(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112470153 B
(45)授权公告日 2024.07.23

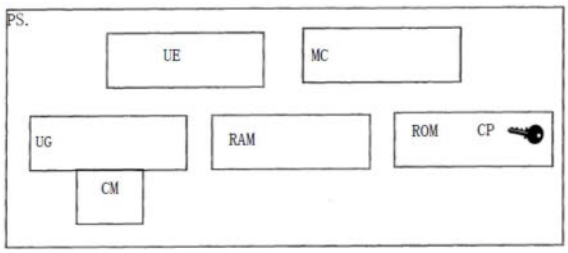
(21)申请号 201980029491.3
(22)申请日 2019.03.13
(65)同一申请的已公布的文献号
申请公布号 CN 112470153 A
(43)申请公布日 2021.03.09
(30)优先权数据
1870286 2018.03.14 FR
(85)PCT国际申请进入国家阶段日
2020.10.30
(86)PCT国际申请的申请数据
PCT/FR2019/000033 2019.03.13
(87)PCT国际申请的公布数据
WO2019/175482 FR 2019.09.19
(73)专利权人 雷吉公司
地址 法国巴黎邮政大街1号
(72)发明人 奥利维尔·托马兹
尼古拉斯·巴卡
(74)专利代理机构 北京律诚同业知识产权代理有限公司 11006
专利代理师 徐金国 吴启超
(51)Int.Cl.
*G06F 21/44*(2006.01)
*G06F 21/51*(2006.01)
*G06F 21/52*(2006.01)
*G06F 21/57*(2006.01)
*G06F 21/62*(2006.01)
(56)对比文件
US 2004187006 A1,2004.09.23
US 2014137178 A1,2014.05.15
审查员 段玥
权利要求书2页 说明书9页 附图3页

(54)发明名称

安全数据处理

(57)摘要

公开用于以自动且安全的方式执行指令的装置和方法。安全处理器(PS)包括:只读存储器(ROM);随机存取存储器(RAM);计算机(UE)能够执行加密功能;单调计数器管理单元(UG)与一或多个单调计数器(CM)相关联,使得安全处理器(PS)不包括任何其他存储器,意味着安全处理器(PS)不存储任何程序或外部数据,允许至少一个初始已注册管理员(A1)进行认证的公开密钥(CP)在其第一次使用之前存储在安全处理器(PS)的只读存储器(ROM),安全处理器(PS)的随机存取存储器(RAM)能够加载由公开密钥加密模块(MC)认证的一组数据和指令,由计算机(UE)对某些指令认证后执行指令,使单调计数器(CM)中的一个递增,以便能够以安全方式自动执行一系列操作,这种安全处理器(PS)包括在用于安全数据处理的组件或基础结构中。




CN 112470153 B

1.一种用于以安全的方式执行具有至少一个上下文的至少一个程序的方法,所述至少一个上下文包括一组指令、代码或数据,所述至少一个程序在所述一组指令、代码或数据下被执行,所述方法包括:

提供安全处理器,所述安全处理器在同一物理单元内至少包括只读存储器、随机存取存储器、能够执行加密功能的加密计算机、至少一个单调计数器、与所述单调计数器相关联的单调计数器管理单元、以及公开密钥算法加密模块,

将用于认证至少一个初始已注册管理员的公开密钥在其第一次使用之前存储在所述安全处理器的所述只读存储器中,

提供所述安全处理器外部的至少一个存储器和能够将所述安全处理器连接到所述安全处理器外部的所述至少一个存储器的至少一个连接构件,

在所述安全处理器外部的所述至少一个存储器中存储旨在由所述安全处理器执行的具有至少一个上下文的所述至少一个程序,

将所述安全处理器连接到所述安全处理器外部的所述至少一个存储器,

在所述安全处理器的所述随机存取存储器中临时加载具有所述至少一个上下文的所述至少一个程序,

由所述公开密钥算法加密模块认证具有至少一个上下文的所述至少一个程序和认证所述初始已注册管理员,

由所述安全处理器基于包括在所述至少一个上下文中的参考值来验证所述至少一个上下文与所述单调计数器的最后状态的同步,

在所述安全处理器的所述加密计算机执行临时加载到所述随机存取存储器中的所述至少一个程序中存在的某些指令之后,递增所述单调计数器,

在所述安全处理器外部的所述存储器中,存储由所述安全处理器的所述加密计算机执行临时加载到所述安全处理器的所述随机存取存储器中的所述至少一个程序中存在的所述某些指令而产生的经认证的文件。

2.如权利要求1所述的方法,其中所述安全处理器被仿真为虚拟机。

3.如权利要求1所述的方法,进一步包括提供连接到所述安全处理器的多个外部存储器。

4.如权利要求1所述的方法,进一步包括就所述安全处理器,认证所述安全处理器外部的所述至少一个存储器。

5.如权利要求1所述的方法,进一步包括提供多个安全处理器并且将所述多个安全处理器中的每个安全处理器连接到至少一个外部存储器。

6.如权利要求1所述的方法,进一步包括提供多个安全处理器和多个外部存储器,并且将所述多个安全处理器中的每个安全处理器连接到所述多个外部存储器中的至少一个外部存储器。

7.如权利要求6所述的方法,进一步包括将所述多个外部存储器彼此同步,并且配置所述多个安全处理器中的每个安全处理器模糊地使用所述多个外部存储器中的一个或另一个外部存储器。

8.如权利要求6所述的方法,进一步包括提供若干对、三件一组、四件一组或更多的外部存储器,并且将所述安全处理器中的每一个与彼此同步的一对、三件一组、四件一组或更

多的外部存储器相关联。

9.如权利要求1所述的方法,进一步包括以下步骤:

具有连接到所述安全处理器的外部存储器的管理员启动所述安全处理器,

一旦启动所述安全处理器就检索所述外部存储器中的公开密钥,并且使用所述公开密钥算法加密模块认证所述管理员,

如果所述安全处理器认证启动它的所述管理员为后续已注册管理员,则所述安全处理器加载并执行由所述后续已注册管理员认证的一组数据和指令,

所述安全处理器产生一组数据,其中可认证所述数据中的一些,并且所述一组数据被存储在由所述后续已注册管理员使用的所述外部存储器中。

10.如权利要求9所述的方法,由至少两个后续已注册管理员实施,每个后续已注册管理员具有外部存储器。

11.如权利要求9所述的方法,其中:

将使用存储在所述只读存储器中的所述公开密钥进行认证和验证的第一组数据和指令加载到所述安全处理器的所述随机存取存储器中,

基于所述第一组数据和指令,所述安全处理器运行后续在册管理员认定程序,之后加载并且执行另一组数据和指令,

所述安全处理器生成加密和签名的文件,所述加密和签名的文件包括所述后续已注册管理员的认证元素,

所述加密和签名的文件由所述后续已注册管理员保存并存储在所述安全处理器外部的所述存储器中,

其中由所述安全处理器对所述第一组数据和指令的执行同时导致所述单调计数器的递增。

12.如权利要求11所述的方法,进一步包括注册不同组的后续已注册管理员,加载和执行不同组的数据和指令,以便由所述安全处理器执行一系列操作,并将所述一系列操作传输到任何电子装置或外部网络。

13.如权利要求9所述的方法,其中:

在先前的注册步骤期间注册的所述后续已注册管理员,在能够将一组数据和指令加载到所述安全处理器的所述随机存取存储器中之前,通过可靠访问控制方法,就按照原样的执行上下文,利用所述安全处理器认证它们本身,

由所述安全处理器对所述一组数据和指令的执行生成新的加密和签名的文件,所述加密和签名的文件包括与所述代码的执行相关的数据,并且所述加密和签名的文件仅由这些后续已注册管理员中的每一个保存并存储在所述安全处理器外部的所述外部存储器中,并且这可致使一个或多个单调计数器的递增。

14.如权利要求13所述的方法,其中所述一组数据和指令一旦被加载到所述安全处理器的所述随机存取存储器中,就只能够在所述安全处理器通过先前的一组数据和指令验证所有后续已注册管理员的所述认证之后执行。

# 安全数据处理

## 技术领域

[0001] 本发明涉及安全数据处理。更确切地,本发明涉及一种类型的安全处理器,所述安全处理器包括只读存储器、随机存取存储器、能够执行加密功能的计算机,以及与至少一个单调计数器相关联的单调计数器管理单元,涉及一种安全数据处理组件,所述安全数据处理组件包括这种安全处理器,并且具有连接构件、外部存储器,涉及一种安全数据处理基础设施,所述安全数据处理基础设施包括若干安全处理器,并且最后地,涉及一种用于实现这种安全数据处理组件的方法。

## 背景技术

[0002] 在本发明的上下文中,安全是指对由指令和与其相关的上下文组成的程序的完整性以及对发出命令以执行所述程序的人的认证的维护和控制。术语“上下文”应当理解为一组参数、指令和条件,并且更广泛地是可在其下实现程序的任一组指令、代码或数据。术语“管理员”一方面是指初始已注册管理员,另一方面是指任何其他后续已注册管理员。“已注册”可理解为已登记过的、已在册的,或者换句话说被授权发出指令。“已注册管理员的认证”是指用于验证发出指令的人是已注册管理员并授权由安全处理器执行有问题的指令的过程。“已注册管理员的认证”是指分别应用于若干人和已注册管理员的类似过程。

[0003] 文档FR2906380描述了一种用于保护存储在物理介质上的数据的系统及其实现方法。数据安全系统被嵌入诸如移动电话的装置中,特别地,所述装置包括具有键盘、屏幕、麦克风、扬声器、用于发送和接收数据的模块、用户识别模块和供应电力的电池的盒子。电子卡至少包括微控制器、随机存取存储器、快闪存储器和总线系统。例如,电话的操作由加载在所述电话的存储器中的操作系统和一组应用程序管理。形成整体的安全系统在适当情况下包括,计算实体(诸如,微处理器),以及系统资源(诸如,随机存取存储器)、单调计数器(可仅由单个单位使其递增)、系统密钥(仅由系统授权的实体才可访问的加密密钥),以及确保计算机数据的持久存储的物理数据介质(诸如,硬盘、快闪存储器等)。此物理数据介质包括大小是可配置的至少一个数据块和两个主块。所述实现方法使用认证密钥。用于实现文档FR2906380的数据安全系统和方法的目的一方面在于解决针对重放(通过非法复制数据管理系统的先前内容进行欺诈性数据访问)的安全问题,并且另一方面在于解决特别是由服务突然中断(诸如,停电或不合时宜的系统重新启动)引起的变更或修改。本文档不涵盖管理员的认证。

[0004] 文档US 2004/0187006涉及数据安全领域,并且更具体地,涉及从外部存储器可靠地检索数据,因为由于外部存储器位于安全环境外部,所以这是不安全的。数据安全系统包括计算实体,以及单调计数器的使用以在安全环境中确定对外部存储器的请求是否返回了最新数据。每当将主要元素写入存储器,单调计数器递增。控制条目记录了链接到它的项目被修改的时间。单调计数器值保持不变,直到下一次将数据写入存储器。尽管本文档描述了单调计数器的实现,但是其并不旨在提供根据本发明的安全性。

[0005] 文档US2014/0137178涉及一种方法,所述方法包括以下步骤:通过计算装置的安

全平台模块TPM接收从计算机装置中的程序传出的访问包含在受保护对象中的信息的请求;确定是否满足允许程序访问信息的条件;允许程序响应于满足条件访问信息;响应于不满足条件而拒绝程序访问信息;以及响应于来自所述程序的阈值数量的请求的未满足条件,将所述信息锁定达无限期,以便防止所述程序访问所述信息。对象由安全平台模块维护。对象中的每一个存储信息并与策略相关联,所述策略标识程序必须满足的条件,以便使程序访问信息。对于对象中的每一个,安全平台模块管理与所述对象相关联的单调计数器。单调计数器用于确定是否进行了不满足与对象相关联的策略模式的条件的阈值数量的对象信息访问请求。可信平台模块向计算装置提供安全存储和/或安全处理功能。安全存储是指受安全平台模块的特定功能或其他部件保护的非易失性存储器,并且所述非易失性存储器可仅由安全平台模块访问。信息存储在数据结构或以受模块保护的对象的名称指定的对象中,并且可采用各种形式,包括加密密钥。可通过不同的方式访问信息,诸如读取信息、写入信息或对其进行修改等。非易失性存储器包括一个或多个单调计数器和一个或多个受保护的对象(请参见本文档的图1)。

[0006] 由KTH CSC发布的Andreas Nilsson撰写的“Key Management with Trusted Platform Modules”文档涉及目的在于使计算平台更加可靠的概念。它基于称为可信平台模块(TPM)的芯片。TPM是提供诸如RSA加密和安全密钥存储的加密功能的芯片。每个TPM具有唯一一对密钥,称为验证密钥,由TPM在制造后但在发货给客户之前在内部创建。密钥对唯一地标识TPM,并且永远不可更改。私有部分永远不离开TPM,而公共部分则用于认证证书。提供了非易失性存储器和易失性存储器,非易失性存储器用于存储持久标识和状态数据以及内部密钥。在所有者的许可下,可向TPM写入和从TPM读取持久和不透明的数据(TPM无权访问这些数据或无法使用这些数据)。易失性存储器主要由TPM在内部使用。

[0007] Luis FG Sarmenta等人撰写的文档“Virtual Monotonic Counters and Count-Limited Objects using a TPM without a trusted OS”描述了带有TPM安全平台模块的不可信机器对虚拟单调计数器的进一步开发。

## 发明内容

[0008] 对于安全处理器,本发明的根本问题在于,所述安全处理器包括只读存储器、随机存取存储器、能够执行加密功能的计算机以及与至少一个单调计数器相关联的单调计数器管理单元,以确保安全处理器在使用中是安全的,以维持其执行程序的完整性以及与之相关的上下文的控制,并验证发出命令以执行所述程序的已注册管理员。

[0009] 本发明提供了针对此问题的解决方案,特别是在处理器不包括任何其他存储存储器的情况下,使得其不存储任何外部程序或数据。因此,存储器相对于处理器是“外部化的”,执行系统与要执行的数据分开和分离,以便维持完美的完整性。

[0010] 下面是本发明的描述。

[0011] 根据第一方面,本发明的主题是一种安全处理器,所述安全处理器至少包括只读存储器、随机存取存储器、能够执行加密功能的计算机以及与至少一个单调计数器相关联的单调计数器管理单元。此安全处理器使得:

[0012] -它不包括任何其他存储存储器,因此它不存储程序、上下文(指令、代码、数据)或外部数据,

[0013] -允许认证至少一个初始已注册管理员的公开密钥在其第一次被使用之前存储在只读存储器中，

[0014] -所述随机存取存储器能够加载可由公开密钥加密模块认证的一组数据(诸如上下文)以及指令，

[0015] -在所述初始已注册管理员对由所述计算机执行的某些指令进行认证之后，将使所述单调计数器中的一个递增，

[0016] 在包括这种安全处理器和外部存储器的安全数据处理组件的上下文中，这种安全处理器使得能够以安全方式自动执行一系列操作。

[0017] 在一个实施例中，所述安全处理器被仿真为虚拟机。

[0018] 根据第二方面，本发明的主题是一种安全数据处理组件，所述安全数据处理组件包括刚刚描述的安全处理器，以及除此之外，此安全处理器外部的至少一个存储器以及诸如，特别地使用电子通信网络将此安全处理器连接到所述安全处理器外部的至少一个存储器的至少一个连接构件。

[0019] 根据一个特性和一个实施例，出于安全原因，所述安全数据处理组件包括连接到所述安全处理器的多个(即，至少两个)外部存储器。

[0020] 根据一个特性，就所述安全处理器认证所述安全数据处理组件的至少一个外部存储器。

[0021] 根据一个实施例，所述安全数据处理组件的所述外部存储器被配置来适于并且具体地旨在：

[0022] -存储旨在加载到所述安全处理器的所述随机存取存储器中的至少一个程序和至少一个上下文(指令、代码、数据)，

[0023] -并且能够接收和存储由所述安全处理器执行的已经临时加载到所述安全处理器的所述随机存取存储器中的至少一个程序和至少一个上下文所产生的任何经认证的文件，

[0024] 而至少一个上下文可包括适于使所述安全处理器能够验证至少一个上下文与单调计数器的最后状态的同步。

[0025] 根据第三方面，本发明的主题是一种安全数据处理基础设施，所述安全数据处理基础设施包括多个(即，至少两个)安全处理器(诸如，先前描述的安全处理器)和至少一个外部存储器(诸如，先前关于所述安全数据处理组件描述的安全处理器的外部存储器)，所述基础设施使得所述多个安全处理器中的每个安全处理器连接到至少一个外部存储器。

[0026] 根据一个实施例，所述安全数据处理基础设施包括多个(即，至少两个)外部存储器，所述多个安全处理器中的每个安全处理器连接到所述多个外部存储器中的至少一个外部存储器。

[0027] 根据一个可能的实施例，所述安全数据处理基础设施包括彼此同步的多个(即，至少两个)外部存储器，所述多个安全处理器的所述安全处理器中的每一个能够模糊地使用所述多个外部存储器中的所述外部存储器的一个或另一个。

[0028] 根据一个可能的实施例，所述安全数据处理基础设施包括若干对、三件一组、四件一组或更多的外部存储器，所述安全处理器中的每一个与在它们之间同步的一对、三件一组、四件一组或更多的外部存储器相关联。

[0029] 因此，所述安全处理器本身不包括任何其他存储存储器。所述安全处理器外部的

一个或多个此类存储存储器形成安全数据处理组件或安全数据处理基础设施。

[0030] 根据第四方面,本发明涉及一种用于由安全数据处理组件安全地执行一系列操作的方法,所述方法至少包括执行以下步骤:

[0031] -A:管理员利用连接到所述安全处理器的外部存储器启动所述安全处理器,

[0032] -B:一旦启动所述安全处理器就检索来自外部存储器的公开密钥,以便能够使用公开密钥加密模块对其进行认证,

[0033] -C:如果所述安全处理器认证启动它的所述管理员为后续已注册管理员,则它加载由所述后续已注册管理员认证的一组数据和指令,并执行它,

[0034] -D:由所述安全处理器的执行产生一组数据,其中可认证所述数据中的一些,并且一旦由所述安全处理器生成所述数据集,此数据集就被存储在由所述后续已注册管理员使用的所述外部存储器中。

[0035] 根据一个特性和一个实施例,并且出于安全原因,刚刚描述的所述方法由两个后续已注册管理员(并且更一般地,多个至少两个后续已注册管理员)执行,每个具有外部存储器。

[0036] 所述方法还包括执行初始步骤,在初始步骤中,初始已注册管理员具有安全数据处理组件,并注册后续已注册管理员。

[0037] 然后,所述方法包括执行以下注册步骤:

[0038] -A':将使用存储在所述只读存储器中的所述公开密钥进行认证和验证的第一组数据和指令加载到所述安全处理器的所述随机访问存储器中,以便使所述随机访问存储器能够执行程序来授权后续已注册管理员,并且上传另一组数据和指令并使其由所述安全处理器执行,

[0039] -B':由所述安全处理器对所述第一组数据和指令的执行生成加密和签名的文件,所述加密和签名的文件包括所述后续已注册管理员的认证元素,并且所述加密和签名的文件由所述后续已注册管理员保存并存储在所述安全处理器的外部的存储器中,

[0040] -C':由所述安全处理器对所述第一组数据和指令的执行同时导致单调计数器的递增。

[0041] 根据一个特性和一个实施例,出于安全原因,刚刚描述的所述注册步骤使得初始的已注册管理员注册至少两个后续已注册管理员,并且更一般地,多个至少两个后续已注册管理员。

[0042] 根据一个实施例,可重复以上描述的三个步骤A'、B'和C'若干次,以便注册不同组的后续已注册管理员来加载和执行不同组的数据和指令,所有这些都是为了使所述安全处理器能够执行一系列操作并将其传输到电子装置或外部网络。

[0043] 所述方法的特征还在于它包括执行以下后续步骤:

[0044] -在之前的注册步骤期间注册的所述后续已注册管理员,在能够将一组数据和指令加载到所述安全处理器的所述RAM中之前,使用诸如电子签名的可靠访问控制方法,就按照原样执行上下文在所述安全处理器上认证它们本身。

[0045] -由所述安全处理器对所述一组数据和指令的执行生成第二加密和签名的文件,所述加密和签名的文件包括与所述代码的执行相关的数据,并且所述加密和签名的文件仅由在所述安全管理器外部的这些后续已注册管理员中的每一个保存并存储在外部存储器

中,这可致使一个或多个单调计数器的递增。

[0046] 出于安全原因,可预期,一旦将所述一组数据和指令加载到所述安全处理器的RAM中,就可仅在所述安全处理器验证了由所述先前的一组数据和指令后续已注册的所有管理员的认证之后执行。

## 附图说明

[0047] 在此简要描述附图中的图。

[0048] 图1示意性地表示构成根据本发明的基本安全处理器的各种部件。此图示出安全处理器仅包括只读存储器、随机存取存储器、计算机、与单调计数器相关联的单调计数器管理单元,并且不包括任何其他存储存储器,使得安全处理器不存储外部程序或数据。

[0049] 图2示意性地表示组成根据本发明的用于基本数据的安全处理组件的不同部件,其包括安全处理器(诸如图1中的安全处理器)、在安全处理器外部的存储器以及能够诸如通过电子通信网络连接所述安全处理器及其外部的存储器的连接构件。

[0050] 图3和图4示意性地表示构成根据本发明的用于安全数据处理的两个基础设施的各种部件。在图3的情况下,基础设施包括两个安全处理器(诸如,图1和图2中的安全处理器),以及彼此同步的三个外部存储器(诸如,图2中的外部存储器),安全处理器中的每一个能够模糊地使用三个外部存储器中的每一者。在图4的情况下,基础设施包括两个安全处理器(诸如,图1和图2中的安全处理器),以及彼此同步的两对外部存储器(诸如,图2中的外部存储器),安全处理器中的每一个与一对外部存储器相关联。

[0051] 图5表示根据本发明的安全数据处理组件的执行步骤的总体图。

[0052] 图6示出两个后续已注册管理员的各种注册步骤。

## 具体实施方式

[0053] 根据本发明的安全处理器PS(图1)包括只读存储器ROM、随机存取存储器RAM、能够执行加密功能的UE、与至少一个单调计数器CM相关联的单调计数器管理单元UG。

[0054] 在第一次使用使认证至少一个初始已注册管理员AI成为可能的公开密钥CP之前,将其存储在只读存储器ROM中。随机存取存储器RAM能够加载可由安全处理器PS包括的公开密钥加密模块MC来认证的一组数据(诸如,上下文)和指令。

[0055] 在它们的认证之后,由计算机UE执行的某些指令可使单调计数器CM递增。

[0056] 在一个实施例中,安全处理器PS被仿真为虚拟机。

[0057] 根据安全处理器PS的一个特性,后者不包括任何其他永久性存储存储器,使得安全处理器PS不永久性存储任何程序、上下文(指令、代码、数据)或外部数据。

[0058] 这样,安全处理器PS包括只读存储器ROM、随机存取存储器RAM、计算机UE、管理单元UG、至少一个单调计数器CM和加密模块MC。

[0059] 然而,提供至少一个这种存储存储器ME用于数据的安全处理,但是后者在安全处理器PS的外部,而不是其一部分或物理上集成到其中。这就是利用这种安全处理器PS和至少一个这种存储存储器ME以及适当的通信手段、安全数据处理组件ETS(图2)或安全数据处理基础设施ITS(图3和图4)形成的方式。在这种安全数据处理组件ETS中或在这种安全数据处理基础设施ITS中,安全处理器PS可以安全方式自动执行一系列操作。从以上限定的意义

上讲,这理解为意指对程序和相关上下文的完整性以及对已注册管理员的认证的维护和控制。

[0060] 可将“安全处理器外部的”存储存储器理解为不包括在构成处理器PS的物理单元中的存储器。因此,此存储器称为“外部存储器”,并且称为ME。

[0061] 存储器ME在安全处理器PS外部的特性具有相对于处理器PS外部化存储的功能,或者换句话说,将执行系统(处理器PS)与数据分开和分离。存储器ME在安全处理器PS外部的特性一方面导致处理器PS的数据处理能力不受限制,并且另一方面导致保证不变性,并且因此保证了处理器处理的完整性,因为外部永久性存储器对安全处理器PS本身没有效果或影响。本发明还涉及诸如刚刚描述的与外部存储存储器ME不同的所有其他构件,但它们实现相同的功能并提供与刚刚说明的结果类似的结果。

[0062] 从以上限定的意义上讲,安全数据处理组件ETS(图2)包括如以上描述的安全处理器PS,以及除此之外的外部存储器ME。组件ETS还包括至少一个连接构件CO,所述连接构件CO能够诸如,特别是通过电子通信网络将外部存储器ME连接到安全处理器PS。

[0063] 安全数据处理组件ETS可仅包括单个外部存储器ME。然而,如果出于安全原因期望不可由单个人执行应用程序决策,则为安全数据处理组件ETS做出使包括用于至少两

[0064] 个后续已注册管理员AU的至少两个外部存储器ME的规定。

[0065] 关于具有两个外部存储器ME的实施例给出以下描述。然而,外部存储器ME的数量的特性不受限制。特别地,可使用两个以上的外部存储器ME。这就是为什么我们可参考多个(即至少两个)外部存储器

[0066] ME(外部存储器ME的数量可更多),并且参考多个(即至少两个)后续已注册管理员AU(后续已注册管理员AU的数量可更多)。

[0067] 连接构件CO可能够在从安全处理器PS到外部存储器ME的方向上进行加密存储,并且在从外部存储器ME朝向安全处理器PS的方向上进行加密检索。就安全处理器PS,对安全数据处理组件ETS的外部存储器ME的内容进行认证。外部存储器ME被配置来适于并且具体地旨在存储至少一个程序和至少一个上下文(指令、代码、数据),旨在被加载到安全处理器PS的随机存取存储器RAM中,并且旨在能够接收和存储由安全处理器PS执行的、已经临时加载到随机存取存储器RAM中的这种程序和这种上下文所产生的任何认证的一组数据,如刚刚说明的。

[0068] 上下文(可在其下实现程序的一组参数和条件)可包括能够允许安全处理器PS检查上下文与单调计数器CM的最后状态的同步的参考值。

[0069] 安全数据处理基础设施ITS(图3和图4)包括多个(即至少两个)如刚刚描述的安全处理器PS(例如,PS1和PS2),以及除此之外,至少一个外部存储器ME,如刚刚描述的。

[0070] 然而,与安全数据处理组件ETS一样,安全数据处理基础设施ITS可包括多个(即至少两个(或更多数量))的外部存储器ME。

[0071] 与组件ETS一样,基础设施ITS还包括能够将外部存储器ME连接到安全处理器PS的至少一个连接构件CO。这种安全数据处理基础设施ITS的结构可以是多个实施例的主题,所述实施例的每一个使得安全处理器PS的每一个连接到至少一个外部存储器ME。这样,根据情况,将安全处理器PS连接到单个外部存储器ME,或者相反地,将其连接到若干外部存储器ME,并且将外部存储器ME连接到单个安全处理器PS,或者相反地,将其连接到若干安全处理

器PS。

[0072] 这样,安全数据处理基础设施ITS可被视为是被组合在一起并且适当时具有共同的一个或多个安全处理器PS和/或一个或多个外部存储器ME的若干安全数据处理组件ETS的结构。

[0073] 在一个可能的实施例中(图3),安全数据处理基础设施ITS包括若干安全处理器PS1、PS2以及彼此同步的若干外部存储器ME1、ME2、ME3,使得安全处理器PS1、PS2中的每一者可模糊地使用外部存储器ME1、ME2、ME3中的一者或另一者。这种结构具有显示出对故障的高抵抗力的优点。

[0074] 在另一个可能的实施例中(图4),安全数据处理基础设施ITS包括若干安全处理器PS1、PS2和若干对(例如,一方面是ME1a和ME1b,另一方面是ME2a和ME2b),或者若干三件一组、四件一组或更多的外部存储器ME,使得安全处理器PS1、PS2中的每一者与彼此同步的一对、三件一组、四件一组……外部存储器ME相关联。这种结构的优点是通过创建数据组和分区来提高系统的性能。

[0075] 现在,我们将描述用于实现如以上所描述的安全数据处理组件ETS的方法,所述方法包括执行连续步骤。

[0076] 在根据本发明的方法的上下文中,我们将需要参考实现这些方法的一个或多个已注册管理员AI、AU。这些管理员是初始的已注册管理员AI和任何后续的已注册管理员AU。如以上所说明,如果出于安全原因期望不可由单个人执行应用程序决策,则需要至少两个后续已注册管理员AU。关于具有两个后续已注册管理员AU(分别为AU1和AU2)的实施例给出以下描述的方法。然而,后续已注册管理员AU的数量的特性不受限制。特别地,可使用两个以上后续已注册管理员AU。

[0077] 现在我们参考图5,以一般方式描述具有两个后续已注册管理员AU1和AU2的安全数据处理组件ETS的执行。

[0078] 在步骤A中,各自具有连接到安全处理器PS的外部存储器ME的两个后续已注册管理员AU1和AU2启动所述安全处理器PS。因此,此步骤A包括以下操作:

[0079] -A1:检索已注册管理员AU1的上下文,

[0080] -A2:检索已注册管理员AU2的上下文,

[0081] A3:由已注册管理员AU1启动安全处理器PS,

[0082] A4:由已注册管理员AU2启动安全处理器PS。

[0083] 在步骤B中,一旦启动安全处理器PS,就检索存储器中的公开密钥CP,以便能够使用实现公开密钥算法的加密模块MC对其进行认证。

[0084] 在步骤C中,如果安全处理器PS认证已注册管理员AU1和AU2,其加载由所述已注册管理员AU1和AU2认证的一组数据和指令(已注册管理员AU1和AU2的操作C1和C2)并执行(操作C3)。

[0085] 在步骤D中,安全处理器PS的所述执行(操作C3)产生一组数据,其中可认证所述数据中的一些。一旦由安全处理器PS产生此组数据,所述数据就被存储在由一个或多个已注册管理员AU1、AU2使用的一个或多个外部存储器ME中。因此,此步骤O包括以下操作:

[0086] 01:检索链接到已注册管理员AU1的数据,

[0087] 02:检索链接到已注册管理员AU2的数据,

[0088] 03:将分配给已注册管理员AU1的数据存储在外部存储器ME中,

[0089] 04:将链接到已注册管理员AU2的数据存储在外部存储器ME中。

[0090] 所述方法还包括以下初始注册步骤,在所述初始步骤中,初始已注册管理员AI具有安全数据处理组件ETS,并注册至少一个后续已注册管理员AU。如以上所描述,如果出于安全原因期望不可由单个人执行应用程序决策,则初始已注册管理员AI注册两个或至少两个后续已注册管理员AU,分别为两个后续已注册管理员AU1和AU2。关于具有两个后续已注册管理员AU1和AU2的实施例描述了注册方法。然而,如所指示,后续已注册管理员的数量的特性不受限制。而且,并且更一般地,初始已注册管理员AI可注册多个至少两个后续已注册管理员(AU)。

[0091] 这些两个后续已注册管理员AU(分别为AU1和AU2)的注册构成第一集合,所述第一集合参与在后续执行中使用的第一认证上下文的限定。

[0092] 初始已注册管理员可后续更改先前已经被注册的后续已注册管理员AU中的一个或另一个。他可添加一个或多个后续已注册管理员AU。他可移除一个或多个后续已注册管理员AU。他可修改一个或多个后续已注册管理员AU的权限。如果后续更改先前已经被注册的后续已注册管理员AU中的一个或另一个,则初始已注册管理员AI实现对应的自适应方法。然后,我们检索更新的上下文和递增的一个或多个单调计数器。

[0093] 现在参考图6,示出两个后续已注册管理员AU1和AU2的各种注册步骤。对于第一两个已注册管理员,这些注册步骤被指定为AU1和AU2,这些注册步骤是在图5中描述和表示的执行步骤之前的初始步骤。如果后续更改第一已注册管理员AU1和AU2中的一个或另一个,或者如果更改预先已注册的后续已注册管理员AU中的一个或另一个,则在管理员更改时进行注册步骤,同时安全数据处理程序组件ETS能够在先前上下文中与其他管理员先前执行指令。

[0094] 在步骤A'中,使用存储在只读存储器ROM中的公开密钥CP进行认证和验证的第一组数据和指令被加载到安全处理器PS的随机存取存储器RAM中,以使所述随机存取存储器RAM能够执行后续两个已注册管理员AU1和AU2的授权程序,以加载其他组数据和指令并使其由安全处理器PS执行。

[0095] 因此,此步骤A'包括以下操作:

[0096] -A'1:初始管理员AI从外部存储器ME中检索授权程序,

[0097] -A'2:检索后续管理员AU1的认证元素,

[0098] A'3:类似地,检索后续管理员AU2的认证元素,

[0099] A'4:将授权程序和认证传输元素到安全处理器PS。

[0100] 在步骤B'中,由安全处理器PS对所述第一组数据和指令的执行生成加密和签名的文件,所述加密和签名的文件包括后续已注册管理员AU1和AU2的认证元素,所述加密和签名的文件由所述后续已注册管理员AU1、AU2中的一者保存并存储在安全处理器PS的外部的存储器ME中。因此,此步骤B'包括以下操作:

[0101] B'1:由安全处理器PS与后面将要讨论的步骤C同时执行第一组数据和指令,

[0102] B'2:传输链接到后续管理员AU1的加密和签名的数据,

[0103] B'3:由后续管理员AU1将这些数据存储在外部存储器ME中,

[0104] B'4:类似地,传输链接到后续管理员AU2的加密和签名的数据,

[0105] -:B’5:并且类似地,由后续管理员AU2将这些数据存储在外部存储器ME中。

[0106] 在步骤C’中,由安全处理器PS对第一组数据和指令(操作B’1)的执行同时导致单调计数器CM的递增。

[0107] 可重复以上描述的三个步骤A’、B’和C’若干次,以便允许不同组的后续已注册管理员AU来加载和运行不同组的数据和指令,所有都是以便能够使所述安全处理器PS执行一系列操作,并其传输到任何电子装置或外部网络。

[0108] 一旦已经注册了两个后续管理员AU1和AU2,他们就可执行以下后续步骤,如先前参考图5所描述。

[0109] 在先前的注册步骤期间注册的后续已注册管理员AU1和AU2,在可将一组数据和指令加载到所述安全处理器PS的随机存取存储器RAM中之前,使用诸如电子签名的可靠访问控制方法,就按照原样执行上下文利用所述安全处理器PS认证它们本身。

[0110] 一旦将此组数据和指令加载到安全处理器PS的随机存取存储器RAM中,就可仅在所述安全处理器PS使用先前的一组数据和指令验证两个后续已注册管理员AU1和AU2的认证之后执行。此步骤不是强制性的,它仅是任选的。这旨在使安全级别提高一倍。如果想要使安全级别提高一倍,请执行此步骤。

[0111] 由安全处理器PS对一组数据和指令的执行生成第二加密和签名的文件,所述加密和签名的文件包括与代码的执行相关的数据,并且所述加密和签名的文件仅由在安全管理器PS外部的这些后续已注册管理员AU1和AU2中的每一个保存并存储在外部存储器ME中,这可致使一个或多个单调计数器CM的递增。

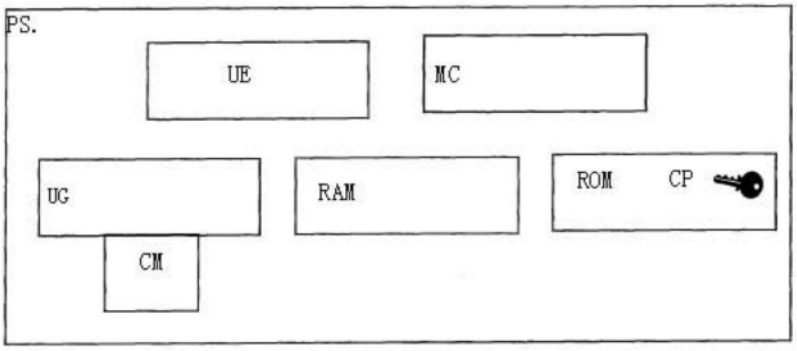



图1

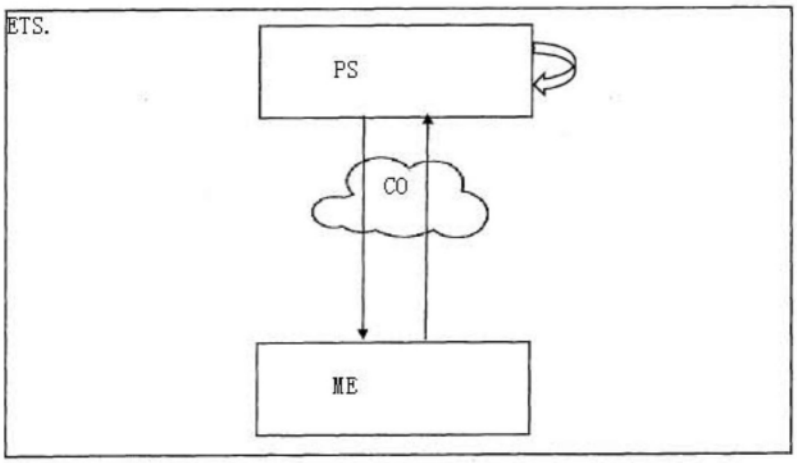



图2

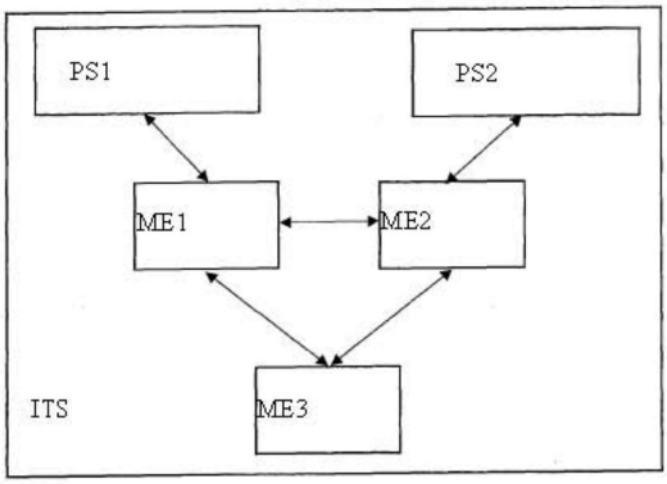



图3

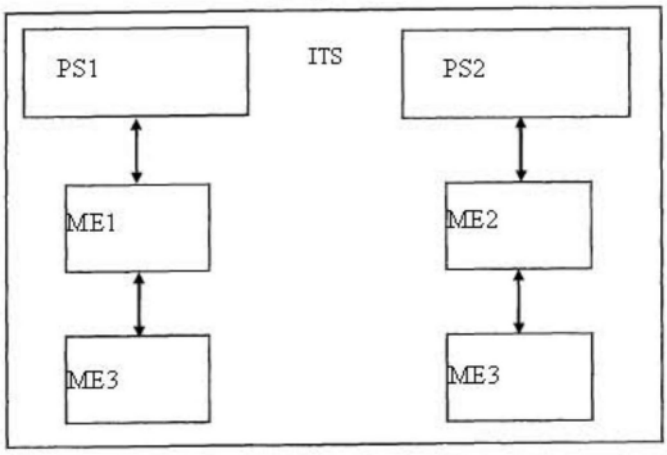

PS1
ITS
PS2
ME1
ME2
ME3
ME3

图4

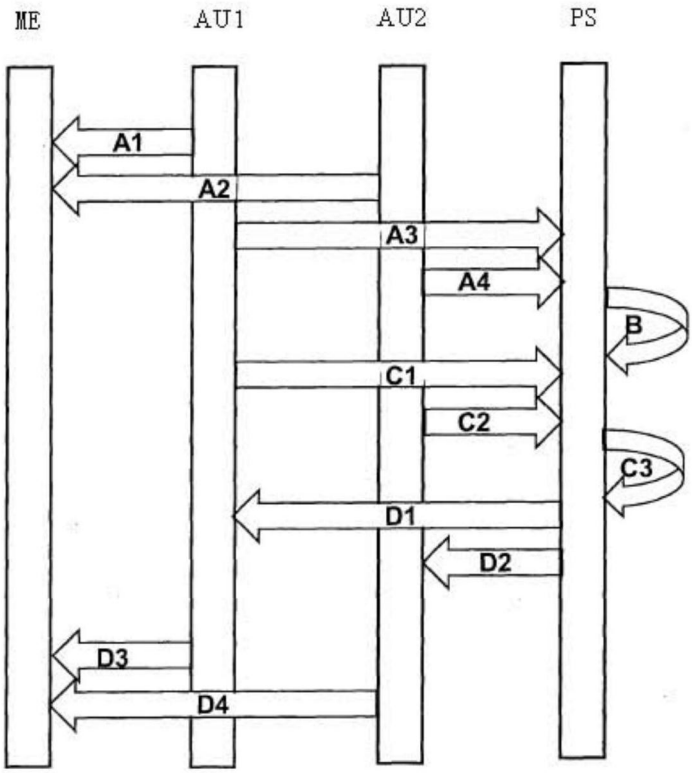

ME
AU1
AU2
PS
A1
A2
A3
A4
B
C1
C2
C3
D1
D2
D3
D4

图5

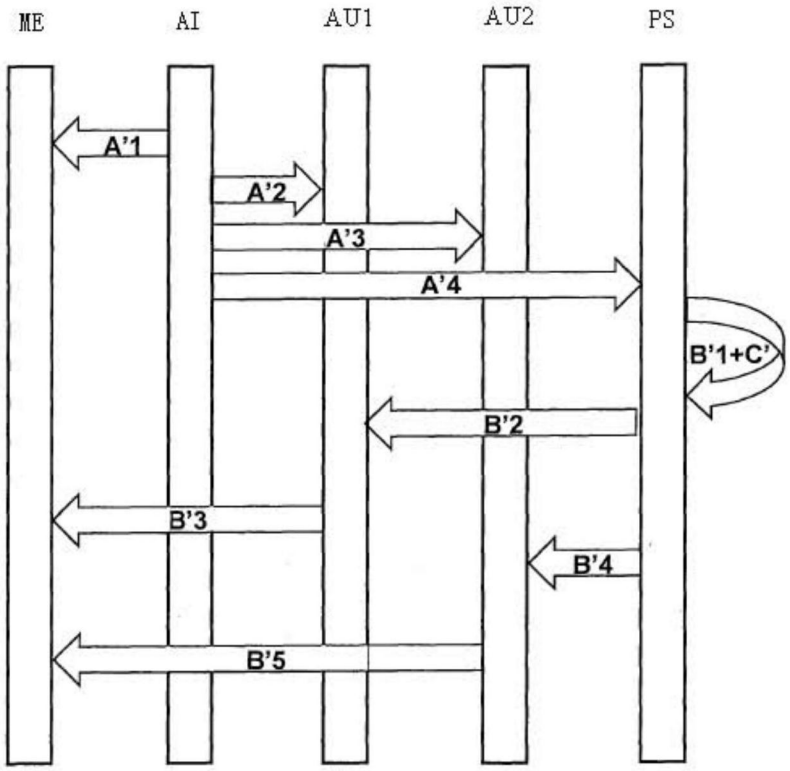



图6