(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114338091 A
(43)申请公布日 2022.04.12

(21)申请号 202111493588.5

(22)申请日 2021.12.08

(71)申请人 杭州逗酷软件科技有限公司
地址 311100 浙江省杭州市余杭区五常街道西溪八方城9幢1001室

(72)发明人 张川 斯丹 唐嘉诚 刘骏佳 夏浩

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 李江 浦彩华

(51)Int.Cl.
*H04L 9/40*(2022.01)

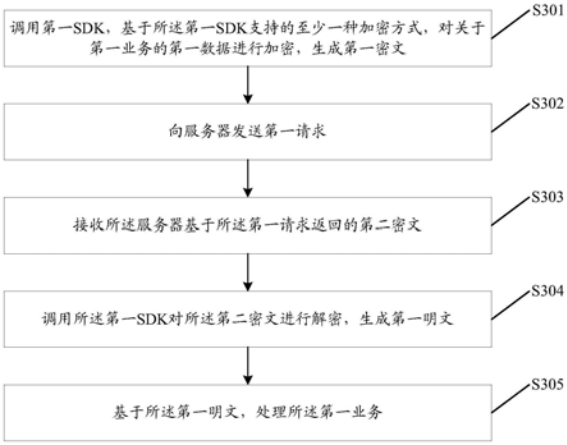
权利要求书4页 说明书23页 附图14页

(54)发明名称

数据传输方法、装置、电子设备及存储介质

(57)摘要

本申请公开了一种数据传输方法、装置、电子设备及存储介质。其中，所述方法应用于客户端，包括：调用第一软件开发工具包SDK，基于所述第一SDK支持的至少一种加密方式，对关于第一业务的第一数据进行加密，生成第一密文；向服务器发送第一请求；所述第一请求中携带所述第一密文；所述第一请求用于请求处理所述第一业务；接收所述服务器基于所述第一请求返回的第二密文；所述第二密文由所述服务器基于所述第一请求对所述第一密文的第一处理结果进行加密得到；调用所述第一SDK对所述第二密文进行解密，生成第一明文；基于所述第一明文，处理所述第一业务。




CN 114338091 A

1.一种数据传输方法,其特征在于,应用于客户端,所述方法包括:

调用第一软件开发工具包SDK,基于所述第一SDK支持的至少一种加密方式,对关于第一业务的第一数据进行加密,生成第一密文;

向服务器发送第一请求;所述第一请求中携带所述第一密文;所述第一请求用于请求处理所述第一业务;

接收所述服务器基于所述第一请求返回的第二密文;所述第二密文由所述服务器基于所述第一请求对所述第一密文的第一处理结果进行加密得到;

调用所述第一SDK对所述第二密文进行解密,生成第一明文;

基于所述第一明文,处理所述第一业务。

2.根据权利要求1所述的方法,其特征在于,所述基于所述第一SDK支持的至少一种加密方式,对所述第一数据进行加密,生成所述第一密文,包括:

在所述第一SDK支持的至少一种加密方式中选择第一加密方式或第二加密方式的情况下,基于第一加密方式的第一加密算法或第二加密方式的第二加密算法,根据客户端的第一私钥信息与服务器的第一公钥信息,对所述第一数据进行加密,生成所述第一密文;第一加密算法为RAS算法;所述第二加密算法为椭圆曲线ECC算法;

所述调用所述第一SDK对所述第二密文进行解密,生成第一明文,包括:

根据服务器的第二私钥信息对所述第二密文进行解密,生成所述第一明文;所述服务器的第二私钥信息是基于客户端的第二公钥信息确定的。

3.根据权利要求2所述的方法,其特征在于,所述基于所述第一SDK支持的至少一种加密方式,对所述第一数据进行加密,生成所述第一密文,包括:

在所述第一SDK支持的至少一种加密方式中选择第三加密方式的情况下,向密钥管理平台发送第二请求;所述第二请求用于请求分配客户端与服务器之间的通信密钥信息;

接收所述密钥管理平台返回的关于所述第二请求的第一响应;所述第一响应包括第一密钥信息和第二密钥信息;

根据所述第一密钥信息加密所述第一数据,生成所述第一密文;

所述调用所述第一SDK对所述第二密文进行解密,生成第一明文,包括:

通过所述第二密钥信息,对所述第二密文进行解密,生成所述第一明文。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括:

向密钥管理平台发送第三请求;所述第三请求用于请求登记客户端的第二公钥信息以使所述服务器根据所述第二公钥信息对所述第一处理结果进行加密;

接收所述密钥管理平台返回的关于所述第三请求的第二响应;所述第二响应表征所述第二公钥信息是否登记成功。

5.根据权利要求2所述的方法,其特征在于,所述方法还包括:

向密钥管理平台发送第四请求;所述第四请求用于请求获取新版本的业务证书;所述业务证书包括所述服务器的第一公钥信息;

接收所述密钥管理平台基于所述第四请求返回的第三响应;所述第三响应表征最新版本的业务证书。

6.一种数据传输方法,其特征在于,应用于服务器,所述方法包括:

接收客户端发送的第一请求;所述第一请求携带第一密文;所述第一密文表征关于第

一业务的第一数据的加密结果;所述第一请求用于请求处理所述第一业务;

调用第二软件开发工具包SDK,根据所述第一密文的加密方式,生成第一解密结果;所述第一解密结果表征关于所述第一请求的解密结果;

根据所述第一解密结果,对所述第一业务进行处理,生成第一处理结果;

调用所述第二SDK对所述第一处理结果进行加密,生成第二密文;

将所述第二密文返回至所述客户端。

7.根据权利要求6所述的方法,其特征在于,所述调用所述第二SDK,根据所述第一密文的加密方式,生成第一解密结果,包括:

在所述客户端适用非证书类鉴权的情况下,调用所述第二SDK,确定第二处理结果;所述第二处理结果表征所述客户端的鉴权结果;

在所述第二处理结果表征所述客户端具有访问所述服务器的权利的情况下,调用所述第二SDK,根据所述第一密文的加密方式,生成所述第一解密结果;

在所述第二处理结果表征所述客户端不具有访问所述服务器的权利的情况下,向所述客户端返回的关于所述第一请求的第四响应;所述第四响应表征拒绝处理所述第一业务。

8.根据权利要求6所述的方法,其特征在于,所述调用所述第二SDK,根据所述第一密文的加密方式,生成第一解密结果,包括:

根据所述第一密文的加密方式,向密钥管理平台发送第五请求;所述第五请求用于请求获取解密所述第一密文的密钥信息;

根据所述密钥管理平台返回的关于所述第五请求的第五响应,对所述第一密文进行解密,生成所述第一解密结果;其中,

在所述第一密文的加密方式为第一加密方式,所述第五响应包括所述服务器的第二私钥信息;

在所述第一密文的加密方式为第一加密方式,所述第五响应包括第三密钥信息;所述第三密钥信息为AES密钥信息;

调用所述第二SDK对所述第一处理结果进行加密,生成第二密文,包括:

基于第一加密方式的第一加密算法或第二加密方式的第二加密算法,根据所述服务器的第二私钥信息与客户端的第二公钥信息,对所述第一处理结果进行加密,生成所述第二密文;第一加密算法为RAS算法;所述第二加密算法为椭圆曲线ECC算法。

9.根据权利要求8所述的方法,其特征在于,在所述加密方式为第三加密方式的情况下,所述第五响应包括第一密钥信息与第二密钥信息;所述第一密钥信息与第二密钥信息表征客户端与所述服务器之间的通信密钥信息;

调用所述第二SDK对所述第一处理结果进行加密,生成第二密文,包括:

根据所述第二密钥信息,对所述第一处理结果进行加密,生成所述第二密文。

10.根据权利要求6所述的方法,其特征在于,所述方法还包括:

在无法生成所述第一解密结果的情况下,向所述密钥管理平台发送第六响应;所述第六响应表征对所述第一密文解密失败。

11.一种数据传输方法,其特征在于,应用于密钥管理平台,所述方法包括:

接收客户端或服务器发送的密钥管理请求;

根据所述密钥管理请求,调用与所述请求相对应的密钥服务,生成关于所述密钥管理

请求的响应；

将关于所述密钥管理请求的响应返回至所述客户端或服务器。

12.根据权利要求11所述的方法，其特征在于，所述根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应，包括：

在所述密钥管理请求为第二请求的情况下，调用第一密钥服务和第一工具，生成关于所述第二请求的第一响应；所述第一响应包括第一密钥信息与第二密钥信息；所述第一密钥服务表征密钥协商服务；所述第二请求用于请求分配所述客户端与所述服务器之间的通信密钥信息。

13.根据权利要求11所述的方法，其特征在于，所述根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应，包括：

在所述密钥管理请求为第三请求的情况下，调用第二密钥服务，确定第三处理结果；所述第三处理结果表征对所述客户端进行鉴权的结果；所述第二密钥服务表征鉴权服务；

在所述第三处理结果表征允许所述客户端访问所述密钥管理平台的情况下，调用第三密钥服务对客户端的第二公钥信息进行登记，生成第二响应；所述第二响应表征所述第二公钥信息登记成功；所述第三密钥服务表征密钥登记服务。

14.根据权利要求11所述的方法，其特征在于，所述根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应，包括：

在所述密钥管理请求为第四请求的情况下，调用第三密钥服务，生成第三响应；所述第三密钥服务表征所述第三密钥服务表征密钥登记服务；所述第三响应表征最新版本的业务证书。

15.根据权利要求11所述的方法，其特征在于，所述根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应，包括：

在所述密钥管理请求为第五请求的情况下，调用第一密钥服务；所述第五请求用于请求获取解密所述第一密文的密钥信息；所述第一密钥服务表征密钥协商服务；

根据所述第一密文的加密方式，生成第五响应；所述第五响应包括解密所述第一密文的密钥信息。

16.根据权利要求15所述的方法，其特征在于，所述根据所述第一密文的加密方式，生成第五响应，包括：

在所述第一密文的加密方式为第一加密方式的情况下，调用第一工具，获取所述服务器的第一私钥信息；

在所述第一密文的加密方式为第二加密方式的情况下，调用第一工具，获取所述第三密钥信息；所述第三密钥信息表征AES密钥信息；

在所述第一密文的加密方式为第三方式的情况下，根据第一标记，获取第一密钥信息与第二密钥信息；所述第一标记表征所述第一密钥服务历史协商所述服务器与所述客户端之间的密钥信息。

17.根据权利要求15所述的方法，其特征在于，所述方法还包括：

在无法获取解密所述第一密文的密钥信息的情况下，生成第七响应；所述第七响应表征协商密钥信息失败。

18.一种数据传输装置，应用于客户端，包括：

第一加密单元，用于调用第一软件开发工具包SDK，基于所述第一SDK支持的至少一种加密方式，对关于第一业务的第一数据进行加密，生成第一密文；

第一发送单元，用于向服务器发送第一请求；所述第一请求中携带所述第一密文；所述第一请求用于请求处理所述第一业务；

第一接收单元，用于接收所述服务器基于所述第一请求返回的第二密文；所述第二密文由所述服务器基于所述第一请求对所述第一密文的第一处理结果进行加密得到；

第一解密单元，用于调用所述第一SDK对所述第二密文进行解密，生成第一明文；

第一处理单元，用于基于所述第一明文，处理所述第一业务。

19.一种数据传输装置，应用于客户端，包括：

第二接收单元，用于接收客户端发送的第一请求；所述第一请求携带第一密文；所述第一密文表征关于第一业务的第一数据的加密结果；所述第一请求用于请求处理所述第一业务；

第二解密单元，用于调用第二软件开发工具包SDK，根据所述第一密文的加密方式，生成第一解密结果；所述第一解密结果表征关于所述第一请求的解密结果；

第二处理单元，用于根据所述第一解密结果，对所述第一业务进行处理，生成第一处理结果；

第二加密单元，用于调用所述第二SDK对所述第一处理结果进行加密，生成第二密文；

第二发送单元，将所述第二密文返回至所述客户端。

20.一种数据传输装置，应用于密钥管理平台，包括：

第三接收单元，用于接收客户端或服务器发送的密钥管理请求；

第一生成单元，用于根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应；

第三发送单元，将关于所述密钥管理请求的响应返回至所述客户端或服务器。

21.一种电子设备，其特征在于，包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，

其中，所述处理器用于运行所述计算机程序时，执行权利要求1至5或6至10或11至17任一项所述方法的步骤。

22.一种存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至5或6至10或11至17任一项所述方法的步骤。

# 数据传输方法、装置、电子设备及存储介质

## 技术领域

[0001] 本申请涉及信息安全技术领域，尤其涉及一种数据传输方法、装置、电子设备及存储介质。

## 背景技术

[0002] 相关技术中，为了保证数据在传输过程中的安全性，会对传输数据进行加密，由于不同的数据加密方式存在一定的安全漏洞或者存在适用场景的限制，导致数据加密的效率与数据的安全性降低的问题。

## 发明内容

[0003] 有鉴于此，本申请实施例提供一种数据传输方法、装置、电子设备及存储介质，以至少解决相关技术出现的数据加密的效率与数据的安全性降低的问题。

[0004] 本申请实施例的技术方案是这样实现的：

[0005] 本申请实施例提供了一种数据传输方法，应用于客户端，所述方法包括：

[0006] 调用第一软件开发工具包(SDK，Software Development Kit)，基于所述第一SDK支持的至少一种加密方式，对关于第一业务的第一数据进行加密，生成第一密文；

[0007] 向服务器发送第一请求；所述第一请求中携带所述第一密文；所述第一请求用于请求处理所述第一业务；

[0008] 接收所述服务器基于所述第一请求返回的第二密文；所述第二密文由所述服务器基于所述第一请求对所述第一密文的第一处理结果进行加密得到；

[0009] 调用所述第一SDK对所述第二密文进行解密，生成第一明文；

[0010] 基于所述第一明文，处理所述第一业务。

[0011] 本申请实施例提供了另一种数据传输方法，应用于服务器，所述方法包括：

[0012] 接收客户端发送的第一请求；所述第一请求携带第一密文；所述第一密文表征关于第一业务的第一数据的加密结果；所述第一请求用于请求处理所述第一业务；

[0013] 调用第二软件开发工具包SDK，根据所述第一密文的加密方式，生成第一解密结果；所述第一解密结果表征关于所述第一请求的解密结果；

[0014] 根据所述第一解密结果，对所述第一业务进行处理，生成第一处理结果；

[0015] 调用所述第二SDK对所述第一处理结果进行加密，生成第二密文；

[0016] 将所述第二密文返回至所述客户端。

[0017] 本申请实施例还提供了另一种数据传输方法，应用于密钥管理平台，所述方法包括：

[0018] 接收客户端或服务器发送的密钥管理请求；

[0019] 根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应；

[0020] 将关于所述密钥管理请求的响应返回至所述客户端或服务器。

[0021] 本申请实施例还提供了一种数据传输装置,应用于客户端,包括:

[0022] 第二接收单元,用于接收客户端发送的第一请求;所述第一请求携带第一密文;所述第一密文表征关于第一业务的第一数据的加密结果;所述第一请求用于请求处理所述第一业务;

[0023] 第二解密单元,用于调用第二软件开发工具包SDK,根据所述第一密文的加密方式,生成第一解密结果;所述第一解密结果表征关于所述第一请求的解密结果;

[0024] 第二处理单元,用于根据所述第一解密结果,对所述第一业务进行处理,生成第一处理结果;

[0025] 第二加密单元,用于调用所述第二SDK对所述第一处理结果进行加密,生成第二密文;

[0026] 第二发送单元,将所述第二密文返回至所述客户端。

[0027] 本申请实施例还提供了一种数据传输装置,应用于密钥管理平台,包括:

[0028] 第三接收单元,用于接收客户端或服务器发送的密钥管理请求;

[0029] 第一生成单元,用于根据所述密钥管理请求,调用与所述请求相对应的密钥服务,生成关于所述密钥管理请求的响应;

[0030] 第三发送单元,将关于所述密钥管理请求的响应返回至所述客户端或服务器。

[0031] 本申请实施例还提供了一种电子设备,包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器,

[0032] 其中,所述处理器用于运行所述计算机程序时,执行上述任一方法的步骤。

[0033] 本申请实施例还提供了一种存储介质,其上存储有计算机程序,所述计算机程序被处理器执行时实现上述任一方法的步骤。

[0034] 在本申请实施例中,客户端通过调用客户端上的软件开发工具包为第一业务的数据进行加密,并为服务器返回的关于第一业务的处理结果的密文进行解密,从而能够保证第一业务的数据在传输过程中的安全性的同时,还能通用的数据加密或解密的基础设施,从而能够提高数据加密和解密的效率。

## 附图说明

[0035] 图1为本申请一实施例提供的密钥管理的服务架构示意图;

[0036] 图2为本申请一实施例提供的密钥管理的技术架构示意图;

[0037] 图3为本申请一实施例提供的数据传输方法的实现流程示意图;

[0038] 图4为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0039] 图5为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0040] 图6为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0041] 图7为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0042] 图8为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0043] 图9为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0044] 图10为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0045] 图11为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0046] 图12为本申请又一实施例提供的数据传输方法的实现流程示意图;

[0047] 图13为本申请一应用实施例提供的密钥管理技术架构对RSA数字信封的处理流程示意图；

[0048] 图14为本申请又一应用实施例提供的密钥管理技术架构对ECC数字信封的处理流程示意图；

[0049] 图15为本申请又一应用实施例提供的密钥管理技术架构对基于客户端与服务器之间的通信密钥加密的第一密文的处理流程示意图；

[0050] 图16为本申请又一应用实施例提供的密钥管理技术架构登记密钥的处理流程；

[0051] 图17为本申请又一应用实施例提供的密钥管理技术架构的业务证书升级的处理流程；

[0052] 图18为本申请又一应用实施例提供的密钥申请业务接入流程；

[0053] 图19为本申请一实施例提供的数据传输装置的结构示意图；

[0054] 图20为本申请又一实施例提供的数据传输装置的结构示意图；

[0055] 图21为本申请又一实施例提供的数据传输装置的结构示意图；

[0056] 图22为本申请一实施例提供电子设备的硬件组成结构示意图。

## 具体实施方式

[0057] 下面结合附图及具体实施例对本申请作进一步详细的说明。

[0058] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0059] 需要说明的是，本申请实施例所记载的技术方案之间，在不冲突的情况下，可以任意组合。

[0060] 另外，在本申请实施例中，“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

[0061] 另外，本文中术语“至少一个”表示多个中的任意一种或多种中的至少两种的任意组合，例如，包括A、B、C中的至少一种，可以表示包括从A、B和C构成的集合中选择的任意一个或多个元素。

[0062] 相关技术中，对于相同的业务，存在不同的安全合规政策，为此不同的设计团队为满足安全合规政策，设计了不同的加密方案与解密方案，并且部分加密方案与解密方案存在较高的安全漏洞，例如，将加密密钥信息追加到统一资源定位器(url，Uniform Resource Locator)请求中，导致数据传输的安全性减弱。

[0063] 基于此，在本申请实施例提供的方案能够提供一套标准化的加密方案与解密方案，并且还能保证数据在传输过程中的安全性。

[0064] 在对本申请实施例的技术方案进行详细说明之前，首先对本申请实施例应用的密钥管理的服务架构与密钥管理的技术架构进行相应的介绍。

[0065] 如图1所示，图1示出了密钥管理的服务架构示意图。在密钥管理的服务架构中，能够处理RSA数字信封、椭圆加密算法(ECC，Elliptic curve cryptography)数字信封，以及基于Noise框架传输的数据，其中，RSA数字信封是基于RSA加密算法对数据进行加密所生成

的,RSA加密算法是一种非对称的加密算法。ECC数字信封是基于ECC加密算法对数据进行加密所生成的。Noise框架是一个用于构建安全协议的框架,为网络协议提供安全信道,从而可以保证数据在传输过程中的安全性。

[0066] 基于密钥管理的服务架构的处理场景,能够提供不同的密钥管理服务,包括密钥登记、密钥协商和流量卸载,其中,不同的密钥管理服务需要调用相应的密钥管理能力协助实现,密钥管理能力包括密钥配置、业务证书分发、密钥采集、协议鉴权、密钥协商等。在实际应用中,密钥管理能力还需要依赖一定的工具,在密钥管理服务架构中,基础设施层提供了密钥管理服务(KMS,Key Management Service)工具、公钥基础设施(PKI,Public Key Infrastructure)等,KMS工具能够确定解密的密钥,PKI能够实现证书的产生、管理、存储、分发和撤销等功能。例如,当需要对ECC数字信封中的密钥进行登记,首先要利用密钥协商服务,通过密钥协商的密钥管理能力从KMS工具中,确定解密ECC数字信封的密钥,在获取密钥后,提供密钥登记服务,通过密钥存储的密钥管理能力从PKI中完成密钥的登记。

[0067] 如图2所示,图2示出了密钥管理的技术架构示意图,在图2中的技术架构中,包括了接入层、应用层、领域层和基础设施层,其中,接入层能够供客户端、服务器、客户端的SDK、服务器的SDK以及运营后台接入,从而调用密钥管理的技术架构中的不同层,完成不同的密钥管理。在实际应用中,客户端的SDK与服务器的SDK集成密钥装卸和流量装卸的能力。应用层中提供了密钥运营、密钥登记以及密钥协商,当接入层调用应用层进行相应的处理的情况下,能够触发领域层的对应能力,领域层中包括密钥管理、密钥同步、密钥协商、密钥采集、业务鉴权等不同的能力,并依赖于基础设施层中的不同工具,完成接入层发起的密钥管理,其中,基础设施层中含有KMS、PKI等。

[0068] 下面结合附图及具体实施例对本申请作进一步详细的说明。

[0069] 本申请实施例提供了一种数据传输方法,图3为本申请实施例的数据传输方法的一种流程示意图,如图3所示,所述方法应用于客户端,所述方法包括:

[0070] S301:调用第一SDK,基于所述第一SDK支持的至少一种加密方式,对关于第一业务的第一数据进行加密,生成第一密文。

[0071] 客户端上配置标准化的第一SDK,第一SDK集成了一定的能力,例如,第一SDK可以进行数据的加密、数据的解密等。

[0072] 第一业务为客户端上进行的数据交互业务,例如,在登录网站的过程中,第一业务可以为登录验证服务,第一业务也可以付款业务,第一业务还可以为数据查询业务等。

[0073] 客户端在进行第一业务的处理过程中,存在客户端与服务器之间的数据交互的需求,例如,第一业务为付款业务的情况下,客户端需要将付款信息、付款密码等信息传输给服务器,服务器根据客户端传输的信息进行相应的验证和数据处理,从而完成付款,其中,客户端传输给服务器的付款信息、付款密码等信息,属于隐私信息,如果在传输的过程中被窃取或泄露,将会影响账户的安全,因此,需要将与第一业务相关的第一数据进行加密后传输给服务器。客户端可以调用第一SDK,为第一数据进行加密,生成第一密文,第一密文为第一数据的加密结果。

[0074] 第一SDK上集成了不同的加密方式,可以通过第一SDK支持的加密方式对第一数据进行加密,在实际应用中,可以根据第一业务的传输要求选择第一数据的加密方式,例如,在第一业务的传输要求更注重数据的安全性的情况下,在第一SDK支持的加密方式中选择

加密安全性最高的加密方式，相应的加密时间会增加，导致第一数据的传输时间也会相应的增加。在第一业务的传输要求更倾向数据的处理效率的情况下，在第一SDK支持的加密方式中选择传输效率最高的加密方式，相应的加密时间会缩短，从而能够减少第一数据的传输时间。

[0075] S302：向服务器发送第一请求；所述第一请求中携带所述第一密文；所述第一请求用于请求处理所述第一业务。

[0076] 在完成第一数据加密的情况下，需要请求服务器协助完成第一业务的处理，从而客户端可以向服务器发送第一请求，其中，第一请求为请求信息，第一请求中携带了第一密文，从而能够在第一数据随着请求发送的过程中得到保护。

[0077] S303：接收所述服务器基于所述第一请求返回的第二密文；所述第二密文由所述服务器基于所述第一请求对所述第一密文的第一处理结果进行加密得到。

[0078] 在服务器完成对第一请求的处理后，客户端能够接收服务器基于第一请求返回的第二密文，第二密文中含有对第一业务的处理结果，客户端通过对第一密文进行解密，能够获取第一业务的处理结果。

[0079] S304：调用所述第一SDK对所述第二密文进行解密，生成第一明文。

[0080] 服务器返回的第二密文是基于第一密文的加密方式加密得到的，客户端可以调用第一SDK，对第二密文进行解密，从而得到第二密文的解密结果。在实际应用中，对第二密文的解密过程与对第一密文的加密过程相反。

[0081] S305：基于所述第一明文，处理所述第一业务。

[0082] 客户端根据第一明文，能够完成第一业务的后续处理，例如，第一业务为付款业务的情况下，获取的第一明文可以为表征支付成功的信息，从而客户端上可以显示支付成功的页面，完成了付款业务的处理。获取的第一明文还可以表征支付失败的信息，从而客户端上可以显示支付失败的页面，继续进行付款业务的处理。

[0083] 在本申请实施例中，第一SDK能够支持三种加密方式，下面通过不同的实施例介绍通过三种加密方式对第一数据进行加密的过程以及对三种加密方式加密得到的数据进行解密的过程。

[0084] 在一实施例中，所述基于所述第一SDK支持的至少一种加密方式，对所述第一数据进行加密，生成所述第一密文，包括：

[0085] 在所述第一SDK支持的至少一种加密方式中选择第一加密方式或第二加密方式的情况下，基于第一加密方式的第一加密算法或第二加密方式的第二加密算法，根据客户端的第一私钥信息与服务器的第一公钥信息，对所述第一数据进行加密，生成所述第一密文；第一加密算法为RAS算法；所述第二加密算法为椭圆曲线ECC算法。

[0086] 第一加密方式是基于RSA算法对第一数据进行加密，生成第一密文，第一密文的具体生成过程为：首先确定客户端的第一私钥信息，其中，第一私钥信息可以为随机产生的对称密钥信息，利用客户端的第一私钥信息对第一数据进行加密，从而得到关于第一数据的加密结果A，再利用服务器的第一公钥信息通过RSA算法对客户端的第一私钥信息进行加密，得到关于客户端的第一私钥信息的加密结果B，将加密结果A与加密结果B进行组合，得到第一密文，在实际应用中，第一密文称为第一数据的数字信封，由于第一密文是使用第一加密方式加密得到的，因而第一密文为RSA数字信封。

[0087] 第二加密方式是基于ECC算法对第一数据进行加密，生成第一密文。第一密文的具体生成过程为：首先确定客户端的第一私钥信息，根据客户端的第一私钥信息，用椭圆曲线迪菲-赫尔曼秘钥交换(ECDH，Elliptic Curve Diffie Hellman key Exchange)，得到AES密钥，通过AES密钥对第一数据进行加密，得到关于第一数据的加密结果A，再利对客户端的AES密钥进行加密，得到关于客户端的第一私钥信息的加密结果B，基于加密结果A与加密结果B，能够生成第一密文。在实际应用中，第一密文为ECC数字信封。

[0088] 第二加密方式相对于第一加密方式而言，具有更高的安全性，在对第一数据进行加密过程中的处理速度也会比第一加密方式更快，并且，在第二加密方式在加密的过程中，生成的AES密钥的尺寸会比第一加密方式在加密过程中生成的密钥尺寸小，从而不需要较多的存储资源。

[0089] 在第二密文的加密方式为第一加密方式或第二加密方式的情况下，所述调用所述第一SDK对所述第二密文进行解密，生成第一明文，包括：

[0090] 根据服务器的第二私钥信息对所述第二密文进行解密，生成所述第一明文；所述服务器的第二私钥信息是基于客户端的第二公钥信息确定的。

[0091] 服务器返回的第二密文是基于第一密文的加密方式加密得到的，当客户端接收到的第二密文是基于第一加密方式或第二加密方式加密的情况下，第一SDK能够对第二密文进行解密，在实际应用中，对第二密文的解密过程与对第一密文的加密过程相反。

[0092] 在第二密文是基于第一加密方式加密得到的情况下，第二密文为RSA数字信封，首先利用客户端的私钥对RSA数字信封进行解密，得到服务器的第二私钥信息，服务器的第二私钥信息是用于加密第一处理结果从而生成第二密文，进而可以通过服务器的第二私钥信息对加密的第一处理结果进行解密，从而得到第一明文。

[0093] 在第二密文是基于第二加密方式加密得到的情况下，第二密文为ECC数字信封，首先利用客户端的私钥对ECC数字信封进行解密，得到服务器的第二私钥信息，服务器的第二私钥信息是用于加密第一处理结果从而生成第二密文，进而可以通过服务器的第二私钥信息对加密的第一处理结果进行解密，从而得到第一明文。

[0094] 在一实施例中，如图4所示，所述基于所述第一SDK支持的至少一种加密方式，对所述第一数据进行加密，生成所述第一密文，包括：

[0095] S401：在所述第一SDK支持的至少一种加密方式中选择第三加密方式的情况下，向密钥管理平台发送第二请求；所述第二请求用于请求分配客户端与服务器之间的通信密钥信息。

[0096] 第三加密方式是通过客户端与服务器之间的通信密钥信息对第一数据进行加密，其中，客户端与服务器之间的通信密钥信息是由密钥管理平台分配。密钥管理平台用于对密钥进行管理，提供密钥登记、密钥分发等不同的密钥管理服务。

[0097] 客户端通过向密钥管理平台发送第二请求，获取密钥管理平台分配的客户端与服务器之间的通信密钥信息。

[0098] 在实际应用中，客户端基于第一SDK生成客户端的临时公钥信息与临时私钥信息，调用initialize函数对协商状态机(HS，Handshake State-machine)进行初始化，协商状态机是用于确定客户端与服务器之间的握手状态，并调用write_message函数对HS进行更新，生成第一缓存数据buffer1，其中，第一缓存数据buffer1中含有第一SDK生成的客户端的临

时公钥信息、以及签名信息等其他信息。客户端基于第一SDK向密钥管理平台发送第二请求中携带有第一缓存数据buffer1。

[0099] S402:接收所述密钥管理平台返回的关于所述第二请求的第一响应;所述第一响应包括第一密钥信息和第二密钥信息。

[0100] 密钥管理平台对第二请求处理完成后,客户端能够接收到密钥管理平台返回的第一密钥信息与第二密钥信息,其中,第一密钥信息与第二密钥信息为客户端与服务器之间的通信密钥信息。

[0101] 客户端接收到的第一响应为利用客户端的临时公钥信息加密生成的第二缓存数据buffer2,第一SDK调用write_message函数对HS进行更新,并且对第二缓存数据buffer2进行解密,从而能够得到第一密钥信息与第二密钥信息。

[0102] S403:根据所述第一密钥信息加密所述第一数据,生成所述第一密文。

[0103] 利用第一密钥信息对第一数据进行加密,从而生成第一密文。

[0104] 在第二密文的加密方式为第三加密方式的情况下,所述调用所述第一SDK对所述第二密文进行解密,生成第一明文,包括:

[0105] 通过所述第二密钥信息,对所述第二密文进行解密,生成所述第一明文。

[0106] 客户端通过第二请求向密钥管理平台请求分配客户端与服务器之间的通信密钥信息,同样地,服务器也能向密钥管理平台获取客户端与服务器之间的通信密钥信息。在密钥管理平台分配的通信密钥信息中,当客户端使用第一密钥信息对数据进行加密,那么服务器将使用第二密钥信息对数据进行加密,在这种情况下,客户端能够通过第二密钥信息对第二密文进行解密,得到第一明文。

[0107] 在一实施例中,如图5所示,所述方法还包括:

[0108] S501:向密钥管理平台发送第三请求;所述第三请求用于请求登记客户端的第二公钥信息以使所述服务器根据所述第二公钥信息对所述第一处理结果进行加密。

[0109] 第一SDK在利用第一加密方式或第二加密方式对第一数据进行加密的过程中,会生成客户端的第一私钥信息,在生成客户端的第一私钥信息的同时,还可以生成客户端的第二公钥信息,其中,服务器可以利用第二公钥信息对传输给客户端的数据进行加密。在实际应用中,服务器可以通过密钥管理平台获取客户端的第二公钥信息,为了保证服务器能够从密钥管理平台获取客户端的第二公钥信息,需要客户端向密钥管理平台登记第二公钥信息。在实际应用中,客户端向密钥管理平台发起登记密钥的第三请求,用于使密钥管理平台对第二公钥信息进行登记,其中,第三请求中携带第二公钥信息,在实际应用中,为了保证第二公钥信息在传输过程中的数据安全,第三请求中携带的是第二公钥信息的加密结果。

[0110] S502:接收所述密钥管理平台返回的关于所述第三请求的第二响应;所述第二响应表征所述第二公钥信息是否登记成功。

[0111] 密钥管理平台根据第二公钥信息的登记情况作出第二响应,客户端能够接收第二响应,从而能够根据第二响应确定第二公钥信息的登记情况。

[0112] 在一实施例中,如图6所示,所述方法还包括:

[0113] S601:向密钥管理平台发送第四请求;所述第四请求用于请求获取新版本的业务证书;所述业务证书包括所述服务器的第一公钥信息。

[0114] 业务证书为服务器的数字证书，是一个经证书授权中心数字签名的文件，最简单的业务证书中含有服务器的第一公钥信息、服务器的名称以及证书授权中心的数字签名，一般情况下，业务证书中还包括服务器的第一公钥信息的有效时间、发证机关的名称、业务证书的序列号等不同的信息。

[0115] 在第一加密方式与第二加密方式下，需要服务器的第一公钥信息对第一数据进行加密，因此，客户端需要获取服务器的第一公钥信息。在实际应用中，客户端可以通过密钥管理平台中查询服务器的第一公钥信息，并将第一公钥信息进行保存，从而能够利用保存的第一公钥信息对第一数据进行加密。由于服务器的第一公钥信息存在有效时间，或者，服务器的第一公钥信息可能会发生改变，因此客户端可以定期向密钥管理平台查询业务证书是否发生变化，客户端通过向密钥管理平台发送第四请求，以使密钥管理平台获取服务器的最新版本的业务证书。

[0116] S602：接收所述密钥管理平台基于所述第四请求返回的第三响应；所述第三响应表征最新版本的业务证书。

[0117] 客户端接收第三响应，其中，第三响应包括服务器的最新版本的业务证书，客户端还可以对业务证书进行保存，从而能够利用最新版本的业务证书中的服务器的第一公钥信息对第一数据进行加密，能够保证服务器对第一密文解密成功，进行第一业务的相关处理。此外，客户端还可以根据服务器的业务证书，对服务器进行验证，从而避免客户端将第一数据传输到非法的服务器。

[0118] 在本申请实施例中，第一SDK提供了标准化的加密方式与解密方式，客户端通过调用第一SDK完成数据的加密与数据的解密，从而能够保证客户端与服务器之间的数据传输的安全性的同时，也可以避免客户端利用存在较高的安全漏洞的加密方式对数据进行加密，还能提高数据的加密效率。

[0119] 本申请是实例还提供了另一种数据传输方法，如图7所示，所述方法应用于服务器，包括：

[0120] S701：接收客户端发送的第一请求；所述第一请求携带第一密文；所述第一密文表征关于第一业务的第一数据的加密结果；所述第一请求用于请求处理所述第一业务。

[0121] 接收客户端的第一请求，客户端通过第一请求，请求服务器对第一业务进行相应的处理，第一业务为客户端上进行的数据交互业务，例如，第一业务为登录验证服务的情况下，客户端通过第一请求，请求服务器对登录验证服务进行相应的处理，服务器会根据关于第一业务的第一数据确认是否通过验证，其中，为了保证客户端与服务器的传输数据的安全性，服务器接收到的是加密后的第一数据，在实际应用中，服务器接收到的第一请求中携带了关于第一数据的第一密文，第一密文为第一数据的加密结果。

[0122] S702：调用第二软件开发工具包SDK，根据所述第一密文的加密方式，生成第一解密结果；所述第一解密结果表征关于所述第一请求的解密结果。

[0123] 服务器需要对第一密文进行解密后，才能根据第一密文对第一业务进行相应的处理，其中，服务器可以通过调用第二SDK对第一密文进行解密，第二SDK上集成了不同的功能，例如，第二SDK可以实现数据的加密与数据的解密。

[0124] 通过第一密文的加密方式，对第一密文进行解密，从而得到第一解密结果，其中，对第一密文的解密是对第一数据的加密的逆过程。

[0125] 在一实施例中，如图8所示，所述调用所述第二SDK，根据所述第一密文的加密方式，生成第一解密结果，包括：

[0126] S801：在所述客户端适用非证书类鉴权的情况下，调用所述第二SDK，确定第二处理结果；所述第二处理结果表征所述客户端的鉴权结果。

[0127] 第二SDK还集成了鉴权的功能。在实际应用中，对客户端进行鉴权可以通过证书类鉴权，也可以通过非证书类鉴权，其中证书类鉴权由于需要通过密钥管理服务平台获取客户端的证书，因而一般在密钥管理平台进行证书类鉴权，在本实施例中，第二SDK的业务鉴权功能适用于简单的业务鉴权，并不适用证书类鉴权。第二SDK在客户端适用非证书类鉴权的情况下，对客户端进行鉴权，得到第二处理结果。

[0128] S802：在所述第二处理结果表征所述客户端具有访问所述服务器的权利的情况下，调用所述第二SDK，根据所述第一密文的加密方式，生成所述第一解密结果。

[0129] 在第二处理结果表征客户端具有访问服务器的权利的情况下，表明客户端为合法的客户端，第一请求是由客户端发出的，并不存在其他非法的客户端盗取信息以获取服务器的处理结果，因而可以对第一密文进行解密，并对第一业务进行后续的处理。

[0130] S803：在所述第二处理结果表征所述客户端不具有访问所述服务器的权利的情况下，向所述客户端返回的关于所述第一请求的第四响应；所述第四响应表征拒绝处理所述第一业务。

[0131] 在第二处理结果表征客户端不具有访问服务器的权利的情况下，表明客户端为非法客户端，非法客户端通过截取合法客户端向服务器发送的第一请求，使服务器接收到的第一请求的发送者由合法客户端转变为非法客户端，进而骗取服务器以获取合法客户端的数据，在这种情况下，为了保护数据安全，服务器不再将第一请求进行相关的处理，并向非法客户端返回拒绝处理第一业务的第四响应。

[0132] S703：根据所述第一解密结果，对所述第一业务进行处理，生成第一处理结果。

[0133] 根据所述第一密钥信息对所述第一密文进行解密，生成所述第一解密结果。

[0134] 在利用第五响应对第一密文进行解密的过程中，是根据第一密钥信息对第一密文进行解密，其中，第一密钥信息为客户端对第一数据进行加密所使用的密钥信息，从而得到第一解密结果。

[0135] S704：调用所述第二SDK对所述第一处理结果进行加密，生成第二密文。

[0136] 第一处理结果会返回至客户端，在服务器处理的第一业务的处理结果含有敏感信息的情况下，直接将第一处理结果返回至客户端，容易造成数据泄露的情况，从而产生各种安全威胁，例如，当第一业务为申请登录验证码的情况下，服务器对于第一业务的第一处理结果为客户端用于登录的验证码，验证码被窃取后，会导致用户的账户信息泄露，因此需要将第一处理结果进行加密。在实际应用中，使用生成第一密文的加密方式对第一处理结果进行加密，从而生成第二密文。

[0137] S705：将所述第二密文返回至所述客户端。

[0138] 在本申请实施例中，可以通过三种不同的加密方式生成第一密文，下面通过不同的实施例介绍通过第一密文在不同加密方式下的解密过程以及第一处理结果的加密过程。

[0139] 在一实施例中，如图9所示，所述调用所述第二SDK，根据所述第一密文的加密方式，生成第一解密结果，包括：

[0140] S901:根据所述第一密文的加密方式,向密钥管理平台发送第五请求;所述第五请求用于请求获取解密所述第一密文的密钥信息。

[0141] 由于解密过程是加密过程的逆过程,因此确定第一密文的加密方式,进而可以根据第一密文的加密方式,对第一密文进行解密,其中,用于解密第一密文的密钥信息需要通过密钥管理平台获取解密第一密文的密钥信息,服务器通过向密钥管理平台发送第五请求,使密钥管理平台能够向服务器提供第一密文的密钥信息。

[0142] S902:根据所述密钥管理平台返回的关于所述第五请求的第五响应,对所述第一密文进行解密,生成所述第一解密结果。

[0143] 服务器接收第五响应,第五响应中含有解密第一密文的密钥信息,从而服务器能够根据第五响应中的第一密文的密钥信息,对第一密文进行机密,得到第一解密结果。在实际应用中,根据第一密文的加密方式的不同,第五响应中的第一密文的密钥信息也不相同。

[0144] 在所述第一密文的加密方式为第一加密方式,所述第五响应包括所述服务器的第二私钥信息。

[0145] 第一加密方式为基于RSA算法进行加密,对应的第一密文为RSA数字信封,RSA数字信封的解密首先要获取服务器的第二私钥信息,服务器的第二私钥信息是服务器通过第五请求向密钥管理平台获取,服务器得到的第五响应中含有服务器的第二私钥信息。利用服务器获取的第二私钥信息,能够解密RSA数字信封,从而获取用于加密第一数据的密钥信息,也就是客户端的第一私钥信息,进而通过第一私钥信息对加密的第一数据进行解密,获取第一数据。

[0146] 在所述第一密文的加密方式为第一加密方式,所述第五响应包括第三密钥信息;所述第三密钥信息为AES密钥信息。

[0147] 第二加密方式为基于ECC算法进行加密,对应的第一密文为ECC数字信封,AES密钥信息为生成第一密文的过程中用于加密第一数据的密钥信息,服务器能够通过AES密钥信息对ECC数字信封进行解密,从而得到第一数据。

[0148] 调用所述第二SDK对所述第一处理结果进行加密,生成第二密文,包括:

[0149] 基于第一加密方式的第一加密算法或第二加密方式的第二加密算法,根据所述服务器的第二私钥信息与客户端的第二公钥信息,对所述第一处理结果进行加密,生成所述第二密文;第一加密算法为RAS算法;所述第二加密算法为椭圆曲线ECC算法。

[0150] 使用第一密文的加密方式对第一处理结果进行加密,生成第二密文。

[0151] 第一加密方式是基于RSA算法,对第一处理结果进行加密,生成第二密文。第二密文的具体生成过程为:利用服务器的第二私钥信息对第一处理结果进行加密,从而得到关于第一处理结果的加密结果A,再利用客户端的第二公钥信通过RSA算法对服务器的第二私钥信息进行加密,得到关于服务器的第二私钥信息的加密结果B,将加密结果A与加密结果B进行组合,生成第二密文,在实际应用中,第二密文为RSA数字信封。

[0152] 第二加密方式是基于ECC算法,对第一处理结果进行加密,生成第二密文。第二密文的具体生成过为:根据服务器的第二私钥信息,通过椭圆曲线迪菲-赫尔曼秘钥交换(ECDH,Elliptic Curve Diffie-Hellman key Exchange)生成服务器的AES密钥,利用服务器的AES密钥对第一处理结果进行加密,从而得到关于第一处理结果的加密结果A,再利用客户端的第二公钥信息对AES密钥进行加密,得到关于服务器的AES密钥的加密结果B,将加

密结果A与加密结果B进行组合，生成第二密文，在实际应用中，第二密文为ECC数字信封。

[0153] 在一实施例中，所述调用所述第二SDK，根据所述第一密文的加密方式，生成第一解密结果，包括：

[0154] 在所述加密方式为第三加密方式的情况下，所述第五响应包括第一密钥信息与第二密钥信息；所述第一密钥信息与第二密钥信息表征客户端与所述服务器之间的通信密钥信息。

[0155] 第三加密方式是通过客户端向密钥管理平台请求分配的密钥信息进行加密，因此服务器通过第五请求向密钥管理平台请求获取密钥管理平台为客户端分配的密钥信息，服务器通过第五响应，得到第一密钥信息与第二密钥信息，可以根据第五响应中的密钥信息，对第一密文进行解密，得到第一密文的第一解密结果。

[0156] 调用所述第二SDK对所述第一处理结果进行加密，生成第二密文，包括：

[0157] 根据所述第二密钥信息，对所述第一处理结果进行加密，生成所述第二密文。

[0158] 在客户端利用第一密钥信息进行加密的情况下，服务器可以利用第二密钥信息对第一处理结果进行加密，生成第二密文。

[0159] 在一实施例中，所述方法还包括：

[0160] 在无法生成所述第一解密结果的情况下，向所述密钥管理平台发送第六响应；所述第六响应表征对所述第一密文解密失败。

[0161] 在一般情况下，服务器接收到密钥管理平台返回的关于第五请求的第五响应中含有的密钥信息，是正确的密钥信息，能够对第一密文进行解密。当存在根据第五响应中的密钥信息无法对第一密文进行解密的情况下，服务器能够将解密失败的情况上报至密钥管理平台，使密钥管理平台对解密失败的情况进行统计和分析，从而能够有利于保证下一次解密能够顺利进行。

[0162] 在上述实施例中，第二SDK提供了标准化的加密方式与解密方式，服务器通过调用第二SDK能够实现第一密文的解密，从而能够根据相应的业务数据处理第一业务，并将处理结果进行加密后返回客户端，提高了客户端与服务器之间的传输数据的安全性，并且还能提高了对传输数据的加密效率以及解密效率。

[0163] 本申请实施例还提供了另一种数据传输方法，如图10所示，应用于密钥管理平台，所述方法包括：

[0164] S1001：接收客户端或服务器发送的密钥管理请求。

[0165] 密钥管理平台能够接收客户端或服务器发送的密钥管理请求，其中，客户端发送的密钥管理请求通常为请求进行密钥登记、分配密钥信息以及获取服务器的业务证书。服务器发送的密钥管理请求通常为请求进行密钥协商。在实际应用中，密钥管理平台能够支持不同的密钥管理服务以及支持调用各种密钥管理工具，例如，KMS工具、PKI工具等，进而完成客户端或服务器发送的密钥管理请求所请求的密钥服务。

[0166] S1002：根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应。

[0167] 密钥管理平台根据密钥管理请求，从而确定密钥管理请求需要的密钥服务，例如，密钥管理请求为密钥登记的情况下，调用密钥登记服务进行密钥的登记。当密钥管理平台调用相应的密钥服务完成密钥管理请求所请求的密钥服务器的情况下，会生成关于密钥管

理请求的响应，例如，调用密钥登记服务完成密钥的登记，能够生成密钥登记成功的响应信息。

[0168] 在一实施例中，所述根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应，包括：

[0169] 在所述密钥管理请求为第二请求的情况下，调用第一密钥服务和第一工具，生成关于所述第二请求的第一响应；所述第一响应包括第一密钥信息与第二密钥信息；所述第一密钥服务表征密钥协商服务；所述第二请求用于请求分配所述客户端与所述服务器之间的通信密钥信息。

[0170] 密钥管理平台接收到第二请求，第二请求为客户端发起的请求，客户端发起的第二请求用于请求密钥管理平台分配客户端与服务器之间的通信密钥信息，使客户端与服务器通过密钥管理平台分配的通信密钥信息进行数据的传输。

[0171] 密钥管理平台接收到的密钥管理请求为第二请求的情况下，需要调用第一密钥服务，通过第一密钥服务，进行密钥协商，从而生成客户端与服务器之间的通信密钥信息。

[0172] 第一响应的生成过程具体为：密钥管理平台接收到第二请求，其中，第二请求中还携带了第一缓存数据buffer1，密钥管理平台调用第一密钥服务请求进行密钥协商，通过第一工具KMS工具，解密得到第一密钥信息，并通过调用密钥分发服务能够分配得到第二密钥信息，在实际应用中，客户端可以根据第一密钥信息实现对客户端的数据进行加密，从而服务器能够根据第一密钥信息实现对客户端加密的数据进行解密，服务器能够根据第二密钥信息实现对服务器的数据进行加密，从而客户端也能够根据第二密钥信息实现对服务器加密的数据进行解密。

[0173] 在实际应用中，直接将第一密钥信息与第二密钥信息返回至客户端容易导致信息的泄露，因此需要对第一密钥信息与第二密钥信息进行加密。第一密钥服务通过两次轮转更新，负责解密第一缓存数据buffer1，并负责对第一密钥信息与第二密钥信息进行加密，其中，第一密钥信息与第二密钥信息通过AES密钥进行加密，从而派生得到经过AES密钥加密的第一密钥信息C1与第二密钥信息C2，只需要对经过AES密钥加密的第一密钥信息与第二密钥信息进行加密保护，即使在传输的过程中泄漏了AES密钥的明文，也不会影响第一密钥信息与第二密钥信息的安全性。第一密钥服务能够对第一密钥信息C1与第二密钥信息C2进行保存，并将第二缓存数据buffer2返回至客户端，其中，第二缓存数据buffer2中含有第一密钥信息与第二密钥信息。

[0174] 在一实施例中，如图11所示，所述根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应，包括：

[0175] S1101：在所述密钥管理请求为第三请求的情况下，调用第二密钥服务，确定第三处理结果；所述第三处理结果表征对所述客户端进行鉴权的结果；所述第二密钥服务表征鉴权服务。

[0176] 第三请求为客户端发起的请求，用于请求密钥管理平台对密钥信息进行登记。当密钥管理平台接收到第三请求的情况下，调用第二密钥服务对客户端进行鉴权，得到第三处理结果，通过第三处理结果能够确定客户端是否为合法客户端，从而避免密钥管理平台登记非法客户端的密钥信息，避免非法客户端与服务器进行通信。

[0177] S1102：在所述第三处理结果表征允许所述客户端访问所述密钥管理平台的情况

下，调用第三密钥服务对客户端的第二公钥信息进行登记，生成第二响应；所述第二响应表征所述第二公钥信息登记成功；所述第三密钥服务表征密钥登记服务。

[0178] 在第三处理结果表征允许客户端访问密钥管理平台的情况下，表明客户端为合法客户端，从而进行客户端的第二公钥信息的登记。密钥管理平台通过调用第三密钥服务对客户端的第二公钥信息进行登记，生成关于第三请求的第二响应，当密钥管理平台成功登记第二公钥信息的情况下，能够生成表征密钥登记成功的第二响应，登记成功的第二公钥信息是通过密钥采集服务，将第二公钥信息写入到密钥管理平台的数据库中。当密钥管理平台没能登记第二公钥信息的情况下，生成表征密钥登记失败的第二响应。

[0179] 在实际应用中，第三请求携带的第二公钥信息是经过加密的，也就是说第二密钥信息装载在数字信封中，在这种情况下，首先对数字信封进行解密，从而获取第二公钥信息，再对第二公钥信息进行登记。具体地，密钥管理平台调用第一密钥服务，对数字信封进行拆解，从而获得AES密钥信息，其中，AES密钥信息是用于加密第二公钥信息的密钥信息，通过AES密钥信息对加密的第二公钥信息进行解密，得到第二公钥信息，再对第二公钥信息进行登记。

[0180] 在一实施例中，所述根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应，包括：

[0181] 在所述密钥管理请求为第四请求的情况下，调用第三密钥服务，生成第三响应；所述第三密钥服务表征所述第三密钥服务表征密钥登记服务；所述第三响应表征最新版本的业务证书。

[0182] 第四请求为客户端发起的请求，用于请求密钥管理平台向客户端返回最新版本的业务证书，其中，业务证书是服务器的数字证书，是一个经证书授权中心数字签名的文件，最简单的业务证书中含有服务器的第一公钥信息、服务器的名称以及证书授权中心的数字签名，一般情况下，业务证书中还包括服务器的第一公钥信息的有效时间、发证机关的名称、业务证书的序列号等不同的信息，客户端通过获取从最新版本的业务证书中获取服务器的第一公钥信息，进而完成数据的加密。

[0183] 当密钥管理平台接收到第四请求的情况下，调用第三密钥管理服务，在密钥管理平台的数据库中查询最新版本的业务证书，并生成关于第四请求的第三响应，其中，第三相应为最新版本的业务证书。

[0184] 在一实施例中，如图12所示，所述根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应，包括：

[0185] S1201：在所述密钥管理请求为第五请求的情况下，调用第一密钥服务；所述第五请求用于请求获取解密所述第一密文的密钥信息；所述第一密钥服务表征密钥协商服务。

[0186] 第五请求为服务器发起的请求，用于请求密钥管理平台获取解密第一密文的密钥信息，其中，解密第一密文的密钥信息是通过第一密钥服务，进行密钥协商得到的。

[0187] S1202：根据所述第一密文的加密方式，生成第五响应；所述第五响应包括解密所述第一密文的密钥信息。

[0188] 解密过程实质上为加密过程的逆过程，不同的加密方式会导致解密的密钥信息以及解密方式不相同，因此，密钥管理平台在调用密钥协商服务的过程中，会根据第一密文的加密方式，协商得到解密第一密文的密钥信息，从而根据第五响应，将解密第一密文的密钥

信息返回至服务器，以使服务器根据第五响应中的密钥信息进行解密。

[0189] 在一实施例中，所述根据所述第一密文的加密方式，生成第五响应，包括：

[0190] 在所述第一密文的加密方式为第一加密方式的情况下，调用第一工具，获取所述服务器的第一私钥信息。

[0191] 第一加密方式表征利用RSA算法对第一数据进行加密，得到的第一密文为RSA数字信封，第一密文的解密步骤为先解密RSA数字信封，再对加密的第一数据进行解密。密钥协商服务能够从第一工具KMS工具中获取用于解密RSA的数字信封的密钥信息，也就是服务器的第二私钥信息，通过第五响应将服务器的第二私钥信息返回至服务器。

[0192] 在所述第一密文的加密方式为第二加密方式的情况下，调用第一工具，获取所述第三密钥信息；所述第三密钥信息表征AES密钥信息。

[0193] 第二加密方式表征利用ECC算法对第一数据进行加密，得到的第一密文为ECC数字信封，要获取第一数据，首先要对ECC数字信封进行解密，再对加密的第一数据进行解密。密钥协商服务能够从第一工具KMS工具中获取服务器的第二私钥信息，并且根据服务器的第二私钥信息确定AES密钥信息，AES密钥信息为加密第一数据的密钥信息，通过第五响应将AES密钥信息返回至服务器。

[0194] 所述第一密文的加密方式为第三方式的情况下，根据第一标记，获取第一密钥信息与第二密钥信息；所述第一标记表征所述第一密钥服务历史协商所述服务器与所述客户端之间的密钥信息。

[0195] 第三加密方式为通过密钥管理平台分配的客户端与服务器之间的通信密钥信息对第一数据进行加密，对第一密文进行解密需要先获取客户端与服务器之间的通信密钥信息，由于密钥管理平台在确定客户端与服务器之间的通信密钥信息的过程中，将客户端与服务器之间的通信密钥信息存储至密钥协商服务中，因此可以通过第一标记从密钥协商服务中获取对应的第一密钥信息与第二密钥信息，第一标记可以用于区分不同客户端与服务器的通信密钥信息，从而能够从密钥协商服务存储的密钥信息中提取到对应的第一密钥信息与第二密钥信息。

[0196] 在一实施例中，所述方法还包括：

[0197] 在无法获取解密所述第一密文的密钥信息的情况下，生成第七响应；所述第七响应表征协商密钥信息失败。

[0198] 密钥管理平台是通过密钥协商服务，确定用于解密第一密文的密钥信息。当密钥协商服务无法协商确定用于解密第一密文的密钥信息的情况下，服务器无法对第一密文进行解密，也就是说密钥管理平台存在错误报告，将无法获取解密第一密文的密钥信息的情况下产生的第七响应进行上报，从而能够统计密钥管理平台协商失败的次数，进而能够进一步分析得到密钥协商失败的原因，能够保证密钥协商成功的几率。

[0199] 在实际应用中，由于第三加密方式是通过密钥管理平台分配的通信密钥信息进行加密的，因而针对第三加密方式不存在协商失败的情况，而第一加密方式与第二加密方式均需要密钥管理平台协商得到服务器的第二私钥信息，从而存在协商失败的情况，因此，在获取第一加密方式或第二加密方式对应的解密密钥信息的情况下，需要监控密钥协商是否成功，在获取第三加密方式对应的解密密钥信息的情况下，不需要监控密钥协商是否成功。

[0200] S1003：将关于所述密钥管理请求的响应返回至所述客户端或服务器。

[0201] 密钥管理平台将关于密钥管理请求的响应返回至客户端或服务器，在实际应用中，当关于密钥管理请求的响应中存在安全需求高的数据的情况下，可以对数据进行加密后再返回至客户端或服务器，从而使客户端或服务器能够接收到关于密钥管理请求的处理结果。

[0202] 在上述实施例中，密钥管理平台通过服务器或客户端发起的密钥管理平台，调用相应的密钥管理服务器完成不同密钥需求对应的密钥管理服务，从而能够通过不同的接口，提供一套标准化的密钥管理服务的处理流程，提高了密钥管理的效率，并且还能够提高密钥管理平台所管理的密钥信息的安全性。

[0203] 本申请还提供了一应用实施例，如图13所示，图13示出了密钥管理技术架构对RSA数字信封的处理流程示意图。

[0204] 客户端向第一SDK发送加密请求，用于请求第一SDK对第一数据进行加密。第一SDK通过第一加密方式对第一数据进行加密，生成第一密文，第一密文为RSA数字信封。

[0205] 客户端向服务器发送第一请求，用于请求服务器协助进行第一业务的处理，其中，第一请求中携带有第一密文。

[0206] 服务器接收到第一请求后，请求第二SDK解密第一密文。第二SDK通过向密钥管理平台发送第五请求，用于请求获取解密第一密文的密钥信息。

[0207] 密钥管理平台接收到第五请求后，密钥协商应用服务调用领域层的业务鉴权能力，对客户端进行鉴权，其中，当进行的是非证书类的简单鉴权，可以集成在第二SDK中。业务鉴权能力得到客户端的鉴权结果后，将鉴权结果返回至密钥协商应用服务。密钥协商应用服务请求密钥协商领域服务进行密钥协商，密钥协商领域服务从KMS中获取服务器的第二私钥信息，并逐层返回至第二SDK。其中，当密钥协商领域服务不能从KMS中获取服务器的第二私钥信息的情况下，向数据统计上报协商失败信息。

[0208] 第二SDK获得服务器的第二私钥信息后，对第一密文进行解密，得到第一密文的解密结果，并将第一密文的解密结果返回至服务器。

[0209] 服务器根据第一密文的解密结果处理业务逻辑，并调用第二SDK对处理结果进行加密，并将第二密文返回至客户端。

[0210] 客户端接收第二密文后，调用第一SDK对第二密文进行解密，第一SDK将第二密文解密得到的第一明文返回至客户端，客户端根据第一明文，处理业务逻辑。

[0211] 本申请还提供了另一应用实施例，如图14所示，图14示出了密钥管理技术架构对ECC数字信封的处理流程示意图。

[0212] 客户端向第一SDK发送加密请求，用于请求第一SDK对第一数据进行加密。第一SDK通过第二加密方式对第一数据进行加密，生成第一密文，第一密文为ECC数字信封。

[0213] 客户端向服务器发送第一请求，用于请求服务器协助进行第一业务的处理，其中，第一请求中携带有第一密文。

[0214] 服务器接收到第一请求后，请求第二SDK解密第一密文。第二SDK通过向密钥管理平台发送第五请求，用于请求获取解密第一密文的密钥信息。

[0215] 密钥管理平台接收到第五请求后，密钥协商应用服务调用领域层的业务鉴权能力，对客户端进行鉴权，其中，当进行的是非证书类的简单鉴权，可以集成在第二SDK中。业务鉴权能力得到客户端的鉴权结果后，将鉴权结果返回至密钥协商应用服务。密钥协商应

用服务请求密钥协商领域服务进行密钥协商，密钥协商领域服务从KMS中获取服务器的第二私钥信息，并根据第二私钥信息使用ECDH计算得到AES密钥，并将AES密钥逐层返回至第二SDK。其中，当密钥协商领域服务不能从KMS中获取AES密钥的情况下，向数据统计上报协商失败信息。

[0216] 第二SDK获得AES密钥后，对第一密文进行解密，得到第一密文的解密结果，并将第一密文的解密结果返回至服务器。

[0217] 服务器根据第一密文的解密结果处理业务逻辑，并调用第二SDK对处理结果进行加密，并将第二密文返回至客户端。

[0218] 客户端接收第二密文后，调用第一SDK对第二密文进行解密，第一SDK将第二密文解密得到的第一明文返回至客户端，客户端根据第一明文，处理业务逻辑。

[0219] 本申请还提供了另一应用实施例，如图15所示，图15示出了密钥管理技术架构对基于客户端与服务器之间的通信密钥加密的第一密文的处理流程示意图。

[0220] 客户端向第一SDK发送加密请求，用于请求第一SDK对第一数据进行加密。第一SDK初始化生成临时公钥信息与私钥信息，调用initialize函数初始化HS，调用write_message函数更新HS，并生成第一缓存数据buffer1，将第一缓存数据buffer1传输给密钥管理平台，其中，第一缓存数据buffer1中含有临时公钥信息、签名等信息。

[0221] 密钥管理平台在接收到第一缓存数据buffer1后，调用密钥协商应用服务，密钥协商应用服务请求密钥协商领域服务器进行密钥协商，密钥协商领域服务通过KMS获取业务私钥，并调用密钥分发服务获取应用公钥，密钥协商领域服务根据业务私钥与应用公钥，生成临时公钥信息与私钥信息，通过两次轮转更新HS，并解密第一缓存数据buffer1，派生得到AES密钥信息，包括第一密钥信息与第二密钥信息，密钥协商领域服务将第二缓存数据buffer2、临时公钥信息、第一密钥信息与第二密钥信息返回至密钥协商应用服务，密钥协商应用服务保持第一密钥信息与第二密钥信息，并将第二缓存数据buffer2、第一密钥信息与第二密钥信息返回至客户端。

[0222] 第一SDK调用write_message函数更新HS，并解密第二缓存数据buffer2，得到第一密钥信息与第二密钥信息。使用第一密钥信息加密第一数据得到第一密文。将第一密文返回至客户端。

[0223] 客户端向服务器发送第一请求，用于请求服务器协助进行第一业务的处理，其中，第一请求中携带有第一密文。

[0224] 服务器接收到第一请求后，请求第二SDK解密第一密文。第二SDK通过向密钥管理平台发送第五请求，用于请求获取解密第一密文的密钥信息。

[0225] 密钥管理平台接收到第五请求后，通过密钥协商应用服务，通过相应的第一标记，得到第一密钥信息与第二密钥信息，将第一密钥信息与第二密钥信息返回至服务器。

[0226] 调用第二SDK利用第一密钥信息对第一密文进行解密，将第一密文的解密结果返回至服务器。

[0227] 服务器根据第一密文的解密结果，处理业务逻辑，并调用第二SDK对第一处理结果进行加密。

[0228] 第二SDK通过第二密钥信息对第一处理结果进行加密，生成第二密文。服务器将第二密文返回至客户端。

[0229] 客户端调用第一SDK,根据第二密钥信息,解密第二密文,得到第一明文,并根据第一明文处理业务逻辑。

[0230] 本申请还提供了另一应用实施例,如图16所示,图16示出了密钥管理技术架构登记密钥的处理流程。

[0231] 客户端初始化第一SDK,第一SDK生成公钥信息与私钥信息,并将公钥信息与私钥信息进行保存。客户端向密钥管理平台发起第三请求,第三请求中携带有公钥信息。

[0232] 密钥管理平台根据第三请求,调用密钥登记应用服务,如果公钥信息经过数字信封进行加密,密钥登记应用服务请求密钥协商领域服务拆解数字信封,密钥领域协商服务拆解数字信封后得到AES密钥,将AES密钥返回至密钥登记应用服务,密钥登记应用服务根据AES密钥解密得到公钥信息,并调用业务鉴权能力,对客户端进行鉴权,并将鉴权结果返回至密钥登记应用服务,在鉴权结果表征客户端为合法客户端的情况下,密钥登记应用服务将公钥信息发送给密钥采集服务,密钥采集服务将公钥信息存储至数据库中,并逐层返回响应。

[0233] 客户端能够接收表征登记成功的响应。

[0234] 本申请还提供了另一应用实施例,如图17所示,图17示出了密钥管理技术架构的业务证书升级的处理流程。

[0235] 客户端初始化第一SDK,并调用第一SDK向密钥管理平台发送第四请求,第四请求用于请求密钥管理平台检测业务证书的更新。

[0236] 密钥管理平台根据第四请求,调用密钥登记应用服务,密钥登记应用服务向密钥分发领域服务获取最新版本的业务证书,密钥分发领域服务在数据库中将查询到的最新版本的业务证书逐层返回至客户端,客户端能够获取最新版本的业务证书。

[0237] 本申请还提供了另一应用实施例,如图18所示,图18示出了密钥申请业务接入流程。

[0238] 业务方提交创建证书的申请,管理后台根据请求创建对应的证书,并将证书送审。审批人员对证书进行第一次审批,再由平台对证书进行第二次审批,根据第二次的审批结果,业务方进行接入SDK的调试,并根据调试结果配置网关转发规则。此外,平台根据第二次的审批结果进行业务量的评估,并通知平台准备相关业务的上线,部署对应的资源。

[0239] 本申请实施例还提供了数据传输装置,如图19所述,应用于客户端,包括:

[0240] 第一加密单元1901,用于调用第一软件开发工具包SDK,基于所述第一SDK支持的至少一种加密方式,对关于第一业务的第一数据进行加密,生成第一密文;

[0241] 第一发送单元1902,用于向服务器发送第一请求;所述第一请求中携带所述第一密文;所述第一请求用于请求处理所述第一业务;

[0242] 第一接收单元1903,用于接收所述服务器基于所述第一请求返回的第二密文;所述第二密文由所述服务器基于所述第一请求对所述第一密文的第一处理结果进行加密得到;

[0243] 第一解密单元1904,用于调用所述第一SDK对所述第二密文进行解密,生成第一明文;

[0244] 第一处理单元1905,用于基于所述第一明文,处理所述第一业务。

[0245] 在一实施例中,所述第一加密单元1901在调用第一软件开发工具包SDK,基于所述

第一SDK支持的至少一种加密方式，对关于第一业务的第一数据进行加密，生成第一密文时，还用于：

[0246] 在所述第一SDK支持的至少一种加密方式中选择第一加密方式或第二加密方式的情况下，基于第一加密方式的第一加密算法或第二加密方式的第二加密算法，根据客户端的第一私钥信息与服务器的第一公钥信息，对所述第一数据进行加密，生成所述第一密文；第一加密算法为RAS算法；所述第二加密算法为椭圆曲线ECC算法；

[0247] 第一解密单元1904在所述调用所述第一SDK对所述第二密文进行解密，生成第一明文时，还用于：

[0248] 根据服务器的第二私钥信息对所述第二密文进行解密，生成所述第一明文；所述服务器的第二私钥信息是基于客户端的第二公钥信息确定的。

[0249] 在一实施例中，所述第一加密单元1901在调用第一软件开发工具包SDK，基于所述第一SDK支持的至少一种加密方式，对关于第一业务的第一数据进行加密，生成第一密文时，还用于：

[0250] 在所述第一SDK支持的至少一种加密方式中选择第三加密方式的情况下，向密钥管理平台发送第二请求；所述第二请求用于请求分配客户端与服务器之间的通信密钥信息；

[0251] 接收所述密钥管理平台返回的关于所述第二请求的第一响应；所述第一响应包括第一密钥信息和第二密钥信息；

[0252] 根据所述第一密钥信息加密所述第一数据，生成所述第一密文。

[0253] 第一解密单元1904在所述调用所述第一SDK对所述第二密文进行解密，生成第一明文时，还用于：

[0254] 通过所述第二密钥信息，对所述第二密文进行解密，生成所述第一明文。

[0255] 在一实施例中，所述装置还用于：

[0256] 向密钥管理平台发送第四请求；所述第四请求用于请求获取新版本的业务证书；所述业务证书包括所述服务器的第一公钥信息；

[0257] 接收所述密钥管理平台基于所述第四请求返回的第三响应；所述第三响应表征最新版本的业务证书。

[0258] 实际应用时，第一加密单元1901、第一发送单元1902、第一接收单元1903、第一解密单元1904、第一处理单元1905可由数据传输装置中的处理器来实现。当然，处理器需要运行存储器中存储的程序来实现上述各程序模块的功能。

[0259] 需要说明的是，上述图19实施例提供的数据传输装置在进行数据传输时，仅以上述各程序模块的划分进行举例说明，实际应用中，可以根据需要而将上述处理分配由不同的程序模块完成，即将装置的内部结构划分成不同的程序模块，以完成以上描述的全部或者部分处理。另外，上述实施例提供的数据传输装置与数据传输方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0260] 本申请实施例还提供了另一种数据传输装置，如图20所示，应用于服务器，包括：

[0261] 第二接收单元2001，用于接收客户端发送的第一请求；所述第一请求携带第一密文；所述第一密文表征关于第一业务的第一数据的加密结果；所述第一请求用于请求处理所述第一业务；

[0262] 第二解密单元2002,用于调用第二软件开发工具包SDK,根据所述第一密文的加密方式,生成第一解密结果;所述第一解密结果表征关于所述第一请求的解密结果;

[0263] 第二处理单元2003,用于根据所述第一解密结果,对所述第一业务进行处理,生成第一处理结果;

[0264] 第二加密单元2004,用于调用所述第二SDK对所述第一处理结果进行加密,生成第二密文;

[0265] 第二发送单元2005,将所述第二密文返回至所述客户端。

[0266] 在一实施例中,所述第二解密单元2002在调用第二软件开发工具包SDK,根据所述第一密文的加密方式,生成第一解密结果时,还用于:

[0267] 在所述客户端适用非证书类鉴权的情况下,调用所述第二SDK,确定第二处理结果;所述第二处理结果表征所述客户端的鉴权结果;

[0268] 在所述第二处理结果表征所述客户端具有访问所述服务器的权利的情况下,调用所述第二SDK,根据所述第一密文的加密方式,生成所述第一解密结果;

[0269] 在所述第二处理结果表征所述客户端不具有访问所述服务器的权利的情况下,向所述客户端返回的关于所述第一请求的第四响应;所述第四响应表征拒绝处理所述第一业务。

[0270] 在一实施例中,所述第二解密单元2002在调用第二软件开发工具包SDK,根据所述第一密文的加密方式,生成第一解密结果时,还用于:

[0271] 根据所述第一密文的加密方式,向密钥管理平台发送第五请求;所述第五请求用于请求获取解密所述第一密文的密钥信息;

[0272] 根据所述密钥管理平台返回的关于所述第五请求的第五响应,对所述第一密文进行解密,生成所述第一解密结果;其中,

[0273] 在所述第一密文的加密方式为第一加密方式,所述第五响应包括所述服务器的第二私钥信息;

[0274] 在所述第一密文的加密方式为第一加密方式,所述第五响应包括第三密钥信息;所述第三密钥信息为AES密钥信息;

[0275] 第二加密单元2004在调用所述第二SDK对所述第一处理结果进行加密,生成第二密文时,还用于:

[0276] 基于第一加密方式的第一加密算法或第二加密方式的第二加密算法,根据所述服务器的第二私钥信息与客户端的第二公钥信息,对所述第一处理结果进行加密,生成所述第二密文;第一加密算法为RAS算法;所述第二加密算法为椭圆曲线ECC算法。

[0277] 在一实施例中,所述加密方式为第三加密方式的情况下,所述第五响应包括第一密钥信息与第二密钥信息;所述第一密钥信息与第二密钥信息表征客户端与所述服务器之间的通信密钥信息;

[0278] 第二加密单元2004在调用所述第二SDK对所述第一处理结果进行加密,生成第二密文时,还用于:

[0279] 根据所述第二密钥信息,对所述第一处理结果进行加密,生成所述第二密文。

[0280] 在一实施例中,所述装置还用于:

[0281] 在无法生成所述第一解密结果的情况下,向所述密钥管理平台发送第六响应;所

述第六响应表征对所述第一密文解密失败。

[0282] 实际应用时，第二接收单元2001、第二解密单元2002、第二处理单元2003、第二加密单元2004、第二发送单元2005可由数据传输装置中的处理器来实现。当然，处理器需要运行存储器中存储的程序来实现上述各程序模块的功能。

[0283] 需要说明的是，上述图20实施例提供的数据传输装置在进行数据传输时，仅以上述各程序模块的划分进行举例说明，实际应用中，可以根据需要而将上述处理分配由不同的程序模块完成，即将装置的内部结构划分成不同的程序模块，以完成以上描述的全部或者部分处理。另外，上述实施例提供的数据传输装置与数据传输方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0284] 本申请实施例还提供了另一种数据传输装置，如图21所示，应用于密钥管理平台，包括：

[0285] 第三接收单元2101，用于接收客户端或服务器发送的密钥管理请求；

[0286] 第一生成单元2102，用于根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应；

[0287] 第三发送单元2103，将关于所述密钥管理请求的响应返回至所述客户端或服务器。

[0288] 在一实施例中，第一生成单元2102在根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应时，还用于：

[0289] 在所述密钥管理请求为第二请求的情况下，调用第一密钥服务和第一工具，生成关于所述第二请求的第一响应；所述第一响应包括第一密钥信息与第二密钥信息；所述第一密钥服务表征密钥协商服务；所述第二请求用于请求分配所述客户端与所述服务器之间的通信密钥信息。

[0290] 在一实施例中，第一生成单元2102在根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应时，还用于：

[0291] 在所述密钥管理请求为第三请求的情况下，调用第二密钥服务，确定第三处理结果；所述第三处理结果表征对所述客户端进行鉴权的结果；所述第二密钥服务表征鉴权服务；

[0292] 在所述第三处理结果表征允许所述客户端访问所述密钥管理平台的情况下，调用第三密钥服务对客户端的第二公钥信息进行登记，生成第二响应；所述第二响应表征所述第二公钥信息登记成功；所述第三密钥服务表征密钥登记服务。

[0293] 在一实施例中，第一生成单元2102在根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应时，还用于：

[0294] 在所述密钥管理请求为第四请求的情况下，调用第三密钥服务，生成第三响应；所述第三密钥服务表征所述第三密钥服务表征密钥登记服务；所述第三响应表征最新版本的业务证书。

[0295] 在一实施例中，第一生成单元2102在根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应时，还用于：

[0296] 在所述密钥管理请求为第五请求的情况下，调用第一密钥服务；所述第五请求用于请求获取解密所述第一密文的密钥信息；所述第一密钥服务表征密钥协商服务；

[0297] 根据所述第一密文的加密方式，生成第五响应；所述第五响应包括解密所述第一密文的密钥信息。

[0298] 在一实施例中，第一生成单元2102在根据所述第一密文的加密方式，生成第五响应时，还用于：

[0299] 在所述第一密文的加密方式为第一加密方式的情况下，调用第一工具，获取所述服务器的第一私钥信息；

[0300] 在所述第一密文的加密方式为第二加密方式的情况下，调用第一工具，获取所述第三密钥信息；所述第三密钥信息表征AES密钥信息；

[0301] 在所述第一密文的加密方式为第三方式的情况下，根据第一标记，获取第一密钥信息与第二密钥信息；所述第一标记表征所述第一密钥服务历史协商所述服务器与所述客户端之间的密钥信息。

[0302] 在一实施例中，所述装置还用于：

[0303] 在无法获取解密所述第一密文的密钥信息的情况下，生成第七响应；所述第七响应表征协商密钥信息失败。

[0304] 基于上述程序模块的硬件实现，且为了实现本申请实施例的方法，本申请实施例还提供了一种电子设备，图22为本申请实施例电子设备的硬件组成结构示意图，如图22所示，电子设备包括：

[0305] 通信接口1，能够与其它设备比如网络设备等进行信息交互；

[0306] 处理器2，与通信接口1连接，以实现与其它设备进行信息交互，用于运行计算机程序时，执行上述一个或多个技术方案提供的数据传输方法。而所述计算机程序存储在存储器3上。

[0307] 当然，实际应用时，电子设备中的各个组件通过总线系统4耦合在一起。可理解，总线系统4用于实现这些组件之间的连接通信。总线系统4除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图22中将各种总线都标为总线系统4。

[0308] 本申请实施例中的存储器3用于存储各种类型的数据以支持电子设备的操作。这些数据的示例包括：用于在电子设备上操作的任何计算机程序。

[0309] 可以理解，存储器3可以是易失性存储器或非易失性存储器，也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(ROM，Read Only Memory)、可编程只读存储器(PROM，Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM，Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM，Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器(FRAM，ferromagnetic random access memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM，Compact Disc Read-Only Memory)；磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器(RAM，Random Access Memory)，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(SRAM，Static Random Access Memory)、同步静态随机存取存储器(SSRAM，Synchronous Static Random Access Memory)、动态随机存取存储器(DRAM，Dynamic Random Access Memory)、同步动态随机存取存储器(SDRAM，Synchronous

Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器(DDRSDRAM,Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器(ESDRAM,Enhanced Synchronous Dynamic Random Access Memory)、同步连接动态随机存取存储器(SLDRAM,SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器(DRRAM,Direct Rambus Random Access Memory)。本申请实施例描述的存储器3旨在包括但不限于这些和任意其它适合类型的存储器。

[0310] 上述本申请实施例揭示的方法可以应用于处理器2中,或者由处理器2实现。处理器2可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器2中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器2可以是通用处理器、DSP,或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器2可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤,可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中,该存储介质位于存储器3,处理器2读取存储器3中的程序,结合其硬件完成前述方法的步骤。

[0311] 处理器2执行所述程序时实现本申请实施例的各个方法中的相应流程,为了简洁,在此不再赘述。

[0312] 在示例性实施例中,本申请实施例还提供了一种存储介质,即计算机存储介质,具体为计算机可读存储介质,例如包括存储计算机程序的存储器3,上述计算机程序可由处理器2执行,以完成前述方法所述步骤。计算机可读存储介质可以是FRAM、ROM、PROM、EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或CD-ROM等存储器。

[0313] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置、终端和方法,可以通过其它的方式实现。以上所描述的设备实施例仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,如:多个单元或组件可以结合,或可以集成到另一个系统,或一些特征可以忽略,或不执行。另外,所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口,设备或单元的间接耦合或通信连接,可以是电性的、机械的或其它形式的。

[0314] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的,作为单元显示的部件可以是、或也可以不是物理单元,即可以位于一个地方,也可以分布到多个网络单元上;可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0315] 另外,在本申请各实施例中的各功能单元可以全部集成在一个处理单元中,也可以是各单元分别单独作为一个单元,也可以两个或两个以上单元集成在一个单元中;上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能单元的形式实现。

[0316] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成,前述的程序可以存储于一计算机可读取存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0317] 或者,本申请上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请实施

例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台电子设备(可以是个人计算机、服务器、或者网络设备等)执行本申请各个实施例所述方法的全部或部分。而前述的存储介质包括：移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0318] 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。


业务场景
RSA数字信封
ECC数字信封
Noise框架
业务域
密钥运营
密钥登记
流量卸载
业务域
密钥配置
业务证书分发
组密钥分发
密钥采集
密钥装载
数据统计
协议鉴权
业务鉴权
基础函数
密钥卸载
密钥协商
密钥存储
应用密钥分发
密钥同步
审批
业务域
底软API
PKI
KMS
MES
云平台
MO
应用网关

图1


接入层
客户端
服务器
运营后台
SDK
集成
应用层
密钥运营
密钥登记
流量卸载
流量卸载
集成
领域层
密钥管理
密钥同步
密钥装载
密钥协商
密钥采集
业务鉴权
密钥分发
数据统计
基础设施层
底软API
PKI
KMS
MES
云平台
MO
应用网关

图2

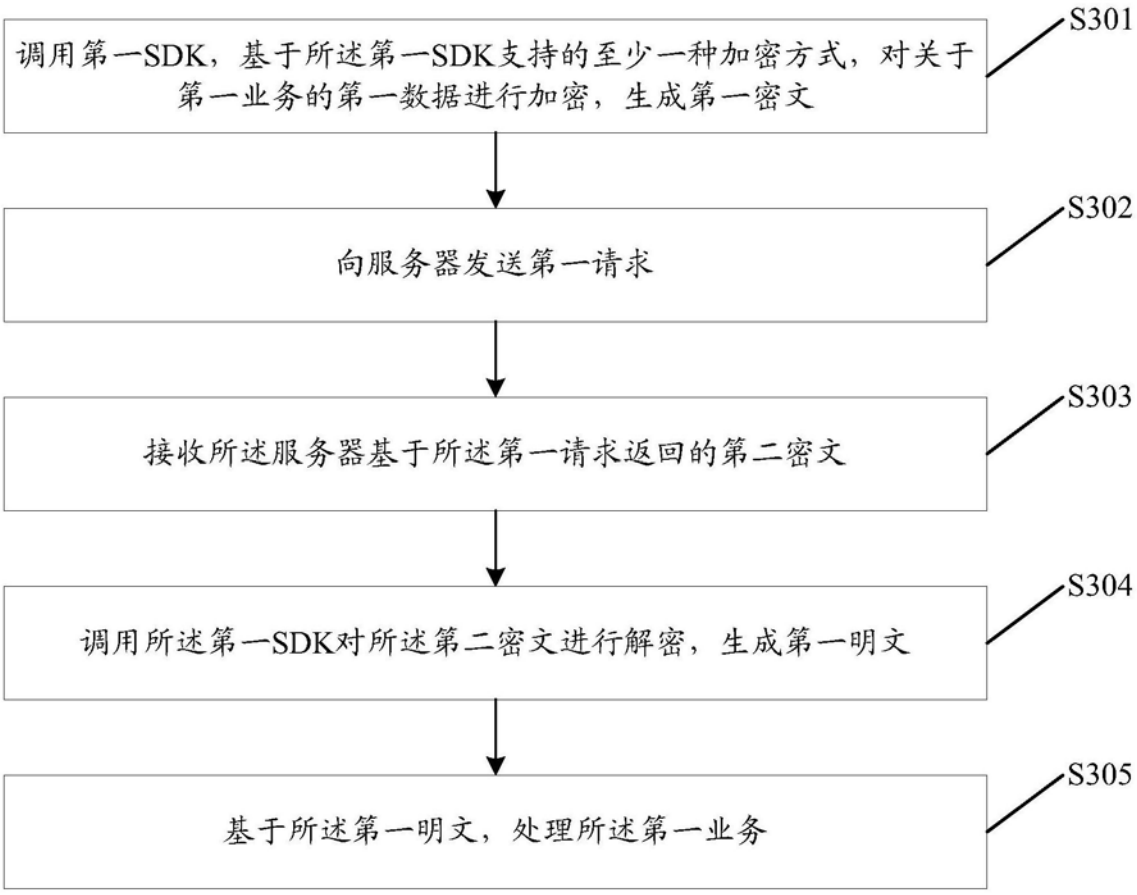

调用第一SDK，基于所述第一SDK支持的至少一种加密方式，对关于第一业务的第一数据进行加密，生成第一密文
S301
向服务器发送第一请求
S302
接收所述服务器基于所述第一请求返回的第二密文
S303
调用所述第一SDK对所述第二密文进行解密，生成第一明文
S304
基于所述第一明文，处理所述第一业务
S305

图3

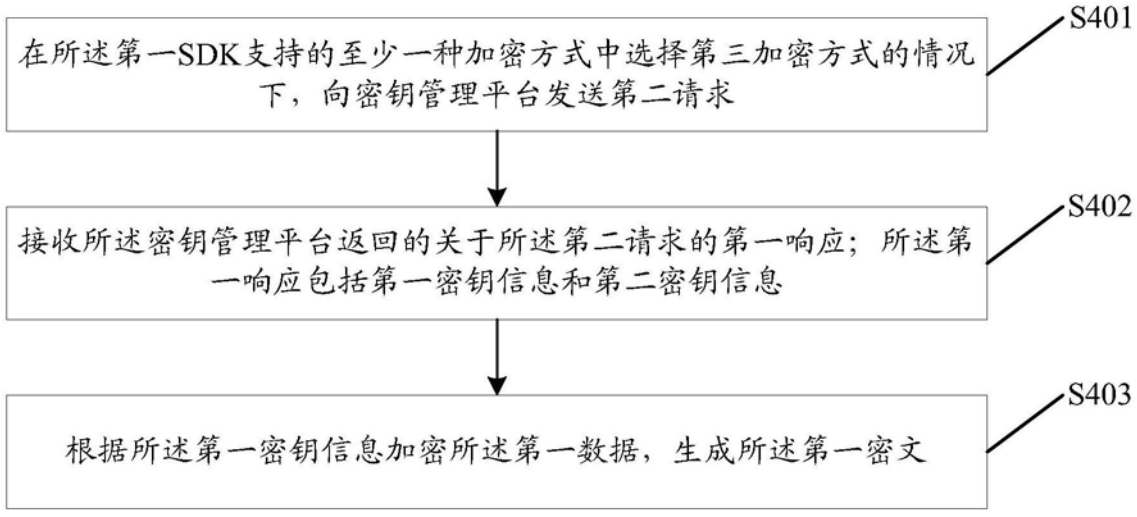

在所述第一SDK支持的至少一种加密方式中选择第三加密方式的情况下，向密钥管理平台发送第二请求
S401
接收所述密钥管理平台返回的关于所述第二请求的第一响应；所述第一响应包括第一密钥信息和第二密钥信息
S402
根据所述第一密钥信息加密所述第一数据，生成所述第一密文
S403

图4

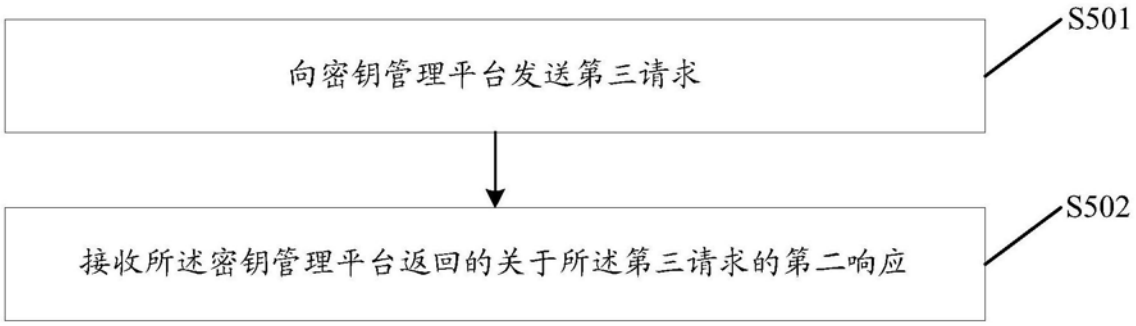

向密钥管理平台发送第三请求
S501
接收所述密钥管理平台返回的关于所述第三请求的第二响应
S502

图5

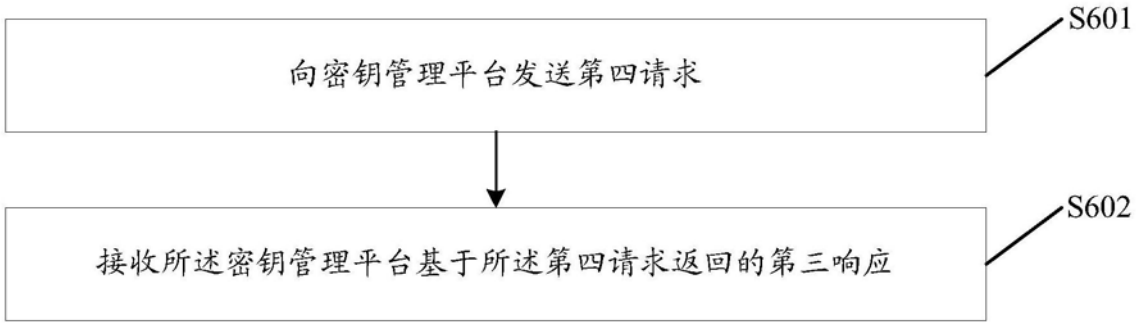

向密钥管理平台发送第四请求
S601
接收所述密钥管理平台基于所述第四请求返回的第三响应
S602

图6

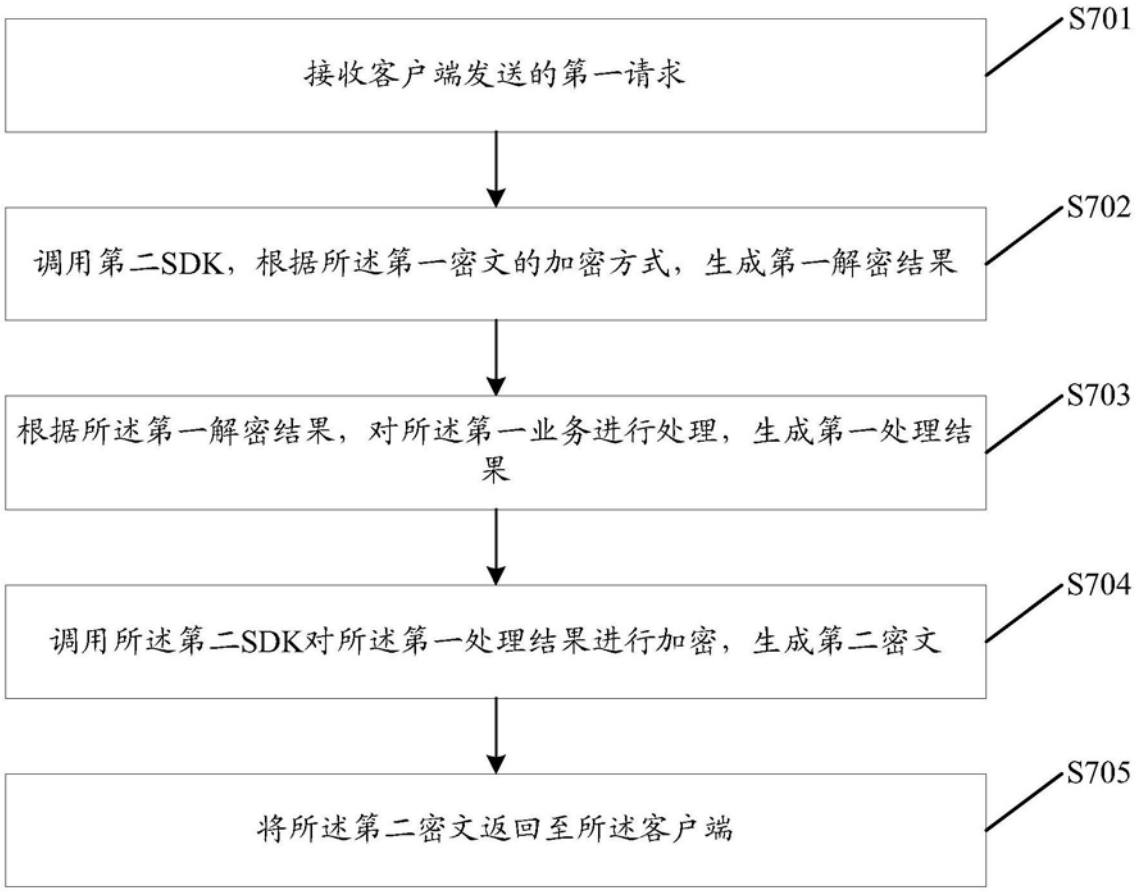

S701
接收客户端发送的第一请求
S702
调用第二SDK，根据所述第一密文的加密方式，生成第一解密结果
S703
根据所述第一解密结果，对所述第一业务进行处理，生成第一处理结果
S704
调用所述第二SDK对所述第一处理结果进行加密，生成第二密文
S705
将所述第二密文返回至所述客户端

图7

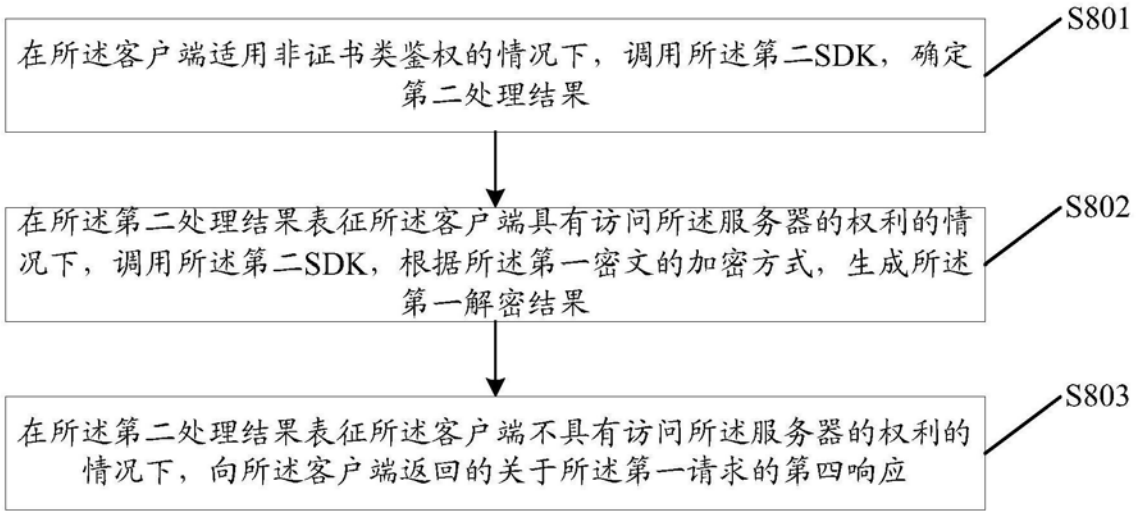

S801
在所述客户端适用非证书类鉴权的情况下，调用所述第二SDK，确定第二处理结果
S802
在所述第二处理结果表征所述客户端具有访问所述服务器的权利的情况下，调用所述第二SDK，根据所述第一密文的加密方式，生成所述第一解密结果
S803
在所述第二处理结果表征所述客户端不具有访问所述服务器的权利的情况下，向所述客户端返回的关于所述第一请求的第四响应

图8

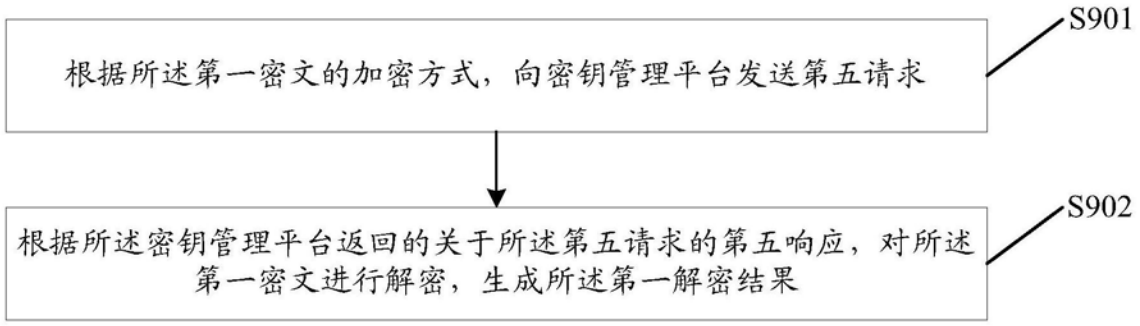

S901
根据所述第一密文的加密方式，向密钥管理平台发送第五请求
S902
根据所述密钥管理平台返回的关于所述第五请求的第五响应，对所述第一密文进行解密，生成所述第一解密结果

图9

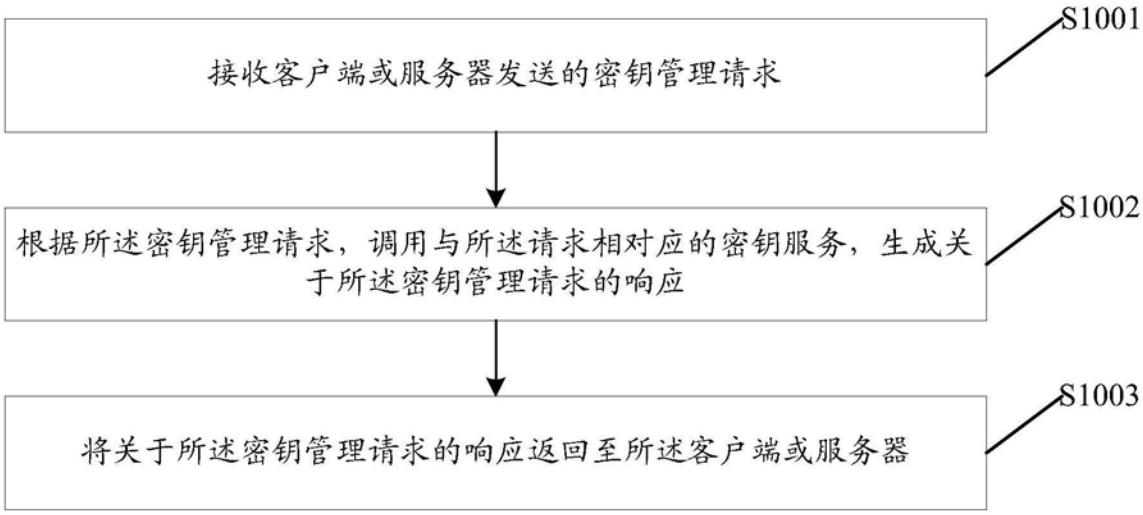

S1001
接收客户端或服务器发送的密钥管理请求
S1002
根据所述密钥管理请求，调用与所述请求相对应的密钥服务，生成关于所述密钥管理请求的响应
S1003
将关于所述密钥管理请求的响应返回至所述客户端或服务器

图10

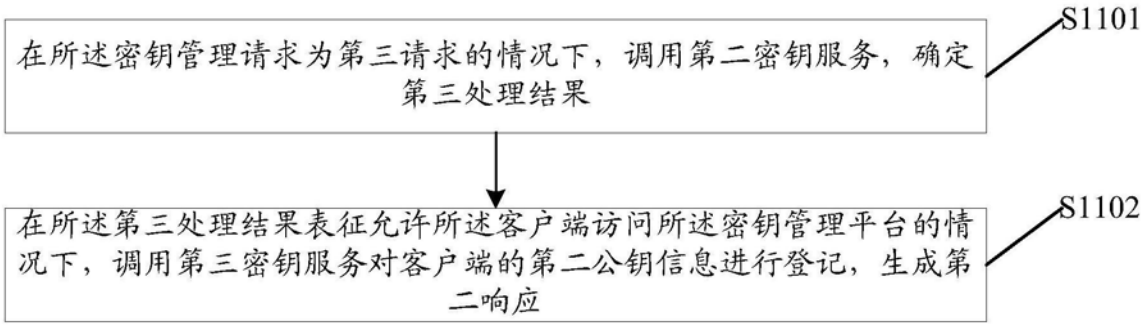

S1101
在所述密钥管理请求为第三请求的情况下，调用第二密钥服务，确定第三处理结果
S1102
在所述第三处理结果表征允许所述客户端访问所述密钥管理平台的情况下，调用第三密钥服务对客户端的第二公钥信息进行登记，生成第二响应

图11

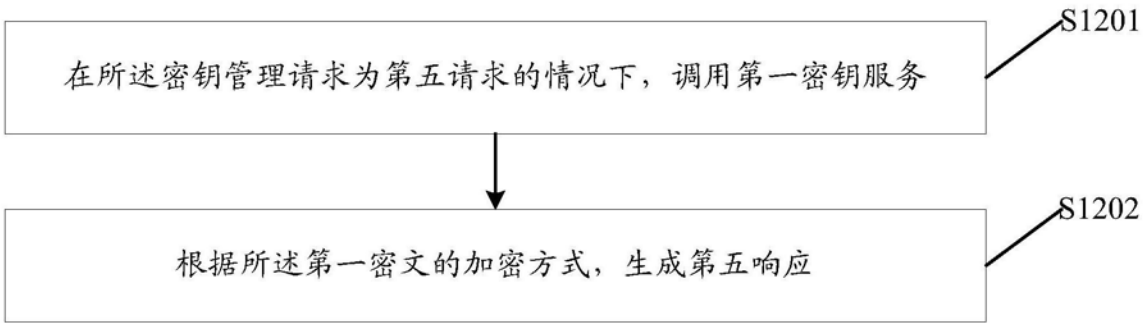

在所述密钥管理请求为第五请求的情况下，调用第一密钥服务
S1201
根据所述第一密文的加密方式，生成第五响应
S1202

图12

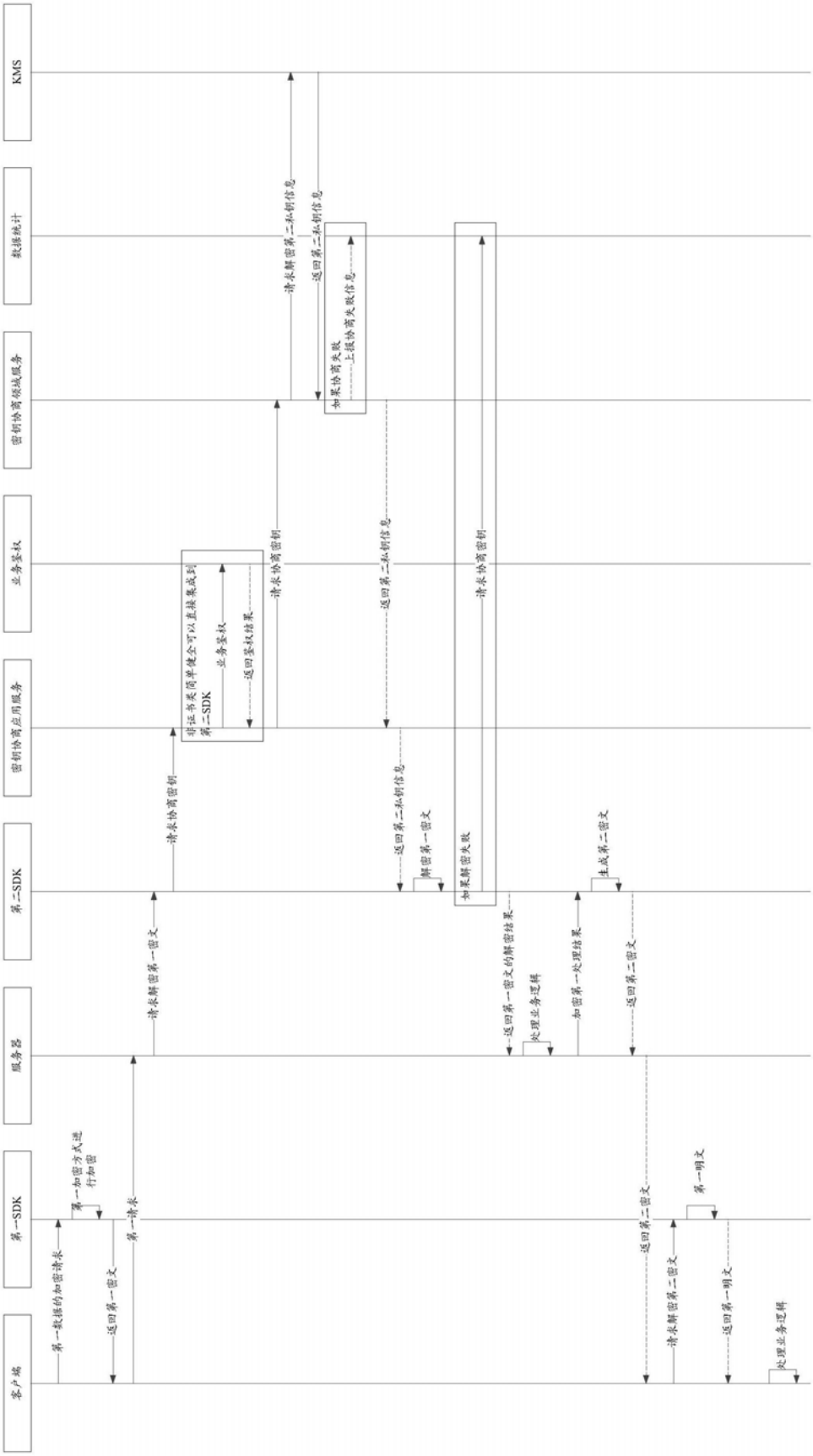

客户端
第一SDK
服务器
第二SDK
密钥协商应用服务
业务鉴权
密钥协商领域服务
数据统计
KMS
第一数据的加密请求
第一加密方式进行加密
返回第一密文
第一请求
请求解密第一密文
请求协商密钥
非法书类简单健全可以直接集成到第二SDK
业务鉴权
返回鉴权结果
请求协商密钥
请求解密第二私钥信息
返回第二私钥信息
如果协商失败
上报协商失败信息
返回第二私钥信息
返回第二私钥信息
解密第一密文
请求协商密钥
如果解密失败
返回第一密文的解密结果
处理业务逻辑
加密第一处理结果
生成第二密文
返回第二密文
返回第二密文
请求解密第二密文
第一明文
返回第一明文
处理业务逻辑

图13

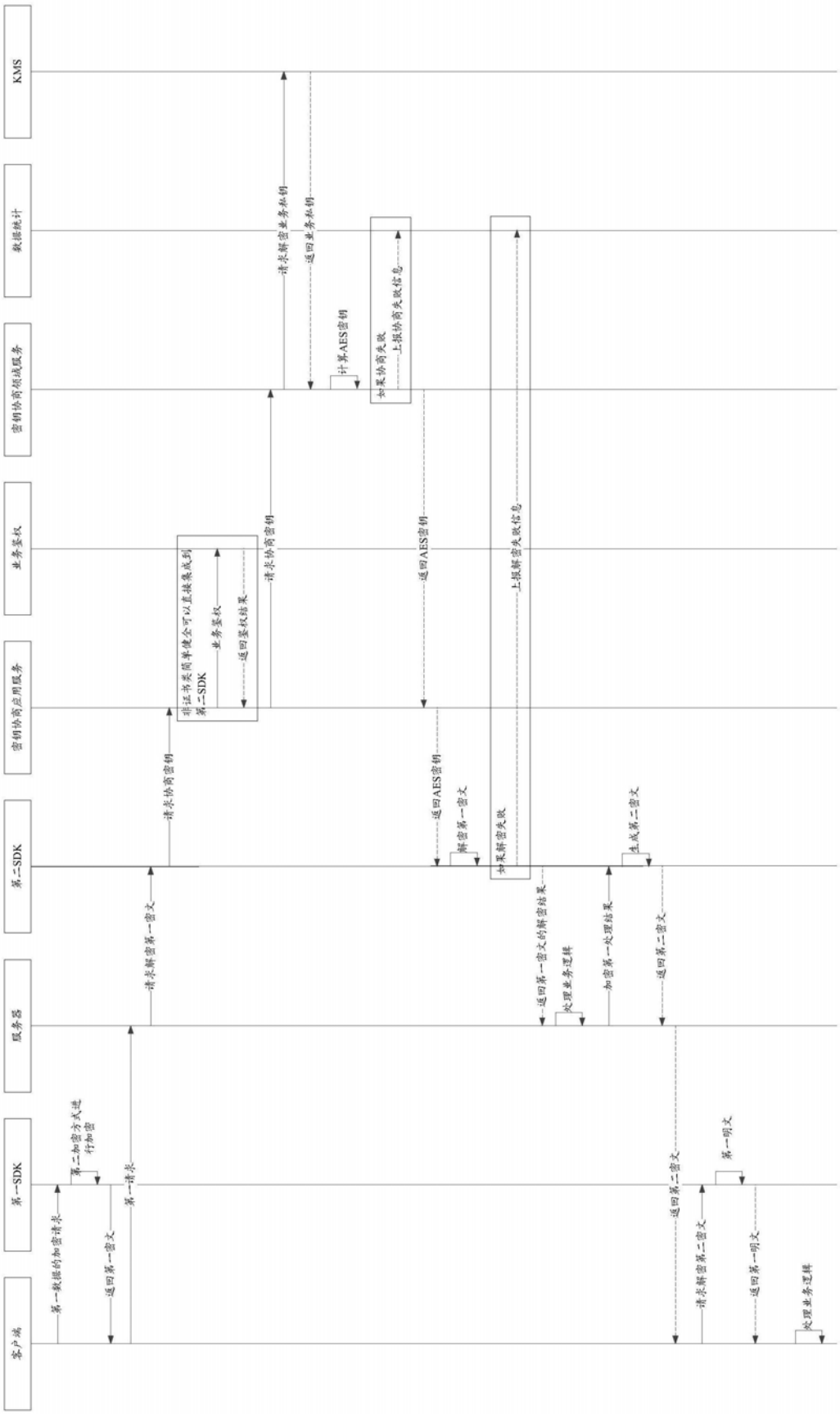

KMS
数据统计
密钥协商领域服务
业务鉴权
密钥协商应用服务
第二SDK
服务器
第一SDK
客户端
第一数据的加密请求
第二加密方式进行加密
返回第一密文
第一请求
请求协商密钥
非证书类简单健全可以直接集成到第二SDK
业务鉴权
返回鉴权结果
请求协商密钥
请求解密业务私钥
返回业务私钥
计算AES密钥
如果协商失败
上报协商失败信息
返回AES密钥
返回AES密钥
解密第一密文
如果解密失败
上报解密失败信息
请求解密第一密文
返回第一密文的解密结果
处理业务逻辑
加密第一处理结果
生成第二密文
返回第二密文
返回第二密文
请求解密第二密文
第一明文
返回第一明文
处理业务逻辑

图14

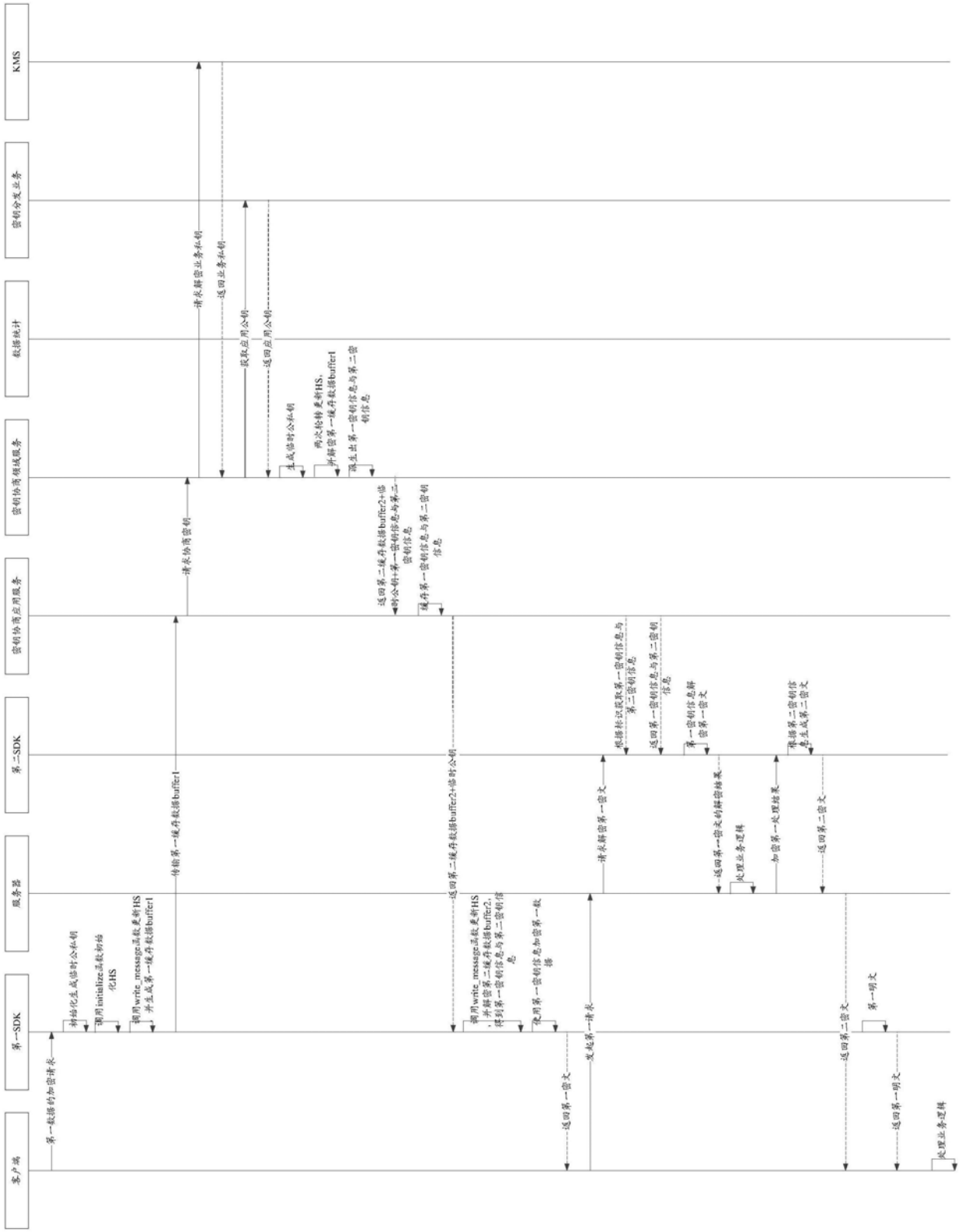

客户端
第一SDK
服务器
第二SDK
密钥协商应用服务
密钥协商领域服务
数据统计
密钥分发业务
KMS
第一数据的加密请求
初始化生成临时公私钥
调用initialize函数初始化HS
调用write_message函数更新HS并生成第一缓存数据buffer1
传输第一缓存数据buffer1
请求协商密钥
请求解密业务私钥
返回业务私钥
获取应用公钥
返回应用公钥
生成临时公私钥
调用write_message函数更新HS，并解密第一缓存数据buffer1得到第一密钥信息与第二密钥信息
派生出第一密钥信息与第二密钥信息
返回第二缓存数据buffer2+临时公钥+第一密钥信息与第二密钥信息
缓存第一密钥信息与第二密钥信息
返回第二缓存数据buffer2+临时公钥
调用write_message函数更新HS，并解密第二缓存数据buffer2，得到第一密钥信息与第二密钥信息
使用第一密钥信息加密第一数据
返回第一密文
发起第一请求
请求解密第一密文
根据标识获取第一密钥信息与第二密钥信息
返回第一密钥信息与第二密钥信息
第一密钥信息解密第一密文
返回第一密文的解密结果
处理业务逻辑
加密第一处理结果
根据第二密钥信息生成第二密文
返回第二密文
返回第二密文
第一明文
返回第一明文
处理业务逻辑

图15

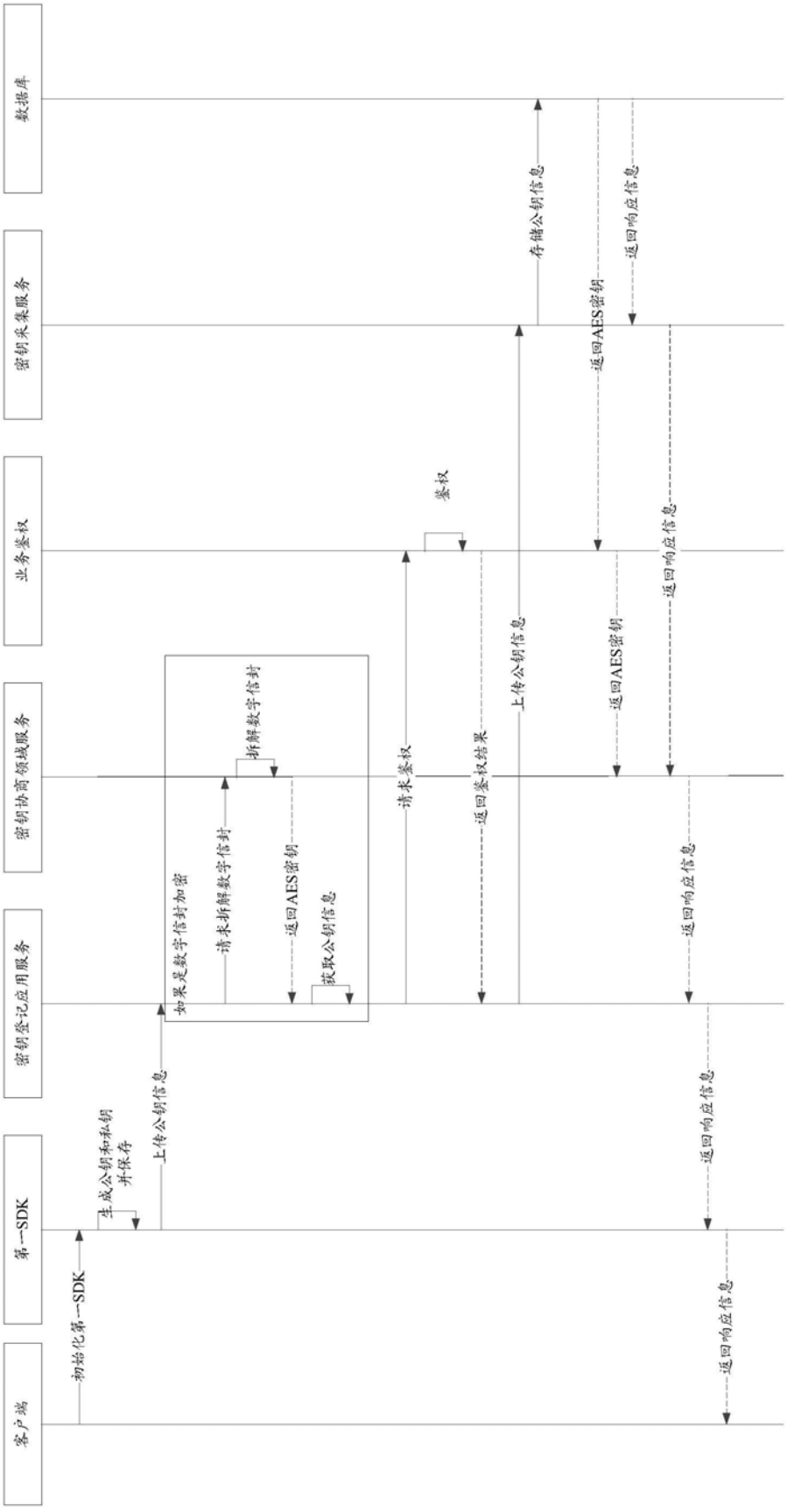

客户端
第一SDK
密钥登记应用服务
密钥协商领域服务
业务鉴权
密钥采集服务
数据库
初始化第一SDK
生成公钥和私钥并保存
上传公钥信息
如果是数字信封加密
请求解密数字信封
返回AES密钥
获取公钥信息
解密数字信封
请求鉴权
返回鉴权结果
鉴权
上传公钥信息
存储公钥信息
返回AES密钥
返回响应信息
返回响应信息
返回响应信息
返回响应信息
返回响应信息

图16

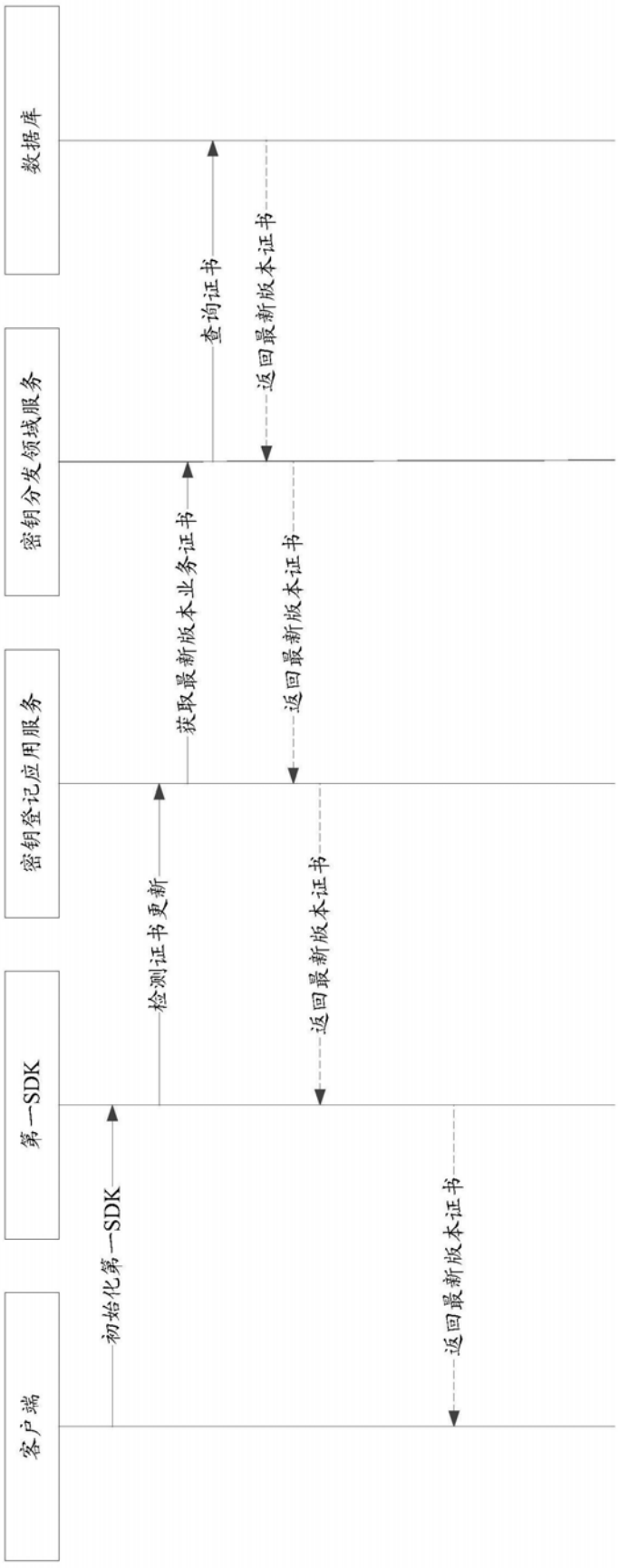

客户端
第一SDK
密钥登记应用服务
密钥分发领域服务
数据库
初始化第一SDK
检测证书更新
获取最新版本业务证书
查询证书
返回最新版本证书
返回最新版本证书
返回最新版本证书
返回最新版本证书

图17

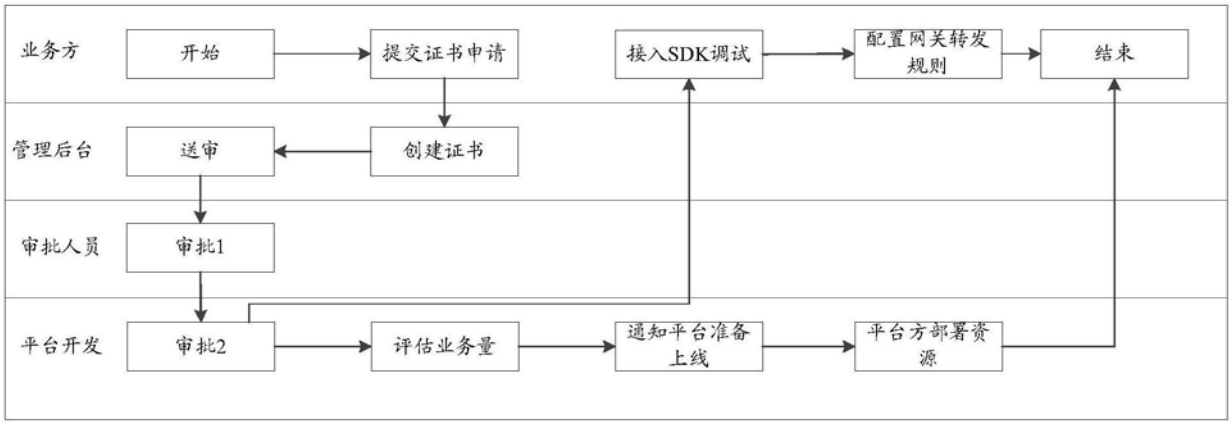

业务方
开始
提交证书申请
接入SDK调试
配置网关转发规则
结束
管理后台
送审
创建证书
审批人员
审批1
平台开发
审批2
评估业务量
通知平台准备上线
平台方部署资源

图18


第一加密单元1901
第一发送单元1902
第一接收单元1903
第一解密单元1904
第一处理单元1905
数据传输装置

图19


第二接收单元2001
第二解密单元2002
第二解密单元2002
第二加密单元2004
第二发送单元2005
数据传输装置

图20

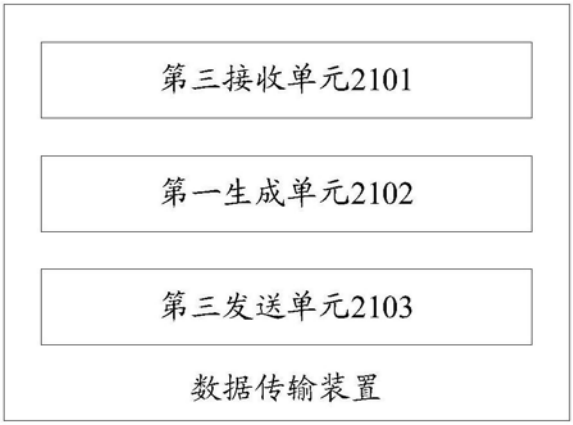

第三接收单元2101
第一生成单元2102
第三发送单元2103
数据传输装置

图21

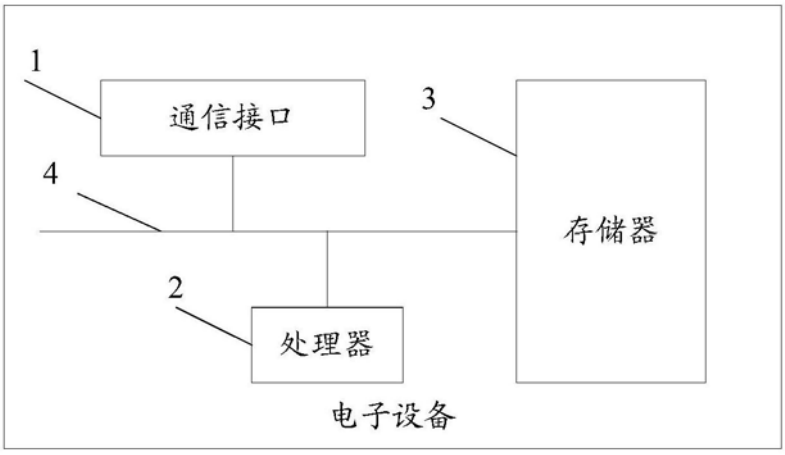



图22