可信应用程序102返回数据销毁成功结果。

[0082] 提供以上实施例仅仅是为了描述本发明的目的，而并非要限制本发明的范围。本发明的范围由所附权利要求限定。不脱离本发明的精神和原理而做出的各种等同替换和修改，均应涵盖在本发明的范围之内。

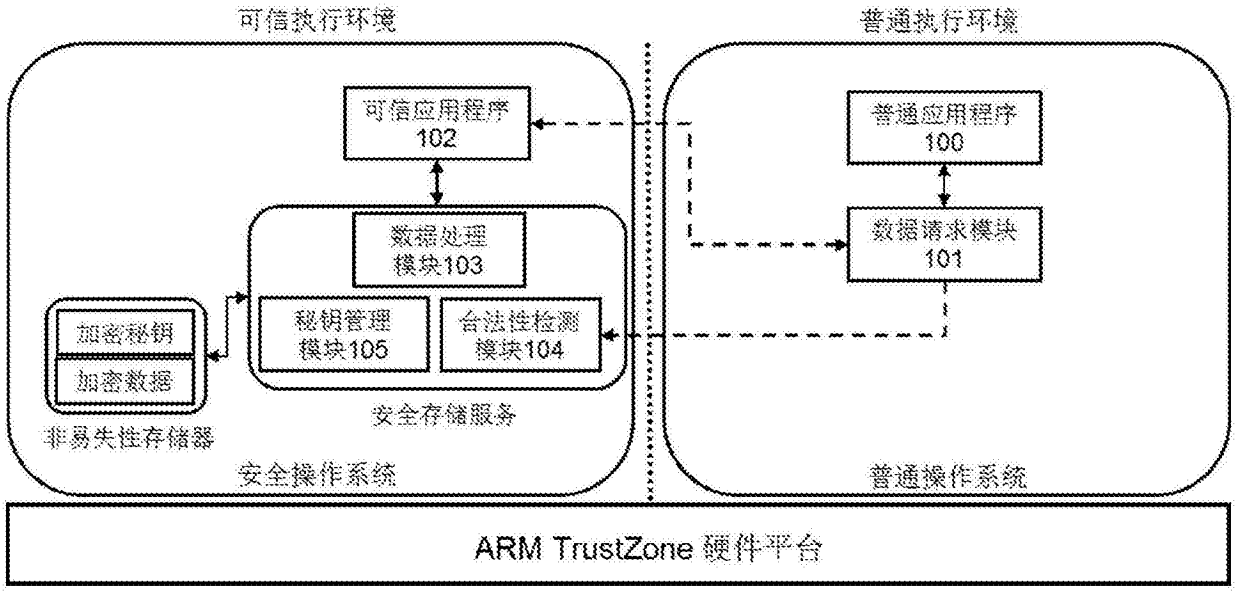

可信执行环境
普通执行环境
可信应用程序
102
普通应用程序
100
数据处理
模块103
数据请求模块
101
加密秘钥
加密数据
秘钥管理
模块105
合法性检测
模块104
安全存储服务
非易失性存储器
安全操作系统
普通操作系统
ARM TrustZone 硬件平台

图1

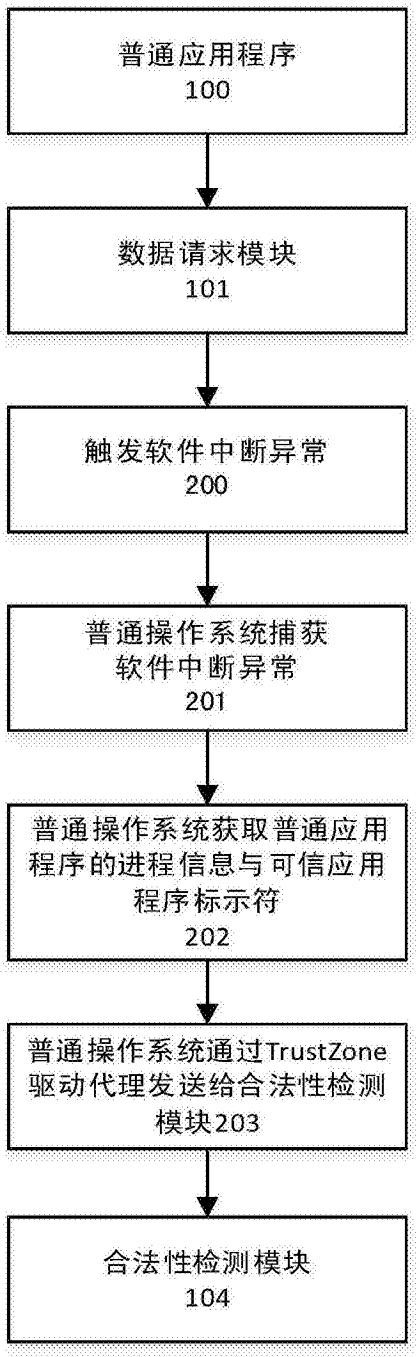

普通应用程序
100
数据请求模块
101
触发软件中断异常
200
普通操作系统捕获
软件中断异常
201
普通操作系统获取普通应用
程序的进程信息与可信应用
程序标示符
202
普通操作系统通过TrustZone
驱动代理发送给合法性检测
模块203
合法性检测模块
104

图2

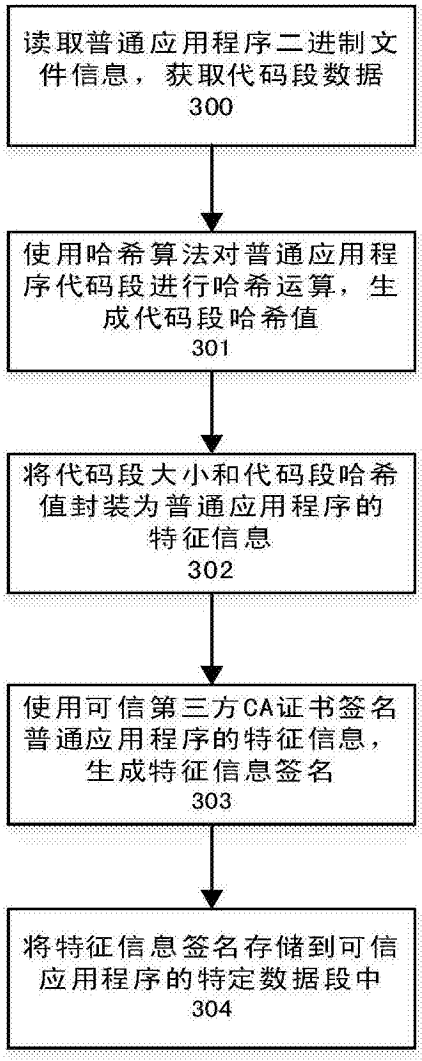

读取普通应用程序二进制文件信息，获取代码段数据
300
使用哈希算法对普通应用程序代码段进行哈希运算，生成代码段哈希值
301
将代码段大小和代码段哈希值封装为普通应用程序的特征信息
302
使用可信第三方CA证书签名普通应用程序的特征信息，生成特征信息签名
303
将特征信息签名存储到可信应用程序的特定数据段中
304

图3

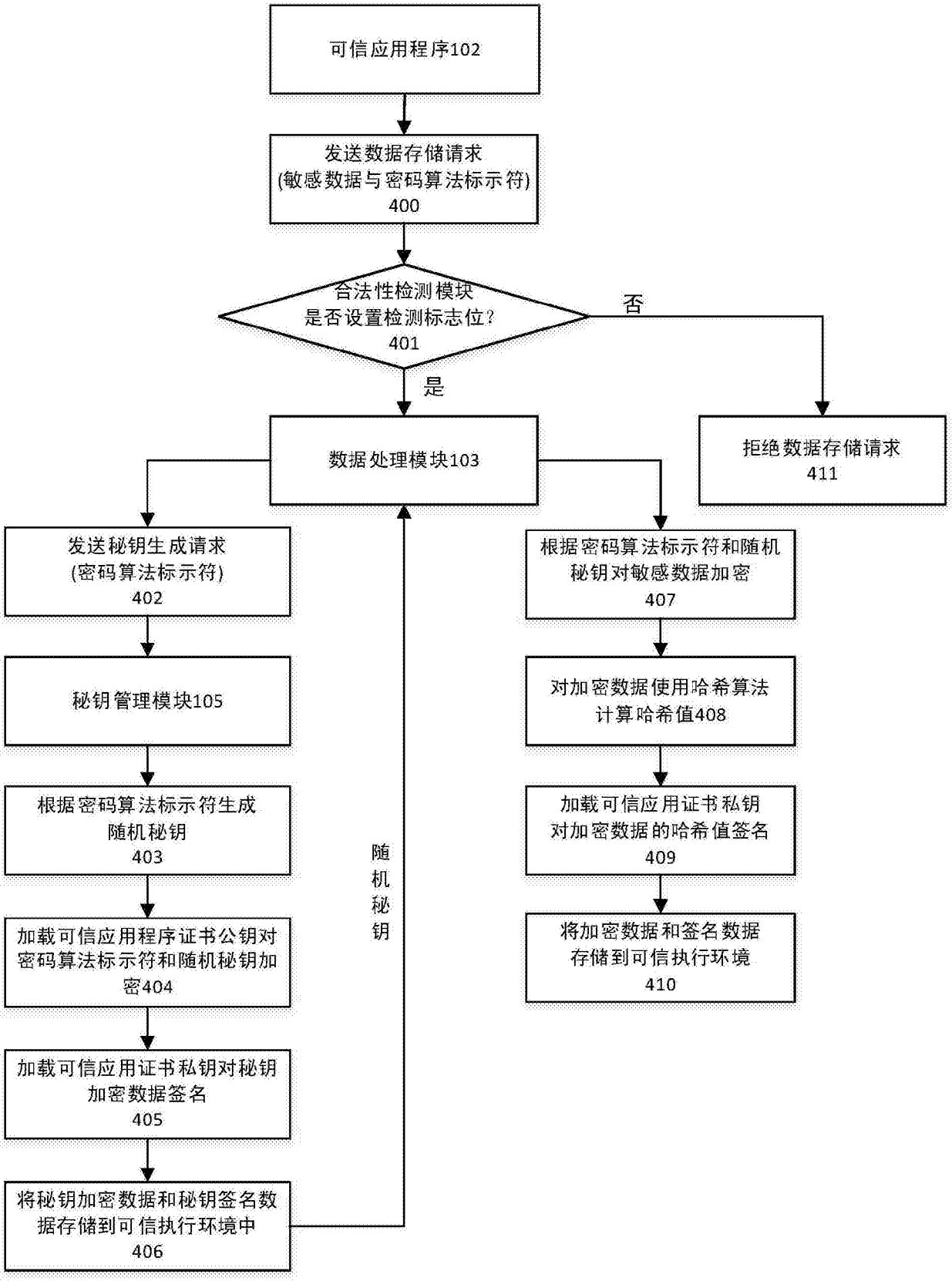

可信应用程序102
发送数据存储请求
(敏感数据与密码算法标示符)
400
合法性检测模块
是否设置检测标志位?
401
否
是
数据处理模块103
拒绝数据存储请求
411
发送秘钥生成请求
(密码算法标示符)
402
秘钥管理模块105
根据密码算法标示符生成
随机秘钥
403
加载可信应用程序证书公钥对
密码算法标示符和随机秘钥加
密404
加载可信应用证书私钥对秘钥
加密数据签名
405
将秘钥加密数据和秘钥签名数
据存储到可信执行环境中
406
随机秘钥
根据密码算法标示符和随机
秘钥对敏感数据加密
407
对加密数据使用哈希算法
计算哈希值408
加载可信应用证书私钥
对加密数据的哈希值签名
409
将加密数据和签名数据
存储到可信执行环境
410

图4

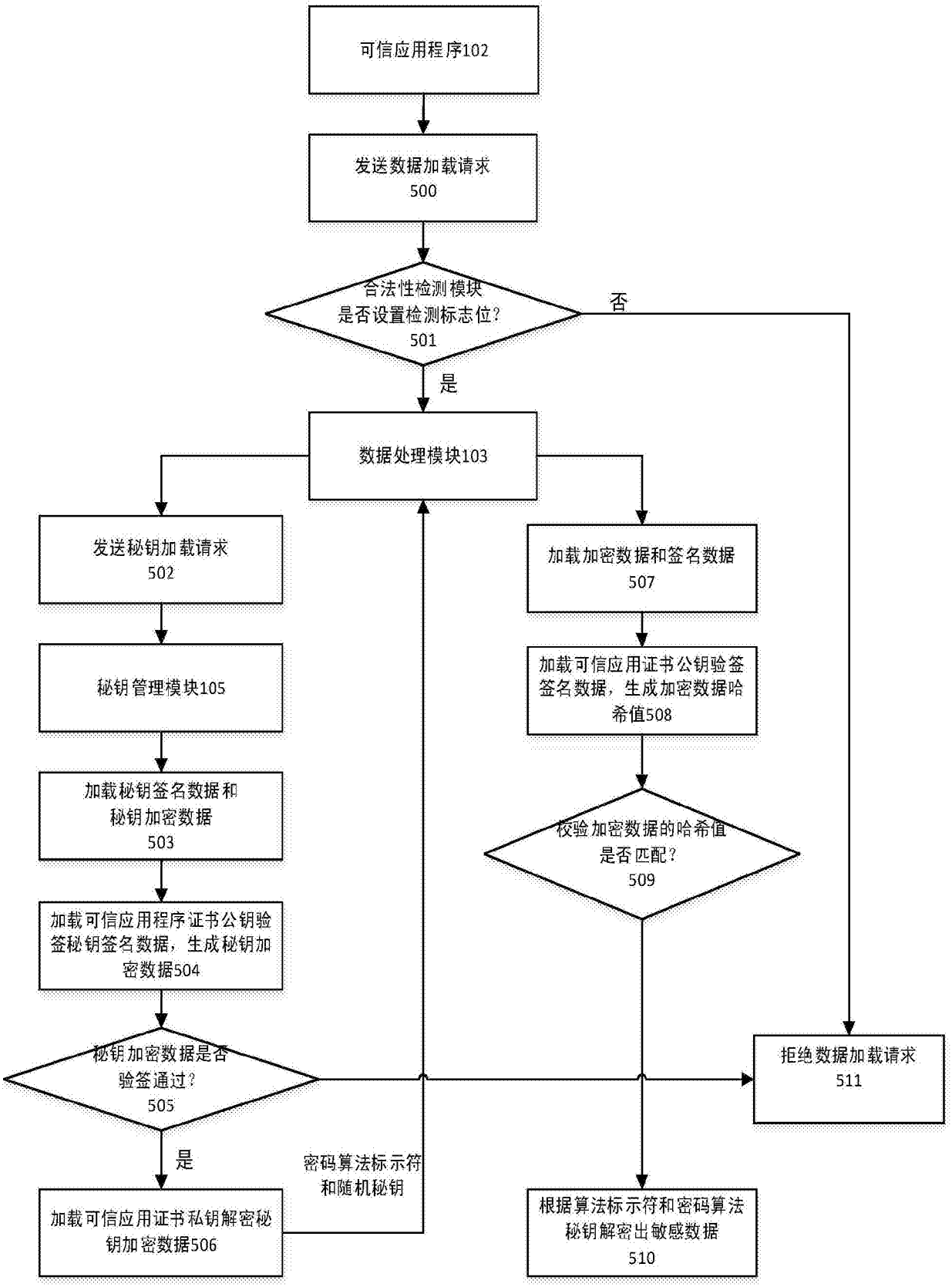

可信应用程序102
发送数据加载请求
500
合法性检测模块
是否设置检测标志位?
501
否
是
数据处理模块103
发送秘钥加载请求
502
秘钥管理模块105
加载秘钥签名数据和
秘钥加密数据
503
加载可信应用程序证书公钥验
签秘钥签名数据，生成秘钥加
密数据504
秘钥加密数据是否
验签通过?
505
是
加载可信应用证书私钥解密秘
钥加密数据506
密码算法标示符
和随机秘钥
加载加密数据和签名数据
507
加载可信应用证书公钥验签
签名数据，生成加密数据哈
希值508
校验加密数据的哈希值
是否匹配?
509
根据算法标示符和密码算法
秘钥解密出敏感数据
510
拒绝数据加载请求
511

图5

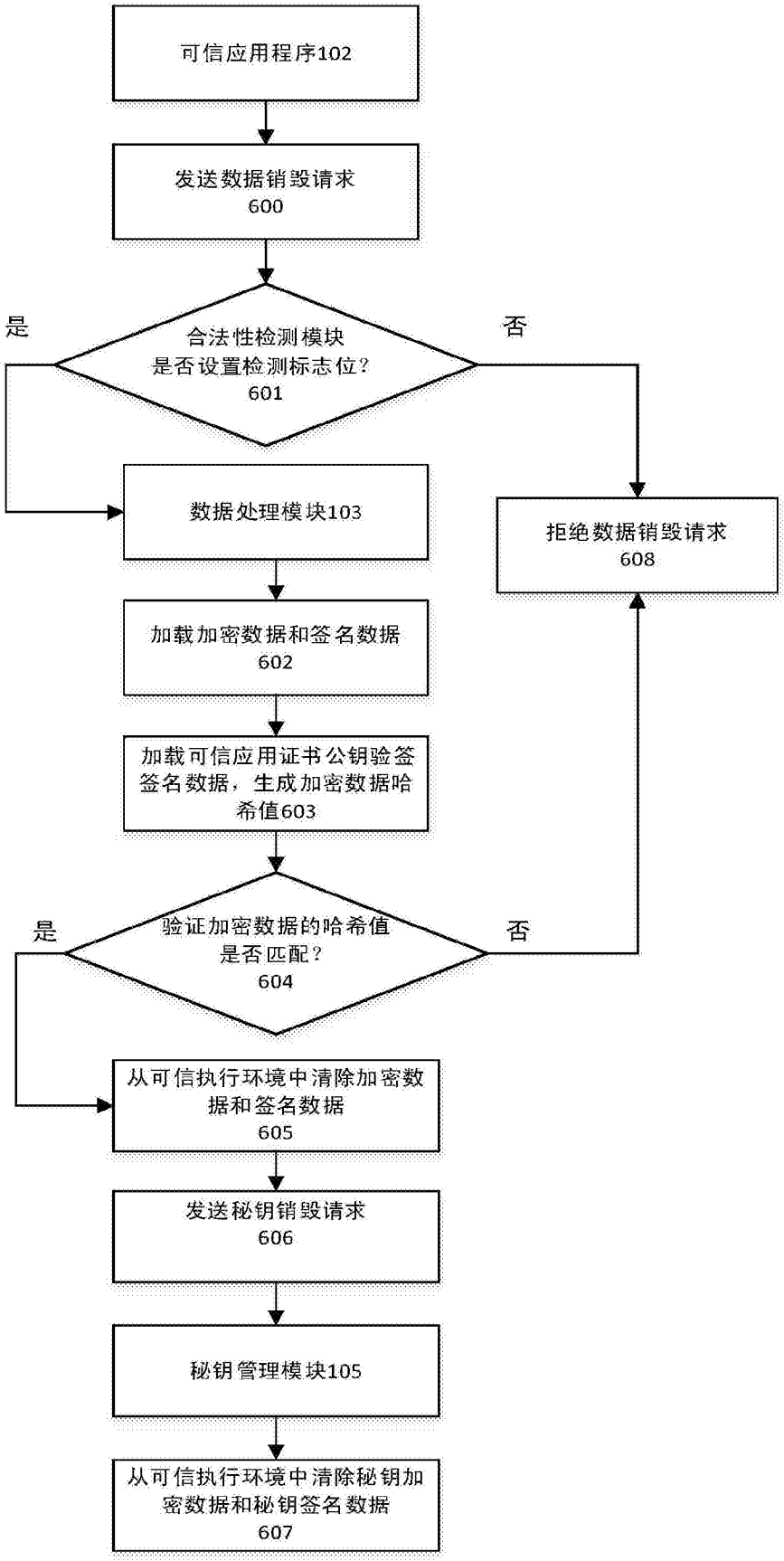

可信应用程序102
发送数据销毁请求
600
合法性检测模块
是否设置检测标志位？
601
是
否
数据处理模块103
拒绝数据销毁请求
608
加载加密数据和签名数据
602
加载可信应用证书公钥验签
签名数据，生成加密数据哈
希值603
验证加密数据的哈希值
是否匹配？
604
是
否
从可信执行环境中清除加密数
据和签名数据
605
发送秘钥销毁请求
606
秘钥管理模块105
从可信执行环境中清除秘钥加
密数据和秘钥签名数据
607

图6