# 一种建立安全基础设施的方法、终端及装置

本申请要求在2018年03月20日提交中国专利局、申请号为201810230134.0、发明名称为“一种建立安全基础设施的方法、终端及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

## 技术领域

本发明实施例涉及支付安全技术领域，尤其涉及一种建立安全基础设施的方法、终端及装置。

## 背景技术

手机U盾（USB key，USB钥匙），是目前已有的支付方案，主要利用SE（Secure Element，安全载体）结合TEE（Trusted Execution Environment，可信执行环境）实现。SE中的U盾应用实现密钥和证书的存储，TEE实现生物特征识别等人机交互。以手机银行转账场景为例：用户确认转账，手机银行客户端调起生物特征识别的TA（Trust App，可信应用），TA完成用户生物特征识别后，允许手机银行客户端访问SE中的U盾程序进行签名并返回签名结果，手机银行客户端将交易送到后台，后台验签并承兑交易。然而，手机U盾主要是手机厂商和银行间的直接业务，一个银行对应一个手机U盾，缺少服务商的服务抽象，导致技术框架的开放性较差。

## 发明内容

本发明实施例提供一种建立安全基础设施的方法、终端及装置，用以提供开放性较好的技术框架。

第一方面，本发明实施例提供一种建立安全基础设施的方法，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。

上述实施例提供的一种建立安全基础设施的方法，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。可以看出，通过中间服务机构能够将第三方服务机构的机构密钥发送给终端，以及通过中间服务机构能够将终端的第一终端公钥发送给第三方服务机构，如此，通过中间服务机构，不仅能够保证终端与第三方服务机构的安全性，而且通过中间服务机构提供通用的安全基础设施，还能够提供开放性较好的技术框架。

较佳的，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。

第二方面，本发明实施例提供一实施例还提供一种建立安全基础设施的

方法，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。

较佳的，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。

较佳的，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。

较佳的，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。

较佳的，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。

较佳的，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。

第三方面，本发明实施例中提供了一种建立安全基础设施的方法，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。

较佳的，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。

第四方面，本发明实施例中提供了一种建立安全基础设施的装置，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。

较佳的，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。

第五方面，本发明实施例中提供了一种终端，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。

较佳的，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。

较佳的，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。

较佳的，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。

较佳的， 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。

较佳的，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。

第六方面，本发明实施例中提供了一种建立安全基础设施的装置，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。

较佳的，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。

第七方面，本发明实施例中提供了一种电子设备，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，用于在所述处理器的控制下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。

第八方面，本发明实施例中提供了一种电子设备，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。

第九方面，本发明实施例中提供了一种电子设备，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。

第十方面，本申请实施例提供一种非暂态计算机可读存储介质，计算机存储介质中存储有指令，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法，或者使得计算机执行第二方面或第二方面的任意可能的实现方式中的方法，或者使得计算机执行第三方面或第三方面的任意可能的实现方式中的方法。

第十一方面，本申请实施例提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法，或者使得计算机执行第二方面或第二方面的任意可能的实现方式中的方法，或者使得计算机执行第三方面或第三方面的任意可能的实现方式中的方法。

## 附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中

所需要使用的附图作简要介绍。

图 1 为本发明实施例提供的一种建立安全基础设施的方法流程图;

图 2 为本发明实施例提供的建立终端与中间服务机构安全通信的方法流程图;

图 3 为本发明另一实施例提供的一种建立安全基础设施的方法流程图;

图 4 为本发明另一实施例提供的建立终端与中间服务机构安全通信的方法流程图;

图 5 为本发明另一实施例提供的一种建立安全基础设施的方法流程图;

图 6~图 7 为本发明实施例提供的在应用层建立安全基础设施的方法流程图;

图 8 为本发明另一实施例提供的在应用层建立安全基础设施的方法流程图;

图 9 为本发明实施例提供的应用场景的流程图;

图 10 为本发明实施例提供的一种建立安全基础设施的装置结构示意图;

图 11 本发明实施例提供的一种终端结构示意图;

图 12 为本发明另一实施例提供的一种建立安全基础设施的装置结构示意图;

图 13 为本发明实施例提供的一种电子设备的结构示意图;

图 14 为本发明实施例提供的一种电子设备的结构示意图;

图 15 为本发明实施例提供的一种电子设备的结构示意图。

具体实施方式

为了使本发明的目的、技术方案及有益效果更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

图 1 示例性示出了本发明实施例提供的一种建立安全基础设施的方法流程图，如图 1 所示，该方法可包括:

S101、中间服务机构接收第三方服务机构发送的机构密钥。

S102、中间服务机构采用第一加密手段对机构密钥进行加密，并将加密后的机构密钥发送给终端的安全存储区域。

其中，第一加密手段为使用中间服务机构的服务私钥签名所述机构密钥，并使用终端的根公钥加密签名后的机构密钥。

S103、中间服务机构接收终端采用第二加密手段进行加密的第一终端公钥。

其中，第二加密手段为使用终端的根私钥签名第一终端公钥，并使用中间服务机构的服务公钥加密签名后的第一终端公钥。

S104、中间服务机构将解密得到的第一终端公钥发送给第三方服务机构。

可以看出，终端通过中间服务机构获得了第三方服务机构的机构公钥，而第三方服务机构通过中间服务机构获得了终端的第一终端公钥，以后，终端在与第三方服务机构进行数据通信时，可以使用机构公钥对发送给第三方服务机构的数据进行加密，而第三方服务机构在与终端进行通信时，可以使用第一终端公钥对发送给终端的数据进行加密，如此，不仅能够保证终端与第三方服务机构之间的数据安全性，而且这样设计，能够提供开放性更好的技术框架。

为了提升中间服务机构与终端之间的通信安全性，以增强机构密钥在传输过程中的安全性，在中间服务机构接收第三方服务机构发送的机构密钥之前，为了终端能与中间服务机构之间建立安全的通信，还可执行下列图 2 所示的方法流程。

S201、中间服务机构向终端的安全存储区域发送服务公钥。

S202、中间服务机构接收终端采用第三加密手段进行加密的根公钥。

其中，第三加密手段为使用根私钥签名根公钥并使用服务公钥加密签名后的根公钥。

S203、中间服务机构解密得到根公钥。

其中，服务公钥和服务私钥为中间服务机构的非对称密钥，第一终端公

钥和第一终端私钥为终端生成且存储在终端的安全存储区域的非对称密钥。

可以看出，通过上述图 2 所示的方法流程，终端获取了中间服务机构的服务公钥，而中间服务机构获取了终端的根公钥，以后，终端在与中间服务机构进行数据通信时，可采用服务公钥对发送给中间服务机构的数据进行加密，而中间服务机构可采用根公钥对发送给终端的数据进行加密，如此，不仅能够保证终端与中间服务机构之间的数据安全性，而且这样设计，还能够提供开放性更好的技术框架。

图 3 示例性示出了本发明实施例提供的一种建立安全基础设施的方法流程图，如图 3 所示，该方法可包括:

S301、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。

其中，第一加密手段为使用中间服务机构的服务私钥对机构密钥进行签名，并使用终端的根公钥对签名后的机构公钥进行加密。

S302、终端使用中间服务机构的服务公钥对加密后的机构公钥进行解密，并使用终端的根私钥对解密得到的机构公钥进行验签。

S303、待验签通过后，终端将机构密钥存储在终端的安全存储区域中。

S304、终端采用第二加密手段对第一终端公钥进行加密处理。

其中，第二加密手段为使用终端的根私钥对第一终端公钥进行签名，并且使用中间服务机构的服务公钥加密签名后的第一终端公钥。第一终端公钥为终端生成的，终端在生成第一终端公钥的同时，还生成第一终端私钥，并且第一终端公钥和第一终端私钥为非对称密钥。第一终端公钥和第一终端私钥，可以是终端在解密得到机构密钥并将该机构密钥存储在安全存储区域以后所生成的，也可以是终端预先生成的。

S305、终端将加密后的第一终端公钥发送给中间服务机构。

为了提升中间服务机构与终端之间的通信安全性，以增强机构密钥在传输过程中的安全性，在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之前，为了终端能与中间服务机构之间建立安全的通

信，还可执行下列图 4 所示的方法流程。

S401、终端接收中间服务机构发送的服务公钥，并将服务公钥存储在安全存储区域中。

S402、终端采用第三加密手段对根公钥进行加密，第三加密手段为使用根私钥签名所述根公钥并使用服务公钥加密签名后的根公钥。

S403、终端将加密后的根公钥发送给中间服务机构。

需要说明的是，根公钥为终端生成的，终端在生成根公钥的同时，还生成根私钥，并且根公钥和根私钥为非对称密钥。根公钥和根私钥，可以是终端在接收到中间服务机构发送的服务公钥并将该服务公钥存储在安全存储区域以后所生成的，也可以是终端预先生成的。

下面通过一个详细的流程图，对上述图 1、图 2、图 3、图 4 所示的流程进行详细的解释说明，参见图 5。

S501、中间服务机构与终端的安全存储区域之间建立安全通道。

具体的，中间服务机构可以基于安全通道协议 GP（GlobalPlatform，全球平台）、SCP（Secure Channel Protocol，安全通道协议）系列协议与终端的安全存储区域建立安全通道。

S502、中间服务机构通过建立的安全通道将服务公钥发送给终端的安全存储区域。

其中，服务公钥为中间服务机构预先生成的，中间服务机构在生成服务公钥的同时，还生成服务私钥，服务公钥和服务私钥为非对称密钥。

S503、终端在接收到中间服务机构所发送的服务公钥后，生成根公钥和根私钥。

可选的，终端也可预先生成根公钥和根私钥。其中，根公钥和根私钥为非对称密钥。

具体的，终端可通过板载生成的方式生成根公钥以及根私钥，以减少根公钥、根私钥在网络中的传输，从而提升根公钥和根私钥的安全性。

S504、终端将根公钥使用根私钥签名，并将签名后的根公钥采用服务公

钥加密，发送给中间服务机构。

S505、中间服务机构使用服务私钥对终端发送的根公钥进行解密，并使用解密获得的根公钥进行验签，待验签通过后，中间服务机构获得了终端的根公钥。

至此，中间服务机构将服务公钥发送给了终端的安全存储区域，服务私钥依然存储在中间服务机构内部，而终端将根公钥发送给了中间服务机构，根私钥依然存储在终端的安全存储区域中，这样，中间服务机构在与终端进行数据通信时，中间服务机构可采用根公钥对发送给终端的数据进行加密，而终端可以采用服务公钥对发送给中间服务机构的数据进行加密，可以看出，终端的根私钥以及中间服务机构的服务私钥均未在安全通道中进行传输，如此，可以提升终端与中间服务机构的数据的安全性。

具体的，当中间服务机构采用根公钥对发送给终端的数据进行加密时，待终端接收到中间服务机构采用根公钥加密的数据后，可采用根私钥对加密数据进行解密，待终端采用根公钥对加密数据进行解密后，如果需要继续与中间服务机构继续进行通信，终端可以采用服务公钥对发送给中间服务机构的数据进行加密，待中间服务机构接收到终端发送的加密数据后，可以采用服务私钥对终端发送的加密数据进行解密。或者，当终端采用服务公钥将发送给中间服务机构的数据进行加密时，中间服务机构在接收到终端发送的加密数据后，可以采用服务私钥对加密数据进行解密，如果中间服务机构需要对终端发送的数据进行恢复，可采用根公钥对回复数据进行加密，待终端接收到中间服务机构发送的加密后的回复数据后，可采用根私钥对回复数据进行解密，以得到中间服务机构所发送的回复数据。由于终端的根私钥以及中间服务机构的服务私钥自始至终未在安全通道中进行传输，因此，能够提升终端与中间服务机构的数据的安全性。

S506、第三方服务机构将机构公钥发送给中间服务机构。

可选的，机构公钥可以是第三方服务机构预先生成的，第三方服务机构在生成机构公钥的同时，还生成机构私钥。

可选的，第三方服务机构在将机构公钥发送给中间服务机构的同时，还可将机构对称密钥发送给中间服务机构。

S507、中间服务机构在接收到机构公钥后，采用第一加密手段对机构公钥进行加密。

其中，第一加密手段为使用中间服务机构的服务私钥签名所述机构密钥，并使用终端的根公钥加密签名后的机构密钥。

可选的，如果在上述步骤 S506 中，第三方服务机构在将机构公钥发送给中间服务机构的同时，还发送了机构对称密钥，则此步骤中，中间服务机构还对机构对称密钥进行加密。

S508、中间服务机构将加密后的机构密钥发送给终端的安全存储区域。

可选的，如果在上述步骤 S506 中，第三方服务机构在将机构公钥发送给中间服务机构的同时，还发送了机构对称密钥，则此步骤中，中间服务机构还可将机构对称密钥发送给终端的安全存储区域中。

S509、终端使用终端的根私钥解密，再使用中间服务机构的服务公钥对签名进行验签，待验签通过后，终端将机构公钥存储在终端的安全存储区域中。

可选的，如果在上述步骤 S506 中，第三方服务机构在将机构公钥发送给中间服务机构的同时，还发送了机构对称密钥，则此步骤中，中间服务机构在将机构公钥存储在终端的安全存储区域的同时，还可将机构对称密钥存储在终端的安全存储区域中，以进一步提供开放性的框架，供第三方服务机构所使用。

至此，终端通过中间服务机构获取了第三方服务机构的机构公钥，这样，终端以后再向第三方服务机构发送数据时，可以使用第三方服务机构的机构公钥对数据进行加密，而第三方服务机构在接收到终端发送的数据时，可以使用第三方服务机构的机构私钥进行解密。

S510、终端生成第一终端公钥和第一终端私钥。

可选的，终端也可预先生成第一终端公钥和第一终端私钥。具体的，终

端可通过板载生成的方式生成第一终端公钥以及第一终端私钥，以减少第一终端公钥、第一终端私钥在网络中的传输，从而提升第一终端公钥和第一终端私钥的安全性。

S511、终端采用第二加密手段对第一终端公钥进行加密，并将加密后的第二终端公钥发送给中间服务机构。

其中，第二加密手段为使用终端的根私钥对第一终端公钥进行签名，并且使用中间服务机构的服务公钥加密签名后的第一终端公钥。

S512、中间服务机构在接收到终端发送的加密后的第二终端公钥以后，采用中间服务机构的服务私钥解密，并使用终端的根公钥对签名进行验签，待验签通过后，获得第一终端公钥。

S513、中间服务机构将第二终端公钥发送给第三方服务机构。

至此，终端获得了第三方服务机构的机构公钥，而第三方服务机构获得了终端的第二终端公钥，这样，以后第三方服务机构在向终端发送数据时，可以使用第二终端公钥对所要发送的数据进行加密，而终端在向第三方服务机构发送数据时，可以使用机构公钥对发送给终端的数据进行加密，并且第三方服务机构的机构私钥以及中断的第二终端私钥均未在网络中传输，如此，不仅能够保证终端与第三方服务机构之间的通信，而且这样设计，能够提供开放性更好的技术框架。

为了能够在通信层的应用层加密，保护应用层的安全，提升技术框架的开放性，在终端将加密后的第一终端公钥发送给中间服务机构之后，还可执行下列图 6 所示的方法流程。

S601、终端接收第三方服务机构采用第四加密手段处理后的应用密钥。

其中，第四加密手段为使用机构私钥签名所述应用密钥并使用第一终端公钥加密签名后的应用密钥。

在一种实施方式中，应用密钥可以仅包括第三方服务机构的应用公钥，应用公钥可以是第三方服务机构预先生成的，第三方服务机构在生成应用公钥的同时，还生成应用私钥。

在另一种实施方式中，应用密钥可以包括第三方机构的应用公钥和应用对称密钥，其中，应用对称密钥的一种应用场景可以为：手机银行在向手机银行后台传递卡号等敏感信息时，可以使用该应用对称密钥进行加密；应用公钥可以是第三方服务机构预先生成的，第三方服务机构在生成应用公钥的同时，还生成应用私钥。

S602、终端使用第一终端私钥和机构公钥解密得到应用密钥，并将该应用密钥存储在终端的安全存储区域中。

具体的，终端首先使用第一终端私钥对加密后的应用密钥解密，然后使用机构公钥对签名后的应用密钥进行验签，待验签通过后，终端获取第三方服务机构发送的应用密钥，并将该应用密钥存储在终端的安全存储区域中。

S603、终端将采用第五加密手段处理后的第二终端公钥发送给第三方服务机构。

其中，第五加密手段为对第二终端公钥采用第二终端私钥签名并使用机构公钥加密。第二终端公钥可以是终端预先生成的，终端在生成第二终端公钥的同时，还生成第二终端私钥。

本发明另一实施例还提供了一种建立安全基础设施的方法，如图 7 所示，该方法可包括:

S701、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。

其中，第四加密手段为使用机构私钥对应用公钥进行签名，并使用第一终端公钥对签名后的应用公钥进行加密。

在一种实施方式中，应用密钥可以仅包括第三方服务机构的应用公钥，应用公钥可以是第三方服务机构预先生成的，第三方服务机构在生成应用公钥的同时，还生成应用私钥。

在另一种实施方式中，应用密钥可以包括第三方机构的应用公钥和应用对称密钥，其中，应用对称密钥的一种应用场景可以为：手机银行在向手机银行后台传递卡号等敏感信息时，可以使用该应用对称密钥进行加密；应用

公钥可以是第三方服务机构预先生成的，第三方服务机构在生成应用公钥的同时，还生成应用私钥。

S702、第三方服务机构接收终端采用第五加密手段处理后的第二终端公钥。

其中，第五加密手段为使用第二终端私钥对第二终端公钥进行签名，并使用机构密钥对签名后的第二终端公钥进行加密。

下面通过图 8 所述的方法流程，对上述图 6、图 7 所示的方法流程进行详细的解释说明。

S801、第三方服务机构采用第四加密手段对应用公钥进行加密。

其中，第四加密手段为使用机构私钥对应用公钥进行签名，并使用第一终端公钥对签名后的应用公钥进行加密。

在一种实施方式中，应用密钥可以仅包括第三方服务机构的应用公钥，应用公钥可以是第三方服务机构预先生成的，第三方服务机构在生成应用公钥的同时，还生成应用私钥。

在另一种实施方式中，应用密钥可以包括第三方机构的应用公钥和应用对称密钥，其中，应用对称密钥的一种应用场景可以为：手机银行在向手机银行后台传递卡号等敏感信息时，可以使用该应用对称密钥进行加密；应用公钥可以是第三方服务机构预先生成的，第三方服务机构在生成应用公钥的同时，还生成应用私钥。

S802、第三方服务机构将加密后的应用密钥发送给终端。

S803、终端使用第一终端私钥和机构公钥解密得到应用密钥，并将该应用密钥存储在终端的安全存储区域中。

具体的，终端首先使用第一终端私钥对加密后的应用密钥解密，然后使用机构公钥对签名后的应用密钥进行验签，待验签通过后，终端获取第三方服务机构发送的应用密钥，并将该应用密钥存储在终端的安全存储区域中。

S804、终端生成第二终端公钥和第二终端私钥。

可选的，终端也可预先生成第二终端公钥和第二终端私钥。具体的，终

端可通过板载生成的方式生成第二终端公钥以及第二终端私钥，以减少第二终端公钥、第二终端私钥在网络中的传输，从而提升第二终端公钥和第二终端私钥的安全性。

S805、终端采用第五加密手段对第二终端公钥进行加密。

其中，第五加密手段为对第二终端公钥采用第二终端私钥签名并使用机构公钥加密。

S806、终端将加密后的第二终端公钥发送给第三方服务机构。

S807、第三方服务机构使用机构私钥对加密后的第二终端公钥进行解密，并使用第二终端公钥进行验签，待验签通过后，获得第二终端公钥。

至此，终端获得了第三方服务机构在应用层的应用密钥，第三方服务机构获得了终端在应用层的第二终端公钥，而第二终端私钥和第三方服务机构的应用私钥均未在网络中进行传输，如此，不仅能够提升终端与第三方服务机构在应用层的安全性，而且这样设计，还能够提供开放性更好的技术框架。。

在通过上述图 6、图 7 所示的方法流程后，终端获取了第三方服务机构的应用公钥，下面通过一个具体的应用场景，对终端如何使用第三方服务机构的应用公钥进行详细的解释说明，参见图 9。

S901、第三方服务机构通过第三方应用向终端发送访问请求，第三方应用为第三方服务机构对应的应用。

在一种实施方式中，第三方应用可以是安装在终端上的客户端软件。

S902、终端接收第三方应用的访问请求，并生成校验内容。

在一种实施方式中，校验内容可以是随机数，当校验内容是随机数时，终端可以通过随机数生成器生成随机数。S903、终端将生成的校验内容发送给第三方服务机构。

S904、第三方服务机构接收终端发送的校验内容，并采用应用私钥对该校验内容进行签名生成校验指令。

S905、第三方服务机构将生成的校验指令发送给终端。

S906、终端在接收到第三方服务机构发送的校验指令后，采用应用公钥

对校验指令进行签名验证。S907、待签名验证通过后，终端允许第三方应用对终端的安全区域进行访问。

在具体实施时，待签名验证通过后，终端可以生成一个令牌，并通过该令牌允许第三方应用在有限的时间段内对终端的安全区域进行访问。

需要说明的是，在强安全场景中，终端的安全存储区域可以为安全载体SE，在弱安全场景中，终端的安全存储区域可以为可信执行环境TEE。

根据以上内容可以看出，第三方服务机构通过中间服务机构获得了终端的根公钥、第一终端公钥、第二终端公钥，而终端通过中间服务机构获得了第三方服务机构的机构公钥、应用公钥，而终端的根私钥、第一终端私钥、第二终端私钥以及第三方服务机构的机构私钥、应用私钥均未在网络中传输，如此，不仅能够保证终端与第三方服务机构的数据通信的安全性，而且还能够通过中间服务机构提供通用的安全基础设施，从而提供开放性更好的技术框架。

基于相同的技术构思，本发明实施例还提供一种建立安全基础设施的装置，如图10所示，该装置可包括:

第一接收模块1001，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1002，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1003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1001，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1003，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。

较佳的，在所述第一接收模块1001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 1003，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 1001，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 1002，还用于解密得到所述根公钥。

本发明另一实施例还提供一种终端，如图 11 所示，该终端可包括：

第二接收模块 1101，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 1102，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 1102，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 1103，用于将加密后的第一终端公钥发送给所述中间服务机构。

较佳的，在所述第二接收模块 1101 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 1101，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 1102，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 1103，还用于将加密后的根公钥发送给所述中间服务

机构。

较佳的，在所述第二发送模块 1103 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 1101，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 1102，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 1103，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。

较佳的，所述第二密钥处理模块 1102，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。

较佳的，

所述第二接收模块 1101，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 1102，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 1101，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 1102，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。

较佳的，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。

本发明另一实施例还提供一种建立安全基础设施的装置，如图 12 所示，该装置可包括:

第三密钥处理模块 1201，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 1202，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。

较佳的，还包括：第三发送模块 1203;

所述第三发送模块 1203，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 1202，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 1203，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 1201 允许所述第三方应用对所述终端的安全区域进行访问。

综上，上述实施例提供的一种建立安全基础设施的方法，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。可以看出，通过中间服

务机构能够将第三方服务机构的机构密钥发送给终端，以及通过中间服务机构能够将终端的第一终端公钥发送给第三方服务机构，如此，通过中间服务机构，不仅能够保证终端与第三方服务机构的安全性，而且通过中间服务机构提供通用的安全基础设施，还能够提供开放性较好的技术框架。

基于相同构思，本申请提供一种电子设备，可用于执行上述建立安全基础设施的装置侧的方法流程。图 13 为本申请提供的一种电子设备的结构示意图。该电子设备包括处理器 1301、存储器 1302、收发器 1303 和总线接口 1304；其中，处理器 1301、存储器 1302、收发器 1303 和总线接口 1304 通过总线 1305 相互连接。

存储器 1302 用于存储程序；具体地，程序可以包括程序代码，程序代码包括计算机操作指令。存储器 1302 可以包括易失性存储器（volatile memory），例如随机存取存储器（random-access memory，简称 RAM）；存储器也可以包括非易失性存储器（non-volatile memory），例如快闪存储器（flash memory），硬盘（hard disk drive，简称 HDD）或固态硬盘（solid-state drive，简称 SSD）；存储器 1302 还可以包括上述种类的存储器的组合。

存储器 1302 存储了如下的元素，可执行模块或者数据结构，或者它们的子集，或者它们的扩展集：

操作指令：包括各种操作指令，用于实现各种操作。

操作系统：包括各种系统程序，用于实现各种基础业务以及处理基于硬件的任务。

总线 1305 可以是外设部件互连标准（peripheral component interconnect，简称 PCI）总线或扩展工业标准结构（extended industry standard architecture，简称 EISA）总线等。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 13 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。

总线接口 1304 可以为有线通信接入口，无线总线接口或其组合，其中，有线总线接口例如可以为以太网接口。以太网接口可以是光接口，电接口或

其组合。无线总线接口可以为 WLAN 接口。

处理器 1301 可以是中央处理器（central processing unit，简称 CPU），网络处理器（network processor，简称 NP）或者 CPU 和 NP 的组合。还可以是硬件芯片。上述硬件芯片可以是专用集成电路（application-specific integrated circuit，简称 ASIC），可编程逻辑器件（programmable logic device，简称 PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（complex programmable logic device，简称 CPLD），现场可编程逻辑门阵列（field-programmable gate array，简称 FPGA），通用阵列逻辑（generic array logic，简称 GAL）或其任意组合。

所述收发器 1303，用于在所述处理器 1301 的控制下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；

所述存储器 1302，用于存储一个或多个可执行程序，可以存储所述处理器 1301 在执行操作时所使用的数据；

所述处理器 1301，用于读取所述存储器 1302 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；

较佳的，在所述收发器 1303，用于接收第三方服务机构发送的机构密钥之前，还用于向所述终端的安全存储区域发送服务公钥；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；

所述处理器 1301，还用于解密得到所述根公钥。

应理解，以上各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例

中，第一接收模块 1001 和第一发送模块 1003 可以由收发器 1303 实现，第一秘钥处理单元 1002 可以由处理器 1301 实现。如图 13 所示，电子设备 1300 可以包括处理器 1301、收发器 1303 和存储器 1302。其中，存储器 1302 可以用于存储电子设备 1300 出厂时预装的程序/代码，也可以存储用于处理器 1301 执行时的代码等。

基于相同构思，本申请提供一种电子设备，可用于执行上述终端侧的方法流程。图 14 为本申请提供的一种电子设备的结构示意图。该电子设备包括处理器 1401、存储器 1402、收发器 1403 和总线接口 1404; 其中，处理器 1401、存储器 1402、收发器 1403 和总线接口 1404 通过总线 1405 相互连接。

存储器 1402 用于存储程序；具体地，程序可以包括程序代码，程序代码包括计算机操作指令。存储器 1402 可以包括易失性存储器（volatile memory），例如随机存取存储器（random-access memory，简称 RAM）；存储器也可以包括非易失性存储器（non-volatile memory），例如快闪存储器（flash memory），硬盘（hard disk drive，简称 HDD）或固态硬盘（solid-state drive，简称 SSD）; 存储器 1402 还可以包括上述种类的存储器的组合。

存储器 1402 存储了如下的元素，可执行模块或者数据结构，或者它们的子集，或者它们的扩展集:

操作指令：包括各种操作指令，用于实现各种操作。

操作系统：包括各种系统程序，用于实现各种基础业务以及处理基于硬件的任务。

总线 1405 可以是外设部件互连标准（peripheral component interconnect，简称 PCI）总线或扩展工业标准结构（extended industry standard architecture，简称 EISA）总线等。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 14 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。

总线接口 1404 可以为有线通信接入口，无线总线接口或其组合，其中，有线总线接口例如可以为以太网接口。以太网接口可以是光接口，电接口或

其组合。无线总线接口可以为 WLAN 接口。

处理器 1401 可以是中央处理器（central processing unit，简称 CPU），网络处理器（network processor，简称 NP）或者 CPU 和 NP 的组合。还可以是硬件芯片。上述硬件芯片可以是专用集成电路（application-specific integrated circuit，简称 ASIC），可编程逻辑器件（programmable logic device，简称 PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（complex programmable logic device，简称 CPLD），现场可编程逻辑门阵列（field-programmable gate array，简称 FPGA），通用阵列逻辑（generic array logic，简称 GAL）或其任意组合。

所述收发器 1403，用于在所述处理器 1401 的控制下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 1401，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。

较佳的，在所述收发器 1403 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，所述收发器 1403，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；所述收发器 1403，还用于将加密后的根公钥发送给所述中间服务机构。

较佳的，在所述收发器 1403 将加密后的第一终端公钥发送给所述中间服务机构之后， 所述收发器 1403，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；所述收发器 1403，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。

较佳的，所述处理器 1401，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。

较佳的， 所述收发器 1403，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；所述处理器 1401，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；所述收发器 1403，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；所述处理器 1401，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。

较佳的，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。

应理解，以上各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，第二接收模块 1101 和第二发送模块 1103 可以由收发器 1403 实现，第二秘钥处理单元 1102 可以由处理器 1401 实现。如图 14 所示，电子设备 1400 可以包括处理器 1401、收发器 1403 和存储器 1402。其中，存储器 1402 可以用于存储电子设备 1400 出厂时预装的程序/代码，也可以存储用于处理器 1401 执行时的代码等。

基于相同构思，本申请提供一种电子设备，可用于执行上述建立安全基础设施的装置侧的方法流程。图 15 为本申请提供的一种电子设备的结构示意

图。该电子设备包括处理器 1501、存储器 1502、收发器 1503 和总线接口 1504；其中，处理器 1501、存储器 1502、收发器 1503 和总线接口 1504 通过总线 1505 相互连接。

存储器 1502 用于存储程序；具体地，程序可以包括程序代码，程序代码包括计算机操作指令。存储器 1502 可以包括易失性存储器（volatile memory），例如随机存取存储器（random-access memory，简称 RAM）；存储器也可以包括非易失性存储器（non-volatile memory），例如快闪存储器（flash memory），硬盘（hard disk drive，简称 HDD）或固态硬盘（solid-state drive，简称 SSD）；存储器 1502 还可以包括上述种类的存储器的组合。

存储器 1502 存储了如下的元素，可执行模块或者数据结构，或者它们的子集，或者它们的扩展集：

操作指令：包括各种操作指令，用于实现各种操作。

操作系统：包括各种系统程序，用于实现各种基础业务以及处理基于硬件的任务。

总线 1505 可以是外设部件互连标准（peripheral component interconnect，简称 PCI）总线或扩展工业标准结构（extended industry standard architecture，简称 EISA）总线等。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 15 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。

总线接口 1504 可以为有线通信接入口，无线总线接口或其组合，其中，有线总线接口例如可以为以太网接口。以太网接口可以是光接口，电接口或其组合。无线总线接口可以为 WLAN 接口。

处理器 1501 可以是中央处理器（central processing unit，简称 CPU），网络处理器（network processor，简称 NP）或者 CPU 和 NP 的组合。还可以是硬件芯片。上述硬件芯片可以是专用集成电路（application-specific integrated circuit，简称 ASIC），可编程逻辑器件（programmable logic device，简称 PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（complex programmable logic

device，简称 CPLD），现场可编程逻辑门阵列（field-programmable gate array，简称 FPGA），通用阵列逻辑（generic array logic，简称 GAL）或其任意组合。

处理器 1501，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；收发器 1503，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。

较佳的，还包括：收发器 1503；所述收发器 1503，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；所述收发器 1503，还用于接收所述终端发送的校验内容，并指示所述处理器 1501 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；所述收发器 1503，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，指示所述处理器 1501 允许所述第三方应用对所述终端的安全区域进行访问。

应理解，以上各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，第三接收模块 1202 和第三发送模块 1203 可以由收发器 1503 实现，第三密钥处理模块 1201 可以由处理器 1501 实现。如图 15 所示，电子设备 1500 可以包括处理器 1501、收发器 1503 和存储器 1502。其中，存储器 1502 可以用于存储电子设备 1500 出厂时预装的程序/代码，也可以存储用于处理器 1501 执行时的代码等。

本领域内的技术人员应明白，本发明实施例可提供为方法、系统、或计算机程序产品。因此，本发明实施例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，本发明实施例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。

本发明实施例是参照根据本发明实施例的方法、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。

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。

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。

显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本发明实施例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。