

权 利 要 求

1、一种建立安全基础设施的方法，其特征在于，包括：

中间服务机构接收第三方服务机构发送的机构密钥；

所述中间服务机构采用第一加密手段对所述机构密钥进行加密，并将加密后的机构密钥发送给终端的安全存储区域，所述第一加密手段为使用所述中间服务机构的服务私钥签名所述机构密钥，并使用所述终端的根公钥加密签名后的机构密钥；

所述中间服务机构接收所述终端采用第二加密手段进行加密的第一终端公钥，所述第二加密手段为使用所述终端的根私钥签名所述第一终端公钥，并使用所述中间服务机构的服务公钥加密签名后的第一终端公钥；

所述中间服务机构将解密得到的所述第一终端公钥发送给所述第三方服务机构。

2、如权利要求1所述的方法，其特征在于，在所述中间服务机构接收第三方服务机构发送的机构密钥之前，还包括：

所述中间服务机构向所述终端的安全存储区域发送服务公钥；

所述中间服务机构接收所述终端采用第三加密手段进行加密的所述根公钥，所述第三加密手段为使用所述根私钥签名所述根公钥并使用所述服务公钥加密签名后的根公钥；

所述中间服务机构解密得到所述根公钥。

3、一种建立安全基础设施的方法，其特征在于，包括：

终端接收中间服务机构采用第一加密手段处理的第三方服务机构的机构密钥；所述第一加密手段为使用所述中间服务机构的服务私钥签名所述机构密钥，并使用所述终端的根公钥加密签名后的机构公钥；

所述终端使用所述终端的根私钥和所述中间服务机构的服务公钥解密得到所述机构密钥并将所述机构密钥存储在所述终端的安全存储区域中；

所述终端采用第二加密手段对第一终端公钥进行加密处理，所述第二加

密手段为使用所述终端的根私钥对所述第一终端公钥进行签名且使用所述中间服务机构的服务公钥加密签名后的第一终端公钥；

所述终端将加密后的第一终端公钥发送给所述中间服务机构。

4、如权利要求3所述的方法，其特征在于，在所述终端接收所述中间服务机构采用第一加密手段处理的第三方服务机构的机构密钥之前，还包括：

所述终端接收所述中间服务机构发送的服务公钥，并将所述服务公钥存储在安全存储区域中；

所述终端采用第三加密手段对所述根公钥进行加密，所述第三加密手段为使用所述根私钥签名所述根公钥并使用所述服务公钥加密签名后的根公钥；

所述终端将加密后的根公钥发送给所述中间服务机构。

5、如权利要求4所述的方法，其特征在于，在所述终端将加密后的第一终端公钥发送给所述中间服务机构之后，还包括：

所述终端接收所述第三方服务机构采用第四加密手段处理后的应用密钥，所述第四加密手段为使用机构私钥签名所述应用密钥并使用所述第一终端公钥加密签名后的应用密钥；

所述终端使用所述第一终端私钥和所述机构公钥解密得到所述应用密钥，并将所述应用密钥存储在所述终端的安全存储区域中；

所述终端将采用第五加密手段处理后的第二终端公钥发送给所述第三方服务机构，所述第五加密手段为对所述第二终端公钥采用所述第二终端私钥签名并使用机构公钥加密。

6、如权利要求5所述的方法，其特征在于，还包括：

所述终端通过板载方式生成所述第三方服务机构对应的所述根公钥及根私钥、所述第一终端公钥及第一终端私钥、所述第二终端公钥及第二终端私钥。

7、如权利要求5所述的方法，其特征在于，还包括：

所述终端接收第三方应用的访问请求，所述第三方应用为所述第三方服

务机构对应的应用；

所述终端生成校验内容并将所述校验内容发送给所述第三方服务机构；

所述终端接收到所述第三方服务机构发送的校验指令，所述校验指令为所述第三方服务机构采用所述应用私钥对所述校验内容进行签名得到的；

所述终端采用所述应用公钥对所述校验指令进行签名验证；

所述终端在验证通过后，允许所述第三方应用对所述终端的安全区域进行访问。

8、如权利要求3至7任一项所述的方法，其特征在于，所述终端的安全存储区域为安全载体SE或可信执行环境TEE。

9、一种建立安全基础设施的方法，其特征在于，包括：

第三方服务机构采用第四加密手段对应用公钥进行加密，并将加密后的应用公钥发送给终端，所述第四加密手段为使用机构私钥签名所述应用公钥并使用所述第一终端公钥加密签名后的应用公钥；

所述第三方服务机构接收所述终端采用第五加密手段处理后的第二终端公钥，所述第五加密手段为采用所述第二终端私钥签名所述第二终端公钥并使用机构公钥加密。

10、如权利要求9所述的方法，其特征在于，还包括：

第三方服务机构通过第三方应用向终端发送访问请求，所述第三方应用为所述第三方服务机构对应的应用；

所述第三方服务机构接收所述终端发送的校验内容，并采用所述应用私钥对所述校验内容进行签名生成校验指令；

所述第三方服务机构将所述校验指令发送给所述终端，以使所述终端采用所述应用公钥对所述校验指令进行签名验证；

待校验通过后，允许所述第三方应用对所述终端的安全区域进行访问。

11、一种建立安全基础设施的装置，其特征在于，包括：

第一接收模块，用于接收第三方服务机构发送的机构密钥；

第一密钥处理模块，用于采用第一加密手段对所述机构密钥进行加密，

并指示第一发送模块将加密后的机构密钥发送给终端的安全存储区域，所述第一加密手段为使用所述中间服务机构的服务私钥签名所述机构密钥，并使用所述终端的根公钥加密签名后的机构密钥；

第一接收模块，还用于接收所述终端采用第二加密手段进行加密的第一终端公钥，所述第二加密手段为使用所述终端的根私钥签名所述第一终端公钥，并使用所述中间服务机构的服务公钥加密签名后的第一终端公钥；

所述第一发送模块，用于将解密得到的所述第一终端公钥发送给所述第三方服务机构。

12、如权利要求 11 所述的装置，其特征在于，在所述第一接收模块接收第三方服务机构发送的机构密钥之前，

所述第一发送模块，还用于向所述终端的安全存储区域发送服务公钥；

所述第一接收模块，还用于接收所述终端采用第三加密手段进行加密的所述根公钥，所述第三加密手段为使用所述根私钥签名所述根公钥并使用所述服务公钥加密签名后的根公钥；

所述第一密钥处理模块，还用于解密得到所述根公钥。

13、一种终端，其特征在于，包括：

第二接收模块，用于接收中间服务机构采用第一加密手段处理的第三方服务机构的机构密钥；所述第一加密手段为使用所述中间服务机构的服务私钥签名所述机构密钥，并使用所述终端的根公钥加密签名后的机构公钥；

第二密钥处理模块，用于使用所述终端的根私钥和所述中间服务机构的服务公钥解密得到所述机构密钥并将所述机构密钥存储在所述终端的安全存储区域中；

所述第二密钥处理模块，还用于采用第二加密手段对第一终端公钥进行加密处理，所述第二加密手段为使用所述终端的根私钥对所述第一终端公钥进行签名且使用所述中间服务机构的服务公钥加密签名后的第一终端公钥；

第二发送模块，用于将加密后的第一终端公钥发送给所述中间服务机构。

14、如权利要求 13 所述的终端，其特征在于，在所述第二接收模块接收

所述中间服务机构采用第一加密手段处理的第三方服务机构的机构密钥之前，

所述第二接收模块，还用于接收所述中间服务机构发送的服务公钥，并将所述服务公钥存储在安全存储区域中；

所述第二密钥处理模块，还用于采用第三加密手段对所述根公钥进行加密，所述第三加密手段为使用所述根私钥签名所述根公钥并使用所述服务公钥加密签名后的根公钥；

所述第二发送模块，还用于将加密后的根公钥发送给所述中间服务机构。

15、如权利要求 14 所述的终端，其特征在于，在所述第二发送模块将加密后的第一终端公钥发送给所述中间服务机构之后，

所述第二接收模块，还用于接收所述第三方服务机构采用第四加密手段处理后的应用密钥，所述第四加密手段为使用机构私钥签名所述应用密钥并使用所述第一终端公钥加密签名后的应用密钥；

所述第二密钥处理模块，还用于使用所述第一终端私钥和所述机构公钥解密得到所述应用密钥，并将所述应用密钥存储在所述终端的安全存储区域中；

所述第二发送模块，还用于将采用第五加密手段处理后的第二终端公钥发送给所述第三方服务机构，所述第五加密手段为对所述第二终端公钥采用所述第二终端私钥签名并使用机构公钥加密。

16、如权利要求 15 所述的终端，其特征在于，所述第二密钥处理模块，还用于：

通过板载方式生成所述第三方服务机构对应的所述根公钥及根私钥、所述第一终端公钥及第一终端私钥、所述第二终端公钥及第二终端私钥。

17、如权利要求 15 所述的终端，其特征在于，

所述第二接收模块，还用于接收第三方应用的访问请求，所述第三方应用为所述第三方服务机构对应的应用；

所述第二密钥处理模块，还用于生成校验内容并将所述校验内容发送给

所述第三方服务机构;

所述第二接收模块,还用于接收所述第三方服务机构发送的校验指令,所述校验指令为所述第三方服务机构采用所述应用私钥对所述校验内容进行签名得到的;

所述第二密钥处理模块,还用于采用所述应用公钥对所述校验指令进行签名验证;

在验证通过后,允许所述第三方应用对所述终端的安全区域进行访问。

18、如权利要求 13 至 17 任一项所述的终端,其特征在于,所述终端的安全存储区域为安全载体 SE 或可信执行环境 TEE。

19、一种建立安全基础设施的装置,其特征在于,包括:

第三密钥处理模块,用于采用第四加密手段对应用公钥进行加密,并将加密后的应用公钥发送给终端,所述第四加密手段为使用机构私钥签名所述应用公钥并使用所述第一终端公钥加密签名后的应用公钥;

第三接收模块,用于接收所述终端采用第五加密手段处理后的第二终端公钥,所述第五加密手段为采用所述第二终端私钥签名所述第二终端公钥并使用机构公钥加密。

20、如权利要求 19 所述的装置,其特征在于,还包括:第三发送模块;

所述第三发送模块,用于通过第三方应用向终端发送访问请求,所述第三方应用为所述第三方服务机构对应的应用;

所述第三接收模块,还用于接收所述终端发送的校验内容,并指示所述第三密钥处理模块采用所述应用私钥对所述校验内容进行签名生成校验指令;

所述第三发送模块,还用于将所述校验指令发送给所述终端,以使所述终端采用所述应用公钥对所述校验指令进行签名验证;

待校验通过后,指示所述第三密钥处理模块允许所述第三方应用对所述终端的安全区域进行访问。

21、一种电子设备,其特征在于,包括处理器、存储器、收发器、总线

接口，其中处理器、存储器与收发器之间通过总线连接；

所述收发器，用于接收第三方服务机构发送的机构密钥；接收所述终端采用第二加密手段进行加密的第一终端公钥，所述第二加密手段为使用所述终端的根私钥签名所述第一终端公钥，并使用所述中间服务机构的服务公钥加密签名后的第一终端公钥；将解密得到的所述第一终端公钥发送给所述第三方服务机构；

所述处理器，用于读取所述存储器中的程序，执行下列方法：采用第一加密手段对所述机构密钥进行加密，并指示第一发送模块将加密后的机构密钥发送给终端的安全存储区域，所述第一加密手段为使用所述中间服务机构的服务私钥签名所述机构密钥，并使用所述终端的根公钥加密签名后的机构密钥；

所述存储器，用于存储一个或多个可执行程序，可以存储所述处理器在执行操作时所使用的数据。

22、如权利要求 21 所述的电子设备，其特征在于，所述收发器，还用于：

向所述终端的安全存储区域发送服务公钥；接收所述终端采用第三加密手段进行加密的所述根公钥，所述第三加密手段为使用所述根私钥签名所述根公钥并使用所述服务公钥加密签名后的根公钥；

所述处理器，还用于解密得到所述根公钥。

23、一种电子设备，其特征在于，包括：处理器、存储器、收发器和总线接口，其中，处理器、存储器、收发器和总线接口之间通过总线连接；

所述收发器，用于接收中间服务机构采用第一加密手段处理的第三方服务机构的机构密钥；所述第一加密手段为使用所述中间服务机构的服务私钥签名所述机构密钥，并使用所述终端的根公钥加密签名后的机构公钥；将加密后的第一终端公钥发送给所述中间服务机构；

所述处理器，用于使用所述终端的根私钥和所述中间服务机构的服务公钥解密得到所述机构密钥并将所述机构密钥存储在所述终端的安全存储区域中；采用第二加密手段对第一终端公钥进行加密处理，所述第二加密手段为

使用所述终端的根私钥对所述第一终端公钥进行签名且使用所述中间服务机构的服务公钥加密签名后的第一终端公钥。

24、如权利要求 23 所述的电子设备，其特征在于，所述收发器，还用于：接收所述中间服务机构发送的服务公钥，并将所述服务公钥存储在安全存储区域中；将加密后的根公钥发送给所述中间服务机构；

所述处理器，还用于采用第三加密手段对所述根公钥进行加密，所述第三加密手段为使用所述根私钥签名所述根公钥并使用所述服务公钥加密签名后的根公钥。

25、如权利要求 24 所述的电子设备，其特征在于，所述收发器，还用于：接收所述第三方服务机构采用第四加密手段处理后的应用密钥，所述第四加密手段为使用机构私钥签名所述应用密钥并使用所述第一终端公钥加密签名后的应用密钥；将采用第五加密手段处理后的第二终端公钥发送给所述第三方服务机构，所述第五加密手段为对所述第二终端公钥采用所述第二终端私钥签名并使用机构公钥加密；

所述处理器，还用于使用所述第一终端私钥和所述机构公钥解密得到所述应用密钥，并将所述应用密钥存储在所述终端的安全存储区域中；

26、如权利要求 25 所述的电子设备，其特征在于，所述收发器，还用于：通过板载方式生成所述第三方服务机构对应的所述根公钥及根私钥、所述第一终端公钥及第一终端私钥、所述第二终端公钥及第二终端私钥。

27、如权利要求 25 所述的电子设备，其特征在于，所述收发器，还用于：接收第三方应用的访问请求，所述第三方应用为所述第三方服务机构对应的应用；接收所述第三方服务机构发送的校验指令，所述校验指令为所述第三方服务机构采用所述应用私钥对所述校验内容进行签名得到的；

所述处理器，还用于：

生成校验内容并将所述校验内容发送给所述第三方服务机构；采用所述应用公钥对所述校验指令进行签名验证；在验证通过后，允许所述第三方应用对所述终端的安全区域进行访问。

28、如权利要求 23 至 27 任一项所述的电子设备，其特征在于，所述终端的安全存储区域为安全载体 SE 或可信执行环境 TEE。

29、一种电子设备，其特征在于，包括：处理器、存储器、收发器和总线接口，其中，处理器、存储器、收发器和总线接口之间通过总线连接；

所述处理器，用于采用第四加密手段对应用公钥进行加密，并将加密后的应用公钥发送给终端，所述第四加密手段为使用机构私钥签名所述应用公钥并使用所述第一终端公钥加密签名后的应用公钥；

所述收发器，用于接收所述终端采用第五加密手段处理后的第二终端公钥，所述第五加密手段为采用所述第二终端私钥签名所述第二终端公钥并使用机构公钥加密。

30、如权利要求 29 所述的电子设备，其特征在于，所述收发器，还用于：

通过第三方应用向终端发送访问请求，所述第三方应用为所述第三方服务机构对应的应用；接收所述终端发送的校验内容，并指示所述第三密钥处理模块采用所述应用私钥对所述校验内容进行签名生成校验指令；将所述校验指令发送给所述终端，以使所述终端采用所述应用公钥对所述校验指令进行签名验证；待校验通过后，指示所述处理器允许所述第三方应用对所述终端的安全区域进行访问。

31、一种非暂态计算机可读存储介质，其特征在于，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行权利要求 1~10 任一所述方法。

32、一种计算机程序产品，其特征在于，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行权利要求 1~10 任一所述方法。