(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113015159 B
(45)授权公告日 2023.05.09

(21)申请号 201911218999.6

(22)申请日 2019.12.03

(65)同一申请的已公布的文献号
申请公布号 CN 113015159 A

(43)申请公布日 2021.06.22

(73)专利权人 中国移动通信有限公司研究院
地址 100053 北京市西城区宣武门西大街32号
专利权人 中国移动通信集团有限公司

(72)发明人 田野 任晓明

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
专利代理师 许静 安利霞

(51)Int.Cl.
H04W 12/041(2021.01)
H04W 12/0431(2021.01)
H04W 12/069(2021.01)
H04W 12/106(2021.01)
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04W 4/40(2018.01)

(56)对比文件
CN 101102190 A,2008.01.09
CN 101822082 A,2010.09.01
CN 102857912 A,2013.01.02
CN 103001940 A,2013.03.27
CN 103686710 A,2014.03.26
CN 104011730 A,2014.08.27
CN 108848496 A,2018.11.20
CN 109218028 A,2019.01.15
CN 1929371 A,2007.03.14
US 2008095361 A1,2008.04.24
US 2011131414 A1,2011.06.02
US 2015281958 A1,2015.10.01
US 2016044505 A1,2016.02.11
WO 2010128348 A1,2010.11.11

审查员 高凯

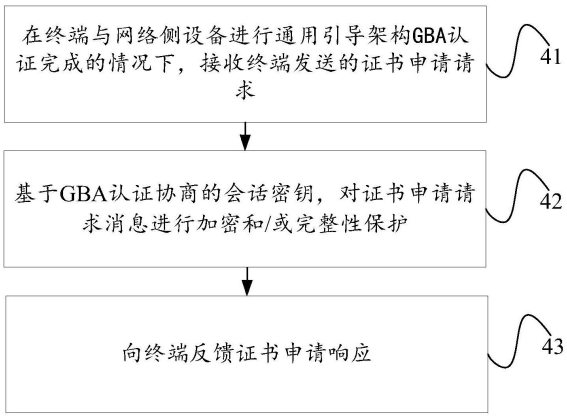
权利要求书3页 说明书16页 附图6页

(54)发明名称

初始安全配置方法、安全模块及终端

(57)摘要

本发明提供一种初始安全配置方法、安全模块及终端，涉及车联网技术领域。该初始安全配置方法，应用于安全模块，包括：在终端与网络侧设备进行GBA认证完成的情况下，接收终端发送的证书申请请求，所述证书申请请求中携带终端的标识信息；基于GBA认证协商的会话密钥，对证书申请请求消息进行加密和/或完整性保护；向终端反馈进行了加密和/或完整性保护的证书申请请求消息；其中，所述安全模块用于实现USIM的功能。上述方案，能够保证初始安全配置的信息安全，提高了消息传输的安全性。



CN 113015159 B

1.一种初始安全配置方法,应用于安全模块,其特征在于,包括:

在终端与网络侧设备进行通用引导架构GBA认证完成的情况下,接收终端发送的证书申请请求,所述证书申请请求中携带终端的标识信息;

基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护,所述会话密钥是安全模块与网络侧设备协商得到的;

向终端反馈进行了加密和/或完整性保护的证书申请请求消息;

其中,所述安全模块用于在终端内实现全球用户识别模块USIM的功能。

2.根据权利要求1所述的初始安全配置方法,其特征在于,所述基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护,包括:

若基于所述会话密钥成功生成第一密钥,根据所述第一密钥,对证书申请请求消息进行加密和/或完整性保护;或者

若基于所述会话密钥未生成第一密钥,根据所述会话密钥,对证书申请请求消息进行加密和/或完整性保护;

其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

3.根据权利要求1所述的初始安全配置方法,其特征在于,在所述向终端反馈进行了加密和/或完整性保护的证书申请请求消息之后,还包括:

接收终端发送的证书写入请求,所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书;

根据所述证书申请响应消息,存储数字证书。

4.根据权利要求3所述的初始安全配置方法,其特征在于,所述根据所述证书申请响应消息,存储数字证书,包括:

在基于GBA认证协商的会话密钥生成第一密钥时,根据所述第一密钥校验并解密证书申请响应消息;

解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储;

其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

5.根据权利要求3所述的初始安全配置方法,其特征在于,所述根据所述证书申请响应消息,存储数字证书,包括:

在基于会话密钥未生成第一密钥时,根据所述会话密钥校验并解密证书申请响应消息;

解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储;

其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

6.一种初始安全配置方法,应用于终端,其特征在于,包括:

与网络侧设备进行通用引导架构GBA认证;

在与网络侧设备进行GBA认证完成的情况下,向安全模块发送证书申请请求,使得所述安全模块基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护,所述会话密钥是安全模块与网络侧设备协商得到的,所述证书申请请求中携带终端的标识信息;

接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息;

其中,所述安全模块用于在终端内实现全球用户识别模块USIM的功能。

7.根据权利要求6所述的初始安全配置方法,其特征在于,在所述接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息之后,还包括:

向证书授权CA服务器发送证书申请消息,所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息;

接收CA服务器反馈的证书响应消息,所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书;

向所述安全模块发送证书写入请求,所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息。

8.根据权利要求6所述的初始安全配置方法,其特征在于,所述与网络侧设备进行通用引导架构GBA认证,包括:

终端的调制解调器调用安全模块与网络侧设备进行GBA认证。

9.一种安全模块,其特征在于,包括:

第一接收模块,用于在终端与网络侧设备进行通用引导架构GBA认证完成的情况下,接收终端发送的证书申请请求,所述证书申请请求中携带终端的标识信息;

第一处理模块,用于基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护,所述会话密钥是安全模块与网络侧设备协商得到的;

第一发送模块,用于向终端反馈进行了加密和/或完整性保护的证书申请请求消息;

其中,所述安全模块用于在终端内实现全球用户识别模块USIM的功能。

10.一种安全模块,其特征在于,包括收发机和处理器;

所述处理器,用于:

通过所述收发机在终端与网络侧设备进行通用引导架构GBA认证完成的情况下,接收终端发送的证书申请请求,所述证书申请请求中携带终端的标识信息;基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护,所述会话密钥是安全模块与网络侧设备协商得到的;向终端反馈进行了加密和/或完整性保护的证书申请请求消息;

其中,所述安全模块用于在终端内实现全球用户识别模块USIM的功能。

11.一种终端,其特征在于,包括:

第一认证模块,用于与网络侧设备进行通用引导架构GBA认证;

第二发送模块,用于在与网络侧设备进行GBA认证完成的情况下,向安全模块发送证书申请请求,使得所述安全模块基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护,所述会话密钥是安全模块与网络侧设备协商得到的,所述证书申请请求中携带终端的标识信息;

第三接收模块,用于接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息;

其中,所述安全模块用于在终端内实现全球用户识别模块USIM的功能。

12.一种终端,其特征在于,包括收发机和处理器;

所述处理器,用于:与网络侧设备进行通用引导架构GBA认证;

所述收发机,用于:

在与网络侧设备进行GBA认证完成的情况下,向安全模块发送证书申请请求,使得所述安全模块基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护,

所述会话密钥是安全模块与网络侧设备协商得到的,所述证书申请请求中携带终端的标识信息;

接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息;

其中,所述安全模块用于在终端内实现全球用户识别模块USIM的功能。

13.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-8任一项所述的初始安全配置方法中的步骤。

初始安全配置方法、安全模块及终端

技术领域

[0001] 本发明涉及车联网技术领域，特别涉及一种初始安全配置方法、安全模块及终端。

背景技术

[0002] 由于车到万物(V2X)终端设备初始化过程涉及终端密码公私钥对的产生以及设备登记注册证书的申请，现有初始安全配置方案对汽车厂商、V2X终端厂商有较高的安全生产要求，企业不得不投入大量的时间、资金和精力对生产线进行改造，对员工进行培训，以满足安全生产合规、安全审计、安全成本管控等多方面要求。

[0003] 目前，国外品牌的车企通常已具备在产线上安全生产的能力，能够通过生产线灌装的方式来实现车载单元(On board Unit，OBU)的初始安全配置。然而，对于大多数中国自主品牌车企而言，他们目前不具备安全的生产环境来实现密钥、证书等敏感参数的初始配置。如果同样采用产线灌装的方式，给企业带来较大的成本开销，因此需要寻求更加简便易行的安全解决方案。

[0004] 5GAA提出的基于通用引导架构(Generic Bootstrapping Architecture，GBA)的解决方案能够避免采用产线灌装的方式来实现V2X终端设备的初始安全配置，降低企业产线改造成本。然而，5GAA仅提出了一种思路，并没有给出实现初始安全配置的业务流程和方法，无法指导V2X终端设备生产实践。除此之外，该方案建立的传输层安全(Transport Layer Security，TLS)安全通道在V2X终端侧终止于硬件安全模块(Hardware Security Module，HSM)，并未终止于生成GBA会话密钥Ks_NAF的全球用户识别模块(Universal Subscriber Identity Module，USIM)上，因此存在会话密钥或数据信息泄露的安全风险。

发明内容

[0005] 本发明实施例提供一种初始安全配置方法、安全模块及终端，以解决现有的5GAA中并没有定义V2X终端设备的初始安全配置的具体方案，无法保证消息传输可靠性以及初始安全配置的信息安全的问题。

[0006] 为了解决上述技术问题，本发明实施例提供一种初始安全配置方法，应用于安全模块，包括：

[0007] 在终端与网络侧设备进行通用引导架构GBA认证完成的情况下，接收终端发送的证书申请请求，所述证书申请请求中携带终端的标识信息；

[0008] 基于GBA认证协商的会话密钥，对证书申请请求消息进行加密和/或完整性保护；

[0009] 向终端反馈进行了加密和/或完整性保护的证书申请请求消息；

[0010] 其中，所述安全模块用于实现全球用户识别模块USIM的功能。

[0011] 可选地，所述基于GBA认证协商的会话密钥，对证书申请请求消息进行加密和/或完整性保护，包括：

[0012] 若基于所述会话密钥成功生成第一密钥，根据所述第一密钥，对证书申请请求消息进行加密和/或完整性保护；或者

[0013] 若基于所述会话密钥未生成第一密钥,根据所述会话密钥,对证书申请请求消息进行加密和/或完整性保护;

[0014] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥

[0015] 可选地,在所述向终端反馈进行了加密和/或完整性保护的证书申请请求消息之后,还包括:

[0016] 接收终端发送的证书写入请求,所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书;

[0017] 根据所述证书申请响应消息,存储数字证书。

[0018] 进一步地,所述根据所述证书申请响应消息,存储数字证书,包括:

[0019] 在基于GBA认证协商的会话密钥生成第一密钥时,根据所述第一密钥校验并解密证书申请响应消息;

[0020] 解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储;

[0021] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0022] 进一步地,所述根据所述证书申请响应消息,存储数字证书,包括:

[0023] 在基于会话密钥未生成第一密钥时,根据所述会话密钥校验并解密证书申请响应消息;

[0024] 解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储;

[0025] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0026] 本发明实施例还提供一种初始安全配置方法,应用于终端,包括:

[0027] 与网络侧设备进行通用引导架构GBA认证;

[0028] 在与网络侧设备进行GBA认证完成的情况下,向安全模块发送证书申请请求,所述证书申请请求中携带终端的标识信息;

[0029] 接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息。

[0030] 可选地,在所述接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息之后,还包括:

[0031] 向证书授权CA服务器发送证书申请消息,所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息;

[0032] 接收CA服务器反馈的证书响应消息,所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书;

[0033] 向所述安全模块发送证书写入请求,所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息。

[0034] 具体地,所述与网络侧设备进行通用引导架构GBA认证,包括:

[0035] 终端的调制解调器调用安全模块与网络侧设备进行GBA认证。

[0036] 本发明实施例还提供一种安全模块,包括:

[0037] 第一接收模块,用于在终端与网络侧设备进行通用引导架构GBA认证完成的情况下,接收终端发送的证书申请请求,所述证书申请请求中携带终端的标识信息;

[0038] 第一处理模块,用于基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护;

[0039] 第一发送模块,用于向终端反馈进行了加密和/或完整性保护的证书申请请求消

息；

[0040] 其中，所述安全模块用于实现全球用户识别模块USIM的功能。

[0041] 本发明实施例还提供一种安全模块，包括收发机和处理器；

[0042] 所述处理器，用于：

[0043] 通过所述收发机在终端与网络侧设备进行通用引导架构GBA认证完成的情况下，接收终端发送的证书申请请求，所述证书申请请求中携带终端的标识信息；基于GBA认证协商的会话密钥，对证书申请请求消息进行加密和/或完整性保护；向终端反馈进行了加密和/或完整性保护的证书申请请求消息；

[0044] 其中，所述安全模块用于实现全球用户识别模块USIM的功能。

[0045] 本发明实施例还提供一种终端，包括：

[0046] 第一认证模块，用于与网络侧设备进行通用引导架构GBA认证；

[0047] 第二发送模块，用于在与网络侧设备进行GBA认证完成的情况下，向安全模块发送证书申请请求，所述证书申请请求中携带终端的标识信息；

[0048] 第三接收模块，用于接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息。

[0049] 本发明实施例还提供一种终端，包括收发机和处理器；

[0050] 所述处理器，用于：与网络侧设备进行通用引导架构GBA认证；

[0051] 所述收发机，用于：

[0052] 在与网络侧设备进行GBA认证完成的情况下，向安全模块发送证书申请请求，所述证书申请请求中携带终端的标识信息；

[0053] 接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息。

[0054] 本发明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安全配置方法中的步骤。

[0055] 本发明的有益效果是：

[0056] 上述方案，通过在进行公钥证书申请时，由能够实现USIM功能的安全模块进行证书申请请求消息的加密和/或完整性保护，能够保证初始安全配置的信息安全，提高了消息传输的安全性。

附图说明

[0057] 图1表示生产线离线灌装的自主方式示意图；

[0058] 图2表示生产线离线灌装的DCM代理方式示意图；

[0059] 图3表示GBA示意图；

[0060] 图4表示本发明实施例的初始安全配置方法的流程示意图之一；

[0061] 图5表示本发明实施例的V2X终端设备架构示意图；

[0062] 图6表示本发明实施例的V2X终端设备的初始安全配置流程示意图；

[0063] 图7表示本发明实施例的安全模块的模块示意图；

[0064] 图8表示本发明实施例的初始安全配置方法的流程示意图之二；

[0065] 图9表示本发明实施例终端的模块示意图；

[0066] 图10表示本发明实施例的初始安全配置方法的流程示意图之三；

[0067] 图11表示本发明实施例的CA服务器的模块示意图；

[0068] 图12表示本发明实施例的初始安全配置方法的流程示意图之四；

[0069] 图13表示本发明实施例的网络侧设备的模块示意图。

具体实施方式

[0070] 下面首先对与本发明实施例相关的现有技术进行简单介绍如下。

[0071] 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。

[0072] 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。

[0073] 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。

[0074] 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。

[0075] 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。

[0076] 图3给出了GBA通用引导架构，该架构由如下部分组成：

[0077] A11、V2X终端设备上提供GBA能力支持的软件——GAA服务器(GAA Server)；

[0078] A12、V2X终端上的V2X客户端软件，它与GAA Server软件接口；

[0079] A13、与GAA Server软件通信的USIM；

[0080] A14、ECA服务器中的网络应用功能(Network Application Function，NAF)软件；

[0081] A15、引导服务功能(Bootstrapping Server Function,BSF)核心网元。

[0082] 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。

[0083] 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。

[0084] 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。

[0085] 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。

[0086] 本发明针对现有的5GAA中并没有定义V2X终端设备的初始安全配置的具体方案,无法保证会话密钥或数据信息安全性的问题,提供一种初始安全配置方法、安全模块及终端。

[0087] 为使本发明的目的、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发明进行详细描述。

[0088] 如图4所示,本发明实施例的初始安全配置方法,应用于安全模块,包括:

[0089] 步骤41,在终端与网络侧设备进行通用引导架构GBA认证完成的情况下,接收终端发送的证书申请请求,所述证书申请请求中携带终端的标识信息;

[0090] 需要说明的是,本发明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。

[0091] 需要说明的是,在终端向安全模块发送证书申请请求之前,安全模块已经与网络侧BSF协商好供终端与证书授权(CA)服务器(例如,可以为注册证书权威机构(Enrollment Certificate Authority,ECA)服务器)在应用层使用的共享的会话密钥(Ks_NAF)。该会话密钥通过GBA认证流程协商。

[0092] 步骤42,基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护;

[0093] 需要说明的是,在安全模块接收到证书申请请求时,需要先根据所述证书申请请求,生成用于进行证书申请的公私钥对,然后组建证书申请请求消息,具体地,所述证书申

请请求消息中包括进行证书申请的公钥;也就是说,安全模块生成公私钥对,并利用进行证书申请的公钥构建证书申请请求消息。

[0094] 具体地,步骤42的实现方式为:

[0095] 若基于所述会话密钥成功生成第一密钥,根据所述第一密钥,对证书申请请求消息进行加密和/或完整性保护;或者

[0096] 若基于所述会话密钥未生成第一密钥,根据所述会话密钥,对证书申请请求消息进行加密和/或完整性保护;

[0097] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0098] 需要说明的是,当安全模块基于所述会话密钥成功生成第一密钥时,则安全模块基于会话密钥生成加密密钥和完整性保护密钥中的至少一项,例如,当只生成了加密密钥时,对证书申请请求消息进行加密保护,当只生成了完整性保护密钥时,对证书申请请求消息进行完整性保护,当生成了加密密钥和完整性保护密钥时,对证书申请请求消息进行加密和完整性保护,若安全模块没有生成加密密钥和完整性保护密钥,则安全模块使用会话密钥对证书申请请求消息进行加密和完整性保护。这里还需要说明的是,安全模块侧的加密和完整性保护方式与CA服务器侧的加密和完整性保护方式是相同的,也就是说,当安全模块利用加密密钥对证书申请请求消息进行加密保护时,CA服务器侧也会采用加密密钥对证书申请响应消息进行加密保护;当安全模块利用完整性保护密钥对证书申请请求消息进行完整性保护时,CA服务器侧也会采用完整性保护密钥对证书申请响应消息进行完整性保护;当安全模块利用加密密钥和完整性保护密钥对证书申请请求消息进行加密和完整性保护时,CA服务器侧也会采用加密密钥和完整性保护密钥对证书申请响应消息进行加密和完整性保护;当安全模块利用会话密钥对证书申请请求消息进行加密和完整性保护时,CA服务器侧也会采用会话密钥对证书申请响应消息进行加密和完整性保护;二者具体选用何种方式进行加密和/或完整性保护是预先约定,由二者都知道的。

[0099] 步骤43,向终端反馈进行了加密和/或完整性保护的证书申请请求消息。

[0100] 进一步地,在安全模块向终端反馈进行了加密和/或完整性保护的证书申请请求消息后,终端需要向CA服务器发送证书申请消息,所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息;CA服务器根据所述证书申请请求消息,从网络侧设备获取会话密钥和用户信息,并基于所述会话密钥,校验并解密证书申请请求消息;生成证书申请响应消息;基于所述会话密钥,对所述证书申请响应消息进行加密和/或完整性保护;向所述终端发送证书响应消息,所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息,终端接收CA服务器反馈的证书响应消息,向所述安全模块发送证书写入请求,所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书;安全模块接收终端发送的证书写入请求,根据所述证书申请响应消息,存储数字证书。

[0101] 具体地,安全模块根据所述证书申请响应消息,存储数字证书的实现方式为:在基于GBA认证协商的会话密钥生成第一密钥时,根据所述第一密钥校验并解密证书申请响应消息;解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储。

[0102] 还需要说明的是,在基于会话密钥未生成第一密钥时,根据所述会话密钥校验并解密证书申请响应消息;解析所述证书申请响应消息中的数字证书,并进行所述数字证书

的存储。

[0103] 在安全模块存储完数字证书后，会向所述终端反馈证书写入响应。

[0104] 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。

[0105] 需要说明的是，本发明实施例中主要涉及终端、安全模块以及CA服务器之间的交互过程，这里需要说明的是，该终端指的是V2X终端设备，V2X终端设备可以是OBU、RSU、行人的可穿戴设备等。

[0106] 如图5所示给出了V2X终端设备的一种架构，这里LTE-Uu通信模组、LTE-V2X通信模组以及硬件安全模块(Hardware Security Module，HSM)以分立模块或元器件的方式展示，即安全模块为USIM。未来它们有可能封装集成为一个模块/模组，但这不影响它们之间的逻辑功能划分。

[0107] 该架构中，CA管理应用是V2X终端设备实现“初始安全一键配置”的控制软件，它负责整个业务流程的逻辑控制。V2X应用是V2X终端设备通过PC5/V5接口实现V2X直连通信的业务应用模块，负责直连通信业务消息的收发控制。它通过调用LTE-V2X接口库访问底层LTE-V2X通信模组，与其他V2X终端设备实现V2X业务交互。

[0108] GBA接口库、USIM接口库、HSM接口库是终端底层硬件模块开放给上层应用的调用接口，分别用于调用LTE-Uu通信模组支持的GBA安全接入认证能力，USIM提供的数字证书管理应用能力和安全能力以及HSM提供的安全存储及运算能力。

[0109] 下面以安全模块为USIM为例，如图6所示，本发明实施例的V2X终端设备的初始安全配置流程具体为：

[0110] S601、配置ECA服务器地址、设备标识等信息；

[0111] 需要说明的是，在需要对V2X终端设备进行初始安全配置的时候，用户可通过终端提供的接口(如人机接口、车辆OBD(On-Board Diagnostics，车载诊断)接口或其他有线或无线接口)将所选择的ECA服务器地址信息，设备标识信息(如车辆VIN(Vehicle Identification Number，车辆识别码)号码等)配置到V2X终端设备上。

[0112] 需要说明的是，这里的“用户”是指V2X终端设备安全配置执行方，可能是汽车制造商、V2X终端设备供应商、个人用户等，具体是谁取决于生产流程及应用场景。

[0113] S602、一键触发终端初始配置操作；

[0114] 通过终端提供的接口触发终端设备发起初始安全配置流程。如果是人机接口，用户可将ECA服务器地址信息、设备标识信息通过触摸屏输入，并通过点击按键的方式进行触发，开始“一键配置”。

[0115] S603、V2X终端设备将接收到的触发指令传递给CA管理应用；

[0116] S604、CA管理应用将GBA启动请求发送给GBA接口库；

[0117] S605、GBA接口库将GBA启动请求发送给Modem；

[0118] 需要说明的是，CA管理应用通过GBA接口库调用底层Modem设备启动GBA认证流程，开始建立至ECA服务器的安全访问连接。同时，CA管理应用向用户返回“GBA开始”的状态提示。

[0119] S606、V2X终端底层Modem与网络交互，按照3GPP TS 33.220“Generic

Bootstrapping Architecture”规范执行标准的GBA认证流程；

[0120] S607、Modem将GBA完成响应发送给GBA接口库；

[0121] S608、GBA接口库将GBA完成响应发送给CA管理应用；

[0122] S609、CA管理应用向用户返回GBA状态提示；

[0123] 也就是说，GBA认证流程结束后，CA管理应用接收底层的响应信息，向用户返回GBA认证流程成功与否的状态提示。

[0124] GBA安全认证完成后，USIM与网络侧BSF就已协商好供V2X终端与ECA服务器在应用层使用的共享会话密钥Ks_NAF。

[0125] S610、CA管理应用发送证书申请请求给USIM接口库；

[0126] S611、USIM接口库转发证书申请请求给USIM；

[0127] 也就是说，CA管理应用通过USIM接口库向USIM发起证书申请请求，其中该证书申请请求中携带所需的设备标识信息，申请ECA证书。

[0128] 接收到证书申请请求消息后，USIM执行如下操作：

[0129] 1、生成申请EC数字证书所需的密码公私钥对；

[0130] 2、按照ECA服务器要求的协议格式，组建证书申请请求消息，其中将包含所生成的EC证书公钥；

[0131] 3、根据需要，以会话密钥Ks_NAF为基础生成分别用于加密和完整性保护的会话密钥Ks_NAFe和Ks_NAFi；

[0132] 4、使用加密密钥Ks_NAFe和完整性保护密钥Ks_NAFi对证书申请请求消息进行加密和完整性保护。

[0133] 需要说明的是，如果没有分别生成加密和完整性保护密钥，则使用会话密钥Ks_NAF对消息进行加密和完整性保护。

[0134] S612、USIM发送进行了加密和/或完整性保护的证书申请请求消息给USIM接口库；

[0135] S613、USIM接口库将进行了加密和/或完整性保护的证书申请请求消息发送给CA管理应用；

[0136] 需要说明的是，USIM在证书申请请求进行加密和完整性保护后，USIM通过USIM接口库向CA管理应用返回进行了加密和/或完整性保护的证书申请请求消息。

[0137] S614、接收到USIM的响应后，CA管理应用组建证书申请消息，并向ECA服务器发送。证书申请消息中包含此前USIM反馈的受保护的证书申请请求消息。

[0138] 同时，CA管理应用向用户返回“证书申请开始”的状态，提示正在申请EC证书。

[0139] V2X终端设备在初次访问ECA服务器时，两者可基于协商生成的共享会话密钥Ks_NAF进行身份认证，如采用HTTP Digest方法。认证通过之后，CA管理应用再向ECA服务器发送证书申请消息。

[0140] 接收到证书申请请求消息后，ECA服务器执行如下操作：

[0141] 1、通过事先建立的安全通道与BSF交互，从BSF获取Ks_NAF及与USIM相关的用户信息；

[0142] 2、根据需要，以会话密钥Ks_NAF为基础生成分别用于加密和完整性保护的会话密钥Ks_NAFe和Ks_NAFi；

[0143] 3、使用加密密钥Ks_NAFe和完整性保护密钥Ks_NAFi对证书申请请求消息进行解

密和完整性校验。如果没有分别生成加密和完整性保护密钥，则使用会话密钥Ks_NAF对消息进行解密和完整性校验。

[0144] 4、ECA服务器审核证书申请，在满足条件的情况下为V2X终端设备签发EC数字证书；

[0145] 5、ECA服务器生成证书申请响应消息，并使用加密密钥Ks_NAFe和完整性保护密钥Ks_NAFi对该消息进行加密和完整性保护。如果没有分别生成加密和完整性保护密钥，则使用会话密钥Ks_NAF对消息进行加密和完整性保护。

[0146] S615、ECA服务器向V2X终端设备CA管理应用返回证书响应消息；

[0147] 其中，该证书响应消息中包含受保护的证书申请响应消息。

[0148] S616、CA管理应用向USIM接口库发送证书写入请求；

[0149] S617、USIM接口库将证书写入请求转发给USIM；

[0150] 需要说明的是，接收到证书申请响应消息后，CA管理应用将受保护的证书申请响应消息提取出来，通过证书写入请求消息将申请获得的ECA证书写入USIM，并向用户返回“证书申请完成”的状态，提示EC证书申请成功，需要说明的是，该证书写入请求消息中携带受保护的证书申请响应。

[0151] USIM接收到证书写入请求消息时，执行下列过程：

[0152] 1、USIM使用加密密钥Ks_NAFe和完整性保护密钥Ks_NAFi对证书申请响应消息进行解密和完整性校验。如果没有分别生成加密和完整性保护密钥，则使用会话密钥Ks_NAF对消息进行解密和完整性校验。

[0153] 2、USIM解析数据包，并将其中的ECA公钥证书在其安全环境中安全存储。

[0154] USIM向CA管理应用返回证书写入响应消息。

[0155] S610、CA管理应用向用户返回“证书安全存储”的状态，提示证书安全存储成功。

[0156] 上述方案中，所涉及到的敏感安全参数和信息，如Ks_NAF密钥、EC证书的密码公私钥对、数字证书等均在安全环境(如终端本地安全环境USIM，终端与ECA服务器之间的GBA安全传输通信通道)中生成、运算、传输、处理，因此可以保证V2X终端初始安全配置过程的安全性。

[0157] S618、USIM向USIM接口库发送证书写入响应；

[0158] S619、USIM接口库转发证书写入响应给CA管理应用；

[0159] S620、CA管理应用进行证书申请状态提示。

[0160] 需要说明的是，本发明实施例给出了基于GBA机制安全实现V2X终端设备初始安全配置的方法，能够保证初始安全配置的信息安全，提高了消息传输的安全性。

[0161] 如图7所示，本发明实施例的安全模块70，包括：

[0162] 第一接收模块71，用于在终端与网络侧设备进行通用引导架构GBA认证完成的情况下，接收终端发送的证书申请请求，所述证书申请请求中携带终端的标识信息；

[0163] 第一处理模块72，用于基于GBA认证协商的会话密钥，对证书申请请求消息进行加密和/或完整性保护；

[0164] 第一发送模块73，用于向终端反馈进行了加密和/或完整性保护的证书申请请求消息；

[0165] 其中，所述安全模块用于实现全球用户识别模块USIM的功能。

[0166] 可选地,所述第一处理模块72,用于实现:

[0167] 若基于所述会话密钥成功生成第一密钥,根据所述第一密钥,对证书申请请求消息进行加密和/或完整性保护;或者

[0168] 若基于所述会话密钥未生成第一密钥,根据所述会话密钥,对证书申请请求消息进行加密和/或完整性保护;

[0169] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0170] 可选地,在所述第一发送模块73向终端反馈进行了加密和/或完整性保护的证书申请请求消息之后,还包括:

[0171] 第二接收模块,用于接收终端发送的证书写入请求,所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书;

[0172] 存储模块,用于根据所述证书申请响应消息,存储数字证书。

[0173] 进一步地,所述存储模块,包括:

[0174] 第一解密单元,用于在基于GBA认证协商的会话密钥生成第一密钥时,根据所述第一密钥校验并解密证书申请响应消息;

[0175] 第一存储单元,用于解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储;

[0176] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0177] 进一步地,所述存储模块,包括:

[0178] 第二解密单元,用于在基于会话密钥未生成第一密钥时,根据所述会话密钥校验并解密证书申请响应消息;

[0179] 第二存储单元,用于解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储;

[0180] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0181] 需要说明的是,本发明实施例提供的安全模块是能够执行上述初始安全配置方法的安全模块,则上述初始安全配置方法实施例中的所有实现方式均适用于该安全模块,且均能达到相同或相似的有益效果。

[0182] 本发明实施例还提供一种安全模块,包括收发机和处理器;

[0183] 所述处理器,用于:

[0184] 通过所述收发机在终端与网络侧设备进行通用引导架构GBA认证完成的情况下,接收终端发送的证书申请请求,所述证书申请请求中携带终端的标识信息;基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护;向终端反馈进行了加密和/或完整性保护的证书申请请求消息;

[0185] 其中,所述安全模块用于实现全球用户识别模块USIM的功能。

[0186] 可选地,所述处理器在执行基于GBA认证协商的会话密钥,对证书申请请求消息进行加密和/或完整性保护时,用于实现:

[0187] 若基于所述会话密钥成功生成第一密钥,根据所述第一密钥,对证书申请请求消息进行加密和/或完整性保护;或者

[0188] 若基于所述会话密钥未生成第一密钥,根据所述会话密钥,对证书申请请求消息进行加密和/或完整性保护;

[0189] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0190] 可选地,所述处理器在向终端反馈进行了加密和/或完整性保护的证书申请请求消息之后,还用于实现:

[0191] 接收终端发送的证书写入请求,所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书;

[0192] 根据所述证书申请响应消息,存储数字证书。

[0193] 可选地,所述处理器执行根据所述证书申请响应消息,存储数字证书,用于实现:

[0194] 在基于GBA认证协商的会话密钥生成第一密钥时,根据所述第一密钥校验并解密证书申请响应消息;

[0195] 解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储;

[0196] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0197] 可选地,所述处理器执行根据所述证书申请响应消息,存储数字证书,用于实现:

[0198] 在基于会话密钥未生成第一密钥时,根据所述会话密钥校验并解密证书申请响应消息;

[0199] 解析所述证书申请响应消息中的数字证书,并进行所述数字证书的存储;

[0200] 其中,所述第一密钥包括:加密密钥和/或完整性保护密钥。

[0201] 本发明实施例还提供一种安全模块,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安全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。

[0202] 本发明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安全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,简称ROM)、随机存取存储器(Random Access Memory,简称RAM)、磁碟或者光盘等。

[0203] 如图8所示,本发明实施例的初始安全配置方法,应用于终端,包括:

[0204] 步骤81,与网络侧设备进行通用引导架构GBA认证;

[0205] 步骤82,在与网络侧设备进行GBA认证完成的情况下,向安全模块发送证书申请请求,所述证书申请请求中携带终端的标识信息;

[0206] 步骤83,接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息。

[0207] 可选地,所述步骤81的具体实现方式为:

[0208] 终端的调制解调器调用安全模块与网络侧设备进行GBA认证。

[0209] 可选地,在步骤83之后,还包括:

[0210] 向证书授权CA服务器发送证书申请消息,所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息;

[0211] 接收CA服务器反馈的证书响应消息,所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书;

[0212] 向所述安全模块发送证书写入请求,所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息。

[0213] 需要说明的是，上述实施例中所有关于终端的描述均适用于该初始安全配置方法的实施例中，也能达到与之相同的技术效果。

[0214] 如图9所示，本发明实施例的终端90，包括：

[0215] 第一认证模块91，用于与网络侧设备进行通用引导架构GBA认证；

[0216] 第二发送模块92，用于在与网络侧设备进行GBA认证完成的情况下，向安全模块发送证书申请请求，所述证书申请请求中携带终端的标识信息；

[0217] 第三接收模块93，用于接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息。

[0218] 可选地，在所述第三接收模块93接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息之后，所述终端，还包括：

[0219] 第三发送模块，用于向证书授权CA服务器发送证书申请消息，所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息；

[0220] 第四接收模块，用于接收CA服务器反馈的证书响应消息，所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息，所述证书申请响应消息中携带数字证书；

[0221] 第四发送模块，用于向所述安全模块发送证书写入请求，所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息；

[0222] 第五接收模块，用于接收所述安全模块反馈的证书写入响应。

[0223] 可选地，所述第一认证模块91，用于：

[0224] 终端的调制解调器调用安全模块与网络侧设备进行GBA认证。

[0225] 需要说明的是，本发明实施例提供的终端是能够执行上述初始安全配置方法的终端，则上述初始安全配置方法实施例中的所有实现方式均适用于该终端，且均能达到相同或相似的有益效果。

[0226] 本发明实施例还提供一种终端，包括收发机和处理器；

[0227] 所述处理器，用于：与网络侧设备进行通用引导架构GBA认证；

[0228] 所述收发机，用于：

[0229] 在与网络侧设备进行GBA认证完成的情况下，向安全模块发送证书申请请求，所述证书申请请求中携带终端的标识信息；

[0230] 接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息。

[0231] 可选地，所述收发机在执行接收安全模块反馈的进行了加密和/或完整性保护的证书申请请求消息之后，还用于实现：

[0232] 向证书授权CA服务器发送证书申请消息，所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息；

[0233] 接收CA服务器反馈的证书响应消息，所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息，所述证书申请响应消息中携带数字证书；

[0234] 向所述安全模块发送证书写入请求，所述证书写入请求中携带进行加密和/或完整性保护的证书申请响应消息。

[0235] 可选地，所述处理器执行与网络侧设备进行通用引导架构GBA认证，具体实现：

[0236] 终端的调制解调器调用安全模块与网络侧设备进行GBA认证。

[0237] 本发明实施例还提供一种终端，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安全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。

[0238] 本发明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安全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，简称ROM)、随机存取存储器(Random Access Memory，简称RAM)、磁碟或者光盘等。

[0239] 如图10所示，本发明实施例的初始安全配置方法，应用于CA服务器，包括：

[0240] 步骤101，接收终端发送的证书申请消息，所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息；

[0241] 步骤102，根据所述证书申请请求消息，向所述终端发送证书响应消息，所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息，所述证书申请响应消息中携带数字证书。

[0242] 可选地，所述步骤102的具体实现方式为：

[0243] 从网络侧设备获取会话密钥和用户信息；

[0244] 基于所述会话密钥，校验并解密证书申请请求消息；

[0245] 生成证书申请响应消息；

[0246] 基于所述会话密钥，对所述证书申请响应消息进行加密和/或完整性保护；

[0247] 向所述终端发送证书响应消息，所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息。

[0248] 具体地，基于所述会话密钥，校验并解密证书申请请求消息，包括:

[0249] 若根据所述会话密钥成功生成所述第二密钥，利用所述第二密钥校验并解密证书申请请求消息；或者

[0250] 若根据所述会话密钥未生成所述第二密钥，则根据所述会话密钥，校验并解密证书申请请求消息；

[0251] 其中，所述第二密钥包括：加密密钥和/或完整性保护密钥。

[0252] 具体地，基于所述会话密钥，对所述证书申请响应消息进行加密和/或完整性保护，包括：

[0253] 若根据所述会话密钥成功生成所述第二密钥，根据所述第二密钥对所述证书申请响应消息进行加密和/或完整性保护；或者

[0254] 若根据所述会话密钥未生成所述第二密钥，则根据所述会话密钥，校验并解密证书申请请求消息；

[0255] 其中，所述第二密钥包括：加密密钥和/或完整性保护密钥。

[0256] 需要说明的是，上述实施例中所有关于CA服务器的描述均适用于该初始安全配置方法的实施例中，也能达到与之相同的技术效果。

[0257] 如图11所示，本发明实施例的CA服务器110，包括：

[0258] 第六接收模块111，用于接收终端发送的证书申请消息，所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息；

[0259] 第五发送模块112,用于根据所述证书申请请求消息,向所述终端发送证书响应消息,所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书。

[0260] 可选地,所述第五发送模块112,包括:

[0261] 获取单元,用于从网络侧设备获取会话密钥和用户信息;

[0262] 第三解密单元,用于基于所述会话密钥,校验并解密证书申请请求消息;

[0263] 第一生成单元,用于生成证书申请响应消息;

[0264] 第一处理单元,用于基于所述会话密钥,对所述证书申请响应消息进行加密和/或完整性保护;

[0265] 第一发送单元,用于向所述终端发送证书响应消息,所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息。

[0266] 进一步地,所述第三解密单元,用于:

[0267] 若根据所述会话密钥成功生成所述第二密钥,利用所述第二密钥校验并解密证书申请请求消息;或者

[0268] 若根据所述会话密钥未生成所述第二密钥,则根据所述会话密钥,校验并解密证书申请请求消息;

[0269] 其中,所述第二密钥包括:加密密钥和/或完整性保护密钥。

[0270] 进一步地,所述第一处理单元,用于:

[0271] 若根据所述会话密钥成功生成所述第二密钥,根据所述第二密钥对所述证书申请响应消息进行加密和/或完整性保护;或者

[0272] 若根据所述会话密钥未生成所述第二密钥,则根据所述会话密钥,校验并解密证书申请请求消息;

[0273] 其中,所述第二密钥包括:加密密钥和/或完整性保护密钥。

[0274] 需要说明的是,本发明实施例提供的CA服务器是能够执行上述初始安全配置方法的CA服务器,则上述初始安全配置方法实施例中的所有实现方式均适用于该CA服务器,且均能达到相同或相似的有益效果。

[0275] 本发明实施例还提供一种CA服务器,包括收发机和处理器;

[0276] 所述收发机,用于:

[0277] 接收终端发送的证书申请消息,所述证书申请消息中携带进行加密和/或完整性保护的证书申请请求消息;

[0278] 根据所述证书申请请求消息,向所述终端发送证书响应消息,所述证书响应消息中携带进行加密和/或完整性保护的证书申请响应消息,所述证书申请响应消息中携带数字证书。

[0279] 可选地,所述处理器具体用于实现:

[0280] 从网络侧设备获取会话密钥和用户信息;

[0281] 基于所述会话密钥,校验并解密证书申请请求消息;

[0282] 生成证书申请响应消息;

[0283] 基于所述会话密钥,对所述证书申请响应消息进行加密和/或完整性保护;

[0284] 向所述终端发送证书响应消息,所述证书响应消息中携带进行加密和/或完整性

保护的证书申请响应消息。

[0285] 进一步地，所述处理器基于所述会话密钥，校验并解密证书申请请求消息时，用于实现：

[0286] 若根据所述会话密钥成功生成所述第二密钥，利用所述第二密钥校验并解密证书申请请求消息；或者

[0287] 若根据所述会话密钥未生成所述第二密钥，则根据所述会话密钥，校验并解密证书申请请求消息；

[0288] 其中，所述第二密钥包括：加密密钥和/或完整性保护密钥。

[0289] 进一步地，所述处理器执行基于所述会话密钥，对所述证书申请响应消息进行加密和/或完整性保护时，用于实现：

[0290] 若根据所述会话密钥成功生成所述第二密钥，根据所述第二密钥对所述证书申请响应消息进行加密和/或完整性保护；或者

[0291] 若根据所述会话密钥未生成所述第二密钥，则根据所述会话密钥，校验并解密证书申请请求消息；

[0292] 其中，所述第二密钥包括：加密密钥和/或完整性保护密钥。

[0293] 本发明实施例还提供一种CA服务器，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安全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。

[0294] 本发明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安全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，简称ROM)、随机存取存储器(Random Access Memory，简称RAM)、磁碟或者光盘等。

[0295] 如图12所示，本发明实施例的初始安全配置方法，应用于网络侧设备，包括：

[0296] 步骤121，与终端进行通用引导架构GBA认证。

[0297] 可选地，在所述步骤121之后，还包括：

[0298] 发送会话密钥和用户信息给证书授权CA服务器。

[0299] 需要说明的是，上述实施例中所有关于网络侧设备的描述均适用于该初始安全配置方法的实施例中，也能达到与之相同的技术效果。

[0300] 如图13所示，本发明实施例的网络侧设备130，包括：

[0301] 第二认证模块131，用于与终端进行通用引导架构GBA认证。

[0302] 可选地，所述网络侧设备130，还包括：

[0303] 第六发送模块，用于发送会话密钥和用户信息给证书授权CA服务器。

[0304] 需要说明的是，本发明实施例提供的网络侧设备是能够执行上述初始安全配置方法的网络侧设备，则上述初始安全配置方法实施例中的所有实现方式均适用于该网络侧设备，且均能达到相同或相似的有益效果。

[0305] 本发明实施例还提供一种网络侧设备，包括收发机和处理器；

[0306] 所述处理器，用于：

[0307] 与终端进行通用引导架构GBA认证。

[0308] 可选地，所述收发机，用于：

[0309] 发送会话密钥和用户信息给证书授权CA服务器。

[0310] 本发明实施例还提供一种网络侧设备，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安全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。

[0311] 本发明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安全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，简称ROM)、随机存取存储器(Random Access Memory，简称RAM)、磁碟或者光盘等。

[0312] 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。

[0313] 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。

[0314] 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。

[0315] 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科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。

[0316] 以上所述的是本发明的优选实施方式，应当指出对于本技术领域的普通人员来说，在不脱离本发明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发明的保护范围内。

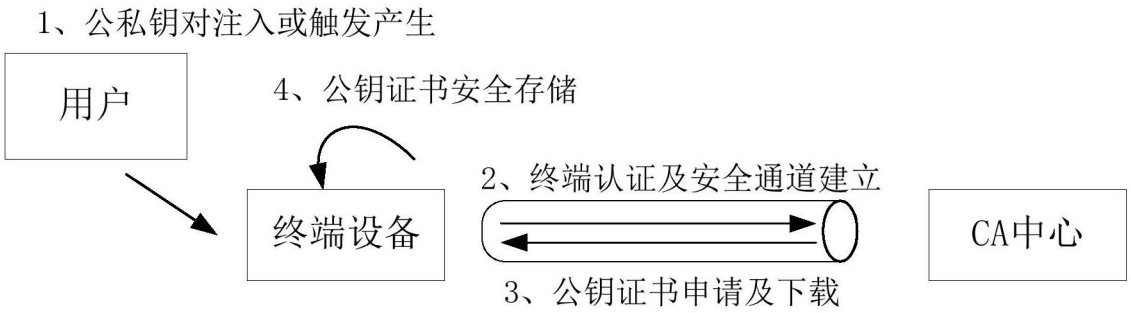

1、公私钥对注入或触发产生
用户
4、公钥证书安全存储
终端设备
2、终端认证及安全通道建立
3、公钥证书申请及下载
CA中心

图1

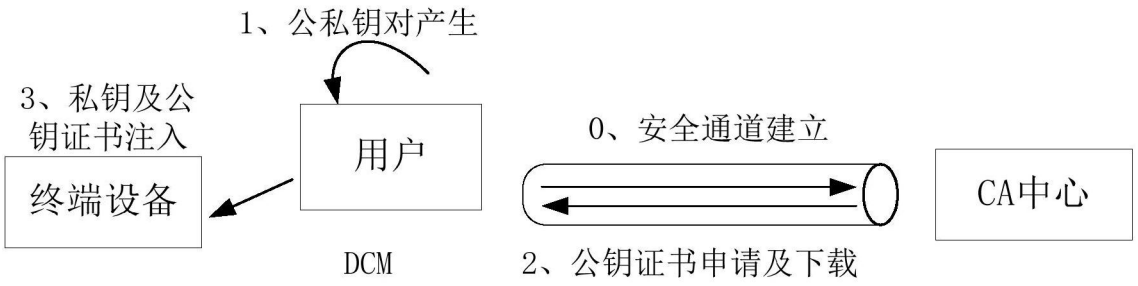

1、公私钥对产生
3、私钥及公钥证书注入
用户
终端设备
DCM
0、安全通道建立
2、公钥证书申请及下载
CA中心

图2

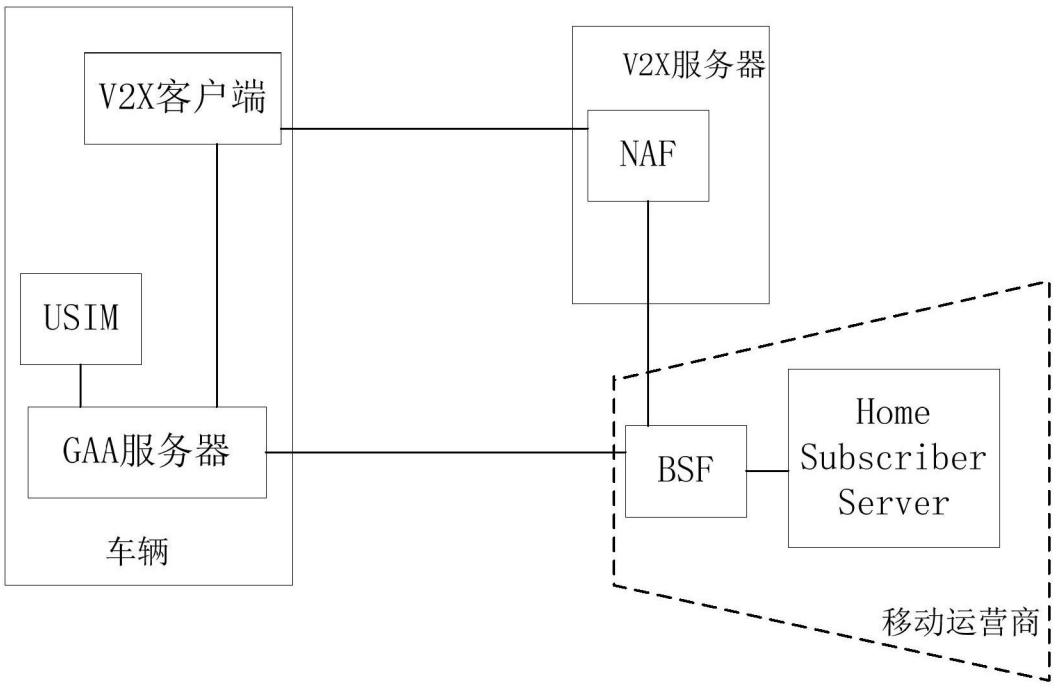

V2X客户端
V2X服务器
NAF
USIM
GAA服务器
BSF
Home Subscriber Server
车辆
移动运营商

图3

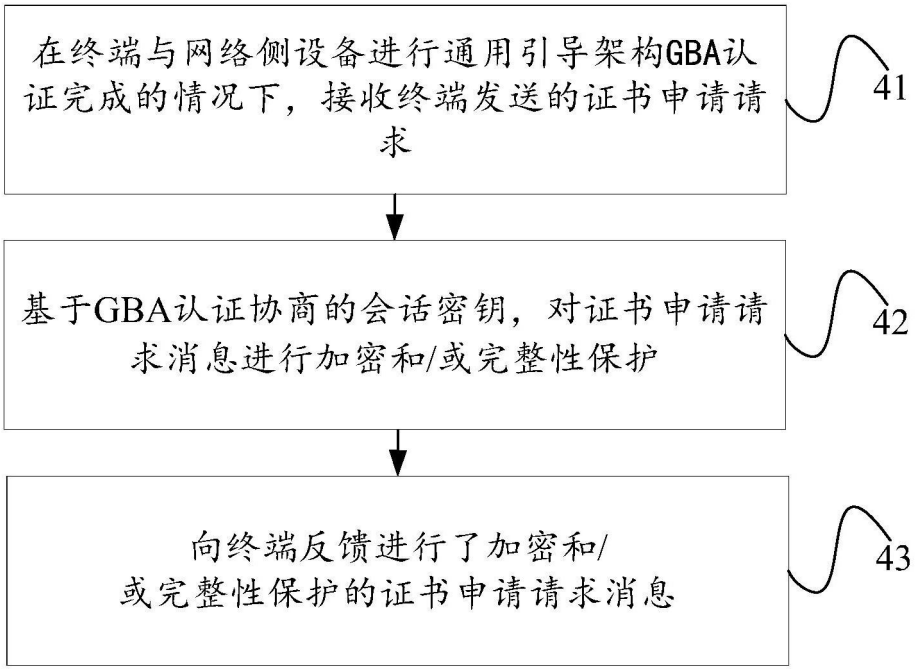

在终端与网络侧设备进行通用引导架构GBA认证完成的情况下，接收终端发送的证书申请请求
41
基于GBA认证协商的会话密钥，对证书申请请求消息进行加密和/或完整性保护
42
向终端反馈进行了加密和/或完整性保护的证书申请请求消息
43

图4

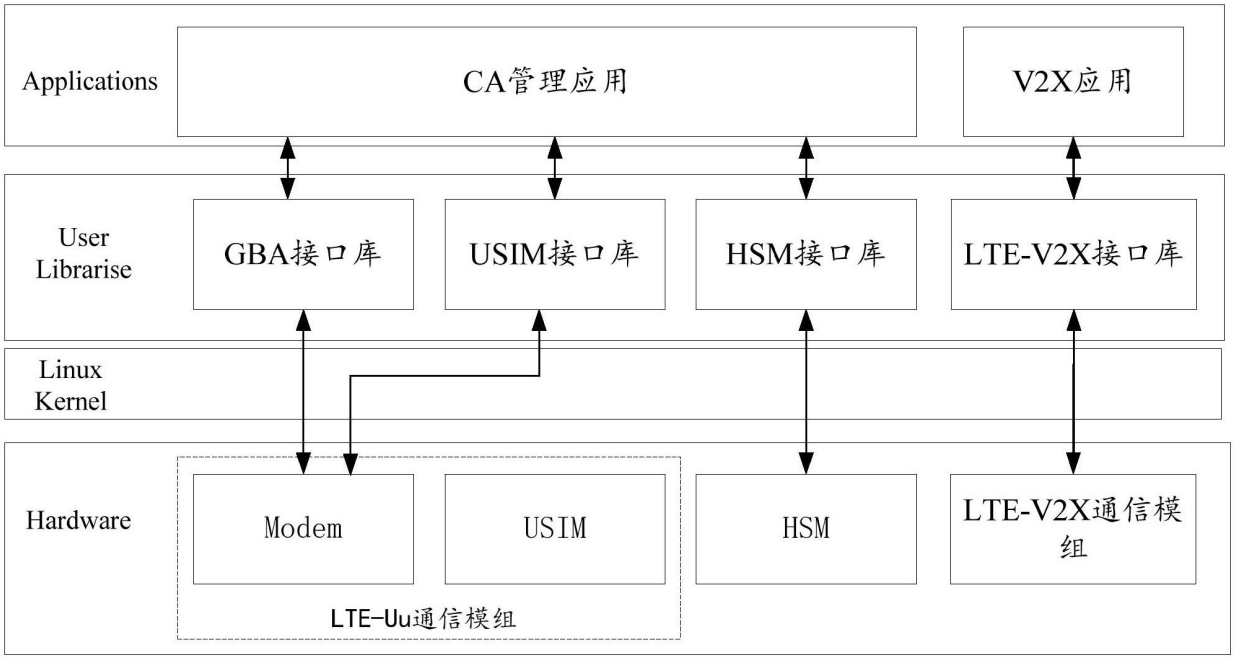

Applications
CA管理应用
V2X应用
User Librarise
GBA接口库
USIM接口库
HSM接口库
LTE-V2X接口库
Linux Kernel
Hardware
Modem
USIM
HSM
LTE-V2X通信模组
LTE-Uu通信模组

图5

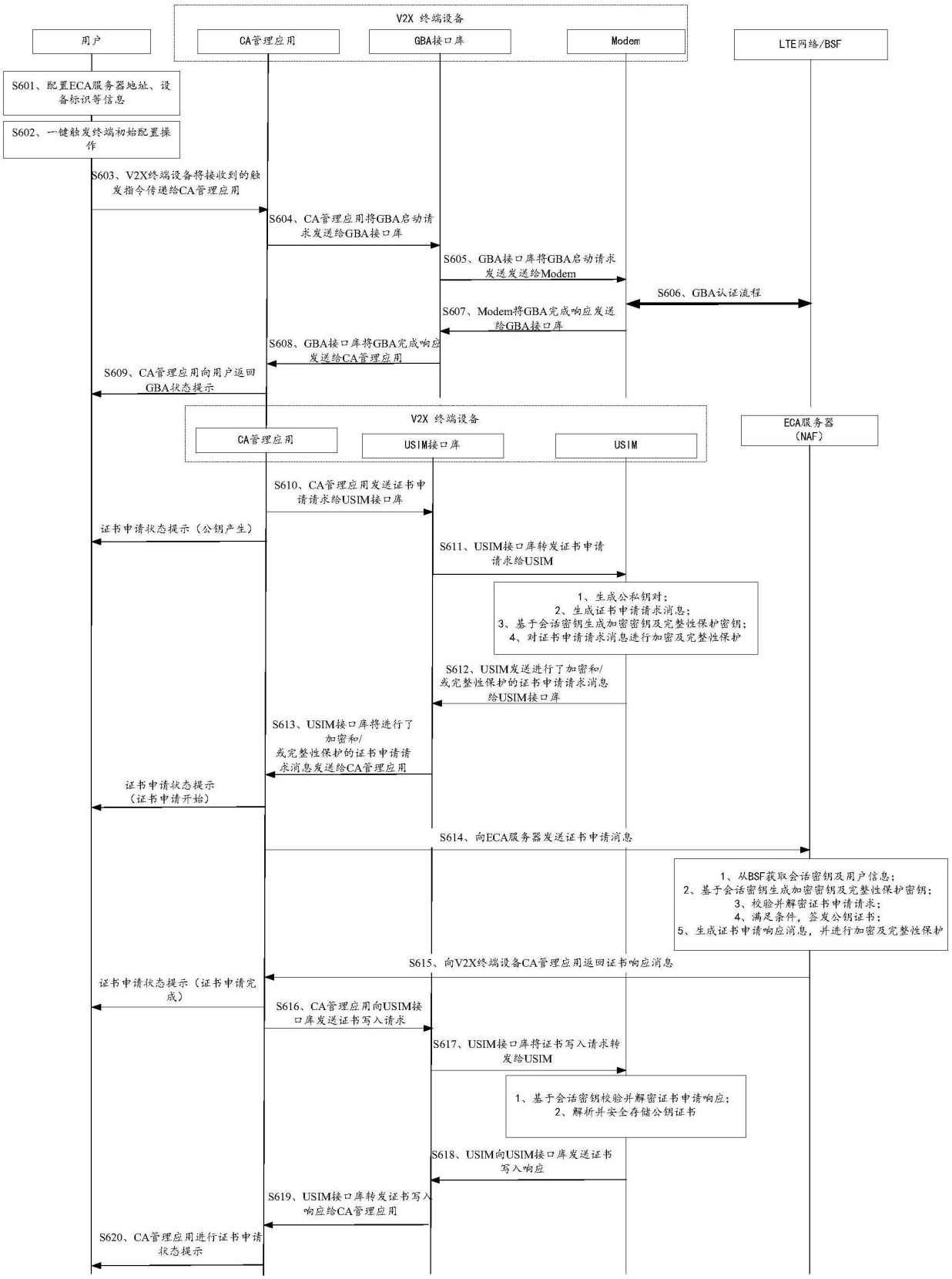

V2X 终端设备
用户
CA管理应用
GBA接口库
Modem
LTE网络/BSF
S601、配置ECA服务器地址、设备标识等信息
S602、一键触发终端初始配置操作
S603、V2X终端设备将接收到的触发指令传递给CA管理应用
S604、CA管理应用将GBA启动请求发送给GBA接口库
S605、GBA接口库将GBA启动请求发送发送给Modem
S606、GBA认证流程
S607、Modem将GBA完成响应发送给GBA接口库
S608、GBA接口库将GBA完成响应发送给CA管理应用
S609、CA管理应用向用户返回GBA状态提示
V2X 终端设备
CA管理应用
USIM接口库
USIM
ECA服务器（NAF）
S610、CA管理应用发送证书申请请求给USIM接口库
证书申请状态提示（公钥产生）
S611、USIM接口库转发证书申请请求给USIM
1、生成公私钥对；
2、生成证书申请请求消息；
3、基于会话密钥生成加密密钥及完整性保护密钥；
4、对证书申请请求消息进行加密及完整性保护
S612、USIM发送进行了加密和/或完整性保护的证书申请请求消息给USIM接口库
S613、USIM接口库将进行了加密和/或完整性保护的证书申请请求消息发送给CA管理应用
证书申请状态提示（证书申请开始）
S614、向ECA服务器发送证书申请消息
1、从BSF获取会话密钥及用户信息；
2、基于会话密钥生成加密密钥及完整性保护密钥；
3、校验并解密证书申请请求；
4、满足条件，签发公钥证书；
5、生成证书申请响应消息，并进行加密及完整性保护
S615、向V2X终端设备CA管理应用返回证书响应消息
证书申请状态提示（证书申请完成）
S616、CA管理应用向USIM接口库发送证书写入请求
S617、USIM接口库将证书写入请求转发给USIM
1、基于会话密钥校验并解密证书申请响应；
2、解析并安全存储公钥证书
S618、USIM向USIM接口库发送证书写入响应
S619、USIM接口库转发证书写入响应给CA管理应用
S620、CA管理应用进行证书申请状态提示

图6

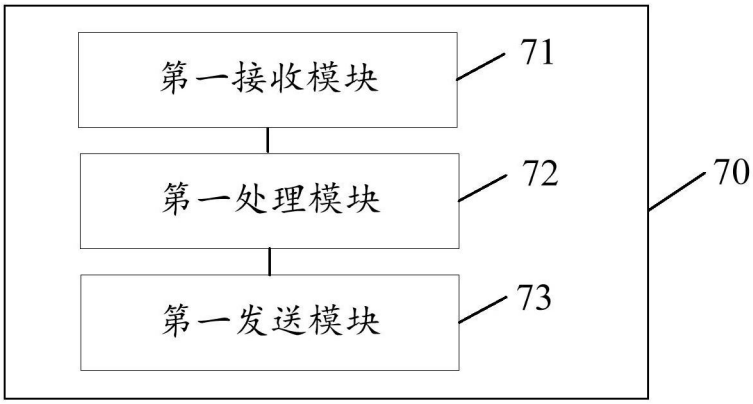

第一接收模块
71
第一处理模块
72
第一发送模块
73
70

图7

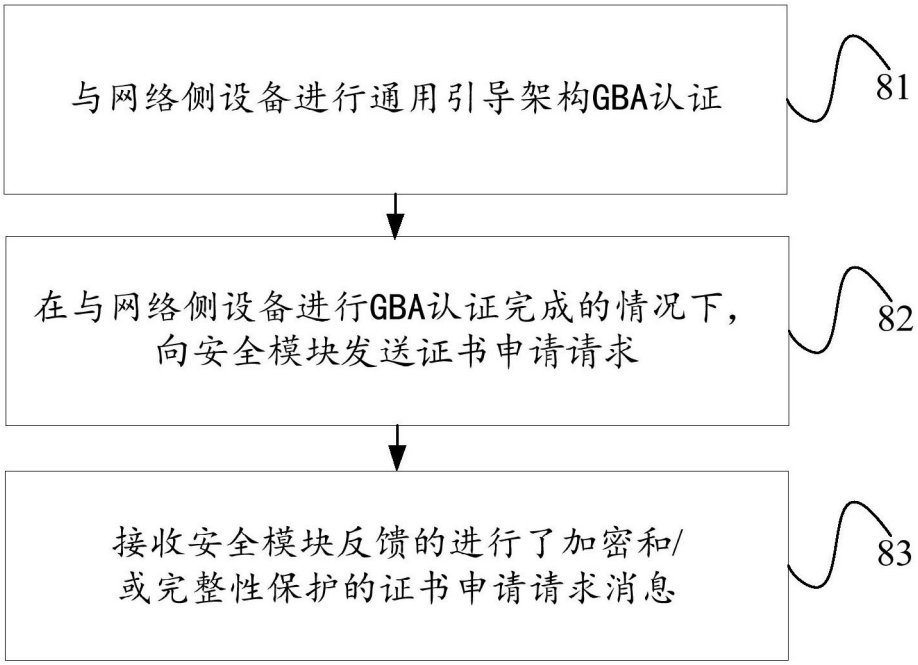

与网络侧设备进行通用引导架构GBA认证
81
在与网络侧设备进行GBA认证完成的情况下，
向安全模块发送证书申请请求
82
接收安全模块反馈的进行了加密和/
或完整性保护的证书申请请求消息
83

图8

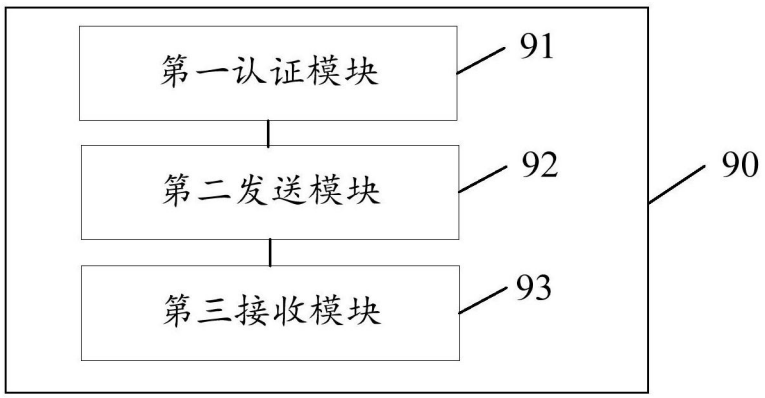

第一认证模块
91
第二发送模块
92
第三接收模块
93
90

图9

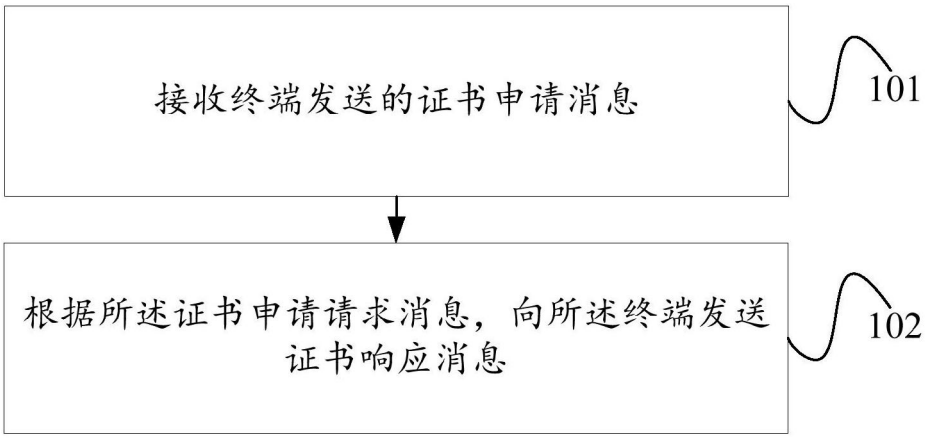

接收终端发送的证书申请消息
101
根据所述证书申请请求消息，向所述终端发送证书响应消息
102

图10

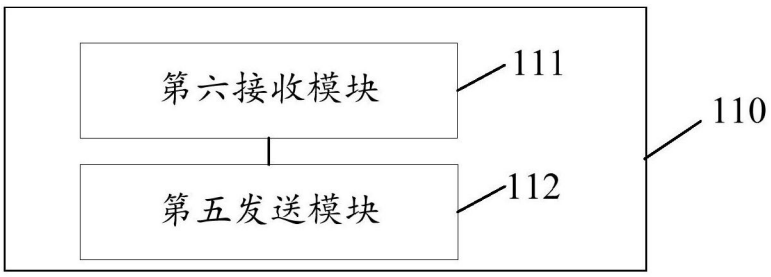

第六接收模块
111
第五发送模块
112
110

图11

图12

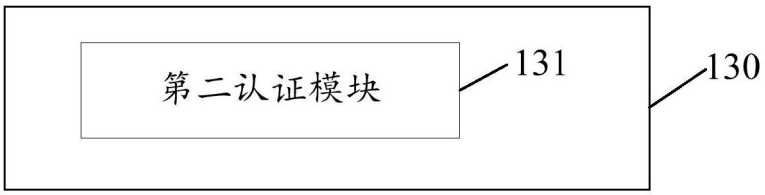


图13