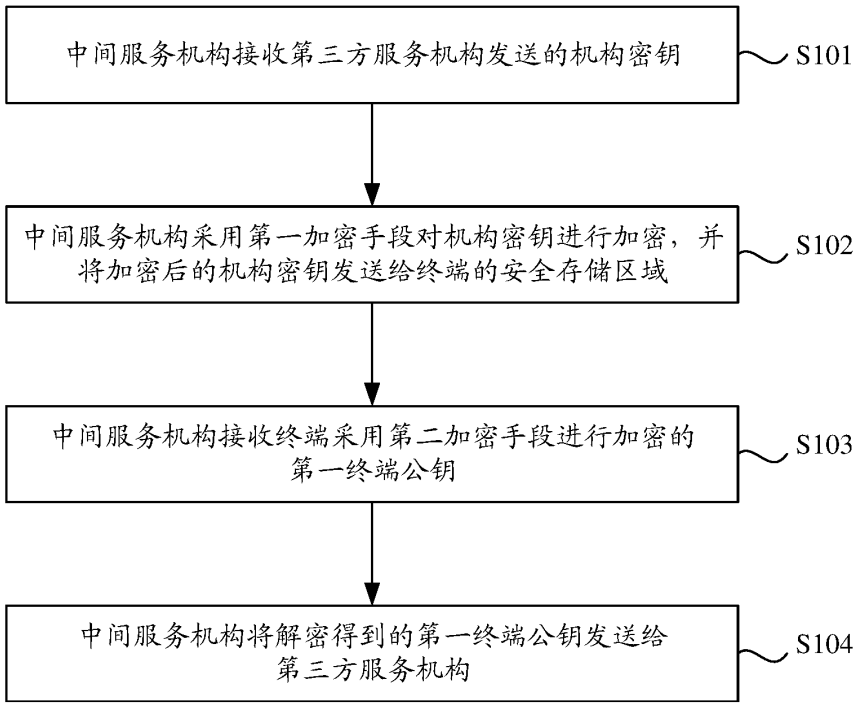
中间服务机构接收第三方服务机构发送的机构密钥
S101
中间服务机构采用第一加密手段对机构密钥进行加密，并将加密后的机构密钥发送给终端的安全存储区域
S102
中间服务机构接收终端采用第二加密手段进行加密的第一终端公钥
S103
中间服务机构将解密得到的第一终端公钥发送给第三方服务机构
S104

图 1

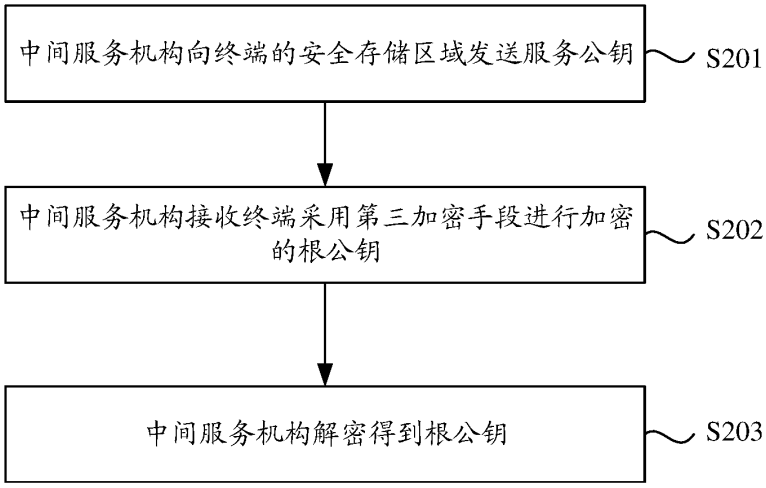
中间服务机构向终端的安全存储区域发送服务公钥
S201
中间服务机构接收终端采用第三加密手段进行加密的根公钥
S202
中间服务机构解密得到根公钥
S203

图 2

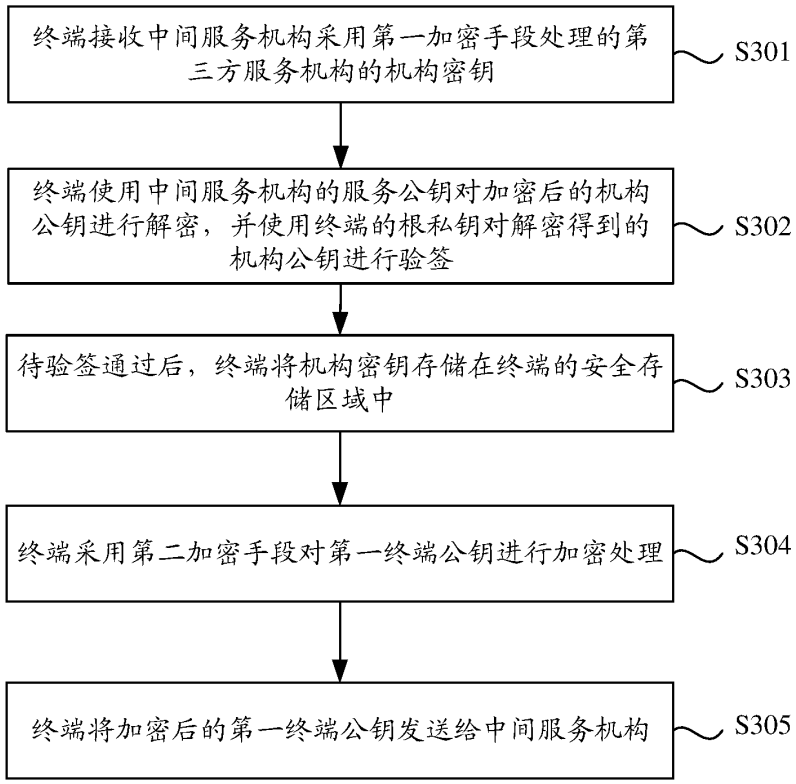
终端接收中间服务机构采用第一加密手段处理的第三方服务机构的机构密钥
S301
终端使用中间服务机构的服务公钥对加密后的机构公钥进行解密，并使用终端的根私钥对解密得到的机构公钥进行验签
S302
待验签通过后，终端将机构密钥存储在终端的安全存储区域中
S303
终端采用第二加密手段对第一终端公钥进行加密处理
S304
终端将加密后的第一终端公钥发送给中间服务机构
S305

图 3

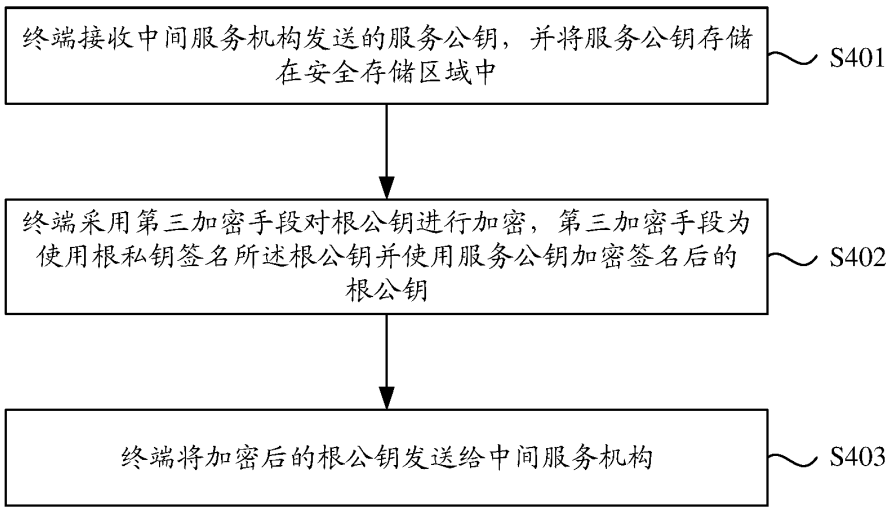
终端接收中间服务机构发送的服务公钥，并将服务公钥存储在安全存储区域中
S401
终端采用第三加密手段对根公钥进行加密，第三加密手段为使用根私钥签名所述根公钥并使用服务公钥加密签名后的根公钥
S402
终端将加密后的根公钥发送给中间服务机构
S403

图 4

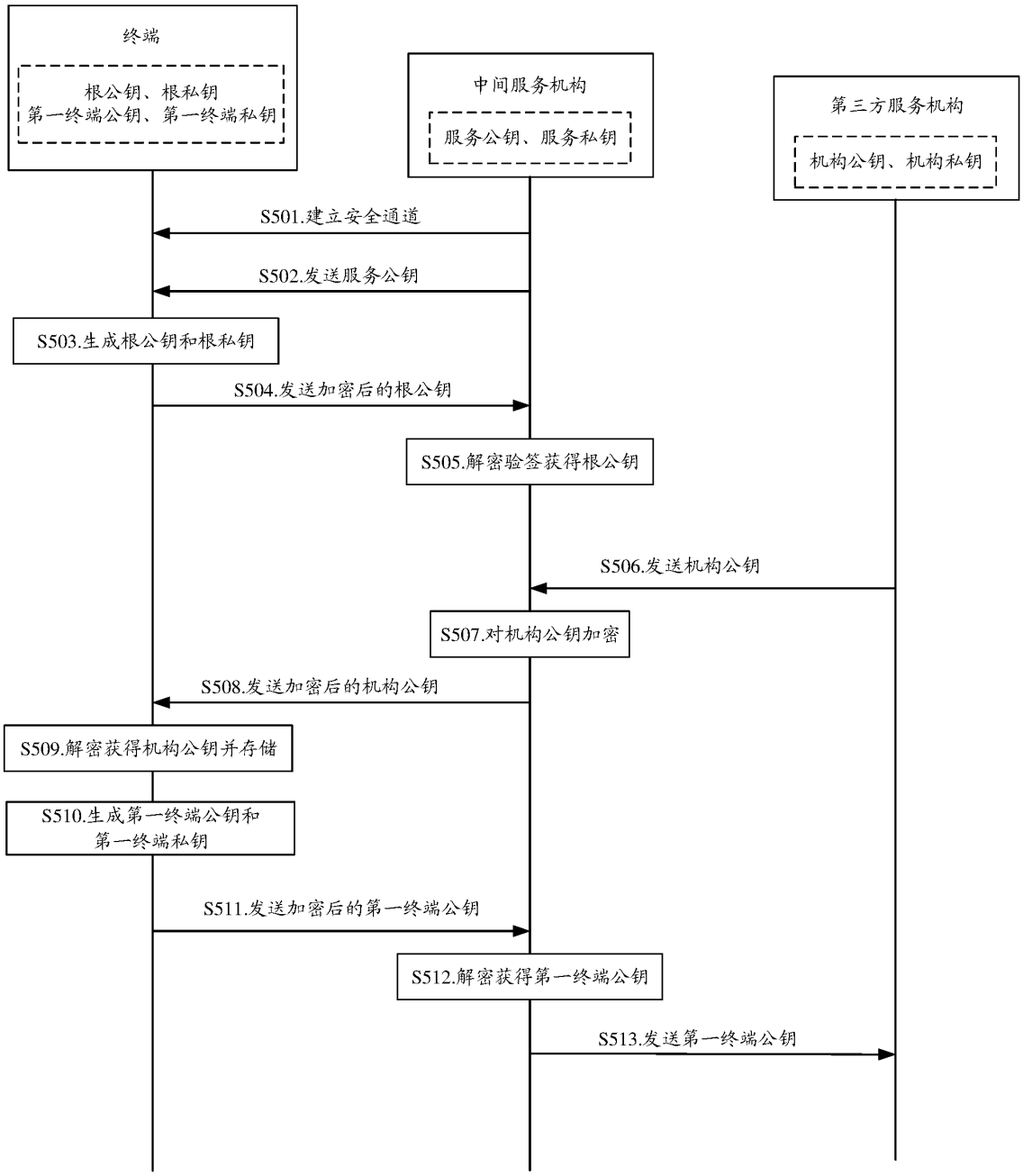
终端
根公钥、根私钥
第一终端公钥、第一终端私钥
中间服务机构
服务公钥、服务私钥
第三方服务机构
机构公钥、机构私钥
S501.建立安全通道
S502.发送服务公钥
S503.生成根公钥和根私钥
S504.发送加密后的根公钥
S505.解密验签获得根公钥
S506.发送机构公钥
S507.对机构公钥加密
S508.发送加密后的机构公钥
S509.解密获得机构公钥并存储
S510.生成第一终端公钥和
第一终端私钥
S511.发送加密后的第一终端公钥
S512.解密获得第一终端公钥
S513.发送第一终端公钥

图 5

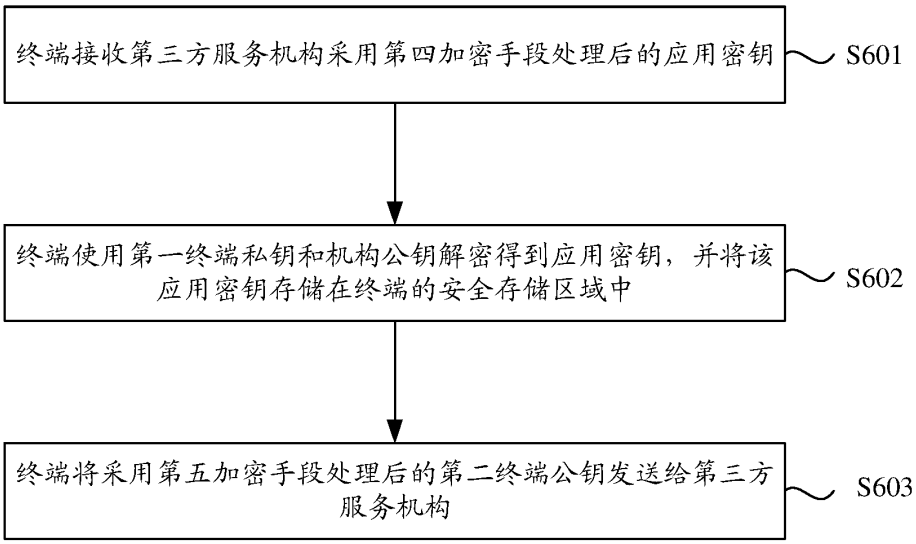
终端接收第三方服务机构采用第四加密手段处理后的应用密钥
S601
终端使用第一终端私钥和机构公钥解密得到应用密钥，并将该应用密钥存储在终端的安全存储区域中
S602
终端将采用第五加密手段处理后的第二终端公钥发送给第三方服务机构
S603

图 6

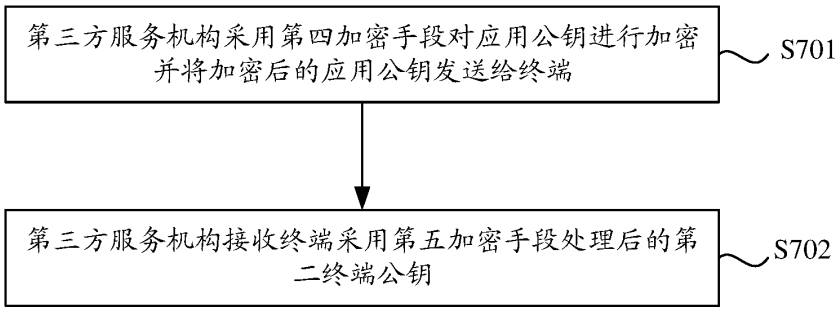
第三方服务机构采用第四加密手段对应用公钥进行加密并将加密后的应用公钥发送给终端
S701
第三方服务机构接收终端采用第五加密手段处理后的第二终端公钥
S702

图 7

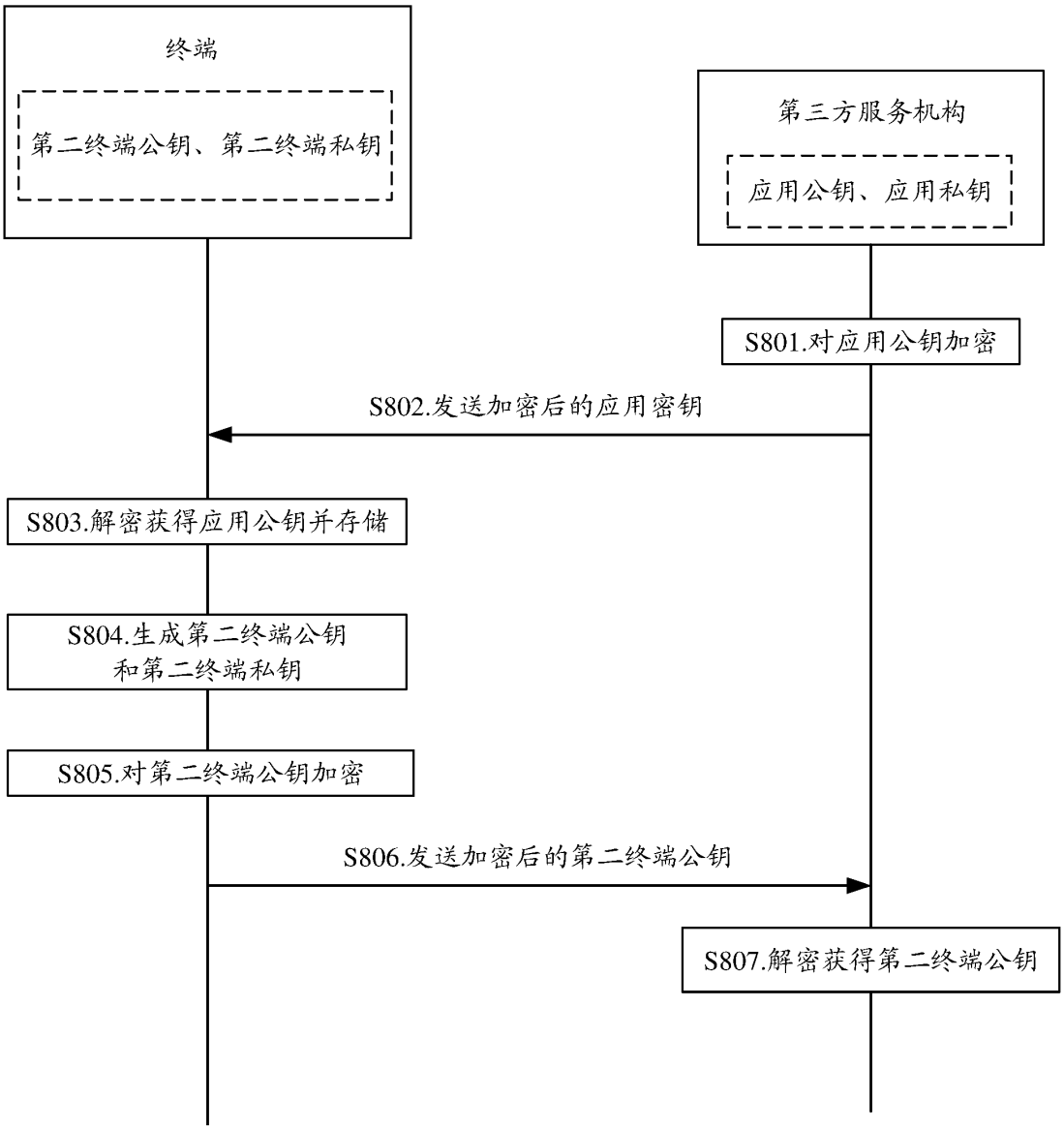
终端
第二终端公钥、第二终端私钥
第三方服务机构
应用公钥、应用私钥
S801.对应用公钥加密
S802.发送加密后的应用密钥
S803.解密获得应用公钥并存储
S804.生成第二终端公钥
和第二终端私钥
S805.对第二终端公钥加密
S806.发送加密后的第二终端公钥
S807.解密获得第二终端公钥

图 8

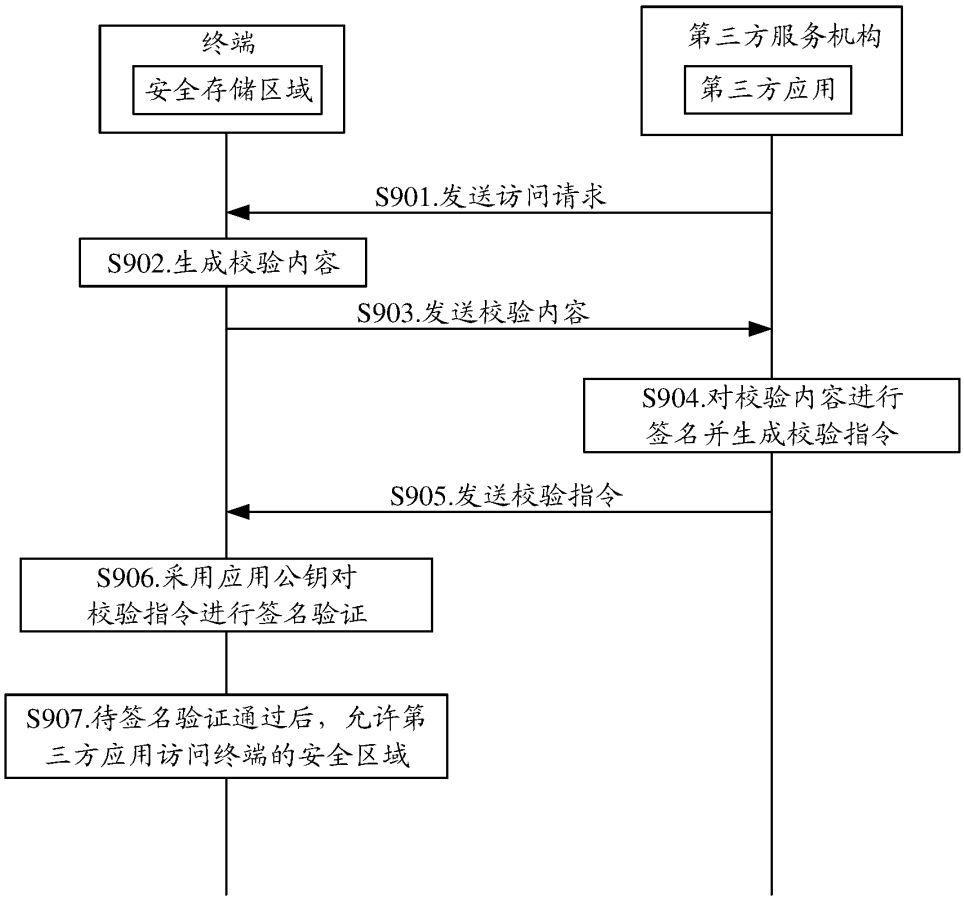
终端
安全存储区域
第三方服务机构
第三方应用
S901.发送访问请求
S902.生成校验内容
S903.发送校验内容
S904.对校验内容进行签名并生成校验指令
S905.发送校验指令
S906.采用应用公钥对校验指令进行签名验证
S907.待签名验证通过后，允许第三方应用访问终端的安全区域

图 9

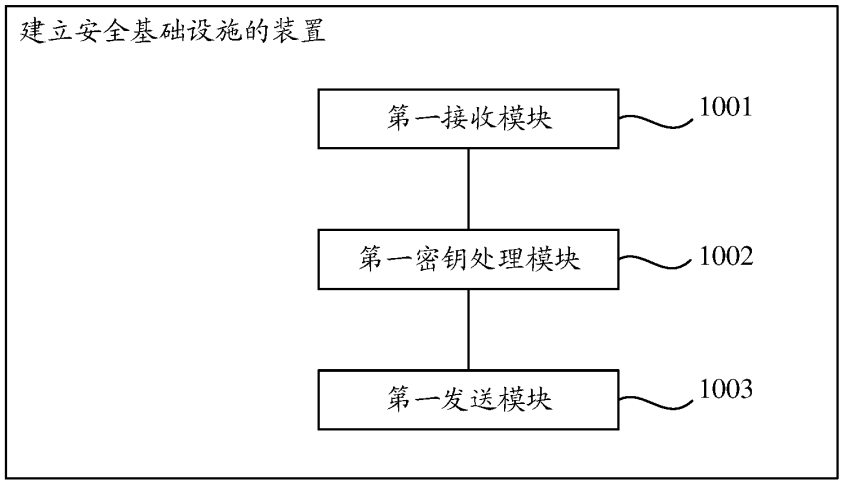
建立安全基础设施的装置
第一接收模块
1001
第一密钥处理模块
1002
第一发送模块
1003

图 10

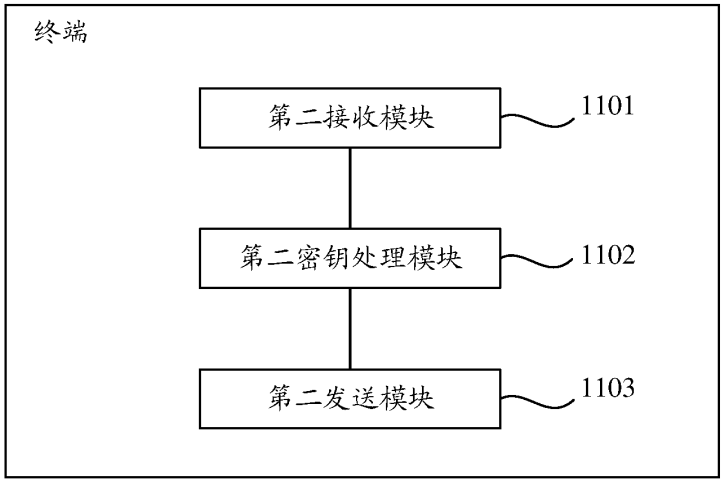
终端
第二接收模块
1101
第二密钥处理模块
1102
第二发送模块
1103

图 11

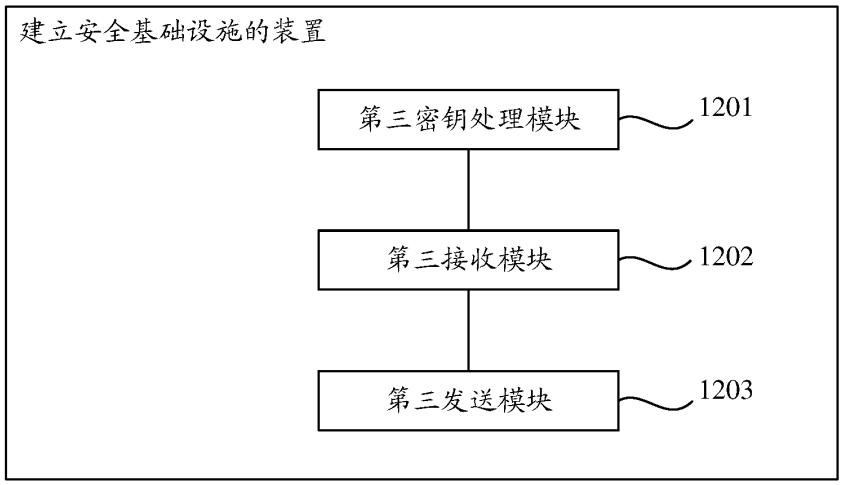
建立安全基础设施的装置
第三密钥处理模块
1201
第三接收模块
1202
第三发送模块
1203

图 12

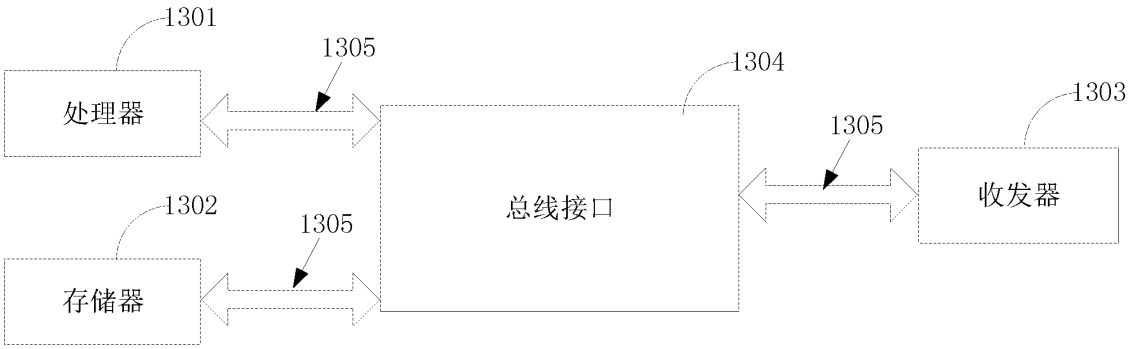
1301
处理器
1305
1304
总线接口
1305
1303
收发器
1302
存储器
1305

图 13

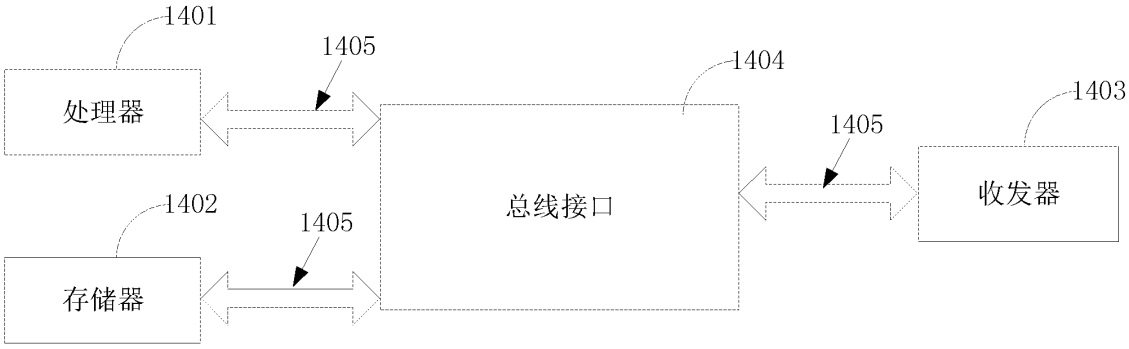
1401
处理器
1405
1404
总线接口
1405
1403
收发器
1402
存储器
1405

图 14

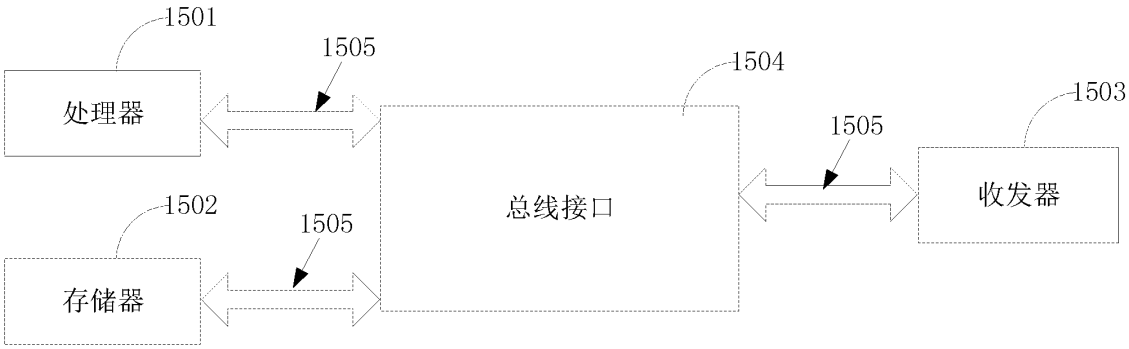
1501
处理器
1505
1504
总线接口
1505
1503
收发器
1502
存储器
1505

图 15