

初始配置方法及终端设备

相关申请的交叉引用

本申请主张在 2019 年 12 月 3 日在中国提交的中国专利申请号 No. 201911219000.X 的优先权，其全部内容通过引用包含于此。

技术领域

本公开涉及车联网领域技术领域，特别涉及一种初始配置方法及终端设备。

背景技术

为了减小车到万物 (Vehicle-to-Everything, V2X) 技术引入给企业生产带来的影响，车联网终端的初始安全配置应尽可能地降低对企业生产安全环境及安全能力的依赖，因此需要寻求更为简洁、有效的 V2X 终端身份认证及信息安全交互的方法，最大限度地降低企业生产线升级改造的成本。

5GAA 提出的基于通用引导架构 (Generic Bootstrapping Architecture, GBA) 的在线初始安全配置方案，避免了产线离线灌装及 X.509 数字证书预配置的生产方式，能够节约企业生产环境安全改造的成本。但是，所提出的方案存在共享会话密钥 (K_s_NAF) 在安全环境之外传输暴露的问题，面临着物理攻击等安全风险。

发明内容

本公开实施例提供一种初始配置方法及终端设备，以解决相关技术中的会话密钥需要在终端设备的 USIM 与 HSM 之间传输，使得会话密钥在安全环境之外传输，存在易被物理攻击等安全风险，无法保证初始配置的安全性的问题。

为了解决上述技术问题，本公开实施例提供一种初始配置方法，应用于终端设备，包括：

安全模块建立与证书授权 CA 服务器之间建立的安全通道；

通过所述安全通道获取会话密钥，并从 CA 服务器获取数字证书；

其中，所述安全模块用于实现全球用户识别模块 USIM 的功能。

可选地，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，所述从 CA 服务器获取数字证书，包括：

安全模块生成进行 EC 申请的密码公私钥对；

利用所述密码公私钥对，从 ECA 服务器获取 EC。

可选地，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，所述从 CA 服务器获取数字证书之后，还包括：

存储 EC。

进一步地，在所述 CA 服务器为匿名证书权威机构 PCA 服务器时，所述数字证书为匿名证书 PC，所述从 CA 服务器获取数字证书，包括：

安全模块使用注册证书 EC 对应的私钥对 PC 申请消息进行签名；

根据 PC 申请消息，从 PCA 服务器获取 PC。

具体地，所述从 PCA 服务器获取 PC，包括：

接收 PCA 服务器发送的反馈消息，并利用 PCA 服务器的公钥对接收的所述反馈消息进行验签，获取 PC。

具体地，在所述从 PCA 服务器获取 PC 之后，还包括：

安全模块使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名；

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

可选地，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，在所述从 CA 服务器获取数字证书之后，还包括：

发送 EC 给硬件安全模块 HSM；

HSM 进行 EC 的存储。

进一步地，所述从 CA 服务器获取数字证书，还包括：

HSM 生成进行 EC 申请的密码公私钥对；

HSM 将进行 EC 申请的密码公钥发送给安全模块；

安全模块利用所述密码公钥，从 ECA 服务器获取 EC。

可选地，在所述 CA 服务器为匿名证书权威机构 PCA 服务器时，所述数字证书为匿名证书 PC，所述从 CA 服务器获取数字证书，包括：

发送 PC 给硬件安全模块 HSM;

HSM 进行 PC 的存储。

进一步地, 所述从 CA 服务器获取数字证书, 包括:

HSM 生成进行 PC 申请的密码公私钥对;

HSM 将进行 PC 申请的密码公钥发送给安全模块;

安全模块利用所述密码公钥, 从 PCA 服务器获取 PC。

进一步地, 所述从 CA 服务器获取数字证书之后, 还包括:

安全模块使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名;

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

具体地, 所述安全模块与 CA 服务器之间采用基于通用集成电路卡 UICC 的通用引导架构 GBA 的方式建立 GBA 安全通道。

本公开实施例还提供一种终端设备, 包括:

安全模块, 用于建立与证书授权 CA 服务器之间建立的安全通道;

通过所述安全通道获取会话密钥, 并从 CA 服务器获取数字证书;

其中, 所述安全模块用于实现全球用户识别模块 USIM 的功能。

本公开实施例还提供一种终端设备, 包括收发机和处理器;

所述处理器, 用于:

控制安全模块建立与证书授权 CA 服务器之间建立的安全通道;

通过所述安全通道获取会话密钥, 并从 CA 服务器获取数字证书;

其中, 所述安全模块用于实现全球用户识别模块 USIM 的功能。

本公开实施例还提供一种计算机可读存储介质, 其上存储有计算机程序, 该程序被处理器执行时实现上述的初始配置方法中的步骤。

本公开的有益效果是:

上述方案, 通过直接在能够实现 USIM 的功能的安全模块与 CA 服务器之间建立安全通道, 并通过所述安全通道从 CA 服务器获取会话密钥和数字证书, 使得用于数字证书申请的会话密钥不会在除安全通道之外的环境传输, 降低了会话密钥被物理攻击的机率, 降低了安全风险, 提高了初始配置的安全性。

附图说明

- 图 1 表示生产线离线灌装的自主方式示意图；
图 2 表示生产线离线灌装的 DCM 代理方式示意图；
图 3 表示 GBA 示意图；
图 4 表示基于 TLS 的 PC 证书申请的架构图；
图 5 表示相关技术中 GBA 终端实现中的安全风险示意图；
图 6 表示 5GAA 基于 GBA 的配置方案应用于 PC 证书申请时的安全风险示意图；
图 7 表示本公开实施例的初始配置方法的流程示意图；
图 8 表示本公开实施例的 EC 申请的 GBA 安全实现架构示意图；
图 9 表示本公开实施例的 PC 申请的 GBA 安全实现架构示意图；
图 10 表示本公开实施例的 USIM 架构示意图；
图 11 表示本公开实施例终端设备的模块示意图。

具体实施方式

下面首先对与本公开实施例相关的相关技术进行简单介绍如下。

目前，生产线离线灌装是实现 V2X 终端设备(包括 OBU、路侧单元(Road Side Unit, RSU)等)初始安全配置的一种主要方法，能够对设备上的 HSM 进行初始化配置。这里以具有 V2X 功能的汽车生产下线前 OBU 设备的初始配置过程为例进行介绍，其他类型的 V2X 终端也有类似的处理过程。

根据实现方法的不同，生产线离线灌装有自主方式和设备配置管理(Device Configuration Manager, DCM)代理方式两种，其过程分别如图 1 和图 2 所示。

在自主方式中，产线工人通过外部设备触发 OBU 设备的 HSM 安全模块产生密码公私钥对，或者由外部密码设备生成密码公私钥对后，将其注入 HSM 中。同时，产线将注册证书权威机构(Enrollment Certificate Authority, ECA)服务器的地址信息及数字证书也一并注入。然后，产线工人触发 OBU 设备接入 ECA 服务器，OBU 设备使用 ECA 服务器的数字证书证明其身份的

合法性，并在两者之间建立起安全的通信通道。最后，在安全通道的保护下，OBU设备向ECA服务器上传密码公钥，申请并下载登记注册证书(Enrollment Certificate, EC)数字证书，将其在HSM中安全存储。

DCM代理方式的工作原理与自主方式基本相同，实现流程有所差异。在DCM代理方式中，产线需要部署DCM代理节点，并且事先与ECA服务器进行相互认证，建立起安全通信通道，为所有即将下线的车辆提供统一服务。初始安全配置过程中，DCM为OBU设备生成密码公私钥对并代替OBU终端设备与ECA服务器交互，申请、下载EC数字证书。最后，DCM将生成的密码公私钥对、获取的EC数字证书、ECA服务器的证书及ECA服务器地址信息以安全的方式注入OBU的HSM中，从而完成OBU设备的初始安全配置。

5GAA在“Efficient Provisioning System Simplifications”研究报告中提出了一种基于GBA技术的V2X终端设备初始安全配置方法。该方案以USIM及其码号(如，国际移动用户识别码(International Mobile Subscriber Identification Number, IMSI)，移动台国际用户号码(Mobile Station International Subscriber Directory Number, MSISDN)，集成电路卡识别码(Integrate circuit card identity, ICCID)等)作为初始时刻V2X终端设备的标识，表征设备身份。基于USIM，V2X终端设备能够接入运营商网络，通过认证与密钥协商(Authentication and Key Agreement, AKA)机制与网络进行双向认证和密钥协商，为应用生成并提供共享的会话密钥Ks_NAF，最终能够在V2X设备和ECA服务器之间建立起安全的传输通道，如TLS安全通道。

图3给出了GBA通用引导架构，该架构由如下部分组成：

A11、V2X终端设备上提供GBA能力支持的软件——GAA服务器(GAA Server)；

A12、V2X终端上的V2X客户端软件，它与GAA Server软件接口；

A13、与GAA Server软件通信的USIM；

A14、ECA服务器中的网络应用功能(Network Application Function, NAF)软件；

A15、引导服务功能(Bootstrapping Server Function, BSF)核心网元。

基于网络 GBA 的安全认证方法，V2X 终端设备可以利用 USIM 卡中的根密钥通过 AKA 机制与移动蜂窝网络进行双向身份认证，与 BSF 协商生成共享的会话密钥 Ks_NAF 。随后，在接收到 V2X 终端设备的证书申请请求时，ECA 服务器可与 BSF 交互获取会话密钥 Ks_NAF ，并且基于 Ks_NAF 验证 V2X 终端设备的身份。身份认证通过后，ECA 受理 V2X 终端设备的 EC 证书申请请求，并且在审核通过后为 V2X 终端设备颁发 EC 数字证书。上述过程中，ECA 服务器与 V2X 终端设备的应用层信息交互是在基于共享会话密钥 Ks_NAF 建立的安全通道中进行的，因此消息传输的安全性也能够得到保证。

上述基于 GBA 的解决方案以 USIM 作为 V2X 终端设备的初始身份标识，无需预配置任何安全凭据（如 X.509 数字证书），就可通过移动蜂窝网络，建立起 V2X 终端设备至 ECA 服务器的安全通道，在线完成设备的初始配置。此方案中，初始安全配置相关操作及交互由 V2X 终端设备自行完成，无需像离线灌装方式那样依靠生产线的安全环境来保证配置操作的安全性，因此大大降低了企业生产线升级改造的成本。

除此之外，该方法能够适用于汽车生产地与汽车销售地不在同一个地区的场景。通过网络侧配置，它允许车载 OBU 终端与汽车销售、使用地的 ECA 对接，解决了在汽车生产过程中为车载 OBU 终端预先配置何地 ECA 服务器的 X.509 数字证书的问题。

在身份认证及安全通道建立的过程中，USIM 中的码号可作为 V2X 设备的唯一标识，避免了初始状态下 V2X 终端设备表示未经认证，仅基于 ECA 服务器 X.509 数字证书无法认证 V2X 终端设备的情况。

在中国智能交通产业联盟目前正在讨论的《基于车路协同的通信（匿名）证书管理技术规范》中，提出了一种 V2X 终端设备（包括 OBU、RSU 等）申请获取匿名证书的方法。该方法总体思路是建议采用传输层安全（Transport Layer Security, TLS）的方式在匿名证书权威机构（Pseudonym Certificate Authority, PCA）服务器与 V2X 终端设备之间进行身份认证并建立 TLS 安全通信通道，之后 V2X 终端设备通过 TLS 安全通道与 PCA 服务器交互申请 PC 数字证书。规范草案稿中，与匿名证书申请相关的章节描述如下。

本规范适用的场景为车载单元（OBU）或路侧单元（RSU）在持有 ECA

颁发的有效注册证书的情况下，利用其向 ACA 申请通信（匿名）证书，以便与 RSU 或 OBU 进行信息交互，从而获取相关信息服务并具备对所获取的信息进行签名验证的能力。此外，本规范同样适用于 OBU 向 ACA 申请通信（匿名）证书并与其他 OBU 进行通信的场景。

本规范中的程序编程接口（API）采用超文本传输安全协议（HTTPS），建议使用不低于传输层安全协议（TLS）1.2 版本，推荐使用传输层安全协议（TLS）1.3 版本，支持标准 HTTPS 传输控制协议（TCP）443 端口，并在各组件间使用 X.509 证书进行身份认证。

这里，授权证书权威机构（Authorization Certificate Authority, ACA）是指对通信（匿名）证书进行管理的机构，即本文所指的 PCA。

为了确保 PC 申请获取过程的安全性，TLS 方案在 V2X 终端上可采用图 4 所示方案实现。在 HSM 中给 V2X 终端设备预置 X.509 设备证书，在 HSM 与 PCA 服务器间建立 TLS 安全通道确保通信安全。PC 证书相关密码公私钥对在 HSM 安全环境内部产生，通过 TLS 安全通道上报公钥及设备信息，申请、下载 PC 数字证书，并安全存储。整个方案在安全环境中进行，可以确保整个过程的安全性。

5GAA 在“Efficient Provisioning System Simplifications”研究报告中提出了一种基于通用引导架构（Generic Bootstrapping Architecture, GBA）技术的 V2X 终端设备初始安全配置方法。如果将该方案用于 PC 证书的申请，则能够避免预配置 X.509 证书，降低企业生产线改造成本。

相关技术的缺点：

由于 V2X 终端设备安全初始化过程涉及密钥，数字证书等敏感参数及信息的初次配置，因此该过程对安全有着非常严格的要求，因此需要确保生产环境、终端设备、消息交互等各个环节的安全性。

1.1 生产线离线灌装

生产线离线灌装的初始安全配置方法需要在 V2X 终端设备外部生成密码公私钥对，甚至代理申请 EC 数字证书，这对车厂或 V2X 终端供货商（取决于初始安全配置工作由谁完成）的生产环境带来了很高的安全要求。企业不得不投入大量的时间、成本对生产线进行升级改造，对产线工人进行安全培

训，以满足在合规、审计、管控等多方面的安全生产要求。

目前，有实力的国外大品牌车企已部署了安全的生产环境，通过离线灌装的方式进行生产。然而，大多数中国自主品牌车企不具备这样的安全生产环境。如果要求他们同样采用离线灌装的方式生产，这将给企业带来很大的成本开销，因此需要寻求更加简便、安全的解决方案。

1.2 基于 GBA 技术在线配置 EC 证书

5GAA 目前提出的方案在 V2X 终端设备侧的实现方法存在安全漏洞，存在着对共享会话密钥 Ks_NAF 物理攻击的安全风险，具体原因如下：

为了保证 V2X 终端设备初始安全配置过程的安全性，通常要求该过程涉及到的敏感安全参数及信息（如密码公私钥对，共享密钥，各种中间密钥等）在设备本地的安全环境中处理，在其生命周期内不能离开终端本地的安全环境。终端本地安全环境通常由经过评测，达到一定安全等级的硬件模块提供，如 USIM，硬件安全模块（Hardware Security Module, HSM）等。此外，为了实现 V2X 终端设备对外通信的安全，还需要保证消息传输的安全性。对应于 V2X 终端设备的初始安全配置过程，则要求在 V2X 终端设备与 ECA 服务器之间通过安全的通信通道通信，且在终端侧安全通道应终止于设备本地的安全模块之中，以确保所有信息是在安全环境中交互的。

在 5GAA 报告中提出的实现方案中，HSM 是 V2X 终端设备初始安全配置的对象。用于申请 EC 证书的密码公私钥对由 HSM 生成，HSM 与 ECA 服务器之间利用 USIM 基于 GBA 技术生成的共享会话密钥 Ks_NAF 来建立 TLS 安全通道。然而，由于 V2X 终端设备架构的限制，USIM 是处于 HSM 之外，独立的安全实体，因此 USIM 需要将 GBA 机制生成的共享会话密钥 Ks_NAF 经过安全环境之外的传输通道传递给 HSM。这就使共享会话密钥 Ks_NAF 暴露在安全环境之外，尤其是经过应用处理器（Application Processor, AP），使其面临着物理攻击等安全风险。一旦用于建立安全通道的共享会话密钥 Ks_NAF 在传递过程中被泄露，V2X 终端设备与 ECA 服务器间消息交互的安全性就无法保证。

受制于上述安全风险，企业在选择技术方案时需要对此风险进行安全评估，只有在该风险可控制的情况下，才可使用 GBA 初始安全配置方案，这极

大地限制了该方案的应用范围。

除此之外，5GAA 提出的 GBA 方案在终端实现时，HSM 负责密码公私钥对的生成，TLS 安全通道的建立，EC 证书的申请、下载与存储，USIM 负责 GBA 技术基础上相关会话密钥的生成。终端实现成本较高。这就要求终端必须同时支持 USIM 及 HSM 两个安全模块，HSM 安全硬件价格贵，终端实现成本高。

针对上述不足，一种较为直接的解决方案是考虑将 USIM 与 HSM 集成封装在同一个物理模块或芯片中，避免密钥传输时的暴露，提高安全性。然而，目前不具有这样的终端芯片或模组产品，现阶段无法在 V2X 终端设备上实现。

1.3 基于 TLS 的 PC 证书部署方案

《基于车路协同的通信（匿名）证书管理技术规范》提出采用 TLS 方式来给 V2X 终端设备申请匿名数字证书，并要求使用 X.509 证书建立 V2X 终端设备至 PCA 服务器的安全通道。这意味着车企或 V2X 终端设备供货商需要为 V2X 终端设备预置 X.509 数字证书，这给生产线带来了升级改造的要求。同时，由于预置 X.509 数字证书涉及到密钥等敏感安全信息的配置，该过程对安全生产环境有着较为严格的要求，这将给企业带来较大的生产线升级改造成本。

1.4 基于 GBA 技术在线部署 PC 证书

5GAA 在“Efficient Provisioning System Simplifications”研究报告中提出的基于 GBA 的初始配置方法主要用于 EC 证书的初始配置。该方法主要用于完成 EC 证书的初始配置，并不针对 PC 证书的初始申请而设计。如果将其用于 PC 证书申请，在终端上会存在物理攻击等潜在安全风险。与图 5 所示问题类似，这样做将使共享会话密钥 Ks_NAF 在传递过程中暴露在安全环境之外，存在着 Ks_NAF 被篡改、泄露的安全风险，如图 6 所示。

本公开针对相关技术中的会话密钥需要在终端设备的 USIM 与 HSM 之间传输，使得会话密钥在安全环境之外传输暴露，存在易被物理攻击等安全风险的问题，提供一种初始配置方法及终端设备。

为使本公开的目的、技术方案和优点更加清楚，下面将结合附图及具体

实施例对本公开进行详细描述。

如图 7 所示，本公开实施例的初始配置方法，应用于终端设备，包括：

安全模块建立与证书授权 CA 服务器之间建立的安全通道；

通过所述安全通道获取会话密钥，并从 CA 服务器获取数字证书。

需要说明的是，本公开实施例中的安全模块用于实现全球用户识别模块（USIM）的功能，也就是说，当安全模块只实现 USIM 的功能时，该安全模块就为 USIM。可选地，在安全模块还用于实现 USIM 的功能和硬件安全模块（HSM）的功能时，表明在终端设备中将 USIM 和 HSM 集成在了一起，也可以理解为终端设备中具有能够实现 USIM 功能的 HSM。

需要说明的是，此种方式是直接在能够实现 USIM 的功能的安全模块与 CA 服务器之间建立的安全通道，在进行数字证书申请时，直接在 USIM 中用会话密钥进行申请消息的加密与保护，无需 USIM 将会话密钥发送给 HSM，使得会话密钥无需暴露在安全环境之外，降低了会话密钥被物理攻击的机率。

需要说明的是，本公开实施例所说的终端设备为基于 GBA 技术的 V2X 终端设备，可以为 OBU、RSU、行人可穿戴设备等其他类型的 V2X 终端设备、物联网终端设备等；能够解决 GBA 协商生成的共享会话密钥（Ks_NAF）在终端本地安全环境之外传输的问题，消除物理攻击等安全风险。

需要说明的是，该实施例既可以用于进行注册证书（EC）的申请，也可以进行匿名证书（PC）的申请，当数字证书为 EC 时，CA 服务器为注册证书权威机构（ECA）服务器；当所述数字证书为 PC 时，CA 服务器为匿名证书权威机构（PCA）服务器。

下面分别从申请 EC 和 PC 的角度，对两种证书的申请的具体实现过程进行说明如下，下面均以安全模块为 USIM 为例进行说明。

一、进行 EC 申请

如图 8 所示，为 GBA 安全实现方法的架构图，其中，V2X 终端设备包括：应用处理器、与应用处理器连接的 LTE-V2X 通信模组，与应用处理器连接的 LTE-Uu 通信模组，该 LTE-Uu 通信模组包括：Modem 和 USIM，具体地，USIM 与 ECA 服务器之间建立安全通道，通过该安全通道 USIM 从 ECA 服务器获取 EC。这里需要说明的是，在此种情况下，HSM 可以存在也可以

不存在。通常情况下，为了降低终端设备的生成成本，可以省略 HSM。

具体地，在从 ECA 服务器获取 EC 之前，USIM 还需要生成进行 EC 申请的密码公私钥对，以利用该密码公私钥对，从 ECA 服务器获取 EC；在获取到 EC 之后，USIM 还用于将所述 EC 进行存储。

具体地，所述 USIM 与 ECA 服务器之间采用基于通用集成电路卡 UICC 的通用引导架构 GBA(GBA_U)的方式建立 GBA 安全通道；需要说明的是，GBA_U 方案能够使共享会话密钥 Ks_NAF 或衍生出的下一级密钥完全由 USIM 生成、存储、使用，确保 V2X 终端设备与 ECA 服务器间的安全通道在终端侧终止于 USIM 内部，这就消除了相关技术中方法需要将共享会话密钥 Ks_NAF 或衍生出的下一级密钥通过不安全环境传输至 HSM 而带来的物理攻击等安全风险。

还需要说明的是，终端设备还可以实现直连通信业务的发送，具体为 USIM 使用 EC 对应的私钥对 PC5 接口直连通信业务消息进行签名；将签名后的 PC5 接口直连通信业务消息发送给外部设备。

也就是说，此种情况下，将 USIM 作为本地安全模块负责实现 V2X 终端设备的初始安全配置，会话密钥和密码公私钥的生成、存储、使用，EC 的申请、存储、使用全部由 USIM 安全模块来处理。USIM 是安全等级达到 EAL 4+ 的多功能安全实体，具有随机数产生、密码算法运算、安全存储等功能，因此具备安全实现 V2X 终端设备初始安全配置的能力。

在此方案中，V2X 终端设备触发 USIM 产生申请 EC 所用的密码公私钥对。之后，V2X 终端设备调用所支持的 GBA 安全认证能力，通过移动蜂窝网络接入 ECA 服务器并且协商生成共享的会话密钥 Ks_NAF ，在 V2X 终端设备与 ECA 服务器之间建立初始安全信任关系。ECA 服务器根据共享的会话密钥 Ks_NAF 验证 V2X 终端设备身份是否合法有效。验证通过之后，ECA 服务器与 V2X 终端设备建立安全的传输通道，用于确保两者间数据交互的安全。安全通道可以使用会话密钥 Ks_NAF 建立，也可以使用以 Ks_NAF 为基础衍生出的下一级会话密钥来建立。衍生密钥的计算在 USIM 安全环境中进行。

综上可知，在此种情况下，终端设备的 USIM 主要的职责包括：

B11、与 ECA 服务器建立 GBA 安全通道，优先采用 GBA_U 方式；

B12、生成密码公私钥对，用于申请 EC；

B13、通过 GBA 安全通信通道与 ECA 服务器交互，申请并下载 EC 数字证书以及 ECA 服务器的证书；

B14、本地安全存储 EC 及相关密码公私钥对。

二、进行 PC 申请

需要说明的是，在此种情况下，V2X 终端设备包括：应用处理器、与应用处理器连接的 LTE-V2X 通信模组，与应用处理器连接的 LTE-Uu 通信模组，该 LTE-Uu 通信模组包括：Modem 和 USIM，具体地，USIM 与 PCA 服务器之间建立安全通道，通过该安全通道 USIM 从 PCA 服务器获取 PC。这里需要说明的是，在此种情况下，HSM 可以存在也可以不存在。通常情况下，为了降低终端设备的生成成本，可以省略 HSM。

具体地，在从 PCA 服务器获取 PC 之前，USIM 还需要生成进行 PC 申请的密码公私钥对，以利用该密码公私钥对，从 PCA 服务器获取 PC；在获取到 PC 之后，USIM 还用于将所述 PC 进行存储。

需要说明的是，因 EC 的作用在于证明 V2X 终端设备身份的合法性，对 PC 申请消息进行签名保护，以申请 PC 证书，具体地，USIM 使用 EC 对应的私钥对 PC 申请消息进行签名，然后 USIM 根据 PC 申请消息，从 PCA 服务器获取 PC，也就是说，PC 的申请需要基于 EC 进行，也就是说，在进行 PC 申请之前，终端设备已经申请得到了 EC。即在安全获取 EC 之后，V2X 终端设备与 PCA 服务器交互，进一步申请 PC 数字证书。在此过程中，V2X 终端设备应对发送的 PC 申请请求消息签名，对接收到的 PC 证书申请响应消息验签，以确保该消息真实性及完整性。根据相关技术中的协议的要求，PC 证书请求消息应使用 EC 证书对应的私钥来签名。为了确保 EC 证书对应私钥使用的安全性，本公开实施例中提出由 USIM 完成 PC 证书申请请求消息的签名保护，以消除 EC 证书私钥在 USIM 与 HSM 之间进行传输所带来的物理攻击等潜在安全风险。为了安全以及简便，PC 证书申请响应消息的验签也可以由 USIM 负责实现。

USIM 具有每秒执行几十至上百次签名/验签处理的能力，而 PC 数字证书申请消息的处理没有很强的实时性要求，因此采用 USIM 进行上述处理完

全能够满足 PC 证书申请在性能方面的要求。

V2X 终端设备在完成初始安全配置，获取 EC 数字证书之后，需要使用 EC 数字证书进一步申请 PC 数字证书来对 PC5 接口直连通信业务消息进行安全保护。

根据相关技术中的协议，V2X 设备向 PCA 服务器申请 PC 数字证书时，需要使用 EC 证书证明身份的合法性，并使用 EC 证书对应的私钥对 PC 证书申请消息进行签名，以确保消息的真实性。

进一步地，在接收 PCA 服务器发送的反馈消息（例如，该反馈消息为证书申请响应消息）时，需要利用 PCA 服务器的公钥对接收的所述反馈消息进行验签，以获取 PC。

为了保证 PC 数字证书获取、配置过程的安全性，防范潜在的物理安全风险，应确保所有的密钥均在 V2X 终端设备本地的安全环境中处理，应避免基于 GBA 技术生成的共享会话密钥 Ks_NAF 在 USIM 与其他安全模块（如 HSM）之间传输。

为此，本公开实施例提出将 USIM 作为本地安全模块负责实现 V2X 终端设备的初始安全配置，会话密钥和密码公私钥的生成、存储、使用，PC 的申请、存储、使用全部由 USIM 安全模块来处理。USIM 是安全等级达到 EAL 4+ 的多功能安全实体，具有随机数产生、密码算法运算、安全存储等功能，因此具备安全实现 V2X 终端设备初始安全配置的能力。

在本公开实施例中，V2X 终端设备触发 USIM 产生申请 PC 所用的密码公私钥对。之后，V2X 终端设备调用所支持的 GBA 安全认证能力，通过移动蜂窝网络接入 PCA 服务器并且协商生成共享的会话密钥 Ks_NAF ，在 V2X 终端设备与 PCA 服务器之间建立初始安全信任关系。PCA 服务器根据共享的会话密钥 Ks_NAF 验证 V2X 终端设备身份是否合法有效。验证通过之后，PCA 服务器与 V2X 终端设备建立安全的传输通道，用于确保两者间数据交互的安全。安全通道可以使用会话密钥 Ks_NAF 建立，也可以使用以 Ks_NAF 为基础衍生出的下一级会话密钥来建立。衍生密钥的计算在 USIM 安全环境中进行。

本公开实施例使用 USIM 产生申请 PC 数字证书所需的密码公私钥对，

并优先使用 GBA_U 方式建立 USIM 至 PCA 服务器的安全通信通道。通过 GBA 安全通道, USIM 与 PCA 交互, 申请 PC 数字证书, 下载 PCA 服务器的证书, 并将下载的数字证书以及密码公私钥对在 USIM 本地安全存储。

V2X 终端设备与 PCA 服务器交互的 PC 证书申请消息等应使用 USIM 中存储的 EC 证书对应的私钥进行数字签名。

考虑到车联网 PC5 接口(即直通链路接口)直连通信消息发送速率较低, 约 10 条/秒, USIM 能够满足对发送消息进行实时签名的需求。因此, 本公开实施例提出使用 USIM 对 PC5 直连通信业务消息进行签名保护, 即 PC5 业务消息发送时, 首先由终端 AP(应用处理器)将 PC5 业务消息发送至 USIM, 由其使用 PC 证书对应的私钥对消息签名后, 再将该业务消息通过 LTE-V2X 通信组发送。同时, 为了减小 PC5 直连通信消息发送时延, USIM 可将获取的 PC 数字证书发送给外部模组或芯片(如, AP、HSM、LTE-V2X 通信模组), 便于它们在发送 PC5 业务消息时将 PC 证书随路发送, 实现车-车、车-路侧设施之间点到点数字证书分发。

本公开实施例可以确保 PC 申请相关的所有密钥(如 EC 证书对应的私钥, PC 证书的公私钥, GBA 协商生成的共享会话密钥 K_s_NAF 或衍生出的下一级密钥等)及密码运算均在 USIM 安全环境中处理, GBA 安全通道终止于 USIM 安全环境内部, 因此 PC 证书的申请、传输、处理、存储等过程是安全的, 避免了 5GAA 方案潜在的物理攻击等安全风险。由于 PC 数字证书是允许公开的, 因此将 PC 证书发送给外部模组或芯片进行处理不会影响方案的安全性。

综上可知, 在此种情况下, 终端设备的 USIM 主要的职责包括:

B21、与 PCA 服务器建立 GBA 安全通道, 优先采用 GBA_U 方式;

B22、生成密码公私钥对, 用于申请 PC 数字证书;

B23、通过 GBA 安全通信通道与 PCA 服务器交互, 申请并下载 PC 数字证书以及 PCA 服务器的证书。在此过程中, 使用 EC 证书对应的私钥对 PC 证书申请消息签名, 使用 PCA 服务器证书的公钥对接收到的消息验签;

B24、本地安全存储 PC 数字证书及相关密码公私钥对;

B25、使用 PC 证书对应的私钥对发送的 PC5 接口直连通信业务消息签

名;

B27、将 PC 证书发送给外部模组或芯片;

B28、对 PC 申请消息签名、验签。

需要说明的是,为了便于与相关技术中的汽车产业终端实现方案兼容,本公开实施例还提供了在 HSM 生成、存储、使用密钥的情况下,基于 GBA 技术安全申请证书的方式,以扩展本公开实施例的适用性,需要说明的是,在此种情况下,安全模块也只实现 USIM 的功能,即安全模块为 USIM。

具体为:在 USIM 从 CA 服务器获取数字证书之后,发送所述数字证书给 HSM;HSM 进行所述数字证书的存储。还需要说明的是,在进行数字证书申请前,HSM 需要先生成进行数字证书申请的密码公私钥对,并存储所述密码公私钥对;然后 HSM 将进行数字证书申请的密码公钥发送给 USIM,由 USIM 利用该密码公钥实现对数字证书的申请,从 CA 服务器获取数字证书。在此种情况下,由 HSM 实现对直连通信业务消息的发送,具体为:HSM 先使用数字证书对应的私钥对 PC5 接口直连通信业务消息进行签名;然后将签名后的 PC5 接口直连通信业务消息发送给外部设备。

下面分别从申请 EC 和 PC 的角度,对两种证书的申请的具体实现过程进行说明如下。

一、进行 PC 申请

此种情况下,使用 HSM 产生申请 PC 所需的密码公私钥对,并优先使用 GBA_U 方式建立 USIM 至 PCA 服务器的安全通信通道。在申请 PC 时,HSM 将生成的 PC 数字证书的公钥传送给 USIM,之后由 USIM 与 PCA 交互,申请 PC 数字证书,下载 PCA 服务器的证书。之后,USIM 将下载的 PC 以及 PCA 服务器证书发送给 HSM 安全存储。证书申请过程中,USIM 使用所存储的 EC 证书对应的私钥对 PC 证书申请消息等进行数字签名。

为了减小 PC5 直连通信消息发送时延,USIM/HSM 还可将获取的 PC 发送给其他外部模组或芯片(如,AP、LTE-V2X 通信模组),便于它们在发送 PC5 业务消息时将 PC 证书随路发送,实现车-车、车-路侧设施之间点到点数字证书分发。

V2X 终端设备在发送 PC5 接口直连通信业务消息时,将消息发送给 HSM

使用 PC 数字证书对应的私钥签名后在通过 LTE-V2X 通信组发送。

如图 9 所示, 此种情况下, 将 PC 的公钥从 HSM 传输至 USIM。由于公钥是允许公开的, 因此不存在公钥泄露的安全风险, 提高了安全性。

综上可知, 在此种情况下, 终端设备的 USIM 主要的职责包括:

C11、与 PCA 服务器建立 GBA 安全通道, 优先采用 GBA_U 方式;

C12、接收 HSM 发送的 PC 证书公钥, 为其申请 PC 数字证书;

C13、通过 GBA 安全通信通道与 PCA 服务器交互, 申请并下载 PC 数字证书以及 PCA 服务器的证书。在此过程中, 使用 EC 证书对应的私钥对 PC 证书申请消息签名, 使用 PCA 服务器证书的公钥对接收到的消息验签;

C14、将 PC 数字证书以及 PCA 服务器的证书发送给 HSM。

综上可知, 在此种情况下, 终端设备的 HSM 主要的职责包括:

C21、生成密码公私钥对, 用于申请 PC 数字证书;

C22、将生成的密码公钥发送给 USIM, 用于申请 PC 数字证书;

C23、本地安全存储接收到的 PC 数字证书及相关密码公私钥对;

C24、使用 PC 证书对应的私钥对发送的 PC5 接口直连通信业务消息签名。

二、进行 EC 申请

此种情况下, 使用 HSM 产生申请 EC 所需的密码公私钥对, 并优先使用 GBA_U 方式建立 USIM 至 ECA 服务器的安全通信通道。在申请 EC 时, HSM 将生成的 EC 数字证书的公钥传送给 USIM, 之后由 USIM 与 ECA 交互, 申请 EC 数字证书, 下载 ECA 服务器的证书。之后, USIM 将下载的 EC 以及 ECA 服务器证书发送给 HSM 安全存储。

为了减小 PC5 直连通信消息发送时延, USIM/HSM 还可将获取的 EC 发送给其他外部模组或芯片 (如, AP、LTE-V2X 通信模组), 便于它们在发送 PC5 业务消息时将 EC 随路发送, 实现车-车、车-路侧设施之间点到点数字证书分发。

V2X 终端设备在发送 PC5 接口直连通信业务消息时, 将消息发送给 HSM 使用 EC 数字证书对应的私钥签名后在通过 LTE-V2X 通信组发送。

此种情况下, 将 EC 的公钥从 HSM 传输至 USIM, 由于公钥是允许公开

的，因此不存在公钥泄露的安全风险，提高了安全性。

综上可知，在此种情况下，终端设备的 USIM 主要的职责包括：

D11、与 ECA 服务器建立 GBA 安全通道，优先采用 GBA_U 方式；

D12、接收 HSM 发送的 EC 的公钥，为其申请 EC；

D13、通过 GBA 安全通信通道与 ECA 服务器交互，申请并下载 EC 以及 PCA 服务器的证书；

D14、将 EC 以及 ECA 服务器的证书发送给 HSM。

综上可知，在此种情况下，终端设备的 HSM 主要的职责包括：

D21、生成密码公私钥对，用于申请 EC；

D22、将生成的密码公钥发送给 USIM，用于申请 EC；

D23、本地安全存储接收到的 EC 及相关密码公私钥对；

D24、使用 EC 对应的私钥对发送的 PC5 接口直连通信业务消息签名。

综上可知，V2X 终端设备初始安全配置需要完成如下操作：

1、生成密码公私钥对，准备申请 EC/PC；

2、建立至 ECA 服务器/PCA 服务器的安全通道，用所生成的公钥向 ECA 服务器/PCA 服务器申请 EC/PC；

3、下载 ECA 服务器/PCA 服务器颁发的 EC/PC 以及 ECA 服务器/PCA 服务器的数字证书；

4、将密码公私钥对、数字证书等在本地安全存储，使用。

为了满足上述证书申请的需求，USIM 需新增证书应用功能模块及相关接口，其架构如图 10 所示，其中：

接口 IF1 和 USIM 应用功能用于实现 GBA 流程；

接口 IF2、IF3 和证书应用功能用于完成 EC/PC 证书的申请，PC5 消息签名处理。

USIM 卡内的交互流程如下：

数字证书申请（高安全性）：

1. 证书应用模块生成公私钥对，构造证书请求消息，并通过 IF3 向 USIM 应用模块请求使用 GBA 生成的 Ks_NAF 或衍生出的下一级密钥对证书请求做加密保护；

2. 证书请求加密完成后，证书应用模块通过 IF2 将保护后的证书请求通过 AP 发送给 ECA/PCA 服务器，申请 EC/PC 数字证书；

3. ECA/PCA 服务器签发的数字证书及 ECA/PCA 服务器的证书通过 IF2 发送给证书应用模块，证书应用模块调用 IF3 接口请求 USIM 应用模块使用 Ks_NAF 或衍生出的下一级密钥对消息进行解密和验证；

4. 如果验证通过，证书应用模块将解密后的 EC/PC 证书及 ECA/PCA 服务器的证书安全存储，并反馈处理结果。

PC 数字证书申请（高兼容性）：

1. 证书应用模块通过 IF2 接收外部 HSM 生成的 PC 证书密码公钥；

2. 证书应用模块构造证书请求消息，并通过 IF3 向 USIM 应用模块请求使用 GBA 生成的 Ks_NAF 或衍生出的下一级密钥对证书请求做加密保护；

3. 证书请求加密完成后，证书应用模块通过 IF2 将保护后的证书请求通过 AP 发送给 PCA 服务器，申请 PC 数字证书；

4. PCA 服务器签发的数字证书及 PCA 服务器的证书通过 IF2 发送给证书应用模块，证书应用模块调用 IF3 接口请求 USIM 应用模块使用 Ks_NAF 或衍生出的下一级密钥对消息进行解密和验证；

5. 如果验证通过，证书应用模块将解密后的 PC 证书及 PCA 服务器的证书发送给 HSM 安全存储。

需要说明的是，本公开实施例具有如下优点：

1、本公开消除了基于 GBA 的 V2X 终端设备初始安全配置过程中存在的物理攻击等安全风险，确保了整个初始安全配置流程的安全性；

2、本公开最大限度地发挥了 V2X 终端设备上 USIM 安全模块的能力，可以使终端无需使用 HSM 硬件模块，在提升全系统安全性的同时，降低了终端实现的成本；

3、本公开能够与汽车行业普遍采用 HSM 来生成、管理密钥的相关技术方案兼容，具有较好的兼容性；

4、本公开为保证 V2X 终端 PC5 接口直连通信的安全奠定了基础。

如图 11 所示，本公开实施例的终端设备，包括：

安全模块 111，用于建立与证书授权 CA 服务器之间建立的安全通道；

通过所述安全通道获取会话密钥，并从 CA 服务器获取数字证书；

其中，所述安全模块用于实现全球用户识别模块 USIM 的功能。

可选地，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，所述安全模块 111 从 CA 服务器获取数字证书，用于实现：

生成进行 EC 申请的密码公私钥对；

利用所述密码公私钥对，从 ECA 服务器获取 EC。

可选地，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，所述安全模块 111 从 CA 服务器获取数字证书之后，还用于实现：

存储 EC。

进一步地，在所述 CA 服务器为匿名证书权威机构 PCA 服务器时，所述数字证书为匿名证书 PC，所述安全模块 111 从 CA 服务器获取数字证书，用于实现：

使用注册证书 EC 对应的私钥对 PC 申请消息进行签名；

根据 PC 申请消息，从 PCA 服务器获取 PC。

具体地，所述安全模块 111 从 PCA 服务器获取 PC，用于实现：

接收 PCA 服务器发送的反馈消息，并利用 PCA 服务器的公钥对接收的所述反馈消息进行验签，获取 PC。

进一步地，在所述安全模块 111 从 PCA 服务器获取 PC 之后，还用于实现：

使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名；

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

可选地，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，在所述安全模块 111 从 CA 服务器获取数字证书之后，还用于实现：

发送 EC 给硬件安全模块 HSM；

HSM，用于进行 EC 的存储。

进一步地，HSM 还用于实现：

生成进行 EC 申请的密码公私钥对;

将进行 EC 申请的密码公钥发送给安全模块;

安全模块 111, 还用于利用所述密码公钥, 从 ECA 服务器获取 EC。

进一步地, 在所述 CA 服务器为匿名证书权威机构 PCA 服务器时, 所述数字证书为匿名证书 PC, 所述安全模块 111 从 CA 服务器获取数字证书, 用于实现:

发送 PC 给硬件安全模块 HSM;

HSM, 用于进行 PC 的存储。

具体地, 所述 HSM 还用于实现: 生成进行 PC 申请的密码公私钥对;

HSM 将进行 PC 申请的密码公钥发送给安全模块;

安全模块 111, 还用于利用所述密码公钥, 从 PCA 服务器获取 PC。

进一步地, 所述安全模块 111 从 CA 服务器获取数字证书之后, 还用于实现:

使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名;

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

具体地, 所述安全模块与 CA 服务器之间采用基于通用集成电路卡 UICC 的通用引导架构 GBA 的方式建立 GBA 安全通道。

需要说明的是, 本公开实施例提供的终端设备是能够执行上述初始配置方法的终端设备, 则上述初始配置方法实施例中的所有实现方式均适用于该终端设备, 且均能达到相同或相似的有益效果。

本公开实施例还提供一种终端设备, 包括收发机和处理器;

所述处理器, 用于:

控制安全模块建立与证书授权 CA 服务器之间建立的安全通道;

通过所述安全通道获取会话密钥, 并从 CA 服务器获取数字证书;

其中, 所述安全模块用于实现全球用户识别模块 USIM 的功能。

可选地, 在所述 CA 服务器为注册证书权威机构 ECA 服务器时, 所述数字证书为注册证书 EC, 所述处理器执行从 CA 服务器获取数字证书时, 用于实现:

控制安全模块生成进行 EC 申请的密码公私钥对;

利用所述密码公私钥对，从ECA服务器获取EC。

可选地，在所述CA服务器为注册证书权威机构ECA服务器时，所述数字证书为注册证书EC，所述处理器执行从CA服务器获取数字证书之后，还用于实现：

存储EC。

进一步地，在所述CA服务器为匿名证书权威机构PCA服务器时，所述数字证书为匿名证书PC，所述处理器执行从CA服务器获取数字证书时，用于实现：

控制安全模块使用注册证书EC对应的私钥对PC申请消息进行签名；

根据PC申请消息，从PCA服务器获取PC。

具体地，所述处理器执行从PCA服务器获取PC，用于实现：

接收PCA服务器发送的反馈消息，并利用PCA服务器的公钥对接收的所述反馈消息进行验签，获取PC。

进一步地，在所述处理器执行从PCA服务器获取PC之后，还用于实现：

控制安全模块使用PC对应的私钥对PC5接口直连通信业务消息进行签名；

将签名后的PC5接口直连通信业务消息发送给外部设备。

可选地，在所述CA服务器为注册证书权威机构ECA服务器时，所述数字证书为注册证书EC，在所述处理器执行从CA服务器获取数字证书之后，还用于实现：

控制收发机发送EC给硬件安全模块HSM；

HSM进行EC的存储。

进一步地，所述处理器执行从CA服务器获取数字证书，还用于实现：

控制HSM生成进行EC申请的密码公私钥对；

HSM将进行EC申请的密码公钥发送给安全模块；

安全模块利用所述密码公钥，从ECA服务器获取EC。

进一步地，在所述CA服务器为匿名证书权威机构PCA服务器时，所述数字证书为匿名证书PC，所述处理器执行从CA服务器获取数字证书，用于实现：

控制收发机发送 PC 给硬件安全模块 HSM;

HSM 进行 PC 的存储。

进一步地, 所述处理器执行从 CA 服务器获取数字证书, 用于实现:

HSM 生成进行 PC 申请的密码公私钥对;

HSM 将进行 PC 申请的密码公钥发送给安全模块;

安全模块利用所述密码公钥, 从 PCA 服务器获取 PC。

进一步地, 所述处理器执行从 CA 服务器获取数字证书之后, 还用于实现:

控制安全模块使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名;

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

具体地, 所述安全模块与 CA 服务器之间采用基于通用集成电路卡 UICC 的通用引导架构 GBA 的方式建立 GBA 安全通道。

本公开实施例还提供一种终端设备, 包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序, 所述处理器执行所述程序时实现如上所述的初始配置方法实施例中的各个过程, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。

本公开实施例还提供一种计算机可读存储介质, 其上存储有计算机程序, 该程序被处理器执行时实现如上所述的初始配置方法实施例中的各个过程, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。其中, 所述的计算机可读存储介质, 如只读存储器 (Read-Only Memory, ROM)、随机存取存储器 (Random Access Memory, RAM)、磁碟或者光盘等。

本领域内的技术人员应明白, 本申请的实施例可提供为方法、系统或计算机程序产品。因此, 本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且, 本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可读存储介质 (包括但不限于磁盘存储器和光学存储器等) 上实施的计算机程序产品的形式。

本申请是参照根据本申请实施例的方法、设备 (系统) 和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和

/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其它可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其它可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其它可编程数据处理设备以特定方式工作的计算机可读存储介质中，使得存储在该计算机可读存储介质中的指令产生包括指令装置的纸制品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其它可编程数据处理设备上，使得计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

各个模块、单元、子单元或子模块可以是配置成实施以上方法的一个或多个集成电路，例如：一个或多个特定集成电路（Application Specific Integrated Circuit, ASIC），或，一个或多个微处理器（digital signal processor, DSP），或，一个或者多个现场可编程门阵列（Field Programmable Gate Array, FPGA）等。再如，当以上某个模块通过处理元件调度程序代码的形式实现时，该处理元件可以是通用处理器，例如中央处理器（Central Processing Unit, CPU）或其它可以调用程序代码的处理器。再如，这些模块可以集成在一起，以片上系统（system-on-a-chip, SOC）的形式实现。

本公开的说明书和权利要求书中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例，例如除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。此外，说明书以及权利要求中使用“和/或”表示所连接对象的至少

其中之一，例如 A 和/或 B 和/或 C，表示包含单独 A，单独 B，单独 C，以及 A 和 B 都存在，B 和 C 都存在，A 和 C 都存在，以及 A、B 和 C 都存在的 7 种情况。类似地，本说明书以及权利要求中使用“A 和 B 中的至少一个”应理解为“单独 A，单独 B，或 A 和 B 都存在”。

以上所述的是本公开的可选实施方式，应当指出对于本技术领域的普通人员来说，在不脱离本公开所述的原理前提下还可以作出若干改进和润饰，这些改进和润饰也在本公开的保护范围内。

权利要求书

1. 一种初始配置方法，应用于终端设备，包括：

安全模块建立与证书授权 CA 服务器之间建立的安全通道；

通过所述安全通道获取会话密钥，并从 CA 服务器获取数字证书；

其中，所述安全模块用于实现全球用户识别模块 USIM 的功能。

2. 根据权利要求 1 所述的初始配置方法，其中，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，所述从 CA 服务器获取数字证书，包括：

安全模块生成进行 EC 申请的密码公私钥对；

利用所述密码公私钥对，从 ECA 服务器获取 EC。

3. 根据权利要求 1 所述的初始配置方法，其中，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，所述从 CA 服务器获取数字证书之后，还包括：

存储 EC。

4. 根据权利要求 1-3 任一项所述的初始配置方法，其中，在所述 CA 服务器为匿名证书权威机构 PCA 服务器时，所述数字证书为匿名证书 PC，所述从 CA 服务器获取数字证书，包括：

安全模块使用注册证书 EC 对应的私钥对 PC 申请消息进行签名；

根据 PC 申请消息，从 PCA 服务器获取 PC。

5. 根据权利要求 4 所述的初始配置方法，其中，所述从 PCA 服务器获取 PC，包括：

接收 PCA 服务器发送的反馈消息，并利用 PCA 服务器的公钥对接收的所述反馈消息进行验签，获取 PC。

6. 根据权利要求 4 所述的初始配置方法，其中，在所述从 PCA 服务器获取 PC 之后，还包括：

安全模块使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名；

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

7. 根据权利要求 1 所述的初始配置方法，其中，在所述 CA 服务器为注

册证书权威机构 ECA 服务器时, 所述数字证书为注册证书 EC, 在所述从 CA 服务器获取数字证书之后, 还包括:

发送 EC 给硬件安全模块 HSM;

HSM 进行 EC 的存储。

8. 根据权利要求 7 所述的初始配置方法, 其中, 所述从 CA 服务器获取数字证书, 还包括:

HSM 生成进行 EC 申请的密码公私钥对;

HSM 将进行 EC 申请的密码公钥发送给安全模块;

安全模块利用所述密码公钥, 从 ECA 服务器获取 EC。

9. 根据权利要求 1、7 或 8 所述的初始配置方法, 其中, 在所述 CA 服务器为匿名证书权威机构 PCA 服务器时, 所述数字证书为匿名证书 PC, 所述从 CA 服务器获取数字证书, 包括:

发送 PC 给硬件安全模块 HSM;

HSM 进行 PC 的存储。

10. 根据权利要求 9 所述的初始配置方法, 其中, 所述从 CA 服务器获取数字证书, 包括:

HSM 生成进行 PC 申请的密码公私钥对;

HSM 将进行 PC 申请的密码公钥发送给安全模块;

安全模块利用所述密码公钥, 从 PCA 服务器获取 PC。

11. 根据权利要求 9 所述的初始配置方法, 其中, 所述从 CA 服务器获取数字证书之后, 还包括:

安全模块使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名;

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

12. 根据权利要求 1 所述的初始配置方法, 其中, 所述安全模块与 CA 服务器之间采用基于通用集成电路卡 UICC 的通用引导架构 GBA 的方式建立 GBA 安全通道。

13. 一种终端设备, 包括:

安全模块, 用于建立与证书授权 CA 服务器之间建立的安全通道;

通过所述安全通道获取会话密钥, 并从 CA 服务器获取数字证书;

其中，所述安全模块用于实现全球用户识别模块 USIM 的功能。

14. 一种终端设备，包括收发机和处理器；

所述处理器，用于：

控制安全模块建立与证书授权 CA 服务器之间建立的安全通道；

通过所述安全通道获取会话密钥，并从 CA 服务器获取数字证书；

其中，所述安全模块用于实现全球用户识别模块 USIM 的功能。

15. 一种计算机可读存储介质，其上存储有计算机程序，其中，该程序被处理器执行时实现如权利要求 1-12 任一项所述的初始配置方法中的步骤。