(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112994873 B
(45)授权公告日 2023.03.24

(21)申请号 201911308628.7
(22)申请日 2019.12.18
(65)同一申请的已公布的文献号
申请公布号 CN 112994873 A
(43)申请公布日 2021.06.18
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 潘凯 李民 陈璟
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
专利代理师 赵小霞
(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
(56)对比文件
US 2010241851 A1,2010.09.23
CN 102905260 A,2013.01.30
CN 108848496 A,2018.11.20
EP 3174324 A1,2017.05.31
审查员 杨丽鲜

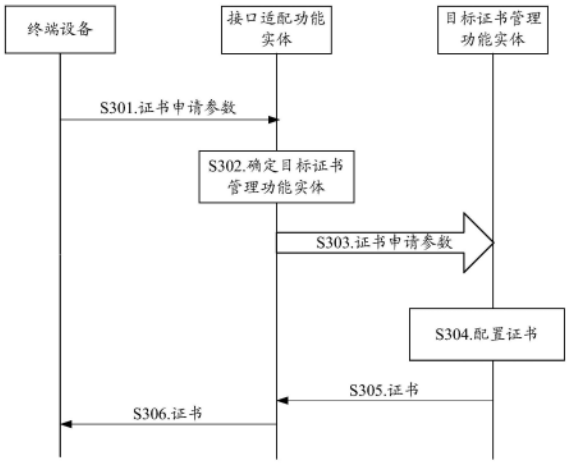
权利要求书5页 说明书26页 附图8页

(54)发明名称

一种证书申请方法及设备

(57)摘要

本申请实施例提供了一种证书申请方法及设备。在该方法中,接口适配功能实体能够适配至少一种证书管理功能实体的接口,因此终端设备可以通过该接口适配功能实体,实现从不同证书管理功能实体申请证书。通过该方案,接口适配功能实体可以向终端设备屏蔽证书管理功能实体的实现或部署,使终端设备可以无感知上层的证书管理功能实体,因此终端设备无需在本地设置证书管理功能实体交互的接口。显然,在保证终端设备能够与不同证书管理功能实体交互的基础上,该方法可以减少终端设备内部与证书管理功能实体交互的接口的数量。



CN 112994873 B

1.一种证书申请方法,其特征在于,包括:

终端设备根据启动执行的业务确定目标证书管理功能实体信息;

所述终端设备向接口适配功能实体发送证书申请参数,以及所述终端设备向所述接口适配功能实体发送所述目标证书管理功能实体信息,所述证书申请参数用于为所述终端设备执行所述业务申请证书,所述目标证书管理功能实体信息用于确定配置所述证书的目标证书管理功能实体;

所述终端设备从所述接口适配功能实体接收所述证书。

2.如权利要求1所述的方法,其特征在于,

在所述终端设备向所述接口适配功能实体发送所述证书申请参数之后,在所述终端设备从所述接口适配功能实体接收所述证书之前,所述方法还包括:

所述终端设备从所述接口适配功能实体接收证书请求消息,其中所述证书请求消息中包含所述证书申请参数;

所述终端设备对所述证书请求消息进行签名处理;

所述终端设备向所述接口适配功能实体发送签名处理后的所述证书请求消息,以使所述接口适配功能实体将签名处理后的所述证书请求消息转发给所述目标证书管理功能实体;

所述终端设备从所述接口适配功能实体接收所述证书,包括:

所述终端设备从所述接口适配功能实体接收证书响应消息,其中,所述证书响应消息为所述接口适配功能实体从所述目标证书管理功能实体接收的,所述证书响应消息中包含所述证书。

3.如权利要求1或2所述的方法,其特征在于,在所述终端设备向所述接口适配功能实体发送所述目标证书管理功能实体信息之后,所述方法还包括:

所述终端设备从所述接口适配功能实体接收到通知消息,其中,所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的目标接口。

4.如权利要求3所述的方法,其特征在于,所述通知消息包含所述目标证书管理功能实体的根证书;

在所述终端设备从所述接口适配功能实体接收所述证书响应消息之后,所述方法还包括:

所述终端设备根据所述目标证书管理功能实体的根证书,对所述证书响应消息中包含的证书进行验证。

5.如权利要求1或2所述的方法,其特征在于,

在所述终端设备向所述接口适配功能实体发送所述目标证书管理功能实体信息之前,所述方法还包括:

所述终端设备从所述接口适配功能实体接收至少一个证书管理功能实体信息,其中,所述至少一个证书管理功能实体信息包含所述目标证书管理功能实体信息,所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口;

所述终端设备在所述至少一个证书管理功能实体中选择所述目标证书管理功能实体。

6.一种证书申请方法,其特征在于,包括:

接口适配功能实体从终端设备接收证书申请参数和目标证书管理功能实体信息，所述目标证书管理功能实体信息是根据所述终端设备启动执行的业务确定的，所述证书申请参数用于为所述终端设备执行所述业务申请证书；

所述接口适配功能实体根据所述目标证书管理功能实体信息确定为所述终端设备配置所述证书的目标证书管理功能实体；

所述接口适配功能实体向所述目标证书管理功能实体发送所述证书申请参数；

所述接口适配功能实体从所述目标证书管理功能实体接收所述证书，并向所述终端设备发送所述证书。

7.如权利要求6所述的方法，其特征在于，所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的目标接口；

所述接口适配功能实体向所述目标证书管理功能实体发送所述证书申请参数，包括：

所述接口适配功能实体通过所述目标接口向所述目标证书管理功能实体发送所述证书申请参数；

所述接口适配功能实体从所述目标证书管理功能实体接收所述证书，包括：

所述接口适配功能实体通过所述目标接口从所述目标证书管理功能实体接收所述证书。

8.如权利要求7所述的方法，其特征在于，

所述接口适配功能实体通过所述目标接口向所述目标证书管理功能实体发送所述证书申请参数，包括：

所述接口适配功能实体根据所述目标接口生成包含所述证书申请参数的证书请求消息，并向所述终端设备发送所述证书请求消息；

所述接口适配功能实体从终端设备接收签名处理后的所述证书请求消息，并通过所述目标接口向所述目标证书管理功能实体发送签名处理后的所述证书请求消息；

所述接口适配功能实体从所述目标证书管理功能实体接收所述证书，包括：

所述接口适配功能实体从所述目标证书管理功能实体接收证书响应消息，其中，所述证书响应消息中包含所述目标证书管理功能实体为所述终端设备配置的所述证书；

所述接口适配功能实体向所述终端设备发送所述证书，包括：

所述接口适配功能实体向所述终端设备所述证书响应消息。

9.如权利要求6-8任一项所述的方法，其特征在于，所述方法还包括：

所述接口适配功能实体确定本地设置有与所述目标证书管理功能实体交互的目标接口，向所述终端设备发送通知消息，其中，所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

10.如权利要求9所述的方法，其特征在于，所述通知消息中包含所述目标证书管理功能实体的根证书。

11.如权利要求6-8任一项所述的方法，其特征在于，所述方法还包括：

所述接口适配功能实体向所述终端设备发送至少一个证书管理功能实体信息，其中，所述至少一个证书管理功能实体中包含所述目标证书管理功能实体，所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口。

12.一种终端设备，其特征在于，包括：

通信单元，用于接收和发送数据；

处理单元，用于根据启动执行的业务确定目标证书管理功能实体信息；通过所述通信单元向接口适配功能实体发送证书申请参数，通过所述通信单元向所述接口适配功能实体发送所述目标证书管理功能实体信息，所述证书申请参数用于为所述终端设备执行所述业务申请证书，所述目标证书管理功能实体信息用于确定配置所述证书的目标证书管理功能实体；以及通过所述通信单元从所述接口适配功能实体接收所述证书。

13.如权利要求12所述的终端设备，其特征在于，所述处理单元，还用于：

在通过所述通信单元向所述接口适配功能实体发送所述证书申请参数之后，在通过所述通信单元从所述接口适配功能实体接收所述证书之前，通过所述通信单元从所述接口适配功能实体接收证书请求消息，其中所述证书请求消息中包含所述证书申请参数；

对所述证书请求消息进行签名处理；

通过所述通信单元向所述接口适配功能实体发送签名处理后的所述证书请求消息，以使所述接口适配功能实体将签名处理后的所述证书请求消息转发给所述目标证书管理功能实体；

所述处理单元，在通过所述通信单元从所述接口适配功能实体接收所述证书时，具体用于：

通过所述通信单元从所述接口适配功能实体接收证书响应消息，其中，所述证书响应消息为所述接口适配功能实体从所述目标证书管理功能实体接收的，所述证书响应消息中包含所述证书。

14.如权利要求12或13所述的终端设备，其特征在于，所述处理单元，还用于：

在通过所述通信单元向所述接口适配功能实体发送所述目标证书管理功能实体信息之后，通过所述通信单元从所述接口适配功能实体接收到通知消息，其中，所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的目标接口。

15.如权利要求14所述的终端设备，其特征在于，所述通知消息包含所述目标证书管理功能实体的根证书；

所述处理单元，还用于：

在通过所述通信单元从所述接口适配功能实体接收所述证书响应消息之后，根据所述目标证书管理功能实体的根证书，对所述证书响应消息中包含的证书进行验证。

16.如权利要求12或13所述的终端设备，其特征在于，所述处理单元，还用于：

在通过所述通信单元向所述接口适配功能实体发送所述目标证书管理功能实体信息之前，通过所述通信单元从所述接口适配功能实体接收至少一个证书管理功能实体信息，其中，所述至少一个证书管理功能实体信息包含所述目标证书管理功能实体信息，所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口；

在所述至少一个证书管理功能实体中选择所述目标证书管理功能实体。

17.一种接口适配功能实体，其特征在于，包括：

通信单元，用于接收和发送数据；

处理单元，用于通过所述通信单元从终端设备接收证书申请参数和目标证书管理功能实体信息，所述目标证书管理功能实体信息是根据所述终端设备启动执行的业务确定的，

所述证书申请参数用于为所述终端设备执行所述业务申请证书;根据所述目标证书管理功能实体信息确定为所述终端设备配置所述证书的目标证书管理功能实体;通过所述通信单元向所述目标证书管理功能实体发送所述证书申请参数;通过所述通信单元从所述目标证书管理功能实体接收所述证书,并通过所述通信单元向所述终端设备发送所述证书。

18.如权利要求17所述的接口适配功能实体,其特征在于,所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的目标接口;

所述处理单元,在通过所述通信单元向所述目标证书管理功能实体发送所述证书申请参数时,具体用于:

根据所述通信单元和所述目标接口向所述目标证书管理功能实体发送所述证书申请参数;

所述处理单元,在通过所述通信单元从所述目标证书管理功能实体接收所述证书时,具体用于:

根据所述通信单元和所述目标接口从所述目标证书管理功能实体接收所述证书。

19.如权利要求18所述的接口适配功能实体,其特征在于,所述处理单元,在根据所述通信单元和所述目标接口向所述目标证书管理功能实体发送所述证书申请参数时,具体用于:

根据所述目标接口生成包含所述证书申请参数的证书请求消息,并通过所述通信单元向所述终端设备发送所述证书请求消息;通过所述通信单元从终端设备接收签名处理后的所述证书请求消息,并根据所述通信单元和所述目标接口向所述目标证书管理功能实体发送签名处理后的所述证书请求消息;

所述处理单元,在通过所述通信单元从所述目标证书管理功能实体接收所述证书时,具体用于:

通过所述通信单元从所述目标证书管理功能实体接收证书响应消息,其中,所述证书响应消息中包含所述目标证书管理功能实体为所述终端设备配置的所述证书;

所述处理单元,在通过所述通信单元向所述终端设备发送所述证书时,具体用于:

通过所述通信单元向所述终端设备所述证书响应消息。

20.如权利要求17-19任一项所述的接口适配功能实体,其特征在于,所述处理单元,还用于:

确定本地设置有与所述目标证书管理功能实体交互的目标接口,通过所述通信单元向所述终端设备发送通知消息,其中,所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

21.如权利要求20所述的接口适配功能实体,其特征在于,所述通知消息中包含所述目标证书管理功能实体的根证书。

22.如权利要求17-19任一项所述的接口适配功能实体,其特征在于,所述处理单元,还用于:

通过所述通信单元向所述终端设备发送至少一个证书管理功能实体信息,其中,所述至少一个证书管理功能实体中包含所述目标证书管理功能实体,所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口。

23.一种终端设备,其特征在于,包括至少一个处理元件和至少一个存储元件;

所述至少一个存储元件用于存储程序；

所述至少一个处理元件用于运行所述程序，以使所述终端设备执行如权利要求1-5任一项所述的方法。

24.一种接口适配功能实体，其特征在于，包括至少一个处理元件和至少一个存储元件；

所述至少一个存储元件用于存储程序；

所述至少一个处理元件用于运行所述程序，以使所述接口适配功能实体执行如权利要求6-11任一项所述的方法。

25.一种通信系统，其特征在于，包括终端设备和接口适配功能实体；

所述终端设备用于执行如权利要求1-5任一项所述的方法；

所述接口适配功能实体用于执行如权利要求6-11任一项所述的方法。

26.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序被计算机执行时，使得所述计算机执行如权利要求1-5任一项所述的方法。

27.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序被计算机执行时，使得所述计算机执行如权利要求6-11任一项所述的方法。

一种证书申请方法及设备

技术领域

[0001] 本申请涉及通信技术领域,尤其涉及一种证书申请方法及设备。

背景技术

[0002] 通信系统中的数据传输的安全性在很多场景中都是至关重要的。目前,为了保证接收设备接收到的消息是真实可信并且未受到攻击者篡改/伪造的,通信系统通常会采用加密算法以及证书机制结合的方式实现数据传输安全。

[0003] 在该方式中,终端设备A需要向证书管理功能实体申请证书,然后对签名处理后的消息以及该证书发送给终端设备B,这样,当终端设备B在签名和证书验证成功后,可以确定该消息是真实、可信和安全的。所述证书管理功能实体可以但不限定为公钥基础设施(public key infrastructure,PKI)或证书管理(证书授权或证书颁发)机构(Certificate Authority,CA)。

[0004] 我们知道,终端设备与上述证书管理功能实体交互的过程中,需要通过相应的接口实现。然而随着业务的多样化,证书管理功能实体的潜在建设机构很多,如在车道万物(vehicle to everything,V2X)通信系统中的公安部、交通部以及其他传统PKI厂商,这些机构在部署各自的证书管理功能实体时,采用的接口方案也不尽相同。因此,为了保证终端设备能够与不同的证书管理功能实体都能够交互对接,那么终端设备内部需要设置多套接口,这会减少终端设备的空闲存储空间,也会增加终端设备的开发成本和开发周期。

发明内容

[0005] 本申请提供了一种证书申请方法及设备,用以在保证终端设备能够与不同证书管理功能实体交互的基础上,减少终端设备内部与证书管理功能实体交互的接口的数量。

[0006] 第一方面,本申请实施例提供了一种证书申请方法,适用于图2所示的证书管理架构中。其中,该证书管理架构中包含终端设备、设置有与至少一个证书管理功能实体进行交互的接口的接口适配功能实体,以及证书管理功能实体。该方法包括:终端设备向接口适配功能实体发送证书申请参数;然后,所述终端设备从所述接口适配功能实体接收证书,所述证书为目标证书管理功能实体为所述终端设备配置的。

[0007] 在以上方法中,接口适配功能实体可以根据终端设备发送的证书申请参数从目标证书管理功能实体为所述终端设备申请证书。显然,接口适配功能实体可以向终端设备屏蔽证书管理功能实体的实现或部署,使终端设备可以无感知上层的证书管理功能实体,因此终端设备无需在本地设置与证书管理功能实体交互的接口。显然,在保证终端设备能够与不同证书管理功能实体交互的基础上,该方法可以减少终端设备内部与证书管理功能实体交互的接口的数量。

[0008] 在一个可能的设计中,在所述终端设备向所述接口适配功能实体发送所述证书申请参数之后,在所述终端设备从所述接口适配功能实体接收所述证书之前,所述终端设备从所述接口适配功能实体接收证书请求消息,其中所述证书请求消息中包含所述证书申请

参数;然后,所述终端设备对所述证书请求消息进行签名处理,并向所述接口适配功能实体发送签名处理后的所述证书请求消息,以使所述接口适配功能实体将签名处理后的所述证书请求消息转发给所述目标证书管理功能实体。

[0009] 通过该设计,所述终端设备可以对证书请求消息进行签名处理,这样,当该证书请求消息传输给所述目标证书管理功能实体后,所述目标证书管理功能实体可以根据签名证明该证书请求消息是所述终端设备发送的,是真实合法的。

[0010] 在一个可能的设计中,所述终端设备可以通过以下方式,从所述接口适配功能实体接收所述证书:所述终端设备从所述接口适配功能实体接收证书响应消息,其中,所述证书响应消息为所述接口适配功能实体从所述目标证书管理功能实体接收的,所述证书响应消息中包含所述证书。通过该设计,所述终端设备可以成功接收证书。可选的,所述证书响应消息可以是所述目标证书管理功能实体进行签名处理后发送的,这样,所述终端设备可以根据签名证明该证书响应消息是所述目标证书管理功能实体发送的,是真实合法的。

[0011] 在一个可能的设计中,在所述终端设备从所述接口适配功能实体接收所述证书之前,所述终端设备向所述接口适配功能实体发送所述目标证书管理功能实体信息。

[0012] 通过该设计,所述终端设备可以提前通知所述接口适配功能实体为所述终端设备配置证书的目标证书管理功能实体。

[0013] 在一个可能的设计中,在所述终端设备向所述接口适配功能实体发送所述目标证书管理功能实体信息之后,所述终端设备从所述接口适配功能实体接收到通知消息,其中,所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

[0014] 通过该设计,所述接口适配功能实体可以通知所述终端设备其本地设置有所述目标接口,能够为所述终端设备申请证书,也可以通知所述终端设可以发送证书申请参数。

[0015] 在一个可能的设计中,所述通知消息包含所述目标证书管理功能实体的根证书。在该场景中,在所述终端设备从所述接口适配功能实体接收所述证书响应消息之后,所述终端设备根据所述目标证书管理功能实体的根证书,对所述证书响应消息中包含的证书进行验证。例如,所述终端设备使用所述目标证书管理功能实体的根证书对所述证书进行解密;然后确定解密后得到的信息中是否包含所述终端设备的公钥,若包含,则确定证书验证成功,所述终端设备可以使用所述证书进行安全的数据通信;否则确定证书验证失败,所述终端设备不能使用所述证书。

[0016] 通过该设计,所述终端设备可以在接收到证书后,根据接收的根证书对接收的证书进行验证,以验证其安全性。

[0017] 在一个可能的设计中,在所述终端设备向所述接口适配功能实体发送所述目标证书管理功能实体信息之前,所述终端设备从所述接口适配功能实体接收至少一个证书管理功能实体信息,其中,所述至少一个证书管理功能实体信息包含所述目标证书管理功能实体信息,所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口;所述终端设备在所述至少一个证书管理功能实体中选择所述目标证书管理功能实体。

[0018] 通过该设计,所述接口适配功能实体可以将其能够交互的至少一个证书管理功能实体通知给所述终端设备,以使所述终端设备可以在其中选择申请证书的目标证书管理功能实体。

[0019] 在一个可能的设计中，在所述终端设备向所述接口适配功能实体发送所述证书申请参数之前，所述终端设备建立与所述接口适配功能实体之间的传输层安全通道。

[0020] 通过该设计，所述终端设备和所述接口适配功能实体可以通过传输层安全通道进行通信交互，以保证通信安全性。

[0021] 在一个可能的设计中，所述证书为注册证书或匿名证书。

[0022] 第二方面，本申请实施例提供了一种证书申请方法，适用于图2所示的证书管理架构中。其中，该证书管理架构中包含终端设备、设置有与至少一个证书管理功能实体进行交互的接口的接口适配功能实体，以及证书管理功能实体。该方法包括：接口适配功能实体从终端设备接收证书申请参数；然后，所述接口适配功能实体确定为所述终端设备配置证书的目标证书管理功能实体，并向所述目标证书管理功能实体发送所述证书申请参数，以使所述目标证书管理功能实体根据所述证书申请参数为所述终端设备配置证书；最后，所述接口适配功能实体通过所述目标接口从所述目标证书管理功能实体接收所述证书，并向所述终端设备发送所述证书。

[0023] 在以上方法中，接口适配功能实体可以根据终端设备发送的证书申请参数从目标证书管理功能实体为所述终端设备申请证书。显然，接口适配功能实体可以向终端设备屏蔽证书管理功能实体的实现或部署，使终端设备可以无感知上层的证书管理功能实体，因此终端设备无需在本地设置与证书管理功能实体交互的接口。显然，在保证终端设备能够与不同证书管理功能实体交互的基础上，该方法可以减少终端设备内部与证书管理功能实体交互的接口的数量。

[0024] 在一个可能的设计中，所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的目标接口；在该场景下，所述接口适配功能实体通过所述目标接口向所述目标证书管理功能实体发送所述证书申请参数，且所述接口适配功能实体通过所述目标接口从所述目标管理功能实体接收所述证书。

[0025] 在一个可能的设计中，所述接口适配功能实体通过以下步骤，通过所述目标接口向所述目标证书管理功能实体发送所述证书申请参数：

[0026] 所述接口适配功能实体根据所述目标接口生成包含所述证书申请参数的证书请求消息，并向所述终端设备发送所述证书请求消息；所述接口适配功能实体从终端设备接收签名处理后的所述证书请求消息，并通过所述目标接口向所述目标证书管理功能实体发送签名处理后的所述证书请求消息。

[0027] 通过该设计，所述接口适配功能实体可以将生成的证书请求消息先发送给终端设备进行签名处理，再将签名处理后的证书请求消息发送给目标管理功能实体。这样，当该证书请求消息传输给所述目标证书管理功能实体后，所述目标证书管理功能实体可以根据签名验证该证书请求消息是所述终端设备发送的，是真实合法的。

[0028] 在一个可能的设计中，所述接口适配功能实体从所述目标证书管理功能实体接收证书响应消息，并向所述终端设备所述证书响应消息；其中，所述证书响应消息中包含所述目标证书管理功能实体为所述终端设备配置的所述证书。通过该设计，所述接口适配功能实体可以从所述目标证书管理功能实体接收所述证书。可选的，所述证书响应消息可以是所述目标证书管理功能实体进行签名处理后发送的，这样，当所述终端设备接收到签名处理后的所述证书响应消息后，可以根据签名证明该证书响应消息是所述目标证书管理功能

实体发送的，是真实合法的。

[0029] 在一个可能的设计中，所述接口适配功能实体可以通过以下方式，确定为所述终端设备配置证书的目标证书管理功能实体：

[0030] 方式一：所述接口适配功能实体从所述终端设备接收所述目标证书管理功能实体信息，根据所述目标证书管理功能实体信息，确定所述目标证书管理功能实体；

[0031] 方式二：所述接口适配功能实体确定所述终端设备的标识，并根据本地保存的终端设备的标识与证书管理功能实体信息的对应关系，确定与所述终端设备的标识对应的所述目标证书管理功能实体信息；所述接口适配功能实体根据所述目标证书管理功能实体信息，确定所述目标证书管理功能实体。

[0032] 通过该设计，所述接口适配功能实体能够确定所述目标证书管理功能实体。

[0033] 在一个可能的设计中，在所述接口适配功能实体从所述终端设备接收所述目标证书管理功能实体信息之后，所述接口适配功能实体确定本地设置有与所述目标证书管理功能实体交互的目标接口，向所述终端设备发送通知消息，其中，所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

[0034] 通过该设计，所述接口适配功能实体可以通知所述终端设备其本地设置有所述目标接口，能够为所述终端设备申请证书，也可以通知所述终端设备发送证书申请参数。

[0035] 在一个可能的设计中，所述通知消息中包含所述目标证书管理功能实体的根证书。这样，当所述终端设备接收到证书后，所述终端设备可以根据该根证书对接收的证书进行验证，以验证其安全性。

[0036] 在一个可能的设计中，在所述接口适配功能实体从所述终端设备接收所述目标证书管理功能实体信息之前，所述接口适配功能实体向所述终端设备发送至少一个证书管理功能实体信息，其中，所述至少一个证书管理功能实体中包含所述目标证书管理功能实体，所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口。

[0037] 通过该设计，所述接口适配功能实体可以将其能够交互的至少一个证书管理功能实体通知给所述终端设备，以使所述终端设备可以在其中选择申请证书的目标证书管理功能实体。

[0038] 在一个可能的设计中，在所述接口适配功能实体从所述终端设备接收所述证书申请参数之前，所述接口适配功能实体建立与所述终端设备之间的传输层安全通道。通过该设计，所述终端设备和所述接口适配功能实体可以通过传输层安全通道进行通信交互，以保证通信安全性。

[0039] 在一个可能的设计中，在所述接口适配功能实体向所述目标证书管理功能实体发送所述证书申请参数之前，所述接口适配功能实体建立与所述目标证书管理功能实体之间的传输层安全通道。通过该设计，所述接口适配功能实体和所述目标证书管理功能实体可以通过传输层安全通道进行通信交互，以保证通信的安全性。

[0040] 在一个可能的设计中，所述证书为注册证书或匿名证书。

[0041] 第三方面，本申请实施例提供了一种证书申请方法，适用于图2所示的证书管理架构中。其中，该证书管理架构中包含终端设备、设置有与至少一个证书管理功能实体进行交互的接口的接口适配功能实体，以及证书管理功能实体。该方法包括：目标证书管理功能实

体从接口适配功能实体接收终端设备的证书申请参数;然后,所述目标证书管理功能实体根据所述证书申请参数,为所述终端设备配置证书;最后,所述目标证书管理功能实体向所述接口适配功能实体发送所述证书。

[0042] 在以上方法中,接口适配功能实体可以根据终端设备发送的证书申请参数从目标证书管理功能实体为所述终端设备申请证书。显然,接口适配功能实体可以向终端设备屏蔽证书管理功能实体的实现或部署,使终端设备可以无感知上层的证书管理功能实体,因此终端设备无需在本地设置与证书管理功能实体交互的接口。显然,在保证终端设备能够与不同证书管理功能实体交互的基础上,该方法可以减少终端设备内部与证书管理功能实体交互的接口的数量。

[0043] 在一个可能的设计中,所述目标证书管理功能实体可以通过以下方式,从接口适配功能实体接收所述终端设备的所述证书申请参数:所述目标证书管理功能实体从所述接口适配功能实体接收所述终端设备签名处理后的证书请求消息,其中,所述证书请求消息中包含所述证书申请参数;在该场景下,所述目标证书管理功能实体在为所述终端设备配置证书之前,需要对签名处理后的所述证书请求消息进行签名验证,且验证成功。通过该设计,所述目标证书管理功能实体可以通过签名验证,确定该证书请求消息是终端设备发送的,是真实合法的。

[0044] 在一个可能的设计中,所述目标证书管理功能实体向所述接口适配功能实体发送证书响应消息,其中,所述证书响应消息中包含所述证书。通过该设计,所述目标证书管理功能实体可以将证书通过接口适配功能实体最终发送给所述终端设备。可选的,所述证书响应消息可以是所述目标证书管理功能实体进行签名处理后发送的,这样,当所述终端设备接收到签名处理后的所述证书响应消息后,可以根据签名证明该证书响应消息是所述目标证书管理功能实体发送的,是真实合法的。

[0045] 在一个可能的设计中,在所述目标证书管理功能实体从所述接口适配功能实体接收所述终端设备的所述证书申请参数之前,所述目标证书管理功能实体建立与所述接口适配功能实体之间的传输层安全通道。通过该设计,所述接口适配功能实体和所述目标证书管理功能实体可以通过传输层安全通道进行通信交互,以保证通信的安全性。

[0046] 在一个可能的设计中,所述证书为注册证书或匿名证书。

[0047] 第四方面,本申请实施例提供了一种通信装置,包括用于执行以上任一方面中各个步骤的单元。

[0048] 第五方面,本申请实施例提供了一种终端设备,包括至少一个处理元件和至少一个存储元件,其中该至少一个存储元件用于存储程序和数据,该至少一个处理元件用于执行本申请以上第一方面提供的方法。

[0049] 第六方面,本申请实施例提供了一种通信设备,包括至少一个处理元件和至少一个存储元件,其中该至少一个存储元件用于存储程序和数据,该至少一个处理元件用于执行本申请以上第二方面或第三方面提供的方法。

[0050] 第七方面,本申请实施例提供了一种通信系统,包括终端设备、接口适配功能实体和证书管理功能实体,其中,所述终端设备具有执行本申请第一方面提供的方法的功能,所述接口适配功能实体具有执行本申请第二方面提供的方法的功能,所述证书管理功能实体具有执行本申请第三方面提供的方法的功能。

[0051] 第八方面，本申请实施例还提供了一种计算机程序，当所述计算机程序在计算机上运行时，使得所述计算机执行上述任一方面提供的方法。

[0052] 第九方面，本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序被计算机执行时，使得所述计算机执行上述任一方面提供的方法。

[0053] 第十方面，本申请实施例还提供了一种芯片，所述芯片用于读取存储器中存储的计算机程序，执行上述任一方面提供的方法。

[0054] 第十一方面，本申请实施例还提供了一种芯片系统，该芯片系统包括处理器，用于支持计算机装置实现上述任一方面提供的方法。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器用于保存该计算机装置必要的程序和数据。该芯片系统可以由芯片构成，也可以包含芯片和其他分立器件。

附图说明

[0055] 图1为现有技术提供的证书申请流程和数据传输过程；

[0056] 图2为本申请实施例提供的一种证书管理架构示意图；

[0057] 图3为本申请实施例提供的一种证书申请方法流程图；

[0058] 图4为本申请实施例提供的一种证书申请方法实例流程图；

[0059] 图5为本申请实施例提供的一种证书申请方法实例流程图；

[0060] 图6为本申请实施例提供的一种证书申请方法实例流程图；

[0061] 图7为本申请实施例提供的一种证书申请方法实例流程图；

[0062] 图8为本申请实施例提供的一种通信装置的结构图；

[0063] 图9为本申请实施例提供的一种终端设备的结构图；

[0064] 图10为本申请实施例提供的一种通信设备的结构图。

具体实施方式

[0065] 本申请提供一种证书申请方法及设备，用以在保证终端设备能够与不同证书管理功能实体交互的基础上，减少终端设备内部与证书管理功能实体交互的接口的数量。其中，方法和设备是基于同一技术构思的，由于方法及设备解决问题的原理相似，因此设备与方法的实施可以相互参见，重复之处不再赘述。

[0066] 在本申请实施例提供的方案中，接口适配功能实体能够与为终端设备配置证书的证书管理功能实体交互，当终端设备在需要申请证书时，可以将自身的证书申请参数发送给该接口适配功能实体，从而使所述接口适配功能实体可以根据所述证书申请参数从证书管理功能实体为所述终端设备申请证书，在证书申请成功后再发送给所述终端设备。通过该方案，接口适配功能实体可以向终端设备屏蔽证书管理功能实体的实现或部署，使终端设备可以无感知上层的证书管理功能实体，因此终端设备无需在本地设置与证书管理功能实体交互的接口。显然，在保证终端设备能够与不同证书管理功能实体交互的基础上，该方法可以减少终端设备内部与证书管理功能实体交互的接口的数量。

[0067] 以下，对本申请中的部分用语进行解释说明，以便于本领域技术人员理解。

[0068] 1)、终端设备，是一种向用户提供语音和/或数据连通性的设备。终端设备又可以

称为用户设备(user equipment,UE)、移动台(mobile station,MS)、移动终端(mobile terminal,MT)等。

[0069] 例如,终端设备可以为具有无线连接功能的手持式设备、车载设备等。目前,一些终端设备的举例为:手机(mobile phone)、平板电脑、笔记本电脑、掌上电脑、移动互联网设备(mobile internet device,MID)、智能销售终端(point of sale,POS)、可穿戴设备,虚拟现实(virtual reality,VR)设备、增强现实(augmented reality,AR)设备、工业控制(industrial control)中的无线终端、无人驾驶(self driving)中的无线终端、远程手术(remote medical surgery)中的无线终端、智能电网(smart grid)中的无线终端、运输安全(transportation safety)中的无线终端、智慧城市(smart city)中的无线终端、智慧家庭(smart home)中的无线终端、各类智能仪表(智能水表、智能电表、智能燃气表)、车联网中的智能汽车、车载单元(on board unit,OBU)、路侧单元(road side unit,RSU)、路侧设备(road side equipment,RSE)等。

[0070] 2)、证书管理功能实体,能够对终端设备的身份进行认证,并为终端设备配置证书的实体。示例性的,所述证书管理功能实体可以为PKI或者CA。

[0071] 3)、接口适配功能实体,作为终端设备和证书管理功能实体之间的中间层,是二者之间的接口适配平台,其中设置有与至少一个证书管理功能实体交互的接口,能够通过该接口与相应的证书管理功能实体交互,从而为终端设备申请证书。

[0072] 需要说明的是,所述接口适配功能实体可以为一个单独立的设备,也可以为一组功能耦合的设备集合,还可以是集成在具有其他功能的设备中。示例性的,所述接口适配功能实体可以为服务器或网络设备。

[0073] 4)、密钥对。在非对称加密算法中,存在两种密钥,分为私钥和公钥。私钥和公钥即密钥对。其中,私钥是密钥对生成者持有,不可对外公布;公钥由密钥对生成这公布给其他设备的。密钥对中的两个密钥分别用于发送方和接收方对传输的内容进行加密和解密。

[0074] 5)、消息的签名,为消息的发送方获取待传输消息的摘要,然后使用发送方生成的密钥对中的私钥将所述摘要加密获得的。

[0075] 示例性的,消息的发送方可以根据预设的哈希(hash)算法从待传输消息中获取摘要,可选的,所述hash算法可以为安全哈希算法(secure hash algorithm,SHA)。

[0076] 6)、签名验证,用于消息的接收方验证消息的完整性。签名验证的具体过程为:消息的接收方接收到添加签名的消息后,从获取的消息中获取摘要1;然后接收方使用发送方的公钥对该消息的签名进行解密,得到摘要2;最后,接收方将摘要1和摘要2进行对比,若两个摘要完全相同,则确定签名验证成功,表示接收的消息完整真实可信、中途未被篡改;若两个摘要不同,则确定签名验证失败,表示接收的消息不完整、不安全。

[0077] 7)、证书申请参数,由申请证书的终端设备发送给证书管理功能实体。所述证书申请参数中包含所述终端设备的公钥。可选的,所述证书申请参数中还可以包含所述终端设备的标识等其它信息。

[0078] 8)、多个,是指两个或两个以上。

[0079] 9)、至少一个,是指一个或多个。

[0080] 10)、“和/或”,描述关联对象的关联关系,表示可以存在三种关系,例如,A和/或B,可以表示:单独存在A,同时存在A和B,单独存在B这三种情况。字符“/”一般表示前后关联对

象是一种“或”的关系。

[0081] 另外，需要理解的是，在本申请的描述中，“第一”、“第二”等词汇，仅用于区分描述的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。

[0082] 下面以图1所示的数据传输过程为例，对通信系统中的采用加密算法和证书机制结合方式的数据传输过程进行介绍。

[0083] 其中在传统的数据安全通信网络中，包括多个终端设备以及证书管理功能实体(下面以PKI中的CA为例进行说明)，各个设备之间通过网络进行通信，如图1中的虚线所示。任一个终端设备在进入通信网络后，进行数据传输之前，需要向PKI中的CA申请注册证书，然后根据申请的注册证书进行安全的数据传输。

[0084] 下面以终端设备A申请注册证书为例，对传统的证书申请流程进行描述：

[0085] 终端设备A在启动执行某一项业务时，确定该业务对应的目标CA。然后终端设备A向PKI中的目标CA发送证书请求消息，其中，所述证书请求信息中包含所述终端设备A的证书申请参数：终端设备A生成的密钥对A中的公钥A(可选的，还可以包括所述终端设备A的标识(即身份信息)等其它信息)。PKI中的所述目标CA在接收到所述终端设备A的证书请求消息后，对终端设备A的身份进行认证，在认证终端设备A的身份合法后，将公钥A以及其他相关信息(例如包含所述终端设备A的标识)通过所述目标CA的密钥对C中的私钥C进行加密，从而生成终端设备A的注册证书，然后所述目标CA将终端设备A的注册证书通过证书响应消息发送给终端设备A，完成终端设备A的证书申请/初始注册过程。

[0086] 示例性的，所述目标CA可以但不限于通过以下方式对所述终端设备A的身份进行认证：方式一：所述目标CA根据终端设备A的证书申请参数中的所述终端设备A的标识，对所述终端设备A的身份进行认证。方式二：所述目标CA可以通过传统的身份认证流程，完成对终端设备A的身份认证。例如，所述目标CA向终端设备A发送身份认证请求消息，在从终端设备A接收到身份认证响应消息后，所述目标CA可以根据所述身份认证响应消息，完成对终端设备A的身份认证。

[0087] 需要说明的是，终端设备A在向所述目标CA申请注册证书后，还可以向该目标CA申请匿名证书。其中终端设备A申请匿名证书的过程与上述申请注册证书的过程类似，不同的是，所述目标CA在接收到证书请求消息后，可以不对申请者(终端设备)的身份认证。

[0088] 终端设备A向终端设备B进行数据传输的过程如下：

[0089] 终端设备A在需要向终端设备B发送数据(为了便于和密文对比，后续简称为明文)时，需要根据预设的哈希(hash)算法从所述明文中获取摘要，然后使用自身的密钥对A中的私钥A将所述摘要加密为签名；并且，终端设备A通过本地保存的终端设备B的公钥B将所述明文加密为密文；最后，终端设备A将携带有所述密文、签名，以及终端设备A申请的证书的消息通过网络发送给终端设备B。其中，终端设备A针对待发送的明文，确定签名，并将签名与明文加密后的密文包含在同一消息中发送的过程称为终端设备A对明文的签名处理过程。

[0090] 终端设备B在接收到终端设备A发送的消息之后，得到其中的密文、签名以及证书；然后，终端设备B使用自身的密钥对B中的私钥B将密文解密为明文，并根据以下步骤进行签名验证，以确保该数据的完整性，未被篡改：

[0091] (1)、终端设备B根据预设的hash算法(与终端设备A使用的hash算法相同)，从得到

的明文中获取摘要1。

[0092] (2)、终端设备B根据获取到的CA的根证书(即CA的密钥对中的公钥C)对得到的证书进行解密,得到终端设备A的公钥A。其中,终端设备B可以通过方式获得所述CA的根证书,例如:终端设备B可以向CA请求其根证书,或者终端设备B在安装CA发布的应用时获取其根证书,或者终端设备B在终端设备A发送的消息中获取CA的根证书。

[0093] (3)、终端设备B使用终端设备A的公钥A对得到的所述签名解密,得到其中的摘要2。

[0094] (4)终端设备B对解密获取的摘要2和从明文中获取的摘要1进行对比,当两个摘要完全相同时,终端设备B确定签名验证成功,得到的明文完整未被篡改;当两个摘要不相同时,终端设备B确定签名验证失败,得到的明文不可信。

[0095] 在以上描述的传统的证书申请方法中,终端设备在与目标CA进行通信交互过程中,需要通过内部设置的与该目标CA交互的接口实现。由于不同业务可以对应不同的CA,且不同的CA由不同的建设机构部署,而不同的建立机构可能采用不同的通信技术部署CA,因此,不同的CA可能需要终端设备使用不同的接口进行交互。因此,若终端设备依然采用上述传统的证书申请方法,为了保证终端设备的业务实现的多样性,那么终端设备内部需要设置与多个业务对应的CA进行交互的接口。这就减少终端设备的空闲存储空间,也会增加终端设备的开发成本和开发周期。

[0096] 为了解决上述问题,本申请提供了一种证书申请方法及设备。下面结合附图对本申请实施例进行具体说明。

[0097] 图2示出了本申请提供的证书申请方法适用的证书管理架构。其中,该架构中包含终端设备、接口适配功能实体、至少一个证书管理功能实体等。下面先对该架构中的各个设备的功能进行介绍。

[0098] 终端设备,为通过执行业务为用户提供相应服务的设备。根据不同的应用场景,所述终端设备的表现形式也不同。示例性的,在V2X通信场景中,终端设备可以是车辆、OBU、RSU、RSE等;在传统的移动通信场景中,终端设备可以是手机、平板电脑等;在物联网(internet of things,IoT)通信场景中,终端设备可以是移动互联网设备、可穿戴设备、工业中或家居中的各种无线终端。

[0099] 接口适配功能实体,是终端设备和证书管理功能实体之间的中间层,是二者之间的接口适配平台,其还可以称为接口适配设备。其中,所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口。因此,所述接口适配功能实体可以通过内部的每个接口分别与相应的证书管理功能实体进行交互,从而可以为终端设备申请证书。

[0100] 其中,所述接口适配功能实体可以为一个单独的设备,也可以为一组功能耦合的设备集合,还可以集成在具有其他功能的设备中。示例性的,所述接口适配功能实体可以为部署在云平台的服务器,也可以是传统的服务器或网络设备。

[0101] 在一些实施方式中,终端设备内部可以设置有与所述接口适配功能实体进行交互的特定接口,这样所述终端设备可以通过该接口与所述接口适配功能实体进行通信交互。由于终端设备内部可以通过与所述接口适配功能实体的接口,实现从多个证书管理功能实体申请证书。

[0102] 在另一些实施方式中,终端设备内部无需设置特殊接口即可与所述接口适配功能

实体进行功能。

[0103] 证书管理功能实体，负责终端设备的证书管理，例如证书配置、更新、注销和验证等。具体的，在本申请实施例中，证书管理功能实体是能够对终端设备的身份进行认证，并为终端设备配置证书(包括注册证书和匿名证书)的实体。示例性的，所述证书管理功能实体可以为PKI或者CA。

[0104] 在一些实施方式中，终端设备内部还可以设置有与至少一个证书管理功能实体交互的接口。这样，当所述终端设备需要从所述至少一个证书管理功能实体申请证书时，可以直接通过本地的接口与所述至少一个证书管理功能实体进行通信交互；当所述终端设备需要从其他证书管理功能实体申请证书时，可以通过所述接口适配功能实体实现。

[0105] 其中，在本申请提供的架构中，终端设备或接口适配功能实体与证书管理功能实体交互的接口并非传统意义上的物理接口，而是设备内存储的一组通信配置或通信协议。该接口是通信双方必须共同遵从的一组约定，该接口可以但不限于包含：与该证书管理功能实体建立连接的方式、通信双方的识别方式、通信交互过程中的消息格式、传输方式、交互流程等。

[0106] 需要说明的是，在本申请提供的架构中，终端设备可以通过移动通信网络(包括接入网和核心网)与所述接口适配功能实体建立通信连接，进行通信交互。接口适配功能实体可以通过传统的IP网络与每个证书管理功能实体建立通信连接，进行通信交互。

[0107] 另外，图2所示的架构可以应用到多种通信场景中，例如，第五代(The 5th Generation，5G)通信系统、未来的第六代通信系统和演进的其他通信系统、长期演进(Long Term Evolution，LTE)通信系统、车到万物(vehicle to everything，V2X)、长期演进-车联网(LTE-vehicle，LTE-V)、车到车(vehicle to vehicle，V2V)、车联网、机器类通信(Machine Type Communications，MTC)、物联网(internet of things，IoT)、长期演进-机器到机器(LTE-machine to machine，LTE-M)、机器到机器(machine to machine，M2M)等通信场景中。

[0108] 为了在保证终端设备能够与不同证书管理功能实体交互的基础上，减少终端设备内部与证书管理功能实体交互的接口的数量，本申请实施例提供了一种证书申请方法。下面参阅图3所示流程图对本申请实施例提供的证书申请方法进行详细介绍。

[0109] S301：终端设备在启动执行一项业务时，为了保证该业务的数据传输安全性，所述终端设备向接口适配功能实体发送证书申请参数。相应的，接口适配功能实体从终端设备接收证书申请参数。其中，所述证书申请参数包含所述终端设备的公钥，还可以包含用于表示所述终端设备身份的所述终端设备的标识。在本申请实施例中，所述终端设备发送所述证书申请参数的消息可以称为第一消息。

[0110] 可选的，所述终端设备的标识可以为所述终端设备的设备标识，所述终端设备的IP地址，或者为使用所述终端设备的用户的用户标识，还可以为其他能够唯一标识该终端设备的信息。

[0111] 所述终端设备的公钥为所述终端设备生成的密钥对中的公钥。所述终端设备的公钥用于：在后续所述终端设备的数据传输过程中，接收到所述终端设备签名处理后的消息的其他设备在对所述消息进行签名认证过程中，对签名进行解密。

[0112] S302：所述接口适配功能实体确定为所述终端设备配置证书的目标证书管理功能

实体。

[0113] 其中,所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的目标接口。

[0114] 在本申请实施例中,所述接口适配功能实体可以但不限于通过以下实施方式,确定所述目标证书管理功能实体:

[0115] 第一种实施方式:所述终端设备确定目标证书管理功能实体,并向所述接口适配功能实体发送所述目标证书管理功能实体信息;然后,所述接口适配功能实体可以从所述终端设备获取目标证书管理功能实体信息,并根据所述目标证书管理功能实体信息,确定所述目标证书管理功能实体。

[0116] 在第一种实施例方式中,所述终端设备可以通过但不限于通过以下方式,确定目标证书管理功能实体:

[0117] 方式一:所述终端设备可以根据启动执行的所述业务,确定所述业务对应的目标证书管理功能实体。

[0118] 方式二:所述接口适配功能实体向所述终端设备发送至少一个证书管理功能实体信息,其中,所述至少一个证书管理功能实体信息包含所述目标证书管理功能实体信息,所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口;所述终端设备可以从所述接口适配功能实体接收所述至少一个证书管理功能实体信息后,可以在所述至少一个证书管理功能实体中选择所述目标证书管理功能实体。在本申请实施例中,所述接口适配功能实体发送所述至少一个证书管理功能实体信息的消息可以称为第二消息。

[0119] 可选的,在所述接口适配功能实体向所述终端设备发送所述至少一个证书管理功能实体信息的情况下,所述接口适配功能实体还可以向所述终端设备发送所述至少一个证书管理功能实体的根证书。这样,当所述终端设备在通过所述接口适配功能实体从所述至少一个证书管理功能实体中任一个证书管理功能实体申请证书后,可以根据该证书管理功能实体的根证书,对申请的证书进行验证。

[0120] 可选的,所述接口适配功能实体可以在与所述终端设备建立通信连接的过程中或者在建立通信连接之后,向所述终端设备发送所述第二消息。

[0121] 其中,所述终端设备和所述接口适配功能实体之间的通信连接可以为传输层安全协议(Transport Layer Security,TLS)通道。若所述接口适配功能实体在建立与所述终端设备之间的TLS通道过程中发送所述第二消息时,所述第二消息可以为所述接口适配功能实体向终端设备发送的server_hello消息,certificate消息,server_key_exchange消息,certificate_request消息,server_hello_done消息,change_cipher_spec消息,或finished消息。

[0122] 另外,在本申请实施例中,所述终端设备与所述接口适配功能实体之间的通信交互是通过上述通信连接实现的。

[0123] 在上述第一种实施方式中,在所述终端设备确定目标证书管理功能实体后,可以通过以下方式向所述接口适配功能实体发送所述目标证书管理功能实体信息。在本申请实施例中,所述终端设备发送所述目标证书管理功能实体信息的消息可以称为第三消息。

[0124] 方式一:所述终端设备可以在执行S301之前,向所述接口适配功能实体发送所述第三消息。

[0125] 可选的,所述终端设备可以在与所述接口适配功能实体建立通信连接的过程中或建立通信连接之后,向所述接口适配功能实体发送所述目标证书管理功能实体信息。

[0126] 其中,所述终端设备和所述接口适配功能实体之间的通信连接可以为TLS通道时,当所述终端设备在建立TLS通道时向所述接口适配功能实体发送所述第三消息时,所述第三消息可以为终端设备在接收所述第二消息之后发送的client_hello消息,certificate消息,client_key_exchange消息,certificate_verify消息,change_cipher_spec消息,或finished消息等。

[0127] 方式二:所述终端设备可以在执行S301中,向所述接口适配功能实体发送所述目标证书管理功能实体信息。即所述第一消息包含所述第三消息,或者所述第一消息与所述第三消息为同一个消息。在本方式中,所述第一消息中不仅包含所述证书申请参数,还包含所述目标证书管理功能实体信息。

[0128] 方式三:所述终端设备可以在执行S301之后,向所述接口适配功能实体发送所述第三消息。

[0129] 在第一种实施方式中,当所述终端设备采用上述方式一确定目标证书管理功能实体的情况下,所述接口适配功能实体在收到所述终端设备发送的所述目标证书管理功能实体信息后,可以在确定本地设置有与所述目标证书管理功能实体进行交互的目标接口之后,向所述终端设备发送通知消息,其中,所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

[0130] 可选的,所述通知消息中还可以包括所述目标证书管理功能实体的根证书,该目标证书管理功能实体中的ECA的证书,该目标证书管理功能实体的地址等信息。其中,所述目标证书管理功能实体的根证书可以用于在所述终端设备接收到证书后,对所述证书进行验证。

[0131] 第二种实施方式:所述接口适配功能实体自行确定为终端设备配置证书的所述目标证书管理功能实体。具体的,所述接口适配功能实体获取所述终端设备的标识,并可以根据本地保存的终端设备的标识与证书管理功能实体信息的对应关系,确定所述终端设备的标识对应的所述目标证书管理功能实体信息;然后在根据所述目标证书管理功能实体信息,确定所述目标证书管理功能实体。其中,所述接口适配功能实体可以从所述证书申请参数中获取所述终端设备的标识,或者从包含所述证书申请参数的第一消息中获取所述终端设备的标识。

[0132] S303:所述接口适配功能实体通过所述目标接口向所述目标证书管理功能实体发送所述证书申请参数,以使所述目标证书管理功能实体为所述终端设备配置证书。所述目标证书管理功能实体从所述接口适配功能实体获取所述终端设备的证书申请参数。

[0133] 在本申请实施例中,所述接口适配功能实体可以通过多种实施方式执行S303。

[0134] 第一种实施方式:所述接口适配功能实体根据所述目标接口生成包含所述证书申请参数的第四消息,并将所述第四消息发送给所述目标证书管理功能实体。

[0135] 相应的,所述目标证书管理功能实体可以从所述接口适配功能实体接收包含所述证书申请参数的第四消息,并从所述第四消息中获取所述终端设备的所述证书申请参数。

[0136] 通过上述第一种实施方式,所述接口适配功能实体可以快速地将所述终端设备的证书申请参数传输给所述目标证书管理功能实体,从而可以尽可能降低所述证书申请参数

的传输时延。

[0137] 第二种实施方式，具体包括以下步骤：

[0138] A、所述接口适配功能实体根据所述目标接口生成包含所述证书申请参数的第四消息。

[0139] B、所述接口适配功能实体向所述终端设备发送所述第四消息，以使所述终端设备对所述第四消息进行签名处理，以证明所述第四消息是所述终端设备为请求证书发送的，而非其他设备伪造的。

[0140] C、所述终端设备从所述接口适配功能实体接收所述第四消息后，对所述第四消息进行签名处理，然后再向所述接口适配功能实体发送签名处理后的所述第四消息。

[0141] D、所述接口适配功能实体从终端设备接收签名处理后的所述第四消息，并通过所述目标接口向所述目标证书管理功能实体发送签名处理后的所述第四消息。

[0142] 相应的，所述目标证书管理功能实体可以从所述接口适配功能实体接收签名处理后的第四消息，然后对签名处理后的第四消息进行签名验证，且验证成功。

[0143] 根据所述终端设备对所述第四消息进行签名处理的过程的不同，所述目标证书管理功能实体进行签名验证的过程也不同，例如以下方案：

[0144] 方案一：在上述步骤C中，所述终端设备对所述第四消息进行签名处理包括：所述终端设备先使用预设的hash算法获取所述第四消息的摘要；然后采用所述终端设备的密钥对中的私钥，对所述摘要加密，得到所述第四消息的签名；最后，在所述第四消息中添加该签名，得到签名处理后的所述第四消息。

[0145] 在该情况下，所述目标证书管理功能实体在接收到签名处理后的第四消息后，可以从所述第四消息中获取所述终端设备的公钥，然后使用所述终端设备的公钥对所述第四消息的签名进行解密，得到摘要a；然后所述目标证书管理功能实体使用预设的hash算法(同终端设备使用的hash算法)，获取所述第四消息的摘要b；所述目标证书管理功能实体确定所述摘要a和所述摘要b完全相同时，确定签名验证成功。

[0146] 方案二：在上述步骤C中，所述终端设备对所述第四消息进行签名处理包括：所述终端设备先使用预设的hash算法获取所述第四消息的摘要；然后采用所述终端设备与所述目标证书管理功能实体协商或预设的设备证书，对所述摘要加密，得到所述第四消息的签名；最后，在所述第四消息中添加该签名，得到签名处理后的所述第四消息。

[0147] 在该情况下，所述目标证书管理功能实体在接收到签名处理后的第四消息后，可以使用上述设备证书对应的根证书对所述第四消息的签名进行解密，得到摘要a；然后所述目标证书管理功能实体使用预设的hash算法(同终端设备使用的hash算法)，获取所述第四消息的摘要b；所述目标证书管理功能实体确定所述摘要a和所述摘要b完全相同时，确定签名验证成功。

[0148] 通过该第二种实施方式，所述接口适配功能实体可以通过所述终端设备对所述第四消息进行签名处理，从而在传输给所述目标证书管理功能实体后，所述目标证书管理功能实体可以根据签名证明该第四消息是所述终端设备发送的，是真实合法的。

[0149] 还需要说明的是，在以上两种实施方式中，所述第四消息可以为传统的证书请求消息，还可以为其他消息，本申请对此不作限定。

[0150] 另外，在上述两种实施方式中，根据所述目标接口生成的第四消息格式符合所述

目标接口的对消息格式的规定，因此，后续所述接口适配功能实体可以成功通过所述目标接口将所述第四消息发送给所述目标证书管理功能实体。

[0151] 值得注意的时，所述接口适配功能实体通过与所述目标证书管理功能实体之间的通信连接，与所述目标证书管理功能实体进行通信交互。可选的，所述通信连接也可以为TLS通道，本申请对此不作限定。

[0152] S304：所述目标证书管理功能实体根据所述证书申请参数，为所述终端设备配置证书。

[0153] 在本步骤中，所述目标证书管理功能实体可以采用传统的方法配置证书。

[0154] 例如，所述目标证书管理功能实体可以通过以下步骤配置注册证书：所述目标证书管理功能实体先对所述终端设备的身份进行认证，在认证所述终端设备的身份合法后，使用所述目标证书管理功能实体的私钥，对包含所述终端设备的公钥在内的信息进行加密，从而生成证书。具体身份认证过程和证书配置过程可以参考图1中对传统的证书申请流程的描述，此处不再赘述。

[0155] 另外，所述目标证书管理功能实体配置匿名证书的过程可以参考以上描述，不同的是，所述目标证书管理功能实体可以不对所述终端设备的身份进行认证。

[0156] S305：所述目标证书管理功能实体向所述接口适配功能实体发送所述证书。所述接口适配功能实体通过所述目标接口从所述目标证书管理功能实体接收所述证书。在本申请实施例中，所述目标证书管理功能实体向所述接口适配功能实体发送所述证书的消息可以称为第五消息。

[0157] 在一种实施方式中，所述目标证书管理功能实体可以向所述接口适配功能实体发送所述第五消息。

[0158] 在另一种实施方式中，为了保证所述第五消息为所述目标证书管理功能实体发送的，所述目标证书管理功能实体在发送所述第五消息之前，先对所述第五消息进行签名处理。具体过程包括：所述目标证书管理功能实体先使用预设的hash算法获取所述第五消息的摘要；然后使用所述目标证书管理功能实体的私钥，对所述摘要加密，得到所述第五消息的签名；最后在所述第五消息中添加该签名，得到签名处理后的所述第五消息。

[0159] 其中，所述第五消息可以为传统的证书响应消息，还可以为其他消息，本申请对此不作限定。

[0160] S306：所述接口适配功能实体向所述终端设备发送所述证书。所述终端设备从所述接口适配功能实体接收证书。通过S305的描述可知，所述接口适配功能实体向所述终端设备发送所述证书的消息可以为所述第五消息，还可以为签名处理后的所述第五消息。

[0161] 当所述终端设备接收到签名处理后的所述第五消息时，所述终端设备可以根据存储的所述目标证书管理功能实体的根证书(即公钥)，对签名处理后的所述第五消息进行签名验证。在签名验证成功后，即可使用所述第五消息中的证书进行安全的数据通信。具体的签名验证过程可以参见以上描述，此处不再赘述。

[0162] 还需要说明的是，所述终端设备存储的所述目标证书管理功能实体的根证书可以为用户输入的，或者从所述接口适配功能实体接收的。例如，所述接口适配功能实体在接收到所述终端设备发送的目标证书管理功能实体信息，且确定本地设置有所述目标接口后，向所述终端设备发送通知消息，并在所述通知消息中携带所述目标证书管理功能实体的根

证书。又例如，所述终端设备可以接收所述接口适配功能实体发送的至少一个证书管理功能实体的根证书。再例如，所述接口适配功能实体可以在发送签名处理后的所述第五消息之前，同时或之后，向所述终端设备发送第六消息，所述第六消息中携带所述目标证书管理功能实体的根证书。

[0163] 另外，所述终端设备在签名验证成功后，还可以使用所述目标证书管理功能实体的根证书，对申请到的证书进行验证。即所述终端设备使用所述目标证书管理功能实体的根证书对所述证书进行解密；然后确定解密后得到的信息中是否包含所述终端设备的公钥，若包含，则确定证书验证成功，所述终端设备可以使用所述证书进行安全的数据通信；否则确定证书验证失败，所述终端设备不能使用所述证书。

[0164] 还需要说明的是，在本申请实施例提供的证书申请方法不限定所述证书的类型，上述证书可以为注册证书，还可以为匿名证书。不同的是，当所述证书为匿名证书时，所述目标证书管理功能实体在为所述终端设备配置证书时，可以不对所述终端设备的身份进行验证。

[0165] 此外，在本申请实施例的以上描述中，证书管理功能实体信息用于标识证书管理功能实体，使终端设备或接口适配功能实体能够确定对应的证书管理功能实体。示例性的，证书管理功能实体信息可以为以下至少一项或组合：证书管理功能实体的标识、证书管理功能实体能够配置的证书的类别信息(例如证书标识)、证书管理功能实体建设机构的标识，或证书管理功能实体的网络地址等唯一能够标识证书管理功能实体的信息。

[0166] 本申请实施例提供了一种证书申请方法。在该方法中，接口适配功能实体能够适配至少一种证书管理功能实体的接口，因此终端设备可以通过该接口适配功能实体，实现从不同证书管理功能实体申请证书。通过该方案，接口适配功能实体可以向终端设备屏蔽证书管理功能实体的实现或部署，使终端设备可以无感知上层的证书管理功能实体，因此终端设备无需在本地设置证书管理功能实体交互的接口。显然，在保证终端设备能够与不同证书管理功能实体交互的基础上，该方法可以减少终端设备内部与证书管理功能实体交互的接口的数量。

[0167] 基于以上实施例，本申请还提供了以下证书申请实例。下面结合具体的证书申请实例，示例性的说明图3所示的证书申请方法的流程。在以下实例中，以证书管理功能实体为CA，所述接口适配功能实体为接口适配设备为例进行说明。其中，实例1-实例3为注册证书申请流程，实例4为匿名证书申请流程。需要说明的是，在以下实例中，涉及的(目标)CA信息可以为以下至少一项或组合：该CA的标识、该CA能够配置的证书的类别信息(例如证书标识)，或该CA的网络地址。

[0168] 实例1：下面参阅图4所示流程图，对本实例的证书申请流程进行详细介绍。

[0169] S401：终端设备有注册证书申请需求时，确定目标CA，然后与接口适配设备建立TLS通道；并在建立TLS通道过程中，将目标CA信息发送给所述接口适配设备。

[0170] 其中，所述终端设备内部存储有所述接口适配设备的根证书，且所述接口适配设备内部也存储有所述终端设备的根证书。这样，所述终端设备和所述接口适配设备可以根据各自存储的对方的根证书，建立二者之间的TLS通道。

[0171] 在本申请实施例中所述终端设备和所述接口适配设备可以采用传统的方法建立TLS通道。可选的，所述终端设备可以利用在建立TLS通道中向所述接口适配设备发送的消

息发送所述目标CA信息。示例性的，携带所述目标CA信息的消息可以为所述终端设备发送的client_hello消息，certificate消息，client_key_exchange消息，certificate_verify消息，change_cipher_spec消息，或finished消息等。

[0172] 另外，在所述终端设备与所述接口适配设备之间的TLS通道建立后，所述终端设备与所述接口适配设备之间的交互，可以通过所述TLS通道传输，以保证传输安全。

[0173] S402：所述接口适配设备根据所述目标CA信息，确定所述目标CA，并确定本地设置有与所述目标CA交互的目标接口。

[0174] S403：所述接口适配设备向所述终端设备发送通知消息，以通知所述终端设备所述接口适配设备中设置有与所述CA交互的所述目标接口。其中，所述通知消息中还携带有所述目标CA的根证书。

[0175] S404：所述接口适配设备确定所述目标CA之后，确定是否与所述目标CA建立通信连接(例如TLS通道)。若所述接口适配设备确定未与所述目标CA建立TLS通道，则启动建立TLS通道流程。若所述接口适配设备确定已建立与所述目标CA之间的TLS通道，则无需执行S404。

[0176] 与所述终端设备与所述接口适配设备建立TLS通道类似的，所述接口适配设备与所述目标CA均存储有对方的根证书。这样，所述接口适配设备与所述目标CA可以根据各自存储的对方的根证书，建立二者之间的TLS通道。

[0177] 另外，在所述接口适配设备与所述目标CA之间的TLS通道建立后，所述终端设备与所述接口适配设备之间的交互，可以均通过所述TLS通道传输，以保证传输安全。

[0178] S405：所述终端设备接收到所述通知消息后，向所述接口适配设备发送证书申请参数。其中，所述证书申请参数中包含所述终端设备的公钥，还可以包含所述终端设备的标识等身份信息。

[0179] S406：所述接口适配设备根据目标接口生成包含所述证书申请参数的证书请求消息。其中，所述证书请求消息的格式符合所述目标接口的规定。

[0180] S407：所述接口适配设备向所述终端设备发送所述证书请求消息。

[0181] S408：所述终端设备接收所述证书请求消息后，对所述证书请求消息进行签名处理，以证明所述第证书请求消息是所述终端设备发送的。具体的签名处理过程可以参考图3所示的实施例中S303中的记载的两个方案，此处不再赘述。

[0182] S409：所述终端设备向所述接口适配设备发送签名处理后的证书请求消息。

[0183] S410：所述接口适配设备在接收到所述终端设备发送的签名处理后的所述证书请求消息后，通过所述目标接口向所述目标CA发送该签名处理后的所述证书请求消息。

[0184] S411：所述目标CA接收到签名处理后的所述证书请求消息后，对所述证书请求消息进行签名验证，并在签名验证成功后，根据所述证书请求消息中的证书申请参数，为所述终端设备配置注册证书。

[0185] 其中，所述目标CA对所述证书请求消息的签名验证过程也可以参考图3所示的实施例中S303中的记载的两个方案，此处不再赘述。

[0186] 在本申请实施例中，所述目标CA为所述终端设备配置注册证书的过程可以图1中的真书申请过程，或者图3所示的实施例中S304中的描述，此处不再赘述。

[0187] S412：所述目标CA生成包含所述注册证书的证书响应消息，并对所述证书响应消

息进行签名处理，然后向所述接口适配设备发送所述签名处理后的所述证书响应消息。

[0188] S413：所述接口适配设备从所述目标CA接收所述签名处理后的所述证书响应消息后，使用所述目标CA的根证书，对签名处理后的所述证书响应消息进行签名验证，在验证成功后，还可以使用所述目标CA的根证书，对所述注册证书进行验证。所述终端设备在确定所述注册证书验证成功后，可以使用所述注册证书进行安全的数据通信。

[0189] 其中，所述终端设备对所述注册证书进行验证的过程可以参考图3所示的实施例中的S306中的描述，此处不再赘述。

[0190] 实例2：下面参阅图5所示的流程图，对本实例的证书申请流程进行详细介绍。

[0191] S501：终端设备与接口适配设备建立TLS通道。

[0192] 其中，所述终端设备内部存储有所述接口适配设备的根证书，且所述接口适配设备内部也存储有所述终端设备的根证书。这样，所述终端设备和所述接口适配设备可以根据各自存储的对方的根证书，建立二者之间的TLS通道。

[0193] 另外，在所述终端设备与所述接口适配设备之间的TLS通道建立后，所述终端设备与所述接口适配设备之间的交互，可以通过所述TLS通道传输，以保证传输安全。

[0194] S502：所述接口适配设备向所述终端设备发送至少一个CA信息，其中，所述接口适配设备中设置有与该至少一个CA交互的接口。

[0195] 可选的，所述接口适配设备还可以向所述终端设备发送所述至少一个CA的根证书，用于后续对注册证书进行验证。

[0196] S503：所述终端设备从所述接口适配设备接收并保存所述至少一个CA信息。在所述终端设备有注册证书申请需求时，在所述至少一个CA中确定目标CA，并向所述皆苦适配设备发送证书申请参数和所述目标CA信息。

[0197] S504：所述接口适配设备在接收到所述证书申请参数和所述目标CA信息后，根据所述目标CA信息，确定目标CA。

[0198] S505：所述接口适配设备确定所述目标CA之后，确定是否与所述目标CA建立通信连接(例如TLS通道)。若所述接口适配设备确定未与所述目标CA建立TLS通道，则启动建立TLS通道流程。若所述接口适配设备确定已建立与所述目标CA之间的TLS通道，则无需执行S505。

[0199] 与所述终端设备与所述接口适配设备建立TLS通道类似的，所述接口适配设备与所述目标CA均存储有对方的根证书。这样，所述接口适配设备与所述目标CA可以根据各自存储的对方的根证书，建立二者之间的TLS通道。

[0200] 另外，在所述接口适配设备与所述目标CA之间的TLS通道建立后，所述终端设备与所述接口适配设备之间的交互，可以均通过所述TLS通道传输，以保证传输安全。

[0201] 在本实例中，其余步骤S506-S513与实例1中的S406-S413相同，因此，这些步骤的具体过程可以参考实例1对相关步骤的具体描述，此处不再赘述。

[0202] 实例3：下面参阅图6所示的流程图，对本实例的证书申请流程进行详细介绍。

[0203] S601：同实例2中的S501，终端设备与接口适配设备建立TLS通道。

[0204] S602：所述终端设备在有注册证书申请需求时，确定目标CA，向所述接口适配设备发送证书申请参数和目标CA信息。

[0205] S603：所述接口适配设备根据所述目标CA信息，确定所述目标CA，并确定本地设置

有与所述目标CA交互的目标接口。

[0206] S604:所述接口适配设备向所述终端设备发送通知消息,以通知所述终端设备所述接口适配设备中设置有与所述CA交互的所述目标接口。其中,所述通知消息中还携带有所述目标CA的根证书。

[0207] 在本实例中,其余步骤S605-613与实例2中的S505-S513相同,此处不再赘述。

[0208] 实例4:匿名证书申请流程是在注册证书申请流程之后进行,即终端设备与接口适配设备之间,以及接口适配设备与目标CA之间已经建立TLS通道。因此,在本实例中不涉及建立TLS通道的步骤。下面参阅图7所示的流程图,对本实例的证书申请流程进行详细介绍。

[0209] S701:在终端设备有匿名证书申请需求时,向接口适配设备发送证书申请参数。

[0210] S702:所述接口适配设备从所述终端设备接收证书申请参数后,根据本地保存的终端设备的标识与CA的对应关系,确定所述证书申请参数中终端设备的标识对应的目标CA。然后,所述接口适配设备根据设置的与所述目标CA交互的目标接口,生成包含所述证书申请参数的整数请求消息。

[0211] 其中,所述接口适配设备在每个终端设备申请注册证书时,均建立该终端设备的标识与为其配置注册证书的CA的对应关系。这样,当任一个终端设备申请注册证书后,再申请匿名证书时,所述接口适配设备可以快速地确定目标CA。

[0212] 在本实例中,其余步骤S703-S709与实例1中的S407-S413相同,因此,这些步骤的具体过程可以参考实例1对相关步骤的具体描述,此处不再赘述。

[0213] 基于相同的技术构思,本申请还提供了一种通信装置,该装置的结构如图8所示,包括通信单元801和处理单元802。所述通信装置800可以应用于图2所示的证书管理架构中的终端设备、接口适配功能实体或证书管理功能实体,并可以实现图3-图7所示证书申请方法。下面对装置800中的各个单元的功能进行介绍。

[0214] 所述通信单元801,用于接收和发送数据。

[0215] 当所述通信装置800应用于终端设备时,所述通信单元801又可以称为收发器,可以通过移动通信模块和/或无线通信模块实现。

[0216] 移动通信模块可以提供应用在所述终端设备上的包括2G/3G/4G/5G等无线通信的解决方案。移动通信模块可以包括至少一个天线、至少一个滤波器,开关,功率放大器,低噪声放大器(low noise amplifier,LNA)等。所述终端设备可以通过所述移动通信模块接入移动通信网络中,进而通过所述移动通信网络接入所述证书管理架构。

[0217] 无线通信模块可以提供应用在终端设备上的包括无线局域网(wireless local area networks,WLAN)(如无线保真(wireless fidelity,Wi-Fi)网络),蓝牙(bluetooth,BT),全球导航卫星系统(global navigation satellite system,GNSS),调频(frequency modulation,FM),近距离无线通信技术(near field communication,NFC)等无线通信的解决方案。无线通信模块160可以包括至少一个天线、至少一个通信处理模块的一个或多个器件。所述终端设备可以通过所述无线通信模块接入无线通信网络中,进而通过所述无线通信网络接入所述证书管理架构。

[0218] 当所述通信装置800应用于接口适配功能实体或证书管理功能实体时,所述通信单元801又可以称为物理接口、通信模块、通信接口、输入输出接口。接口适配功能实体或证书管理功能实体可以通过该通信单元连接网线或电缆,进而与其他设备建立物理连接。

[0219] 下面对所述通信装置800应用于终端设备时，所述处理单元802的功能进行介绍。

[0220] 处理单元802，用于通过所述通信单元801向接口适配功能实体发送证书申请参数；以及通过所述通信单元801从所述接口适配功能实体接收证书，所述证书为目标证书管理功能实体为所述终端设备配置的。

[0221] 在一种实施方式中，所述处理单元802，还用于：

[0222] 在通过所述通信单元801向所述接口适配功能实体发送所述证书申请参数之后，在通过所述通信单元801从所述接口适配功能实体接收所述证书之前，通过所述通信单元801从所述接口适配功能实体接收证书请求消息，其中所述证书请求消息中包含所述证书申请参数；

[0223] 对所述证书请求消息进行签名处理；

[0224] 通过所述通信单元801向所述接口适配功能实体发送签名处理后的所述证书请求消息，以使所述接口适配功能实体将签名处理后的所述证书请求消息转发给所述目标证书管理功能实体；

[0225] 所述处理单元802，在通过所述通信单元801从所述接口适配功能实体接收所述证书时，具体用于：

[0226] 通过所述通信单元801从所述接口适配功能实体接收证书响应消息，其中，所述证书响应消息为所述接口适配功能实体从所述目标证书管理功能实体接收的，所述证书响应消息中包含所述证书。

[0227] 在一种实施方式中，所述处理单元802，还用于：

[0228] 在通过所述通信单元801从所述接口适配功能实体接收所述证书之前，通过所述通信单元801向所述接口适配功能实体发送所述目标证书管理功能实体信息。

[0229] 在一种实施方式中，所述处理单元802，还用于：

[0230] 在通过所述通信单元801向所述接口适配功能实体发送所述目标证书管理功能实体信息之后，通过所述通信单元801从所述接口适配功能实体接收到通知消息，其中，所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

[0231] 在一种实施方式中，所述通知消息包含所述目标证书管理功能实体的根证书；

[0232] 所述处理单元802，还用于：

[0233] 在通过所述通信单元801从所述接口适配功能实体接收所述证书响应消息之后，根据所述目标证书管理功能实体的根证书，对所述证书响应消息中包含的证书进行验证。

[0234] 在一种实施方式中，所述处理单元802，还用于：

[0235] 在通过所述通信单元801向所述接口适配功能实体发送所述目标证书管理功能实体信息之前，通过所述通信单元801从所述接口适配功能实体接收至少一个证书管理功能实体信息，其中，所述至少一个证书管理功能实体信息包含所述目标证书管理功能实体信息，所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口；

[0236] 在所述至少一个证书管理功能实体中选择所述目标证书管理功能实体。

[0237] 下面对所述通信装置800应用于接口适配功能实体时，所述处理单元802的功能进行介绍。

[0238] 处理单元802，用于通过所述通信单元801从终端设备接收证书申请参数；确定为

所述终端设备配置证书的目标证书管理功能实体;通过所述通信单元801向所述目标证书管理功能实体发送所述证书申请参数,以使所述目标证书管理功能实体根据所述证书申请参数为所述终端设备配置证书;通过所述通信单元801从所述目标证书管理功能实体接收所述证书,并通过所述通信单元801向所述终端设备发送所述证书。

[0239] 在一种实施方式中,所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的目标接口;

[0240] 所述处理单元802,在通过所述通信单元801向所述目标证书管理功能实体发送所述证书申请参数时,具体用于:

[0241] 根据所述通信单元801和所述目标接口向所述目标证书管理功能实体发送所述证书申请参数;

[0242] 所述处理单元802,在通过所述通信单元801从所述目标证书管理功能实体接收所述证书时,具体用于:

[0243] 根据所述通信单元801和所述目标接口从所述目标证书管理功能实体接收所述证书。

[0244] 在一种实施方式中,所述处理单元802,在根据所述通信单元801和所述目标接口向所述目标证书管理功能实体发送所述证书申请参数时,具体用于:

[0245] 根据所述目标接口生成包含所述证书申请参数的证书请求消息,并通过所述通信单元801向所述终端设备发送所述证书请求消息;通过所述通信单元801从终端设备接收签名处理后的所述证书请求消息,并根据所述通信单元801和所述目标接口向所述目标证书管理功能实体发送签名处理后的所述证书请求消息;

[0246] 所述处理单元802,在通过所述通信单元801从所述目标证书管理功能实体接收所述证书时,具体用于:

[0247] 通过所述通信单元801从所述目标证书管理功能实体接收证书响应消息,其中,所述证书响应消息中包含所述目标证书管理功能实体为所述终端设备配置的所述证书;

[0248] 所述处理单元802,在通过所述通信单元801向所述终端设备发送所述证书时,具体用于:

[0249] 通过所述通信单元801向所述终端设备所述证书响应消息。

[0250] 在一种实施方式中,所述处理单元802,在确定为所述终端设备配置证书的目标证书管理功能实体时,具体用于:

[0251] 通过所述通信单元801从所述终端设备接收所述目标证书管理功能实体信息,根据所述目标证书管理功能实体信息,确定所述目标证书管理功能实体;或者

[0252] 确定所述终端设备的标识,并根据本地保存的终端设备的标识与证书管理功能实体信息的对应关系,确定与所述终端设备的标识对应的所述目标证书管理功能实体信息;根据所述目标证书管理功能实体信息,确定所述目标证书管理功能实体。

[0253] 在一种实施方式中,所述处理单元802,还用于:在通过所述通信单元801从所述终端设备接收所述目标证书管理功能实体信息之后,确定本地设置有与所述目标证书管理功能实体交互的目标接口,通过所述通信单元801向所述终端设备发送通知消息,其中,所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

[0254] 在一种实施方式中,所述通知消息中包含所述目标证书管理功能实体的根证书。

[0255] 在一种实施方式中,所述处理单元802,还用于:

[0256] 在通过所述通信单元801从所述终端设备接收所述目标证书管理功能实体信息之前,通过所述通信单元801向所述终端设备发送至少一个证书管理功能实体信息,其中,所述至少一个证书管理功能实体中包含所述目标证书管理功能实体,所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口。

[0257] 下面对所述通信装置800应用于证书管理功能实体时,所述处理单元802的功能进行介绍。

[0258] 处理单元802,用于通过所述通信单元801从接口适配功能实体接收终端设备的证书申请参数;根据所述证书申请参数,为所述终端设备配置证书;以及通过所述通信单元801向所述接口适配功能实体发送所述证书。

[0259] 在一种实施方式中,所述处理单元802,在通过所述通信单元801从接口适配功能实体接收所述终端设备的所述证书申请参数时,具体用于:

[0260] 通过所述通信单元801从所述接口适配功能实体接收所述终端设备签名处理后的证书请求消息,其中,所述证书请求消息中包含所述证书申请参数;

[0261] 所述处理单元802,还用于:

[0262] 在根据所述证书申请参数,为所述终端设备配置证书之前,对签名处理后的所述证书请求消息进行签名验证,且验证成功;

[0263] 所述处理单元802,在通过所述通信单元801向所述接口适配功能实体发送所述证书时,具体用于:

[0264] 通过所述通信单元801向所述接口适配功能实体发送证书响应消息,其中,所述证书响应消息中包含所述证书。

[0265] 基于相同的技术构思,本申请还提供了一种终端设备,所述终端设备可以应用于如图2所示的证书管理架构中,可以实现图3-图7所示证书申请方法中终端设备的功能。参阅图9所示,所述终端设备包括:收发器901、处理器902以及存储器903。其中,所述收发器901、所述处理器902以及所述存储器903之间相互连接。

[0266] 可选的,所述收发器901、所述处理器902以及所述存储器903之间通过总线904相互连接。所述总线904可以是外设部件互连标准(peripheral component interconnect,PCI)总线或扩展工业标准结构(extended industry standard architecture,EISA)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图9中仅用一条粗线表示,但并不表示仅有一根总线或一种类型的总线。

[0267] 所述收发器901,用于接收和发送数据,实现与其他设备之间的通信交互。示例性的,所述收发器901可以通过移动通信模块和/或无线通信模块实现。

[0268] 所述处理器902,用于通过所述收发器901向接口适配功能实体发送证书申请参数;以及通过所述收发器901从所述接口适配功能实体接收证书,所述证书为目标证书管理功能实体为所述终端设备900配置的。

[0269] 可选的,所述处理器902,还用于:

[0270] 在通过所述收发器901向所述接口适配功能实体发送所述证书申请参数之后,在通过所述收发器901从所述接口适配功能实体接收所述证书之前,通过所述收发器901从所

述接口适配功能实体接收证书请求消息，其中所述证书请求消息中包含所述证书申请参数；

[0271] 对所述证书请求消息进行签名处理；

[0272] 通过所述收发器901向所述接口适配功能实体发送签名处理后的所述证书请求消息，以使所述接口适配功能实体将签名处理后的所述证书请求消息转发给所述目标证书管理功能实体；

[0273] 所述处理器902，在通过所述通信单元从所述接口适配功能实体接收所述证书时，具体用于：

[0274] 通过所述收发器901从所述接口适配功能实体接收证书响应消息，其中，所述证书响应消息为所述接口适配功能实体从所述目标证书管理功能实体接收的，所述证书响应消息中包含所述证书。

[0275] 可选的，所述处理器902，还用于：

[0276] 在通过所述收发器901从所述接口适配功能实体接收所述证书之前，通过所述收发器901向所述接口适配功能实体发送所述目标证书管理功能实体信息。

[0277] 可选的，所述处理器902，还用于：

[0278] 在通过所述收发器901向所述接口适配功能实体发送所述目标证书管理功能实体信息之后，通过所述收发器901从所述接口适配功能实体接收到通知消息，其中，所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

[0279] 可选的，所述通知消息包含所述目标证书管理功能实体的根证书；所述处理器902，还用于：

[0280] 在通过所述收发器901从所述接口适配功能实体接收所述证书响应消息之后，根据所述目标证书管理功能实体的根证书，对所述证书响应消息中包含的证书进行验证。

[0281] 可选的，所述处理器902，还用于：

[0282] 在通过所述收发器901向所述接口适配功能实体发送所述目标证书管理功能实体信息之前，通过所述收发器901从所述接口适配功能实体接收至少一个证书管理功能实体信息，其中，所述至少一个证书管理功能实体信息包含所述目标证书管理功能实体信息，所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口；

[0283] 在所述至少一个证书管理功能实体中选择所述目标证书管理功能实体。

[0284] 所述存储器903，用于存放程序指令和数据等。具体地，程序指令可以包括程序代码，该程序代码包括计算机操作指令。存储器903可能包含随机存取存储器(random access memory，RAM)，也可能还包括非易失性存储器(non-volatile memory)，例如至少一个磁盘存储器。处理器902执行存储器903所存放的程序指令，并使用所述存储器903中存储的数据，实现上述功能，从而实现上述实施例提供的证书管理方法。

[0285] 基于相同的技术构思，本申请还提供了一种通信设备，所述通信设备可以应用于如图2所示的证书管理架构中，可以实现图3-图7所示证书申请方法中接口适配功能实体或证书管理功能实体的功能。参阅图10所示，所述通信设备包括：通信模块1001、处理器1002以及存储器1003。其中，所述收发器1001、所述处理器1002以及所述存储器1003之间相互连接。

[0286] 可选的，所述通信模块1001、所述处理器1002以及所述存储器1003之间通过总线1004相互连接。所述总线1004可以是外设部件互连标准(peripheral component interconnect，PCI)总线或扩展工业标准结构(extended industry standard architecture，EISA)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图10中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0287] 所述通信模块1001，用于接收和发送数据，实现与其他设备之间的通信交互。示例性的，所述通信模块1001可以通过物理接口实现。

[0288] 在一种实施方式中，所述通信设备1000应用于接口适配功能实体中，所述处理器1002具体用于：

[0289] 通过所述通信模块1001从终端设备接收证书申请参数；确定为所述终端设备配置证书的目标证书管理功能实体；通过所述通信模块1001向所述目标证书管理功能实体发送所述证书申请参数，以使所述目标证书管理功能实体根据所述证书申请参数为所述终端设备配置证书；通过所述通信模块1001从所述目标证书管理功能实体接收所述证书，并通过所述通信模块1001向所述终端设备发送所述证书。

[0290] 可选的，所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的目标接口；所述处理器1002，在通过所述通信模块1001向所述目标证书管理功能实体发送所述证书申请参数时，具体用于：根据所述通信模块1001和所述目标接口向所述目标证书管理功能实体发送所述证书申请参数；

[0291] 所述处理器1002，在通过所述通信模块1001从所述目标证书管理功能实体接收所述证书时，具体用于：根据所述通信模块1001和所述目标接口从所述目标证书管理功能实体接收所述证书。

[0292] 可选的，所述处理器1002，在根据所述通信模块1001和所述目标接口向所述目标证书管理功能实体发送所述证书申请参数时，具体用于：

[0293] 根据所述目标接口生成包含所述证书申请参数的证书请求消息，并通过所述通信模块1001向所述终端设备发送所述证书请求消息；通过所述通信模块1001从终端设备接收签名处理后的所述证书请求消息，并根据所述通信模块1001和所述目标接口向所述目标证书管理功能实体发送签名处理后的所述证书请求消息；

[0294] 所述处理器1002，在通过所述通信模块1001从所述目标证书管理功能实体接收所述证书时，具体用于：通过所述通信模块1001从所述目标证书管理功能实体接收证书响应消息，其中，所述证书响应消息中包含所述目标证书管理功能实体为所述终端设备配置的所述证书；

[0295] 所述处理器1002，在通过所述通信模块1001向所述终端设备发送所述证书时，具体用于：通过所述通信模块1001向所述终端设备所述证书响应消息。

[0296] 可选的，所述处理器1002，在确定为所述终端设备配置证书的目标证书管理功能实体时，具体用于：

[0297] 通过所述通信模块1001从所述终端设备接收所述目标证书管理功能实体信息，根据所述目标证书管理功能实体信息，确定所述目标证书管理功能实体；或者

[0298] 确定所述终端设备的标识，并根据本地保存的终端设备的标识与证书管理功能实体信息的对应关系，确定与所述终端设备的标识对应的所述目标证书管理功能实体信息；

根据所述目标证书管理功能实体信息，确定所述目标证书管理功能实体。

[0299] 可选的，所述处理器1002，还用于：在通过所述通信模块1001从所述终端设备接收所述目标证书管理功能实体信息之后，确定本地设置有与所述目标证书管理功能实体交互的目标接口，通过所述通信模块1001向所述终端设备发送通知消息，其中，所述通知消息用于通知所述终端设备所述接口适配功能实体中设置有与所述目标证书管理功能实体交互的所述目标接口。

[0300] 可选的，所述通知消息中包含所述目标证书管理功能实体的根证书。

[0301] 可选的，所述处理器1002，还用于：

[0302] 在通过所述通信模块1001从所述终端设备接收所述目标证书管理功能实体信息之前，通过所述通信模块1001向所述终端设备发送至少一个证书管理功能实体信息，其中，所述至少一个证书管理功能实体中包含所述目标证书管理功能实体，所述接口适配功能实体中设置有与所述至少一个证书管理功能实体交互的接口。

[0303] 在另一种实施方式中，所述通信设备1000应用于证书管理功能实体中，所述处理器1002具体用于：

[0304] 通过所述通信模块1001从接口适配功能实体接收终端设备的证书申请参数；根据所述证书申请参数，为所述终端设备配置证书；以及通过所述通信模块1001向所述接口适配功能实体发送所述证书。

[0305] 可选的，所述处理器1002，在通过所述通信模块1001从接口适配功能实体接收所述终端设备的所述证书申请参数时，具体用于：通过所述通信模块1001从所述接口适配功能实体接收所述终端设备签名处理后的证书请求消息，其中，所述证书请求消息中包含所述证书申请参数；

[0306] 所述处理器1002，还用于：在根据所述证书申请参数，为所述终端设备配置证书之前，对签名处理后的所述证书请求消息进行签名验证，且验证成功；

[0307] 所述处理器1002，在通过所述通信模块1001向所述接口适配功能实体发送所述证书时，具体用于：通过所述通信模块1001向所述接口适配功能实体发送证书响应消息，其中，所述证书响应消息中包含所述证书。

[0308] 所述存储器1003，用于存放程序指令和数据等。具体地，程序指令可以包括程序代码，该程序代码包括计算机操作指令。存储器1003可能包含随机存取存储器(random access memory，RAM)，也可能还包括非易失性存储器(non-volatile memory)，例如至少一个磁盘存储器。处理器1002执行存储器1003所存放的程序指令，并使用所述存储器1003中存储的数据，实现上述功能，从而实现上述实施例提供的证书管理方法。

[0309] 可以理解，本申请图9和图10中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(Read-Only Memory，ROM)、可编程只读存储器(Programmable ROM，PROM)、可擦除可编程只读存储器(Erasable PROM，EPROM)、电可擦除可编程只读存储器(Electrically EPROM，EEPROM)或闪存。易失性存储器可以是随机存取存储器(Random Access Memory，RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的RAM可用，例如静态随机存取存储器(Static RAM，SRAM)、动态随机存取存储器(Dynamic RAM，DRAM)、同步动态随机存取存储器(Synchronous DRAM，SDRAM)、双倍数据速率同步动态随机存取存储器(Double Data Rate

SDRAM,DDR SDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM,ESDRAM)、同步连接动态随机存取存储器(Synchlink DRAM,SLDRAM)和直接内存总线随机存取存储器(Direct Rambus RAM,DR RAM)。应注意,本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

[0310] 基于以上实施例,本申请实施例还提供了一种计算机程序,当所述计算机程序在计算机上运行时,使得所述计算机执行图3-图7所示的实施例提供的证书申请方法。

[0311] 基于以上实施例,本申请实施例还提供了一种计算机可读存储介质,该计算机可读存储介质中存储有计算机程序,所述计算机程序被计算机执行时,使得计算机执行图3-图7所示的实施例提供的证书申请方法。其中,存储介质可以是计算机能够存取的任何可用介质。以此为例但不限于:计算机可读介质可以包括RAM、ROM、EEPROM、CD-ROM或其他光盘存储、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质。

[0312] 基于以上实施例,本申请实施例还提供了一种芯片,所述芯片用于读取存储器中存储的计算机程序,实现图3-图7所示的实施例提供的证书申请方法。

[0313] 基于以上实施例,本申请实施例提供了一种芯片系统,该芯片系统包括处理器,用于支持计算机装置实现图3-图7所示的实施例中终端设备、接口适配功能实体或证书管理功能实体所涉及的功能。在一种可能的设计中,所述芯片系统还包括存储器,所述存储器用于保存该计算机装置必要的程序和数据。该芯片系统,可以由芯片构成,也可以包含芯片和其他分立器件。

[0314] 综上所述,本申请提供了一种证书申请方法及设备。在该方案中,接口适配功能实体能够与为终端设备配置证书的证书管理功能实体交互,当终端设备在需要申请证书时,可以将自身的证书申请参数发送给该接口适配功能实体,从而使所述接口适配功能实体可以根据所述证书申请参数从证书管理功能实体为所述终端设备申请证书,在证书申请成功后再发送给所述终端设备。通过该方案,接口适配功能实体可以向终端设备屏蔽证书管理功能实体的实现或部署,使终端设备可以无感知上层的证书管理功能实体,因此终端设备无需在本地设置与证书管理功能实体交互的接口。显然,在保证终端设备能够与不同证书管理功能实体交互的基础上,该方法可以减少终端设备内部与证书管理功能实体交互的接口的数量。

[0315] 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用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0316] 本申请是参照根据本申请的方法、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、嵌入式处理机或其他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他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/或方框图一个方框或多个方框中指定的功能的装置。

[0317] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，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。

[0318] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在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。

[0319] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

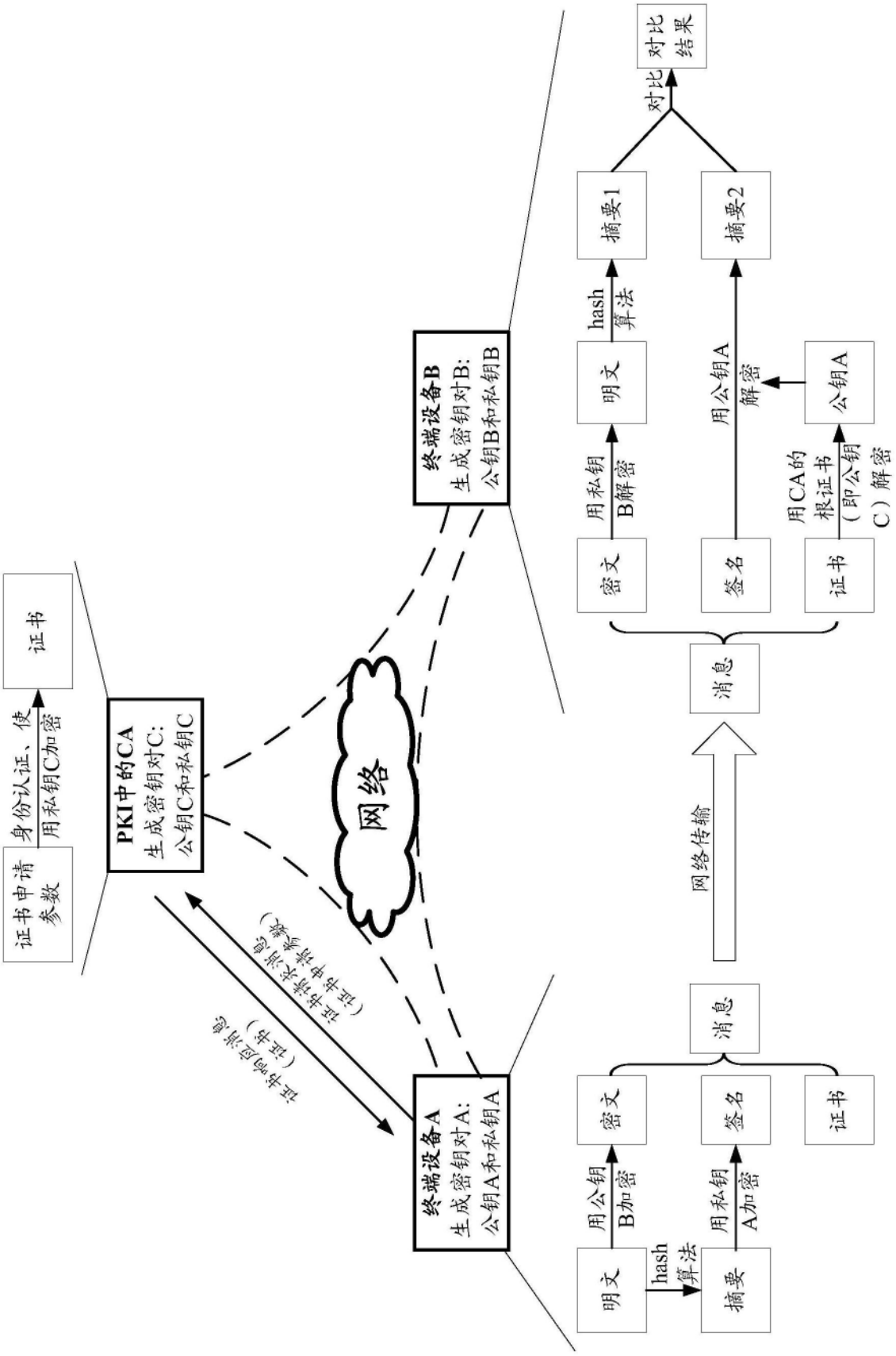

证书申请参数
身份认证、使用私钥C加密
证书
PKI中的CA
生成密钥对C:
公钥C和私钥C
网络
终端设备A
生成密钥对A:
公钥A和私钥A
终端设备B
生成密钥对B:
公钥B和私钥B
证书响应消息（证书）
证书请求消息（证书申请参数）
网络传输
明文
hash算法
摘要
用私钥A加密
签名
用公钥B加密
密文
消息
证书
用CA的根证书（即公钥C）解密
公钥A
用公钥A解密
用私钥B解密
hash算法
摘要1
摘要2
明文
密文
签名
证书
消息
对比结果

图1

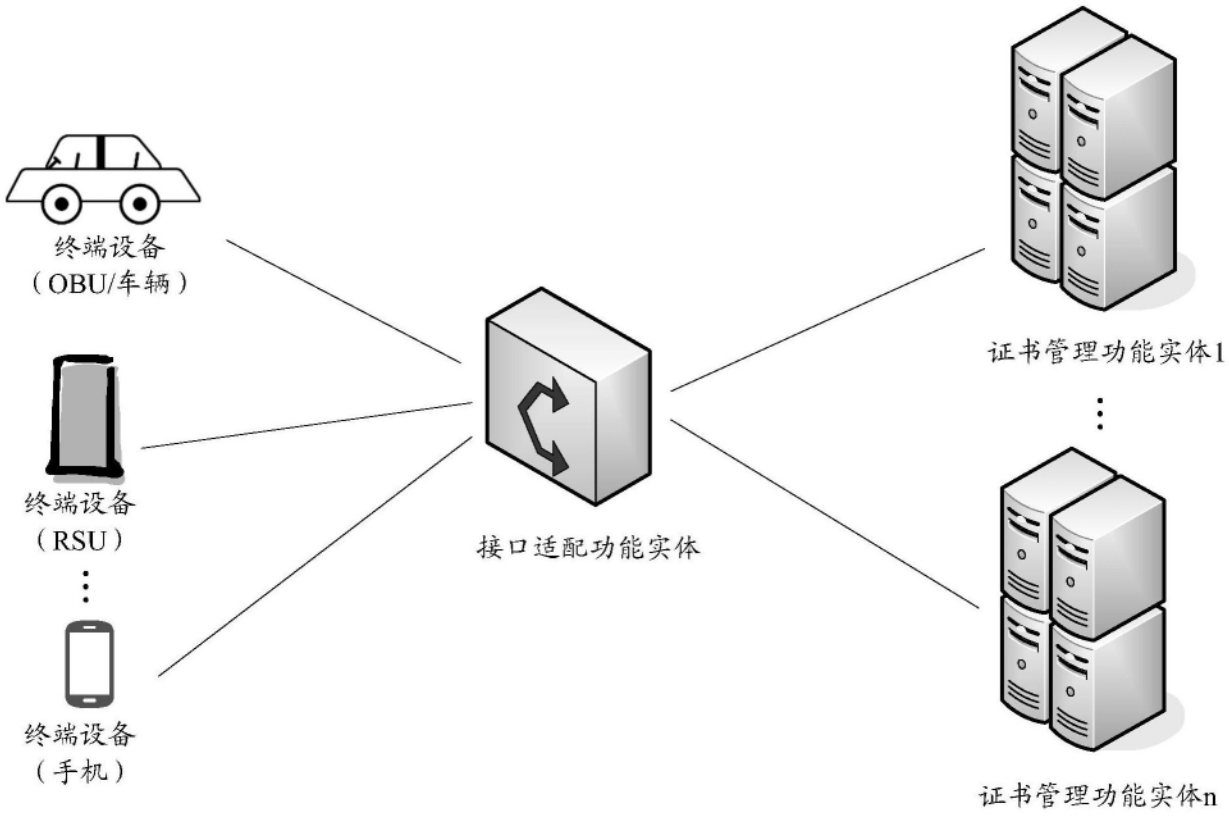


图2

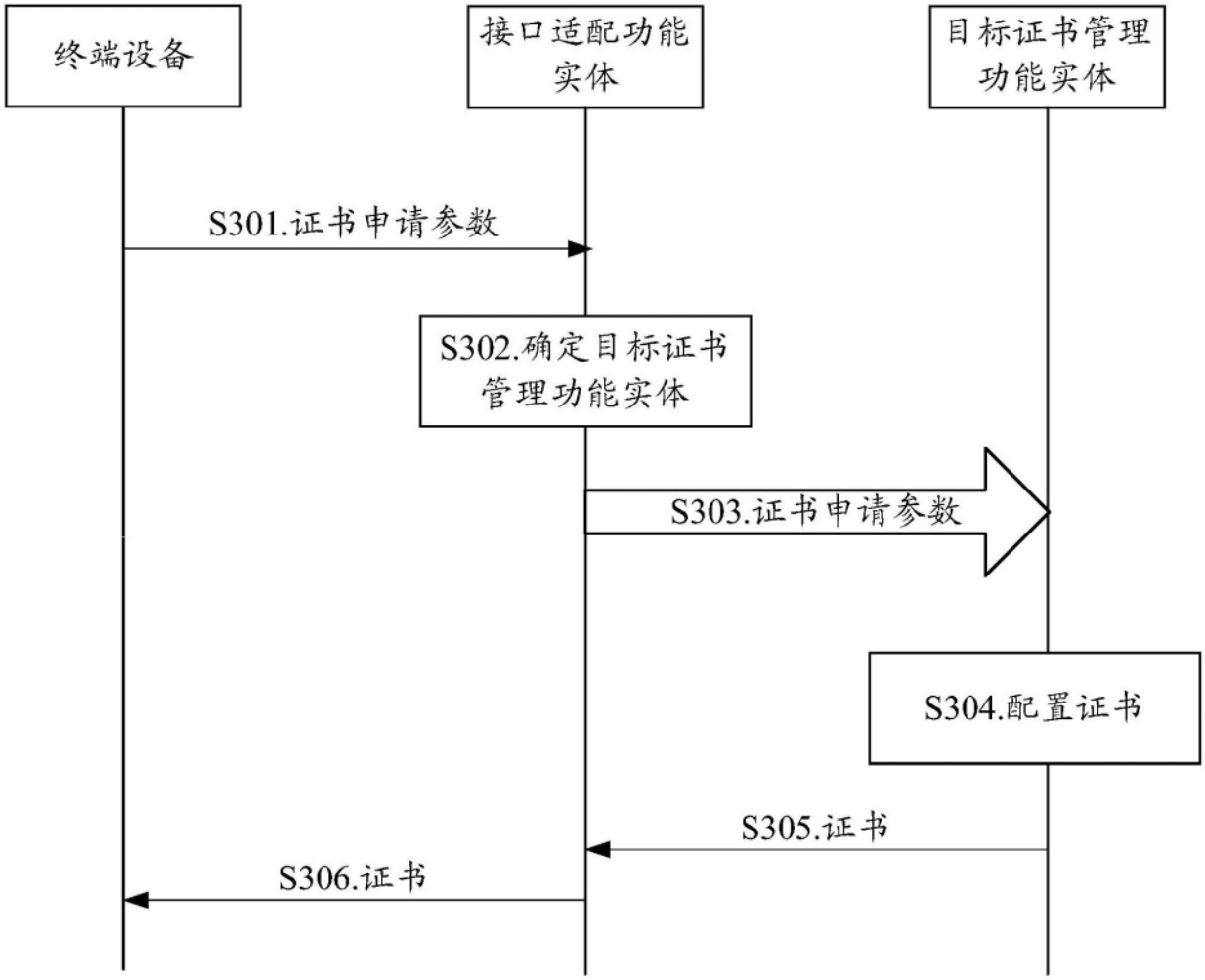

终端设备
接口适配功能实体
目标证书管理功能实体
S301.证书申请参数
S302.确定目标证书管理功能实体
S303.证书申请参数
S304.配置证书
S305.证书
S306.证书

图3

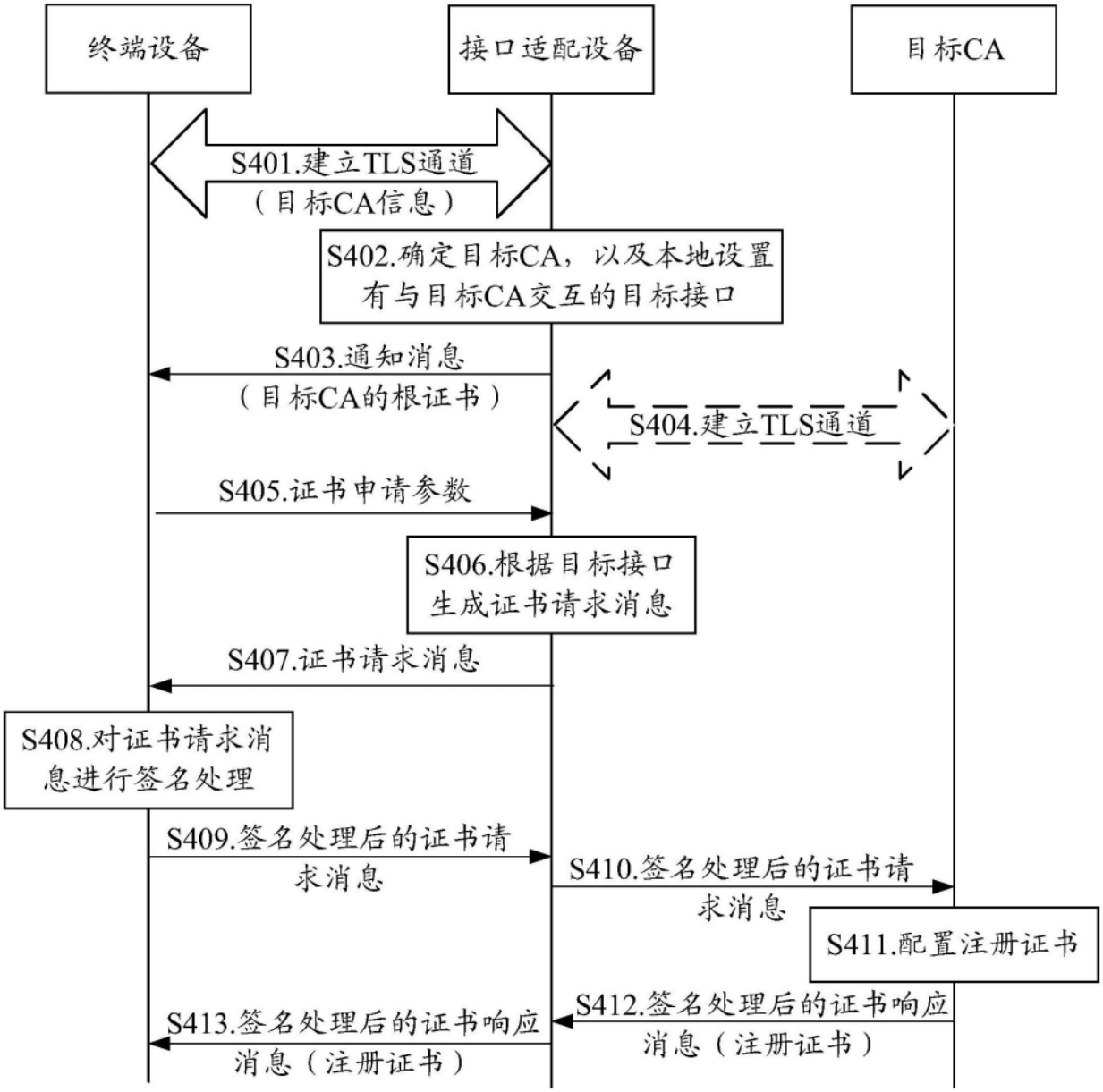

终端设备
接口适配设备
目标CA
S401.建立TLS通道
（目标CA信息）
S402.确定目标CA，以及本地设置有与目标CA交互的目标接口
S403.通知消息
（目标CA的根证书）
S404.建立TLS通道
S405.证书申请参数
S406.根据目标接口生成证书请求消息
S407.证书请求消息
S408.对证书请求消息进行签名处理
S409.签名处理后的证书请求消息
S410.签名处理后的证书请求消息
S411.配置注册证书
S412.签名处理后的证书响应消息（注册证书）
S413.签名处理后的证书响应消息（注册证书）

图4

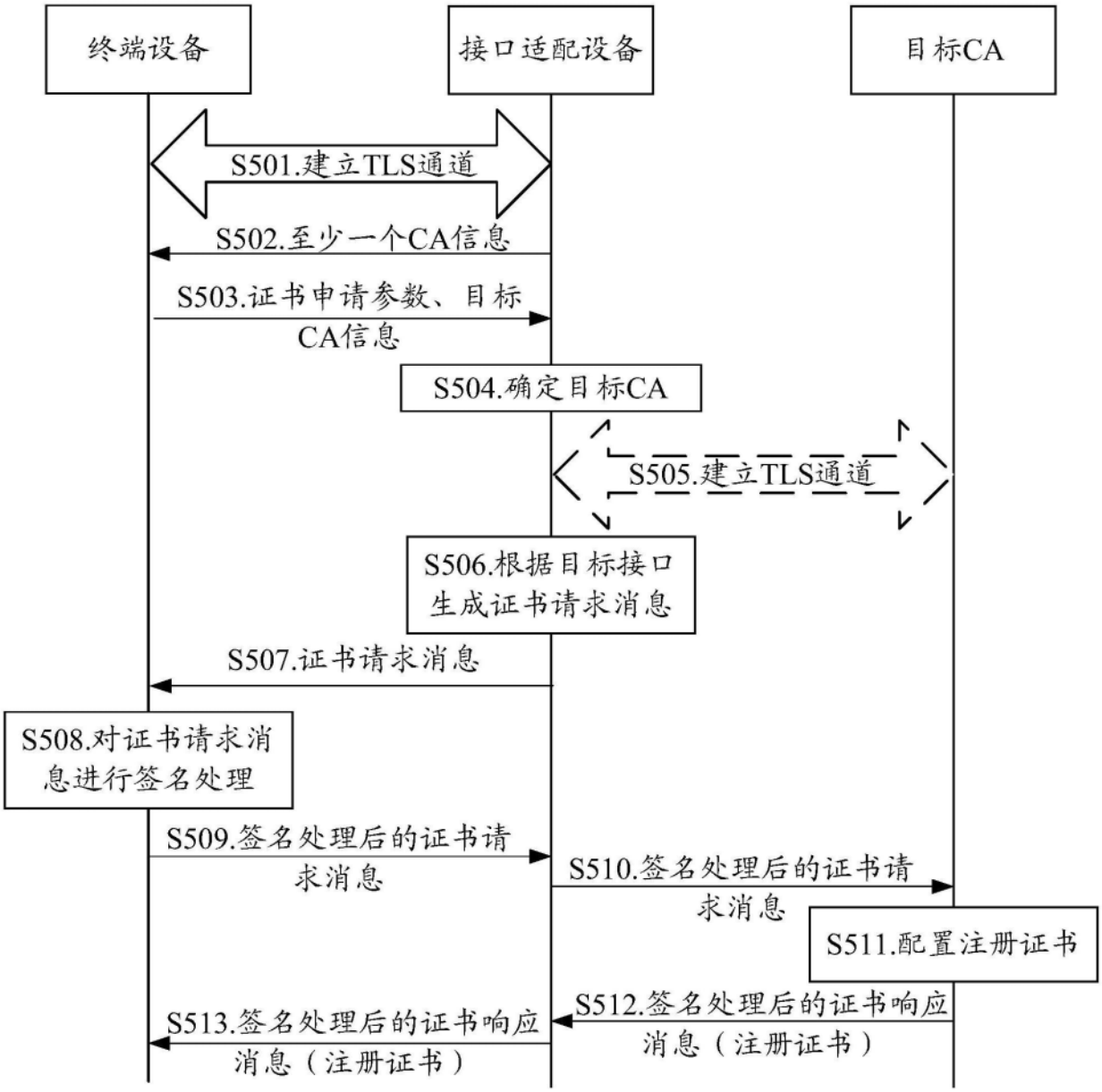

终端设备
接口适配设备
目标CA
S501.建立TLS通道
S502.至少一个CA信息
S503.证书申请参数、目标CA信息
S504.确定目标CA
S505.建立TLS通道
S506.根据目标接口生成证书请求消息
S507.证书请求消息
S508.对证书请求消息进行签名处理
S509.签名处理后的证书请求消息
S510.签名处理后的证书请求消息
S511.配置注册证书
S512.签名处理后的证书响应消息（注册证书）
S513.签名处理后的证书响应消息（注册证书）

图5

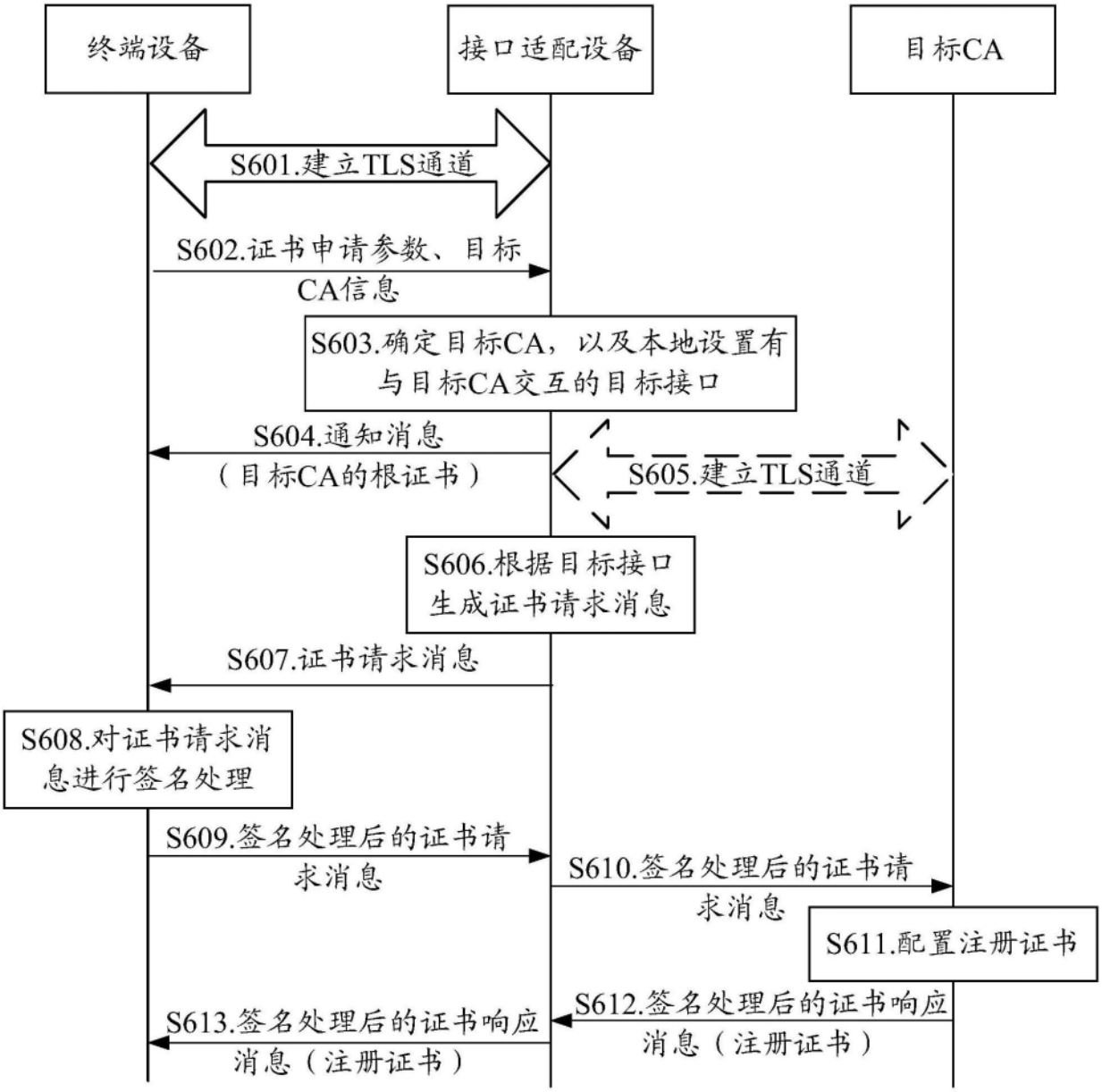

终端设备
接口适配设备
目标CA
S601.建立TLS通道
S602.证书申请参数、目标CA信息
S603.确定目标CA，以及本地设置有与目标CA交互的目标接口
S604.通知消息（目标CA的根证书）
S605.建立TLS通道
S606.根据目标接口生成证书请求消息
S607.证书请求消息
S608.对证书请求消息进行签名处理
S609.签名处理后的证书请求消息
S610.签名处理后的证书请求消息
S611.配置注册证书
S612.签名处理后的证书响应消息（注册证书）
S613.签名处理后的证书响应消息（注册证书）

图6

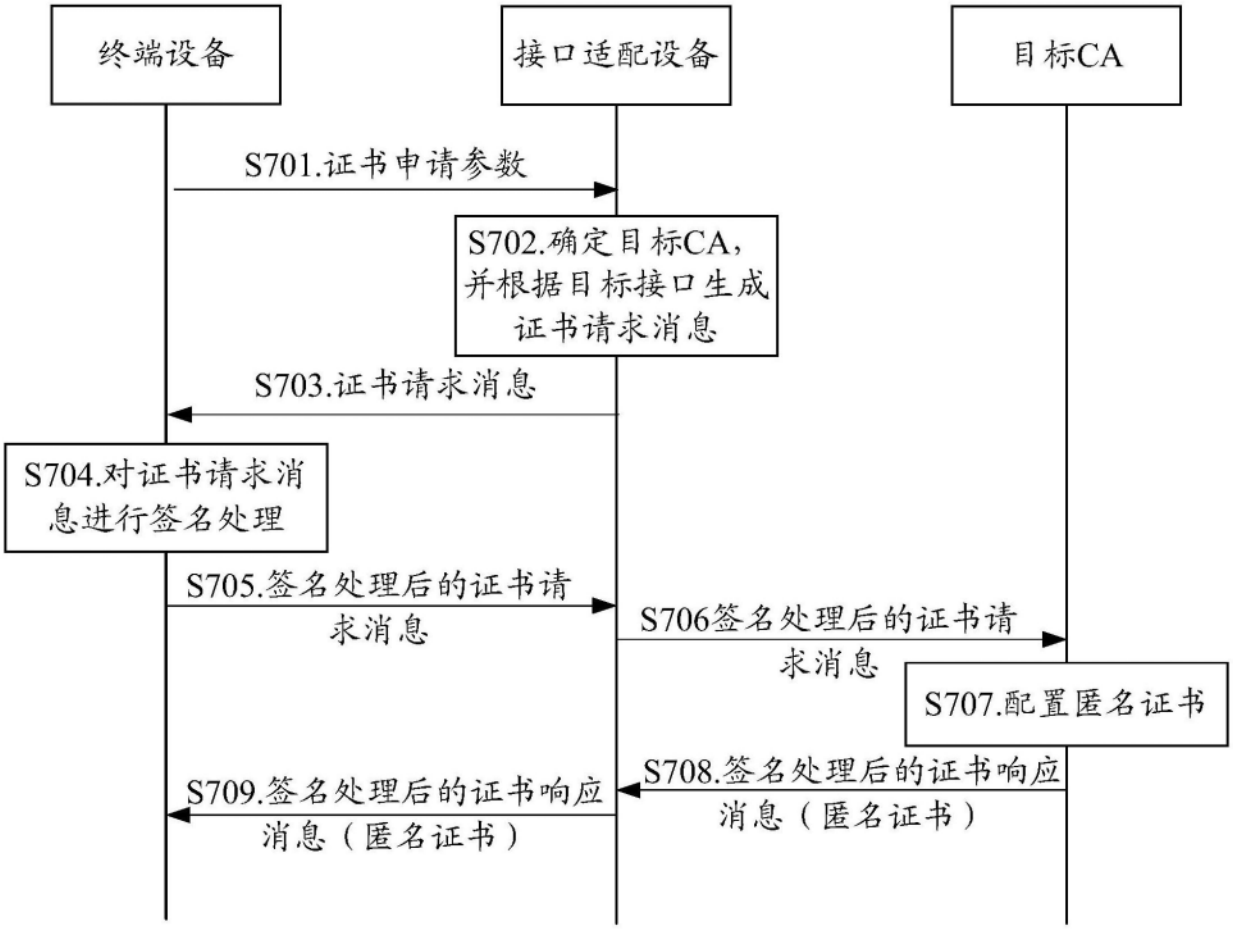

终端设备
接口适配设备
目标CA
S701.证书申请参数
S702.确定目标CA，并根据目标接口生成证书请求消息
S703.证书请求消息
S704.对证书请求消息进行签名处理
S705.签名处理后的证书请求消息
S706签名处理后的证书请求消息
S707.配置匿名证书
S708.签名处理后的证书响应消息（匿名证书）
S709.签名处理后的证书响应消息（匿名证书）

图7

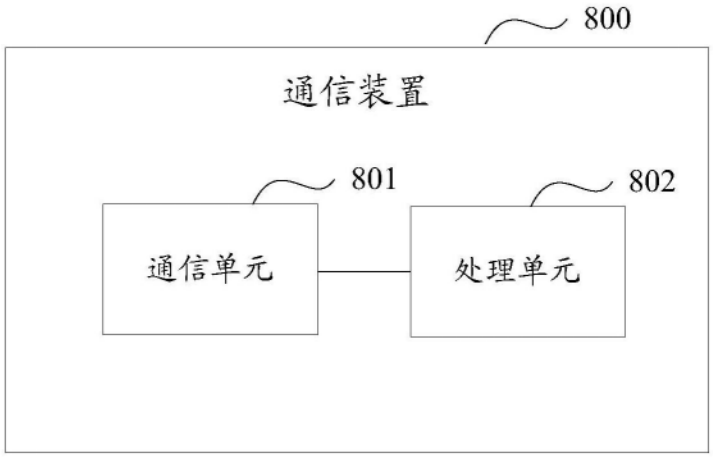

800
通信装置
801
802
通信单元
处理单元

图8

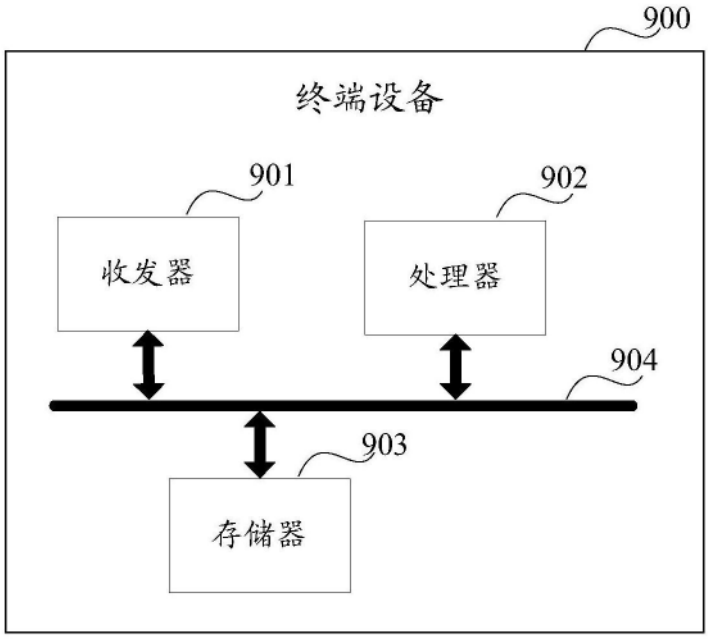

900
终端设备
901
902
收发器
处理器
904
903
存储器

图9

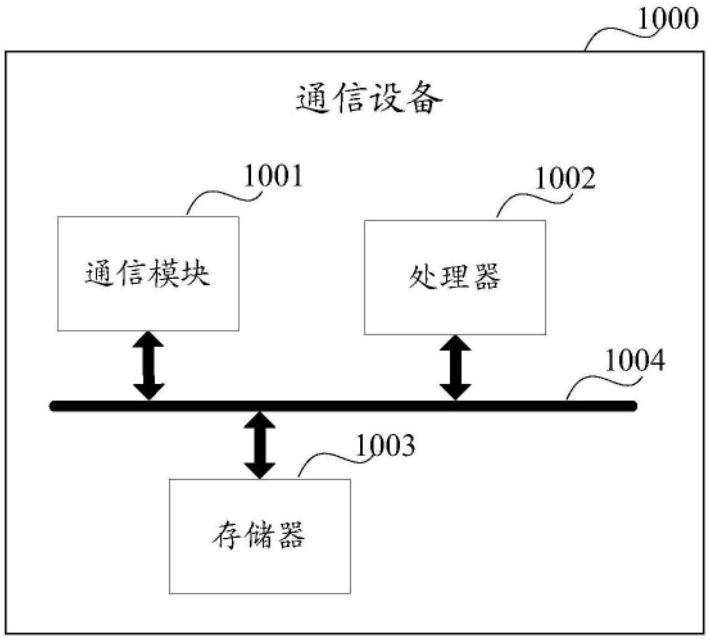

1000
通信设备
1001
1002
通信模块
处理器
1004
1003
存储器

图10