(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 112448810 A
(43)申请公布日 2021.03.05

(21)申请号 201910819754.2

(22)申请日 2019.08.31

(71)申请人 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 李泳 张冠男 王益丰

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 朱琳琳

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)

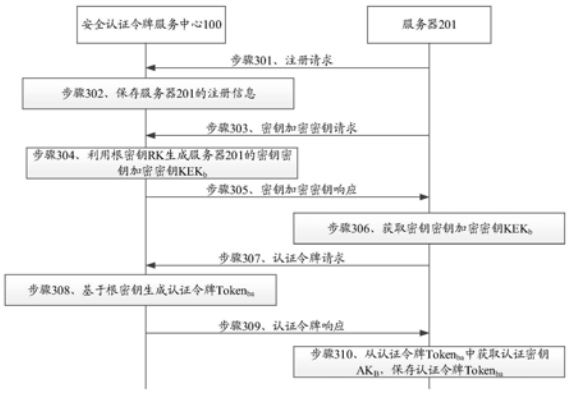
权利要求书5页 说明书20页 附图4页

(54)发明名称

一种认证方法以及装置

(57)摘要

一种认证方法以及装置，用以提高一种服务器之间的认证效率。本申请中，第一服务器可以先从安全认证令牌服务中心获取基于根密钥生成的第一服务器的密钥加密密钥和第一服务器与第二服务器认证所需的认证令牌，认证令牌包括第一认证参数；之后，第一服务器可以根据第一服务器的密钥加密密钥对认证令牌中的第一认证参数进行认证；当第一服务器在对第一认证参数认证成功后，第一服务器从第一认证参数中获取第一服务器的认证密钥，保存认证令牌；后续第一服务器和第二服务器之间的认证是基于从安全认证令牌服务中心获取的认证令牌进行的，能够有效的简化服务器之间认证流程，以提高服务器之间的认证效率。



CN 112448810 A

1.一种认证方法,其特征在于,该方法包括:

安全认证令牌服务中心基于根密钥生成第一服务器的密钥加密密钥、所述第一服务器的认证密钥以及第二服务器的密钥加密密钥;

所述安全认证令牌服务中心生成包括第一认证参数和第二认证参数的认证令牌,其中,所述第一认证参数是利用所述第一服务器的密钥加密密钥对所述第一服务器的认证密钥进行认证加密生成的,所述第二认证参数是利用第二服务器的密钥加密密钥对所述第一服务器的认证密钥进行认证加密生成的;

所述安全认证令牌服务中心向所述第一服务器发送所述第一服务器的密钥加密密钥和所述认证令牌;

所述安全认证令牌服务中心向所述第二服务器发送所述第二服务器的密钥加密密钥。

2.如权利要求1所述的方法,其特征在于,所述方法还包括:

所述安全认证令牌服务中心基于根密钥生成第一服务器的数据密钥;

所述第一认证参数是利用所述第一服务器的密钥加密密钥对所述第一服务器的认证密钥和数据密钥进行认证加密生成的。

3.如权利要求2所述的方法,其特征在于,所述第二认证参数是利用所述第二服务器的密钥加密密钥对所述第一服务器的认证密钥和数据密钥进行认证加密生成的。

4.如权利要求1～3任一所述的方法,其特征在于,所述安全认证令牌服务中心向所述第一服务器发送所述第一服务器的密钥加密密钥,包括:

所述安全认证令牌服务中心接收来自所述第一服务器的第一请求,所述第一请求用于请求所述第一服务器的密钥加密密钥,所述第一请求包括所述第一服务器的随机公钥;

所述安全认证令牌服务中心利用所述第一服务器的随机公钥对所述第一服务器的密钥加密密钥进行加密生成第三认证参数;

所述安全认证令牌服务中心向所述第一服务器发送第一响应,所述第一响应中包括所述第三认证参数。

5.如权利要求4所述的方法,其特征在于,所述第一请求还包括第一签名值,所述安全认证令牌服务中心利用所述第一服务器的随机公钥对所述第一服务器的密钥加密密钥进行加密生成第三认证参数之前,还包括:

所述安全认证令牌服务中心利用所述第一服务器的证书公钥对所述第一签名值验证成功。

6.如权利要求4或5所述的方法,其特征在于,所述第一响应还包括第二签名值,所述第二签名值是根据所述安全认证令牌服务中心的证书私钥对所述第一服务器的密钥加密密钥进行签名生成的。

7.一种认证方法,其特征在于,该方法包括:

第一服务器从安全认证令牌服务中心获取所述第一服务器的密钥加密密钥和所述第一服务器与第二服务器认证所需的认证令牌,所述认证令牌包括第一认证参数;其中,所述第一认证参数是所述安全认证令牌服务中心利用所述第一服务器的密钥加密密钥对所述第一服务器的认证密钥进行认证加密生成的;

所述第一服务器根据所述第一服务器的密钥加密密钥对所述认证令牌中的第一认证参数进行认证;

所述第一服务器在对所述第一认证参数认证成功后，利用所述第一服务器的密钥加密密钥对所述第一认证参数进行解密获取所述第一服务器的认证密钥；

所述第一服务器向所述第二服务器发送服务请求，所述服务请求用于请求所述第二服务器为所述第一服务器提供服务，所述服务请求中包括所述认证令牌、认证信息、以及指示信息；其中，所述认证信息是利用所述第一服务器的认证密钥对所述指示信息进行认证加密生成的，所述指示信息用于指示所述第一服务器所请求的服务类型。

8.如权利要求7所述的方法，其特征在于，还包括：

所述第一服务器利用所述第一服务器的密钥加密密钥对所述第一认证参数进行解密后，从所述第一认证参数中获取所述第一服务器的数据密钥；

所述服务请求中还包括第一密文，所述第一密文是利用所述第一服务器的数据密钥对所述第一服务器的敏感数据加密生成的，所述敏感数据为需要加密的数据。

9.如权利要求7或8所述的方法，其特征在于，所述第一服务器从安全认证令牌服务中心获取所述第一服务器的密钥加密密钥，包括：

所述第一服务器向所述安全认证令牌服务中心发送第一请求，所述第一请求用于请求所述第一服务器的密钥加密密钥，所述第一请求包括所述第一服务器的随机公钥；

所述第一服务器接收所述安全认证令牌服务中心的第一响应，所述第一响应中包括第三认证参数，其中，所述第三认证参数是所述安全认证令牌服务中心利用所述第一服务器的随机公钥对所述第一服务器的密钥加密密钥进行加密生成的；

所述第一服务器利用所述第一服务器的随机私钥对所述第三认证参数解密后，从所述第三认证参数中获取所述第一服务器的密钥加密密钥。

10.如权利要求9所述的方法，其特征在于，所述第一请求还包括第一签名值，所述第一签名值是根据所述第一服务器的证书私钥对所述第一服务器的随机公钥进行签名生成的。

11.如权利要求9或10所述的方法，其特征在于，所述第一响应还包括第二签名值；

所述第一服务器从所述第三认证参数中获取所述第一服务器的密钥加密密钥之前，还包括：

所述第一服务器利用所述安全认证令牌服务中心的证书公钥对所述第二签名值验证成功。

12.一种认证方法，其特征在于，该方法包括：

第二服务器从安全认证令牌服务中心获取所述第二服务器的密钥加密密钥；

所述第二服务器接收来自第一服务器的服务请求，所述服务请求用于请求所述第二服务器为所述第一服务器提供服务，所述服务请求中包括所述认证令牌、认证信息、以及指示信息，所述指示信息用于指示所述第一服务器所请求的服务类型；

其中，所述认证信息是利用所述第一服务器的认证密钥对所述指示信息进行认证加密生成的；所述认证令牌包括第二认证参数；所述第二认证参数是所述安全认证令牌服务中心利用所述第二服务器的密钥加密密钥对所述第一服务器的认证密钥进行认证加密生成的；

所述第二服务器根据所述第二服务器的密钥加密密钥对所述认证令牌中的第二认证参数进行认证；

所述第二服务器在对所述第二认证参数认证成功后，利用所述第二服务器的密钥加密

密钥对所述第二认证参数进行解密获取所述第一服务器的认证密钥；

所述第二服务器利用所述第一服务器的认证密钥和所述指示信息对所述认证信息认证成功后，向所述第一服务器提供所述指示信息所指示的服务。

13.如权利要求12所述的方法，其特征在于，所述服务请求还包括第一密文，所述方法还包括：

所述第二服务器利用所述第二服务器的密钥加密密钥对所述第二认证参数进行解密后，从所述第二认证参数中获取所述第一服务器的数据密钥；

所述第二服务器利用所述第一服务器的数据密钥，对所述第一密文进行解密获取所述第一服务器的敏感数据，所述敏感数据为需要加密的数据。

14.一种装置，其特征在于，该装置包括生成单元和发送单元：

所述生成单元，用于基于根密钥生成第一服务器的密钥加密密钥、所述第一服务器的认证密钥以及第二服务器的密钥加密密钥；生成包括第一认证参数和第二认证参数的认证令牌，其中，所述第一认证参数是利用所述第一服务器的密钥加密密钥对所述第一服务器的认证密钥进行认证加密生成的，所述第二认证参数是利用第二服务器的密钥加密密钥对所述第一服务器的认证密钥进行认证加密生成的；

所述发送单元，用于向所述第一服务器发送所述第一服务器的密钥加密密钥和所述认证令牌；向所述第二服务器发送所述第二服务器的密钥加密密钥。

15.如权利要求14所述的装置，其特征在于，所述生成单元，还用于基于根密钥生成第一服务器的数据密钥；

所述第一认证参数是利用所述第一服务器的密钥加密密钥对所述第一服务器的认证密钥和数据密钥进行认证加密生成的。

16.如权利要求15所述的装置，其特征在于，所述第二认证参数是利用所述第二服务器的密钥加密密钥对所述第一服务器的认证密钥和数据密钥进行认证加密生成的。

17.如权利要求14～16任一所述的装置，其特征在于，所述装置还包括接收单元，

所述接收单元用于接收来自所述第一服务器的第一请求，所述第一请求用于请求所述第一服务器的密钥加密密钥，所述第一请求包括所述第一服务器的随机公钥；

所述生成单元，还用于利用所述第一服务器的随机公钥对所述第一服务器的密钥加密密钥进行加密生成第三认证参数；

所述发送单元，还用于向所述第一服务器发送第一响应，所述第一响应中包括所述第三认证参数。

18.如权利要求17所述的装置，其特征在于，所述第一请求还包括第一签名值，所述生成单元利用所述第一服务器的随机公钥对所述第一服务器的密钥加密密钥进行加密生成第三认证参数之前，还用于：

利用所述第一服务器的证书公钥对所述第一签名值验证成功。

19.如权利要求17或18所述的装置，其特征在于，所述第一响应还包括第二签名值，所述第二签名值是根据所述安全认证令牌服务中心的证书私钥对所述第一服务器的密钥加密密钥进行签名生成的。

20.一种装置，其特征在于，该装置包括接收单元、处理单元以及发送单元：

所述接收单元，用于从安全认证令牌服务中心获取第一服务器的密钥加密密钥和所述

第一服务器与第二服务器认证所需的认证令牌，所述认证令牌包括第一认证参数，其中，所述第一认证参数是所述安全认证令牌服务中心利用所述第一服务器的密钥加密密钥对所述第一服务器的认证密钥进行认证加密生成的；

所述处理单元，用于根据所述第一服务器的密钥加密密钥对所述认证令牌中的第一认证参数进行认证；在对所述第一认证参数认证成功后，利用所述第一服务器的密钥加密密钥对对所述第一认证参数进行解密获取所述第一服务器的认证密钥；

所述发送单元，用于向所述第二服务器发送服务请求，所述服务请求用于请求所述第二服务器为所述第一服务器提供服务，所述服务请求中包括所述认证令牌、认证信息、以及指示信息；其中，所述认证信息是利用所述第一服务器的认证密钥对所述指示信息进行认证加密生成的，所述指示信息用于指示所述第一服务器所请求的服务类型。

21.如权利要求20所述的装置，其特征在于，所述接收单元，还用于利用所述第一服务器的密钥加密密钥对所述第一认证参数进行解密后，从所述第一认证参数中获取所述第一服务器的数据密钥。

22.如权利要求20或21所述的装置，其特征在于，所述服务请求还包括第一密文，所述第一密文是利用所述第一服务器的数据密钥对所述第一服务器的敏感数据加密生成的，所述敏感数据为需要加密的数据。

23.如权利要求20或21所述的装置，其特征在于，所述发送单元，还用于向所述安全认证令牌服务中心发送第一请求，所述第一请求用于请求所述第一服务器的密钥加密密钥，所述第一请求包括所述第一服务器的随机公钥；

所述接收单元，用于接收所述安全认证令牌服务中心的第一响应，所述第一响应中包括第三认证参数，其中，所述第三认证参数是所述安全认证令牌服务中心利用所述第一服务器的随机公钥对所述第一服务器的密钥加密密钥进行加密生成的；

所述处理单元，还用于利用所述第一服务器的随机私钥对所述第三认证参数解密后，从所述第三认证参数中获取所述第一服务器的密钥加密密钥。

24.如权利要求23所述的装置，其特征在于，所述第一请求还包括第一签名值，所述第一签名值是根据所述第一服务器的证书私钥对所述第一服务器的随机公钥进行签名生成的。

25.如权利要求23或24所述的装置，其特征在于，所述第一响应还包括第二签名值，所述处理单元在所述获取单元从所述第三认证参数中获取所述第一服务器的密钥加密密钥之前，还用于：

利用所述安全认证令牌服务中心的证书公钥对所述第二签名值验证成功。

26.一种装置，其特征在于，该装置包括接收单元、认证单元以及处理单元：

所述接收单元，用于从安全认证令牌服务中心获取第二服务器的密钥加密密钥；接收来自第一服务器的服务请求，所述服务请求用于请求所述第二服务器为所述第一服务器提供服务，所述服务请求中包括所述认证令牌、认证信息、以及指示信息，所述指示信息用于指示所述第一服务器所请求的服务类型，其中，所述认证信息是利用所述第一服务器的认证密钥对所述指示信息进行认证加密生成的；所述认证令牌包括第二认证参数；所述第二认证参数是所述安全认证令牌服务中心利用所述第二服务器的密钥加密密钥对所述第一服务器的认证密钥进行认证加密生成的；

所述认证单元，用于根据所述第二服务器的密钥加密密钥对所述认证令牌中的第二认证参数进行认证；在对所述第二认证参数认证成功后，利用所述第二服务器的密钥加密密钥对所述第二认证参数进行解密获取所述第一服务器的认证密钥；利用所述第一服务器的认证密钥和所述指示信息对所述认证信息进行认证；

所述处理单元，用于在所述认证单元利用所述第一服务器的认证密钥和所述指示信息对所述认证信息认证成功后，向所述第一服务器提供所述指示信息所指示的服务。

27.如权利要求28所述的装置，其特征在于，所述服务请求还包括第一密文，所述认证单元，还用于利用所述第二服务器的密钥加密密钥对所述第二认证参数进行解密后，从所述第二认证参数中获取所述第一服务器的数据密钥；利用所述第一服务器的数据密钥，对所述第一密文进行解密获取所述第一服务器的敏感数据，所述敏感数据为需要加密的数据。

28.一种装置，其特征在于，该装置包括存储器和处理器，所述存储器用于存储计算机程序指令：所述处理器用于调用所述存储器中存储的计算机程序指令执行如权利要求1～6任一所述的方法。

29.一种装置，其特征在于，该装置包括存储器和处理器，所述存储器用于存储计算机程序指令：所述处理器用于调用所述存储器中存储的计算机程序指令执行如权利要求7～11任一所述的方法。

30.一种装置，其特征在于，该装置包括存储器和处理器，所述存储器用于存储计算机程序指令：所述处理器用于调用所述存储器中存储的计算机程序指令执行如权利要求12～13任一所述的方法。

一种认证方法以及装置

技术领域

[0001] 本申请涉及通信技术领域，尤其涉及一种认证方法以及装置。

背景技术

[0002] 基于预共享密钥的认证方式是设备之间的常用的认证方式，在基于预共享密钥的认证方式中要求在需要交互的双方中预先配置共享密钥K。

[0003] 这里以设备A和设备B为例对基于预共享密钥的认证方式进行说明，当设备A需要向设备B请求数据时，设备A可以向设备B发送设备A的身份信息，设备B为了验证设备A的身份信息是否正确，可以生成一个随机数，发送给设备A；设备A在接收到随机数后，可利用共享密钥K对随机数进行加密，并将加密后的随机数发送给设备B；设备B在接收到熬加密后的随机数后，可以利用本地保存的共享密钥K也对随机数进行加密，设备B对比生成的加密后的随机数与从设备A接收的加密后的随机数；若相同则认证成功，可以向设备A发送认证成功的应答消息；若不同则认证失败，向设备A发送认证失败的应答消息。同样的，设备A也可以向设备B发送随机数，对设备B进行认证，在双方都认证成功后，才可以进行数据交互。

[0004] 基于预共享密钥的认证方式具备认证速度快、安全性较高的问题，但是基于预共享密钥的认证方式需要事先在交互的双方配置共享密钥，在服务器集群数量较大或多对多认证场景下，若每两个需要交互的设备配置不同的共享密钥，共享密钥的配置和管理操作就会非常复杂；若均配置相同的共享密钥，一旦某一个设备的共享密钥泄露，则会使得所有设备的共享密钥都泄露。

[0005] 故而亟需一种新型的认证方式，可以简化密钥的预置过程，还可以保证设备之间可以进行高效的认证。

发明内容

[0006] 本申请提供一种认证方法以及装置，用以提高设备之间的认证效率。

[0007] 第一方面，本申请提供了一种认证方法，该方法包括：第一服务器可以先从安全认证令牌服务中心获取第一服务器的密钥加密密钥和第一服务器与第二服务器认证所需的认证令牌，认证令牌包括第一认证参数，其中，第一认证参数是安全认证令牌服务中心利用第一服务器的密钥加密密钥对第一服务器的认证密钥进行认证加密生成的；之后，第一服务器可以根据第一服务器的密钥加密密钥对认证令牌中的第一认证参数进行认证；当第一服务器在对第一认证参数认证成功后，第一服务器利用第一服务器的密钥加密密钥对第一认证参数进行解密获取第一服务器的认证密钥，保存认证令牌；若第一服务器需要第二服务器提供服务，第一服务器可以向第二服务器发送服务请求，服务请求用于请求第二服务器为第一服务器提供服务，服务请求中包括认证令牌、认证信息、以及指示信息；其中，认证信息是利用第一服务器的认证密钥对指示信息进行认证加密生成的，指示信息用于指示第一服务器所请求的服务类型。

[0008] 通过上述方法，第一服务器和第二服务器之间的认证是基于从安全认证令牌服务

中心获取的认证令牌进行的，该认证令牌只针对特定的两个服务器，能够有效的简化服务器之间认证流程，进而可以提高服务器之间的认证效率。

[0009] 在一种可能的设计中，第一服务器利用第一服务器的密钥加密密钥对第一认证参数进行解密后，除了能够从第一认证参数中获取第一服务器的认证密钥外，还可以从第一认证参数中获取第一服务器的数据密钥。

[0010] 通过上述方法，认证令牌中可以携带多种不同的密钥，第一服务器可以较为方便从认证令牌中获取所需要的密钥，以便第一服务器后续在向第二服务器发送服务请求时使用。

[0011] 在一种可能的设计中，服务请求还可以包括第一密文，第一密文是利用第一服务器的数据密钥对第一服务器的敏感数据加密生成的，敏感数据为需要加密的数据。

[0012] 通过上述方法，对于一些需要加密的数据可以利用数据密钥进行加密，能够保证数据传输的安全性。

[0013] 在一种可能的设计中，第一服务器从安全认证令牌服务中心获取第一服务器的密钥加密密钥时，第一服务器可以向安全认证令牌服务中心发送第一请求，第一请求用于请求第一服务器的密钥加密密钥，第一请求包括第一服务器的随机公钥；之后，第一服务器可以接收安全认证令牌服务中心的第一响应，第一响应中包括第三认证参数，第三认证参数是安全认证令牌服务中心利用第一服务器的随机公钥对第一服务器的密钥加密密钥进行加密生成的；在第一服务器利用第一服务器的随机私钥对第三认证参数解密的情况下，可以确定该第三认证参数为安全认证令牌服务中心发送的真实参数，第一服务器可以从第三认证参数中获取第一服务器的密钥加密密钥。

[0014] 通过上述方法，第一服务器从安全认证令牌服务中心获取第一服务器的密钥加密密钥，需要利用随机私钥对第三认证参数进行认证，能够保证第三认证参数的来源真实可靠。

[0015] 在一种可能的设计中，第一请求还包括第一签名值，第一服务器根据第一服务器的证书私钥对第一服务器的随机公钥进行签名生成第一签名值，并将第一签名值携带在第一请求中。

[0016] 通过上述方法，通过携带第一签名值，可以使得安全认证令牌服务中心利用第一签名值对第一签名值的来源(第一服务器)的身份进行认证，进一步保证第一请求来自与第一服务器，保证数据传输的可靠性。

[0017] 在一种可能的设计中，第一请求还包括第一服务器的证书，第一服务器的证书记录第一服务器的证书私钥对应的证书公钥。

[0018] 通过上述方法，以便安全认证令牌服务中心能够较为方便的从第一请求中获取第一服务器的证书公钥。

[0019] 在一种可能的设计中，第一响应还可以包括第二签名值，第一服务器可以利用安全认证令牌服务中心的证书公钥对第二签名值进行验证，在对第二签名值验证成功后，第一服务器从第三认证参数中获取第一服务器的密钥加密密钥。

[0020] 通过上述方法，通过携带第二签名值，可以使得第一服务器利用第二签名值对第二签名值的来源(安全认证令牌服务中心)的身份进行认证，进一步保证第一响应来自与安全认证令牌服务中心，保证数据传输的可靠性。

[0021] 第二方面，本申请提供了一种认证方法，该方法包括：安全认证令牌服务中心可以基于根密钥生成第一服务器的密钥加密密钥、第一服务器的认证密钥以及第二服务器的密钥加密密钥；之后，生成包括第一认证参数和第二认证参数的认证令牌，其中，第一认证参数是利用第一服务器的密钥加密密钥对第一服务器的认证密钥进行认证加密生成的，第二认证参数是利用第二服务器的密钥加密密钥对第一服务器的认证密钥进行认证加密生成的；之后，安全认证令牌服务中心可以向第一服务器发送第一服务器的密钥加密密钥和认证令牌；还可以向第二服务器发送第二服务器的密钥加密密钥。

[0022] 通过上述方法，安全认证令牌服务中心只需基于根密钥就可以生成各个服务器之间认证所需的认证令牌，还可以生成每个服务器的密钥加密密钥，使得认证令牌的生成过程有效简化，便于安全认证令牌服务中心便捷的派发认证令牌。

[0023] 在一种可能的设计中，安全认证令牌服务中心还可以基于根密钥生成第一服务器的数据密钥；并利用第一服务器的密钥加密密钥对第一服务器的认证密钥和数据密钥进行认证加密生成第一认证参数。

[0024] 通过上述方法，第一认证参数携带多种不同的密钥，以便第一服务器可以较为方便从认证令牌中获取所需要的密钥，以便第一服务器后续在向第二服务器发送服务请求时使用。

[0025] 在一种可能的设计中，安全认证令牌服务中心还可以利用第二服务器的密钥加密密钥对第一服务器的认证密钥和数据密钥进行认证加密生成第二认证参数。

[0026] 通过上述方法，第二认证参数携带多种不同的密钥，以便第二服务器可以较为方便从认证令牌中获取所需要的密钥，以便第二服务器后续在处理与第一服务器发送服务请求时使用。

[0027] 在一种可能的设计中，安全认证令牌服务中心向第一服务器发送第一服务器的密钥加密密钥时，安全认证令牌服务中心可以先接收来自第一服务器的第一请求，第一请求用于请求第一服务器的密钥加密密钥，第一请求包括第一服务器的随机公钥；之后，利用第一服务器的随机公钥对第一服务器的密钥加密密钥进行加密生成第三认证参数；之后，安全认证令牌服务中心向第一服务器发送第一响应，第一响应中包括第三认证参数。

[0028] 通过上述方法，安全认证令牌服务中心利用随机公钥生成第三认证参数，以便第一服务器在接收到第一响应后，能够利用第三认证参数验证第一响应的来源真实可靠。

[0029] 在一种可能的设计中，第一请求还包括第一签名值，安全认证令牌服务中心利用第一服务器的随机公钥对第一服务器的密钥加密密钥进行加密生成第三认证参数之前，可以利用第一服务器的证书公钥对第一签名值验证成功。

[0030] 通过上述方法，通过携带第一签名值，可以使得安全认证令牌服务中心利用第一签名值对第一签名值的来源(第一服务器)的身份进行认证，进一步保证第一请求来自与第一服务器，保证数据传输的可靠性。

[0031] 在一种可能的设计中，第一请求还包括第一服务器的证书，第一服务器的证书记录第一服务器的证书公钥。

[0032] 通过上述方法，第一请求还包括第一服务器的证书，第一服务器的证书记录第一服务器的证书私钥对应的证书公钥，便于能够高效的生成第三认证参数。

[0033] 在一种可能的设计中，第一响应还包括第二签名值，第二签名值是根据安全认证

令牌服务中心的证书私钥对第一服务器的密钥加密密钥进行签名生成的。

[0034] 通过上述方法，通过携带第二签名值，可以使得第一服务器在接收到第一响应后，能够利用第二签名值对第二签名值的来源(安全认证令牌服务中心)的身份进行认证，进一步保证第一响应来自与安全认证令牌服务中心，保证数据传输的可靠性。

[0035] 第三方面，本申请提供了一种认证方法，该方法包括：第二服务器从安全认证令牌服务中心获取第二服务器的密钥加密密钥；当第二服务器接收来自第一服务器的服务请求，服务请求用于请求第二服务器为第一服务器提供服务，服务请求中包括认证令牌、认证信息、以及指示信息，指示信息用于指示第一服务器所请求的服务类型，认证信息是利用第一服务器的认证密钥对指示信息进行认证加密生成的；认证令牌包括第二认证参数；第二认证参数是安全认证令牌服务中心利用第二服务器的密钥加密密钥对第一服务器的认证密钥进行认证加密生成的；第二服务器可以根据第二服务器的密钥加密密钥对认证令牌中的第二认证参数进行认证；并在对第二认证参数认证成功后，利用第二服务器的密钥加密密钥对第二认证参数进行解密获取第一服务器的认证密钥；

[0036] 第二服务器利用第一服务器的认证密钥和所述指示信息对认证信息认证成功之后，向第一服务器提供指示信息所指示的服务。

[0037] 通过上述方法，第一服务器和第二服务器之间的认证是基于从安全认证令牌服务中心获取的认证令牌进行的，可以有效的简化服务器之间认证流程，进而可以提高服务器之间的认证效率。

[0038] 在一种可能的设计中，服务请求还可以包括第一密文，第二服务器在对第二认证参数验证成功后，利用第二服务器的密钥加密密钥对第二认证参数进行解密后，从第二认证参数中获取第一服务器的数据密钥；并利用第一服务器的数据密钥，对第一密文进行解密获取第一服务器的敏感数据，敏感数据为需要加密的数据。

[0039] 通过上述方法，对于一些需要加密的数据可以利用第一服务器的数据密钥进行加密，第二服务器可以利用数据密钥进行解密，能够保证数据传输的安全性。

[0040] 第四方面，本申请实施例还提供了一种装置，装置应用于第一服务器，有益效果可以参见第一方面的描述此处不再赘述。该装置具有实现上述第一方面的方法实例中行为的功能。功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，装置的结构中包括获取单元、处理单元以及发送单元，这些单元可以执行上述第一方面方法示例中的相应功能，具体参见方法示例中的详细描述，此处不做赘述。

[0041] 第五方面，本申请实施例还提供了一种装置，通信装置应用于安全认证令牌服务中心，有益效果可以参见第二方面的描述此处不再赘述。该装置具有实现上述第二方面的方法实例中行为的功能。功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，装置的结构中包括接收单元、生成单元和发送单元，这些单元可以执行上述第二方面方法示例中的相应功能，具体参见方法示例中的详细描述，此处不做赘述。

[0042] 第六方面，本申请实施例还提供了一种装置，通信装置应用于第二服务器，有益效果可以参见第三方面的描述此处不再赘述。该装置具有实现上述第三方面的方法实例中行为的功能。功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括

一个或多个与上述功能相对应的模块。在一个可能的设计中，装置的结构中包括接收单元、认证单元和发送单元，这些单元可以执行上述第三方面方法示例中的相应功能，具体参见方法示例中的详细描述，此处不做赘述。

[0043] 第七方面，本申请实施例还提供了一种装置，装置应用于第一服务器，有益效果可以参见第一方面的描述此处不再赘述。装置的结构中包括处理器和存储器，处理器被配置为支持第一服务器执行上述第一方面方法中相应的功能。存储器与处理器耦合，其保存装置必要的程序指令和数据。装置的结构中还包括通信接口，用于与其他设备进行通信。

[0044] 第八方面，本申请实施例还提供了一种装置，装置应用于安全认证令牌服务中心，有益效果可以参见第二方面的描述此处不再赘述。装置的结构中包括处理器和存储器，处理器被配置为支持安全认证令牌服务中心执行上述第二方面方法中相应的功能。存储器与处理器耦合，其保存装置必要的程序指令和数据。装置的结构中还包括通信接口，用于与其他设备进行通信。

[0045] 第九方面，本申请实施例还提供了一种装置，装置应用于第二服务器，有益效果可以参见第三方面的描述此处不再赘述。装置的结构中包括处理器和存储器，处理器被配置为支持基站执行上述第三方面方法中相应的功能。存储器与处理器耦合，其保存装置必要的程序指令和数据。装置的结构中还包括通信接口，用于与其他设备进行通信。

[0046] 第十方面，本申请实施例还提供了一种认证系统，有益效果可以参见第一方面、第二方面、第三方面的描述此处不再赘述。系统包括第一服务器和安全认证令牌服务中心。

[0047] 第一服务器，用于从安全认证令牌服务中心获取第一服务器的密钥加密密钥和第一服务器与第二服务器认证所需的认证令牌，认证令牌包括第一认证参数；根据第一服务器的密钥加密密钥对认证令牌中的第一认证参数进行认证；以及在对第一认证参数认证成功后，利用第一服务器的密钥加密密钥对第一认证参数进行解密获取第一服务器的认证密钥，保存认证令牌；

[0048] 安全认证令牌服务中心，用于基于根密钥生成第一服务器的密钥加密密钥、第一服务器的认证密钥以及第二服务器的密钥加密密钥；生成包括第一认证参数的认证令牌，其中，第一认证参数是利用第一服务器的密钥加密密钥对第一服务器的认证密钥进行认证加密生成的，第二认证参数是利用第二服务器的密钥加密密钥对第一服务器的认证密钥进行认证加密生成的；以及向第一服务器发送第一服务器的密钥加密密钥和认证令牌；

[0049] 在一种可能的设计中，安全认证令牌服务中心，还用于基于根密钥生成第一服务器的数据密钥；第一认证参数是利用第一服务器的密钥加密密钥对第一服务器的认证密钥和数据密钥进行认证加密生成的。

[0050] 在一种可能的设计中，第二认证参数是安全认证令牌服务中心利用第二服务器的密钥加密密钥对第一服务器的认证密钥和数据密钥进行认证加密生成的。

[0051] 在一种可能的设计中，第一服务器在获取从安全认证令牌服务中心获取第一服务器的密钥加密密钥时，具体用于：向安全认证令牌服务中心发送第一请求，第一请求用于请求第一服务器的密钥加密密钥，第一请求包括第一服务器的随机公钥；

[0052] 安全认证令牌服务中心，具体用于接收来自第一服务器的第一请求，第一请求用于请求第一服务器的密钥加密密钥，第一请求包括第一服务器的随机公钥；利用第一服务器的随机公钥对第一服务器的密钥加密密钥进行加密生成第三认证参数；向第一服务器发

送第一响应，第一响应中包括第三认证参数。

[0053] 第一服务器，具体用于接收安全认证令牌服务中心的第一响应，第一响应中包括第三认证参数；利用第一服务器的随机私钥对第三认证参数解密后，从第三认证参数中获取第一服务器的密钥加密密钥。

[0054] 在一种可能的设计中，第一请求还包括第一签名值，第一签名值是根据第一服务器的证书私钥对第一服务器的随机公钥进行签名生成的。

[0055] 在一种可能的设计中，第一请求还包括第一服务器的证书，第一服务器的证书记录第一服务器的证书私钥对应的证书公钥。

[0056] 在一种可能的设计中，第一响应还包括第二签名值，第二签名值是根据安全认证令牌服务中心的证书私钥对第一服务器的密钥加密密钥进行签名生成的；第一服务器从第三认证参数中获取第一服务器的密钥加密密钥之前，还用于：利用安全认证令牌服务中心的证书公钥对第二签名值验证成功。

[0057] 在一种可能的设计中，该认证系统还包括第二服务器。

[0058] 安全认证令牌服务中心，还用于向第二服务器发送第二服务器的密钥加密密钥；

[0059] 第二服务器，用于从安全认证令牌服务中心获取第二服务器的密钥加密密钥。

[0060] 在一种可能的设计中，第一服务器，还用于向第二服务器发送服务请求，服务请求用于请求第二服务器为第一服务器提供服务，服务请求中包括认证令牌、认证信息、以及指示信息；其中，认证信息是利用第一服务器的认证密钥对指示信息进行认证加密生成的，指示信息用于指示第一服务器所请求的服务类型。

[0061] 第二服务器，还用于接收来自第一服务器的服务请求，服务请求用于请求第二服务器为

[0062] 第一服务器提供服务，服务请求中包括认证令牌、认证信息、以及指示信息，指示信息用于指示第一服务器所请求的服务类型；根据第二服务器的密钥加密密钥对认证令牌中的第二认证参数进行认证；在对第二认证参数认证成功后，利用所述第二服务器的密钥加密密钥对所述第二认证参数进行解密获取第一服务器的认证密钥；在利用所述第一服务器的认证密钥和所述指示信息对所述认证信息认证成功后，向第一服务器提供指示信息所指示的服务。

[0063] 在一种可能的设计中，服务请求还包括第一密文，第一密文是利用第一服务器的数据密钥对第一服务器的敏感数据加密生成的，敏感数据为需要加密的数据。

[0064] 第二服务器，还用于在利用所述第二服务器的密钥加密密钥对所述第二认证参数进行解密后，获取第一服务器的数据密钥；利用第一服务器的数据密钥，对第一密文进行解密获取第一服务器的敏感数据，敏感数据为需要加密的数据。

[0065] 第十一方面，本申请还提供一种计算机可读存储介质，计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行上述各方面的方法。

[0066] 第十二方面，本申请还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，使得计算机执行上述各方面的方法。

[0067] 第十三方面，本申请还提供一种计算机芯片，芯片与存储器相连，芯片用于读取并执行存储器中存储的软件程序，执行上述各方面的方法。

附图说明

[0068] 图1为本申请提供的一种系统的架构示意图；

[0069] 图2为本申请提供的一种基于根密钥RK所能生成的密钥示意图；

[0070] 图3为本申请提供的一种发送密钥加密密钥以及认证令牌的方法示意图；

[0071] 图4为本申请提供的一种服务器之间认证方法示意图；

[0072] 图5为本申请提供的一种认证方法示意图；

[0073] 图6～图9为本申请提供的一种装置的结构示意图。

具体实施方式

[0074] 如图1所示，为本申请实施例提供的一种系统架构示意图，该系统中包括安全认证令牌服务中心(security token service，STS)100以及多个服务器集群，每个服务器集群中包括一个或多个服务器。一个服务器集群为能够提供特定业务(也可称为特定服务)的集群，一个服务器集群中的每个服务器可以提供该特定业务，一个服务器集群中的多个服务器之间可以互相配合提供该特定业务。

[0075] 本申请实施例并不限定系统中包括的服务器集群数量以及每个服务器集群中的数量。如图1中仅是以系统中包括两个服务器集群，分别为服务器集群200和服务器集群300为例，每个服务器集群中包括3个服务器。服务器集群200包括服务器201、服务器202、以及服务器203，服务器集群300包括服务器301、服务器302、以及服务器303。

[0076] 安全认证令牌服务中心100，用于基于一个根密钥为各个服务器集群中每个服务器分配用于对服务器之间交互使用的密钥加密的密钥加密密钥、服务器之间认证所需的认证令牌、以及认证密钥和加密密钥。

[0077] 不同服务器集群的服务器之间可以进行数据交互，请求服务。例如，若服务器集群200所提供的业务为通话业务，服务器集群300所提供的业务为语音去噪业务，当服务器集群200中的服务器需要对通话过程中产生的语音进行去噪时，可以发送服务请求，向服务器集群300中的服务器请求语音去噪业务，该请求用于请求语音去噪，该请求中可以携带待去噪的语音数据，待去噪的语音数据为服务器集群300提供语音去噪服务的所需要的服务数据。又例如，若服务器集群200所提供的业务为视频存储业务，服务器集群300所提供的业务为视频编解码业务，当服务器集群200中的服务器需要对视频流进行编码时，可以发送服务请求，向服务器集群300中的服务器请求视频编码业务，该请求用于请求为视频流进行编码，该请求中可以携带待编码的视频数据，待编码的视频数据为服务器集群300提供视频编码服务的所需要的服务数据。

[0078] 而为了保证不同服务器集群中的服务器之间的数据安全性，业务请求方(发送服务请求的服务器)在向业务提供方(提供服务的服务器)传输数据之前，可以先对业务请求方进行认证，业务请求方与业务提供方之间的认证是基于业务请求方向业务提供方发送认证令牌进行的，只有在业务提供方利用认证令牌对业务请求方认证成功后，才能为业务请求方提供业务。

[0079] 需要说明的是，在上述系统架构中以安全认证令牌服务中心100所管理的集群为服务器集群为例进行说明，本申请实施例也适用于其他类型的能够提供特定业务的集群，如由部署在不同服务器中的虚拟机构成的集群，或由虚拟机和服务器构成的能够提供特定

业务的集群。在本申请实施例中，集群中的一个虚拟机或一个服务器可以称为该集群的一个实例，在这类系统架构下，一个集群中的实例向安全认证令牌服务中心100申请密钥加密密钥和认证令牌的方式以及该实例与其他集群的实例认证方式，与本申请实施例中服务器向安全认证令牌服务中心100申请密钥加密密钥和认证令牌的方式，以及不同服务器集群中服务器之间的认证方式相同，区别仅在于执行主体的不同，本申请实施例中仅是以服务器集群为例进行说明。

[0080] 在本申请实施例中，安全认证令牌服务中心100仅需要保存根密钥，可以生成每个服务器集群中各个服务与其他服务器集群中的服务器认证所需的认证令牌、认证密钥，能够较好的简化密钥派发的方式；由于服务器之间认证所需的认证令牌是针对于两个需要交互的服务器设置的，不同服务器之间所需的认证令牌是不同的，能够保证认证过程的安全性。

[0081] 下面先对安全认证令牌服务中心100基于根密钥RK所能生成密钥进行说明，如图2所示，针对任一服务器集群中的每个服务器，安全认证令牌服务中心100基于根密钥RK可以生成三种密钥，分别为认证密钥SK(如申请实施例中的SK_b)、密钥加密密钥KEK(如申请实施例中的KEK_b)以及数据加密密钥DK(如申请实施例中的DK_b)。每个服务器的认证密钥SK对应一个密钥标识，认证密钥SK对应一个密钥标识是安全认证令牌服务中心100对服务器的认证密钥设置的一个标识，不同服务器的认证密钥SK对应的密钥标识不同，也就是说，认证密钥SK对应的密钥标识能够唯一标识该认证密钥SK。

[0082] 类似的，每个服务器的数据加密密钥DK也对应一个密钥标识，数据加密密钥DK对应一个密钥标识是安全认证令牌服务中心100对服务器的数据加密密钥DK设置的一个标识，不同服务器的数据加密密钥DK对应的密钥标识不同，也就是说，数据加密密钥DK对应的密钥标识能够唯一标识该数据加密密钥DK。

[0083] 对于一个服务器，该服务器的认证密钥SK对应的密钥标识与该服务器的数据加密密钥DK对应的密钥标识可以相同，也可以不同。在本申请实施例中仅是以服务器的认证密钥SK对应的密钥标识与该服务器的数据加密密钥DK对应的密钥标识可以相同，密钥标识为AK(如申请实施例中的AK_b)为例进行说明，本申请实施例并不限定密钥标识AK的生成方式，示例性的，AK＝随机数||时间戳，该时间戳用于指示密钥(如数据加密密钥DK或认证密钥SK)的有效时间，也就是说，安全认证令牌服务中心100可以通过随机数加密钥对应的有效时间生成AK。

[0084] 安全认证令牌服务中心100可以采用KDF函数，基于根密钥RK可以生成三种密钥，所采用KDF函数可以相同，也可以不同，当采用相同的密钥生成算法时，可以选择不同的参数，以生成三种不同的密钥，本申请实施例并不限定基于根密钥RK生成密钥的方式，可以为哈希为基础的消息认证码(hash-based message authentication code，HMAC)，也可以是伪随机函数(pseudo random function，PRF)，还可以是哈希函数为基础的密钥导出函数(hash based key derivation function，HKDF)。

[0085] 作为一种可能的实施方式，安全认证令牌服务中心100可以基于根密钥RK、以及其他信息生成这三种密钥，其他信息包括但不限于对应的服务器的标识、密钥(认证密钥SK、密钥加密密钥KEK以及数据加密密钥DK)的密钥字符串和时间戳，该时间戳用于指示生成的密钥的有效时间。

[0086] 其中，认证密钥SK用于对业务请求方所发送的服务数据加密。数据加密密钥DK对业务请求方的一些需要加密的数据进行加密。密钥加密密钥KEK用于对一些密钥，如认证密钥SK以及数据加密密钥DK，进行加密。

[0087] 下面以安全认证令牌服务中心100向服务器集群200中的服务器201派发密钥加密密钥以及认证令牌为例，对安全认证令牌服务中心100派发密钥加密密钥以及认证令牌的方式进行说明。

[0088] 如图3所示，为本申请实施例提供的一种发送密钥加密密钥以及认证令牌的方法，该方法包括：

[0089] 步骤301：服务器201向安全认证令牌服务中心100发送注册请求，该注册请求用于请求注册到安全认证令牌服务中心100中。

[0090] 注册请求包括服务器201的标识以及服务器201的访问权限信息。

[0091] 服务器201的标识为能够唯一标识服务器201的信息，本申请实施例并不限定服务器201的标识的具体形式，可以是服务器201的设备号，也可以预先为服务器201配置的编号。

[0092] 服务器201的访问权限信息包括服务器201所能够访问的服务器集群或服务器集群中的特定服务器；也就是能够为服务器201提供服务器的服务器集群或服务器集群中的特定服务器。

[0093] 服务器201的访问权限信息还包括服务器201所能够访问的服务器集群或服务器集群中的特定服务器可以提高的服务类型或业务类型。

[0094] 例如，服务器201的访问权限信息可以指示服务器201能够访问服务器集群300中的任一服务器，服务器集群300中的任一服务器可以向服务器201提高视频编码服务；又例如，服务器201能够访问服务器集群300中的服务器301以及服务器302，服务器301以及服务器302可以向服务器201提高视频编码服务。

[0095] 注册请求中还可以包括服务器201的证书，服务器201的证书可以是从认证管理中心(certificate authority，CA)获取的X.509标准证书。服务器201的证书用于指示服务器201的真实身份。服务器201的证书中记录了CA为服务器201分配的证书公钥PK_{cert-b}；而该证书公钥PK_{cert-b}对应的证书私钥SKcert-b可以预先配置在服务器201中，还可以由CA采用较为安全的方式发送给服务器201。

[0096] 步骤302：安全认证令牌服务中心100接收到服务器201的注册请求后，保存服务器201的注册信息。

[0097] 若服务器201的注册请求中还携带有服务器201的证书，安全认证令牌服务中心100在接收到该注册请求后，还可以先通过服务器201的证书对服务器201进行认证，在认证通过后，将注册请求中携带的数据(如服务器201的标识、服务器201的证书、以及服务器201的访问权限信息)组我服务器201的注册信息保存在数据库中。

[0098] 本申请实施例并不限定安全认证令牌服务中心100通过服务器201的证书对服务器201进行认证的方式，例如，安全认证令牌服务中心100先可以向CA发送认证请求，用于请求服务器201的证书的真实性。又例如，服务器201可以利用证书私钥SK_{cert-b}对一个随机数进行签名，并将签名后的数值携带在注册请求中，安全认证令牌服务中心100可以利用服务器201的证书公钥PK_{cert-b}对签名后的随机数进行认证，若对签名后的随机数认证成功，则对

服务器201认证成功，否则认证失败。

[0099] 安全认证令牌服务中心100在保存了服务器201的注册信息后，可以向服务器201发送注册响应，以指示服务器201注册成功。

[0100] 步骤301～步骤302为服务器201的注册过程。

[0101] 步骤303：服务器201向安全认证令牌服务中心100发送密钥加密密钥请求，该密钥加密密钥请求中包括服务器201的标识，随机公钥PK_{enc-b}。

[0102] 密钥加密密钥请求中还可以携带第一密钥认证信息，用于安全认证令牌服务中心100对服务器201进行认证。

[0103] 下面介绍一种第一密钥认证信息的生成方式：

[0104] 服务器201可以随机生成随机公私钥对(PK_{enc-b},SK_{enc-b})，之后，服务器201利用服务器201的证书私钥SK_{cert-b}对随机公钥PK_{enc-b}进行签名，生成签名值S1。服务器201在生成签名值S1时，服务器201可以利用服务器201的证书私钥SK_{cert-b}对包括随机公钥PK_{enc-b}的第一信息组合进行签名，该第一信息组合还包括时间戳(该时间戳可以指示签名值S1的有效时间)以及服务器201的标识。

[0105] 服务器201在对随机公钥PK_{enc-b}。进行签名时可以利用签名算法，本申请实施例并不限定服务器201所采用的签名算法，可以是RSA-2048，也可以是ECDSA算法。

[0106] 服务器201可以将签名值S1为第一密钥认证信息携带在密钥加密密钥请求中。

[0107] 可选的，服务器201也可以在密钥加密密钥请求中携带服务器201的证书，以便安全认证令牌服务中心100可以获取服务器201的认证公钥PK_{cert-b}。当然，密钥加密密钥请求中也可以不携带服务器201的证书，安全认证令牌服务中心100可以从数据库中或其他设备中获取服务器201的证书。

[0108] 步骤304：安全认证令牌服务中心100接收到密钥加密密钥请求后，可以利用根密钥RK生成服务器201的密钥密钥加密密钥KEK_b。

[0109] 若密钥加密请求中还包括第一密钥认证信息，安全认证令牌服务中心100可以利用第一密钥认证信息对服务器201进行认证，在认证通过之后，再生成服务器201的密钥密钥加密密钥。

[0110] 以密钥认证信息为S1为例，安全认证令牌服务中心100利用服务器201的认证公钥PK_{cert-b}验证签名值S1的正确性，若正确，安全认证令牌服务中心100对服务器201认证通过，否则，不通过。

[0111] 由上可知，第一密钥认证信息用于安全认证令牌服务中心100对服务器201进行认证，以确保服务器201的真实身份，本申请实施例并不限定采用其他能够用于对服务器201进行认证的信息作为第一密钥认证信息，签名值S1仅是举例。

[0112] 步骤305：安全认证令牌服务中心100向服务器201发送密钥加密密钥响应，该密钥加密密钥响应中携带有服务器201的密钥加密密钥KEK_b。

[0113] 本申请实施例并不限定该密钥加密密钥响应中携带服务器201的密钥加密密钥KEK_b的方式，安全认证令牌服务中心100可以直接将服务器201的密钥加密密钥KEK_b携带在密钥加密密钥响应中，也可以采用加密的方式，将加密后的服务器201的密钥加密密钥KEK_b携带在密钥加密密钥响应中。

[0114] 下面介绍一种密钥加密密钥响应中携带服务器201的密钥加密密钥KEK_b的方式：

[0115] 安全认证令牌服务中心100可以利用安全认证令牌服务中心100的证书私钥SK_{cert-s}对服务器201的密钥加密密钥KEK_b和随机公钥PK_{enc-b}进行签名，生成签名值S2，安全认证令牌服务中心100在生成签名值S2时，安全认证令牌服务中心100可以利用安全认证令牌服务中心100的证书私钥SK_{cert-s}对包括服务器201的密钥加密密钥KEK_b的第二信息组合进行签名，该第二信息组合中还可以包括时间戳(该时间戳可以指示签名值S2的有效时间)。

[0116] 需要说明的是，安全认证令牌服务中心100的证书与服务器201的证书类似，是由CA发送给安全认证令牌服务中心100的。安全认证令牌服务中心100的证书用于指示安全认证令牌服务中心100的真实身份。安全认证令牌服务中心100的证书中记录了CA为安全认证令牌服务中心100分配的证书公钥PK_{cert-s}；而该证书公钥PK_{cert-s}对应的证书私钥SK_{cert-s}可以预先配置在安全认证令牌服务中心100中，还可以由CA采用较为安全的方式发送给安全认证令牌服务中心100。

[0117] 之后，安全认证令牌服务中心100利用服务器201的随机公钥PK_{enc-b}。对签名值S2进行加密，生产第二密钥认证信息。

[0118] 安全认证令牌服务中心100可以将第二密钥认证信息携带在密钥加密密钥响应中。

[0119] 步骤306：服务器201接收到安全认证令牌服务中心100发送的密钥加密密钥响应后，从密钥加密密钥响应中获取服务器201的密钥加密密钥KEK_b。

[0120] 若密钥加密密钥响应中通过携带第二密钥认证信息的方式携带服务器201的密钥加密密钥KEK_b，则服务器201需要利用第二密钥认证信息对安全认证令牌服务中心100进行认证。

[0121] 服务器201先利用随机私钥SK_{enc-b}对第二密钥认证信息进行解密，获取签名值S2，之后利用安全认证令牌服务中心100的证书公钥PK_{cert-s}验证签名值S2的正确性，若正确，则服务器201从签名值S2中获取服务器201的密钥加密密钥KEK_b。

[0122] 需要说明的是，本申请实施例并不限定服务器201获取安全认证令牌服务中心100的证书公钥PK_{cert-s}的方式，证书公钥PK_{cert-s}可以是由安全认证令牌服务中心100携带在密钥加密密钥响应中的，也可以是安全认证令牌服务中心100预先发送给服务器201的。

[0123] 由上可知，第二密钥认证信息用于服务器201对安全认证令牌服务中心100进行认证，以确保接收到第二密钥认证信息来自真正的安全认证令牌服务中心100，并保证第二密钥认证信息携带的服务器201的密钥加密密钥KEK_b真实有效，本申请实施例并不限定采用其他能够用于对安全认证令牌服务中心100进行认证的信息作为第二密钥认证信息，上述第二密钥认证信息仅是举例。

[0124] 步骤303～步骤306为服务器201向安全认证令牌服务中心100申请密钥加密密钥的过程。

[0125] 步骤307：服务器201向安全认证令牌服务中心100发送认证令牌请求，该认证令牌请求中包括服务器201的标识。该认证令牌请求用于向安全认证令牌服务中心100请求服务器201与其他服务器认证所需的认证令牌。

[0126] 本申请实施例并不限定所述请求的认证令牌的数量，服务器201可以向安全认证令牌服务中心100请求服务器201与服务器201能够访问的所有可能的服务器之间认证所需

的认证令牌，认证令牌请求可以携带指示信息，用于指示服务器201请求与服务器201能够访问的所有可能的服务器之间认证所需的认证令牌，该指示信息可以是服务器201与安全认证令牌服务中心100预先约定的信息，如指示信息为1时，表明该认证令牌请求用于请求服务器201与服务器201能够访问的所有可能的服务器之间认证所需的认证令牌；该指示信息也可以是服务器201能够访问的所有可能的服务器的标识。

[0127] 服务器201也可以向安全认证令牌服务中心100请求服务器201与特定的一个或多个服务器之间认证所需的认证令牌。认证令牌请求中可以携带特定的一个或多个服务器的标识。

[0128] 在本申请实施例中仅是以服务器201向安全认证令牌服务中心100请求服务器201与服务器301之间认证所需的认证令牌为例进行说明，对于服务器201请求与特定的多个服务器之间认证所需的认证令牌多个认证令牌的情况，可以参见本申请实施例，区别仅在于认证令牌请求中携带了多个服务器的标识，相应的，认证令牌响应中也携带了服务器201与特定的一个或多个服务器之间认证所需的认证令牌，此处不再赘述。

[0129] 步骤308：安全认证令牌服务中心100接收到服务器201发送的认证令牌请求后，安全认证令牌服务中心100基于根密钥生成服务器201与服务器301认证所需的认证令牌$Token_{ba}$。

[0130] 安全认证令牌服务中心100并不限定基于根密钥生成服务器201与服务器301认证所需的认证令牌$Token_{ba}$的方式。

[0131] 下面以服务器201与服务器301认证所需的认证令牌$Token_{ba}$为例，介绍一种认证令牌的生成方式：

[0132] 安全认证令牌服务中心100基于根密钥RK分别生成服务器201的认证密钥SK_b、密钥加密密钥KEK_b以及数据加密密钥DK_b以及服务器301的密钥加密密钥KEK_a。

[0133] 服务器201的密钥加密密钥KEK_b＝KDF(RK,ServiceID_B||KEKServiceID_B||时间戳)。

[0134] 其中，ServiceID_B为服务器201的标识，KEKServiceID_B为安全认证令牌服务中心100为KEK_B分配的密钥字符串，本申请实施例并不限定KEKServiceID_B的分配方式，可以按生成顺序分配，也可以随机分配，时间戳指示KEK_b的有效时间。

[0135] 服务器301的密钥加密密钥KEK_a＝KDF(RK,ServiceID_A||KEKServiceID_A||时间戳)。

[0136] 其中，ServiceID_A为服务器301的标识，KEKServiceID_A为安全认证令牌服务中心100为KEK_a分配的密钥字符串，本申请实施例并不限定KEKServiceID_A的分配方式，可以按生成顺序分配，也可以随机分配，时间戳指示KEK_a的有效时间。

[0137] 服务器201的认证密钥SK_b＝KDF(RK,ServiceID_B||AK_b||SKServiceID_B||时间戳)。

[0138] 其中，SKServiceID_B为安全认证令牌服务中心100为SK_b分配的密钥字符串，本申请实施例并不限定SKServiceID_B的分配方式，可以按生成顺序分配，也可以随机分配，时间戳指示SK_B的有效时间，AK_b为安全认证令牌服务中心100为服务器201的SK_b和DK_b分配的密钥标识。

[0139] 服务器201的数据加密密钥DK_b＝KDF(RK,ServiceID_B||AK_b||DKServiceID_B||时

间戳)。

[0140] DKServiceID_B为安全认证令牌服务中心100为DK_b分配的密钥字符串,本申请实施例并不限定DKServiceID_B的分配方式,可以按生成顺序分配,也可以随机分配,时间戳指示DK_B的有效时间。

[0141] 安全认证令牌服务中心100利用服务器201的密钥加密密钥KEK_b对服务器201的认证密钥SK_s进行加密生成第一认证参数C1。可选的,安全认证令牌服务中心100可以利用服务器201的密钥加密密钥KEK_s统一对服务器201的认证密钥SK_b和服务器201的数据加密密钥DK_b进行加密生成第一认证参数C1。

[0142] 示例性的,第一认证参数C1＝AES-GCM(KEK_B,TokenVersion||SK_b||AK_b||DK_b),其中,AES(advanced encryption standard)-GCM(galois counter mode)为一种可认证的加密算法,是AES算法中的一种标准算法,本申请实施例并不限定具体的加密算法,此处仅是以AES-GCM为例进行说明;TokenVersion为认证令牌的版本号,版本号可以指示派发认证令牌$Token_{ba}$的时间、或系列等关于Token的描述信息。AK_b的生成方式本申请实施例并不限定,例如,AK_b＝随机数||时间戳,该时间戳用于指示密钥(如数据加密密钥DK_b和认证密钥SK_b)的有效时间。

[0143] 安全认证令牌服务中心100利用服务器301的密钥加密密钥KEK_a对服务器201的认证密钥SK_b进行加密生成第二认证参数C2。可选的,安全认证令牌服务中心100可以利用服务器301的密钥加密密钥KEK_a统一对服务器201的认证密钥SK_b和服务器201的数据加密密钥DK_b进行加密生成第二认证参数C2。

[0144] 示例性的,第二认证参数C2＝AES-GCM(KEK_a,TokenVersion||SK_b||AK_b||DK_b)。

[0145] 安全认证令牌服务中心100再根据第一认证参数C1和第二认证参数C2生成服务器201与服务器301认证所需的认证令牌$Token_{ba}$。

[0146] 示例性的,服务器201与服务器301认证所需的认证令牌$Token_{ba}$＝C1||C2。

[0147] 步骤309:安全认证令牌服务中心100向服务器201发送的认证令牌响应,该认证令牌响应中携带服务器201与服务器301认证所需的认证令牌$Token_{ba}$。

[0148] 步骤310:服务器201接收到安全认证令牌服务中心100的认证令牌响应后,从该认证令牌$Token_{ba}$的第一认证参数C1中获取服务器201的认证密钥SK_b,可选的,服务器201还可以从第一认证参数C1中获取服务器201的数据加密密钥DK_b。服务器201还可以保存该认证令牌$Token_{ba}$。

[0149] 以认证令牌$Token_{ba}$是通过步骤309示例的方式生成的为例,对服务器201从该认证令牌$Token_{ba}$的第一认证参数C1中获取服务器201的认证密钥SK_b、服务器201的数据加密密钥DK_b的方式进行说明。

[0150] 服务器201可以利用服务器201的密钥加密密钥KEK_b对第一认证参数C1进行验证,在验证通过之后,利用服务器201的密钥加密密钥KEK_b对第一认证参数C1进行解密,获得服务器201的认证密钥SK_b、服务器201的数据加密密钥DK_b。

[0151] 服务器201在获取了服务器201与服务器301认证所需的认证令牌$Token_{ba}$后,可以向服务器301请求服务,并在发送的服务请求中携带认证令牌$Token_{ba}$,服务器301就可以通过认证令牌$Token_{ba}$对服务器201进行认证,在认证通过后,向服务器1提供服务器201所请求的服务。

[0152] 下面结合图4,以服务器201与服务器301的认证过程为例,对服务器之间的认证方法进行说明,该方法包括:

[0153] 步骤401:服务器201向服务器301发送服务请求,所述服务请求用于向服务器301请求服务器,该服务请求中还可以携带指示信息,指示信息用于指示服务器201所请求的服务类型。

[0154] 例如,服务器201向服务器301请求语音去噪服务,则指示信息指示语音去噪服务;又例如,服务器201向服务器301请求视频编码服务,则指示信息指示视频编码服务;又例如,服务器201向服务器301请求数据库服务,也就是说,服务器301能够将服务器201需要保存的数据保存在数据库中,当服务器201需要该数据库中的数据,服务器201可以向服务器301请求数据库服务;指示信息指示数据库服务。

[0155] 服务请求还可以认证令牌$Token_{ba}$以及认证信息C。

[0156] 该认证信息C用于服务器301对服务器201进行认证(该认证过程可见后续步骤402),该认证信息C是服务器201利用服务器201的认证密钥SK_b对指示信息M加密生成的。

[0157] 示例性,认证信息C=HMAC(SK_b,M),其中,本申请实施例并不限定具体的加密算法,此处仅是以HMAC为例进行说明。

[0158] 可选的,数据请求中还可以携带服务的相关信息,服务的相关信息为服务器301为服务器201提供服务所需的数据,例如,服务器201向服务器301请求语音去噪服务,则服务的相关信息包括待去噪的语音;又例如,服务器201向服务器301请求视频编码服务,则服务的相关信息包括待编码的视频数据;又例如,服务器201向服务器301请求数据库服务,也就是说,服务器301能够将服务器201需要保存的数据保存在数据库中,当服务器201需要该数据库中的数据,服务器201可以向服务器301请求数据库服务;服务的相关信息包括是服务器201在数据库注册的账户信息等信息。

[0159] 为了保证服务器201的相关信息的安全性,服务器201可以对服务器201的相关信息中的全部或部分信息进行加密。

[0160] 在本申请实施例中将需要加密的服务器的1的相关信息称为敏感数据,敏感数据可以包括一种或多种类别的数据,敏感数据中包括的一种或多种类别的数据可以是安全认证令牌服务中心100预先设置好的,并通知给服务器201的,也可以是服务器201自己设置的,还可以是用户配置的。本申请实施例并不限定敏感数据的设置方式。

[0161] 例如,当服务器201可以向服务器301请求数据库服务时,可以将服务器201在数据库注册的账户信息作为敏感数据,对服务器201在数据库注册的账户信息进行加密。

[0162] 服务器201利用服务器201的数据加密密钥DK_b对服务器201的敏感数据进行加密,生成密文C*,本申请实施例并不限定具体的加密算法,例如可以采用AES-GCM算法,也可以采用AES-CCM(Counter with CBC-MAC)算法,还可以是AES-CBC(Cipher Block Chaining)算法与HMAC(Hash based Authenticated Message Code)结合的加密算法(先采用AES-CBC算法,后采用HMAC算法)。

[0163] 示例性的,密文C*=AES-GCM(DK_B,m),其中,m为敏感数据。

[0164] 步骤402:服务器301接收到服务器201发送的服务请求后,服务器301利用认证令牌$Token_{ba}$对认证信息C进行认证。

[0165] 服务器301可以从服务请求中获取认证令牌$Token_{ba}$,利用服务器301的密钥加密密

钥KEK_a对认证令牌$Token_{ba}$中的第二认证参数C2进行验证，在验证通过后，利用服务器201的密钥加密密钥KEK_a对第二认证参数C2进行解密，获得服务器201的认证密钥SK_b、服务器201的数据加密密钥DK_b。

[0166] 服务器301利用服务器201的认证密钥SK_b对认证信息C进行验证，本申请实施例提供了两种验证方式：

[0167] 方式一、服务器301可以利用服务器201的认证密钥SK_b对认证信息C进行解密，确定解密获取的指示信息M与服务请求中携带的指示信息M是否相同，如相同，验证成功，否则失败。

[0168] 方式二、服务器301可以利用服务器201的认证密钥SK_b对指示信息M进行加密，生成参考认证信息C'，加密的方式与服务器201利用服务器201的认证密钥SK_b对指示信息M加密的方式相同。比较认证信息C与参考认证信息C'，若完全相同，则验证通过。

[0169] 示例性，认证信息C＝HMAC(SK_b,M)，则参考认证信息C'＝HMAC(SK_b,M|)。服务器301只需比较服务器301生成的参考认证信息C'与认证信息C是否相同，若相同，则验证成功，否则失败。

[0170] 若服务请求中还携带有密文C*，则服务器301可以利用服务器201的数据加密密钥DK_b对密文C*进行解密，获取服务器201的敏感数据。

[0171] 步骤403：服务器301在对认证信息C认证通过后，基于服务的相关数据为服务器201提供服务。

[0172] 例如，若服务器集群200所提供的业务为通话业务，服务器集群300所提供的业务为语音去噪业务，当服务器201需要对通话过程中产生的语音进行去噪时，可以发送服务请求，向服务器301请求语音去噪业务，该请求用于请求语音去噪，该请求中可以携带待去噪的语音数据，服务器301可以对待去噪的语音数据进行去噪，并将去噪后的语音数据发送给服务器201。

[0173] 又例如，若服务器集群200所提供的业务为视频存储业务，服务器集群300所提供的业务为视频编解码业务，当服务器201需要对视频流进行编码时，可以发送服务请求，向服务器301请求视频编码业务，该请求用于请求为视频流进行编码，该请求中可以携带待编码的视频数据，服务器301可以对待编码的视频数据进行编码，并将编码后的视频数据发送给服务器201。

[0174] 下面结合附图5所示，本申请实施例提供的一种认证方法进行说明，该方法包括：

[0175] 步骤501：服务器201向安全认证令牌服务中心100发送第一密钥加密密钥请求，第一密钥加密密钥请求用于向安全认证令牌服务中心100请求服务器201的密钥加密密钥。同步骤303，具体可参见步骤303的相关说明，此处不再赘述。

[0176] 步骤502：服务器301向安全认证令牌服务中心100发送第二密钥加密密钥请求，第二密钥加密密钥请求用于向安全认证令牌服务中心100请求服务器301的密钥加密密钥。同步骤303，具体可参见步骤303的相关说明，区别在于发起密钥加密密钥请求的服务器不同，此处不再赘述。

[0177] 本申请实施例并不限定步骤501和步骤502的执行顺序。

[0178] 步骤503：安全认证令牌服务中心100基于根密钥RK生成服务器201的密钥加密密钥KEK_b、第二服务器的密钥加密密钥KEK_a。安全认证令牌服务中心100生成服务器201的密钥

加密密钥KEK_b、第二服务器的密钥加密密钥KEK_a的方式类似，具体可参见步骤304的相关说明此处不再赘述。

[0179] 步骤504：安全认证令牌服务中心向服务器201发送第一密钥加密密钥响应，第一密钥加密响应中携带服务器201的密钥加密密钥KEK_b。同步骤305，具体可参见步骤305的相关说明，此处不再赘述。

[0180] 步骤505：服务器201接收到安全认证令牌服务中心100发送的第一密钥加密密钥响应后，从第一密钥加密密钥响应中获取服务器201的密钥加密密钥KEK_b。

[0181] 步骤506：安全认证令牌服务中心向服务器301发送第二密钥加密密钥响应，第二密钥加密响应中携带服务器301的密钥加密密钥KEK_b。同步骤305，具体可参见步骤305的相关说明，区别在于接收密钥加密密钥响应的服务器不同，此处不再赘述。

[0182] 本申请实施例并不限定步骤504和步骤505的执行顺序。

[0183] 步骤507：服务器301接收到安全认证令牌服务中心100发送的第二密钥加密密钥响应后，从第二密钥加密密钥响应中获取服务器301的密钥加密密钥KEK_a。

[0184] 步骤508：服务器201向安全认证令牌服务中心100发送认证令牌请求，该认证令牌请求用于向安全认证令牌服务中心100请求服务器201与其他服务器认证所需的认证令牌$Token_{ba}$。同步骤307，具体可参见步骤307的相关说明，此处不再赘述。

[0185] 步骤509：安全认证令牌服务中心100基于根密钥生成服务器201与服务器301认证所需的认证令牌$Token_{ba}$。同步骤308，具体可参见步骤308的相关说明，此处不再赘述。

[0186] 步骤510：安全认证令牌服务中心100向服务器201发送的认证令牌响应，该认证令牌响应中携带服务器201与服务器301认证所需的认证令牌$Token_{ba}$。同步骤309，具体可参见步骤309的相关说明，此处不再赘述。

[0187] 步骤511：服务器201从该认证令牌$Token_{ba}$的第一认证参数中获取服务器201的认证密钥SK_b。同步骤310，具体可参见步骤310的相关说明，此处不再赘述。

[0188] 步骤512：服务器201向服务器301发送服务请求，所述服务请求用于向服务器301请求服务器，该服务请求中还可以携带指示信息，指示信息用于指示服务器201所请求的服务类型。同步骤401，具体可参见步骤401的相关说明，此处不再赘述。

[0189] 步骤513：服务器301接收到服务器201发送的服务请求后，服务器301利用认证令牌$Token_{ba}$对认证信息C进行认证。同步骤402，具体可参见步骤402的相关说明，此处不再赘述。

[0190] 步骤514：服务器301在对认证信息C认证通过后，基于服务的相关数据为服务器201提供服务。同步骤403，具体可参见步骤403的相关说明，此处不再赘述。

[0191] 基于与方法实施例同一技术构思，本申请实施例还提供了一种装置，用于执行上述如图3、4、5所示的方法实施例中服务器201执行的方法，相关特征可参见上述方法实施例，此处不再赘述，如图6所示，该装置包括接收单元601、处理单元602以及发送单元603：

[0192] 接收单元601，用于从安全认证令牌服务中心获取第一服务器的密钥加密密钥和第一服务器与第二服务器认证所需的认证令牌，认证令牌包括第一认证参数和第二认证参数。接收单元601可以执行如图3所示的方法实施例中服务器201执行的步骤，如步骤306、步骤309。接收单元601可以执行如图5所示的方法实施例中服务器201执行的步骤，如步骤505、步骤510。

[0193] 处理单元602，用于根据第一服务器的密钥加密密钥对认证令牌中的第一认证参数进行认证；在对第一认证参数认证成功后，从第一认证参数中获取第一服务器的认证密钥，保存认证令牌。处理单元602可以执行如图3所示的方法实施例中服务器201执行的步骤，如步骤310。处理单元602可以执行如图5所示的方法实施例中服务器201执行的步骤，如步骤510。

[0194] 发送单元603，用于向第二服务器发送服务请求，服务请求用于请求第二服务器为第一服务器提供服务，服务请求中包括认证令牌、认证信息、以及指示信息；其中，认证信息是利用第一服务器的认证密钥对指示信息进行认证加密生成的，指示信息用于指示第一服务器所请求的服务类型。发送单元603可以执行如图4所示的方法实施例中服务器201执行的步骤，如步骤401。

[0195] 在一种可能的实施方式中，接收单元601还可以从第一认证参数中获取第一服务器的数据密钥。

[0196] 在一种可能的实施方式中，服务请求还可以包括第一密文，第一密文是利用第一服务器的数据密钥对第一服务器的敏感数据加密生成的，敏感数据为需要加密的数据。

[0197] 在一种可能的实施方式中，接收单元601在从安全认证令牌服务中心获取第一服务器的密钥加密密钥时，发送单元603可以先向安全认证令牌服务中心发送第一请求，第一请求用于请求第一服务器的密钥加密密钥，第一请求包括第一服务器的随机公钥；之后，接收单元601接收安全认证令牌服务中心的第一响应，第一响应中包括第三认证参数；处理单元602可以在利用第一服务器的随机私钥对第三认证参数解密后，从第三认证参数中获取第一服务器的密钥加密密钥。

[0198] 在一种可能的实施方式中，第一请求还包括第一签名值，第一签名值是根据第一服务器的证书私钥对第一服务器的随机公钥进行签名生成的。

[0199] 在一种可能的实施方式中，第一请求还包括第一服务器的证书，第一服务器的证书记录第一服务器的证书私钥对应的证书公钥。

[0200] 在一种可能的实施方式中，第一响应还包括第二签名值，处理单元602在接收单元601从第三认证参数中获取第一服务器的密钥加密密钥之前，可以利用安全认证令牌服务中心的证书公钥对第二签名值验证成功。

[0201] 基于与方法实施例同一发明构思，本申请实施例还提供了一种装置，用于执行如图3、5所示的方法实施例中安全认证令牌服务中心100执行的方法，相关特征可参见上述方法实施例，此处不再赘述，如图7所示，该装置包括生成单元701和发送单元702：

[0202] 生成单元701，用于基于根密钥生成第一服务器的密钥加密密钥、第一服务器的认证密钥以及第二服务器的密钥加密密钥；根据第一认证参数和第二认证参数生成认证令牌，其中，第一认证参数是利用第一服务器的密钥加密密钥对第一服务器的认证密钥进行认证加密生成的，第二认证参数是利用第二服务器的密钥加密密钥对第一服务器的认证密钥进行认证加密生成的；生成单元701可以执行如图3所示的方法实施例中安全认证令牌服务中心100执行的步骤，如步骤304、步骤308。生成单元701可以执行如图5所示的方法实施例中安全认证令牌服务中心100执行的步骤，如步骤503、步骤509。

[0203] 发送单元702，用于向第一服务器发送第一服务器的密钥加密密钥和认证令牌；向第二服务器发送第二服务器的密钥加密密钥。发送单元702可以执行如图3所示的方法实施

例中安全认证令牌服务中心100执行的步骤，如步骤305、步骤309。发送单元702可以执行如图5所示的方法实施例中安全认证令牌服务中心100执行的步骤，如步骤504、步骤505以及步骤510。

[0204] 在一种可能的实施方式中，生成单元701还可以基于根密钥生成第一服务器的数据密钥；并利用第一服务器的密钥加密密钥对第一服务器的认证密钥和数据密钥进行认证加密生成第一认证参数。

[0205] 在一种可能的实施方式中，生成单元701可以利用第二服务器的密钥加密密钥对第一服务器的认证密钥和数据密钥进行认证加密生成第二认证参数。

[0206] 在一种可能的实施方式中，装置还包括接收单元703，接收单元703可以接收来自第一服务器的第一请求，第一请求用于请求第一服务器的密钥加密密钥，第一请求包括第一服务器的随机公钥；生成单元701还可以利用第一服务器的随机公钥对第一服务器的密钥加密密钥进行加密生成第三认证参数；之后，发送单元702可以向第一服务器发送第一响应，第一响应中包括第三认证参数。

[0207] 在一种可能的实施方式中，第一请求还包括第一签名值，生成单元701可以利用第一服务器的证书公钥对第一签名值进行验证，在对第一签名值验证成功后利用第一服务器的随机公钥对第一服务器的密钥加密密钥进行加密生成第三认证参数。

[0208] 在一种可能的实施方式中，第一响应还包括第二签名值，第二签名值是生成单元701根据安全认证令牌服务中心的证书私钥对第一服务器的密钥加密密钥进行签名生成的。

[0209] 基于与方法实施例同一发明构思，本申请实施例还提供了一种第二服务器，用于执行如图4、5所示的方法实施例中服务器301执行的方法，相关特征可参见上述方法实施例，此处不再赘述，如图8所示，该装置包括接收单元801、认证单元802以及处理单元803：

[0210] 接收单元801，用于从安全认证令牌服务中心获取第二服务器的密钥加密密钥；接收来自第一服务器的服务请求，服务请求用于请求第二服务器为第一服务器提供服务，服务请求中包括认证令牌、认证信息、以及指示信息，指示信息用于指示第一服务器所请求的服务类型。接收单元801可以执行如图5所示的方法实施例中服务器301执行的步骤，如步骤507、步骤513中接收服务请求的方法。

[0211] 认证单元802，用于根据第二服务器的密钥加密密钥对认证令牌中的第二认证参数进行认证；在对第二认证参数认证成功后，从第二认证密钥中获取第一服务器的认证密钥；利用第一服务器的认证密钥和指示信息对认证信息进行认证；认证单元802可以执行如图4所示的方法实施例中服务器301执行的步骤，如步骤402。认证单元802可以执行如图5所示的方法实施例中服务器301执行的步骤，如步骤513。

[0212] 处理单元803，用于在认证单元利用第一服务器的认证密钥和指示信息对认证信息认证成功后，向第一服务器提供指示信息所指示的服务。处理单元803可以执行如图4所示的方法实施例中服务器301执行的步骤，如步骤403。处理单元803可以执行如图5所示的方法实施例中服务器301执行的步骤，如步骤514。

[0213] 在一种可能的实施方式中，服务请求还包括第一密文，认证单元可以在对第二认证参数验证成功后，从第二认证密钥中获取第一服务器的数据密钥；利用第一服务器的数据密钥，对第一密文进行解密获取第一服务器的保密数据。

[0214] 在本申请实施例中，所安全认证令牌服务中心100、服务器201和服务器301均可以采用集成的方式划分各个功能模块的形式来呈现。这里的“模块”可以指特定ASIC，电路，执行一个或多个软件或固件程序的处理器和存储器，集成逻辑电路，和/或其他可以提供上述功能的器件。

[0215] 在一个简单的实施例中，本领域的技术人员可以想到安全认证令牌服务中心100、服务器201和服务器301可采用图9所示的形式。

[0216] 如图9所示的通信装置900，包括至少一个处理器901、存储器902，可选的，还可以包括通信接口903。

[0217] 存储器902可以是易失性存储器，例如随机存取存储器；存储器也可以是非易失性存储器，例如只读存储器，快闪存储器，硬盘(hard disk drive，HDD)或固态硬盘(solid-state drive，SSD)、或者存储器902是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，但不限于此。存储器902可以是上述存储器的组合。

[0218] 本申请实施例中不限定上述处理器901以及存储器902之间的具体连接介质。本申请实施例在图中以存储器902和处理器901之间通过总线904连接，总线904在图中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。该总线904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。

[0219] 如图9装置中，可以设置独立的数据收发模块，例如通信接口903，用于收发数据；处理器901在与其他设备进行通信时，可以通过通信接口903进行数据传输。

[0220] 当服务器201采用图9所示的形式时，图9中的处理器901可以通过调用存储器902中存储的计算机执行指令，使得所述服务器201可以执行上述任一方法实施例中的所述服务器201执行的方法。

[0221] 具体的，图5的接收单元、处理单元和发送单元的功能/实现过程均可以通过图9中的处理器901调用存储器902中存储的计算机执行指令来实现。或者，图5中的处理单元的功能/实现过程可以通过图9中的处理器901调用存储器902中存储的计算机执行指令来实现，图5的发送单元和接收单元的功能/实现过程可以通过图9中的通信接口903来实现。

[0222] 当安全认证令牌服务中心100采用图9所示的形式时，图9中的处理器901可以通过调用存储器902中存储的计算机执行指令，使得所述安全认证令牌服务中心可以执行上述任一方法实施例中的所述安全认证令牌服务中心执行的方法。

[0223] 具体的，图6的接收单元、生成单元和发送单元的功能/实现过程均可以通过图9中的处理器901调用存储器902中存储的计算机执行指令来实现。或者，图6中的生成单元的功能/实现过程可以通过图9中的处理器901调用存储器902中存储的计算机执行指令来实现，图6的发送单元和接收单元的功能/实现过程可以通过图9中的通信接口903来实现。

[0224] 当服务器301采用图9所示的形式时，图9中的处理器901可以通过调用存储器902中存储的计算机执行指令，使得所述服务器301可以执行上述任一方法实施例中的所述服务器201执行的方法。

[0225] 具体的，图7的接收单元、处理单元和认证单元的功能/实现过程均可以通过图9中的处理器901调用存储器902中存储的计算机执行指令来实现。或者，图7中的处理单元和认

证单元的功能/实现过程可以通过图9中的处理器901调用存储器902中存储的计算机执行指令来实现，图7的接收单元的功能/实现过程可以通过图9中的通信接口903来实现。

[0226] 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。

[0227] 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。

[0228] 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。

[0229] 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。

[0230] 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。

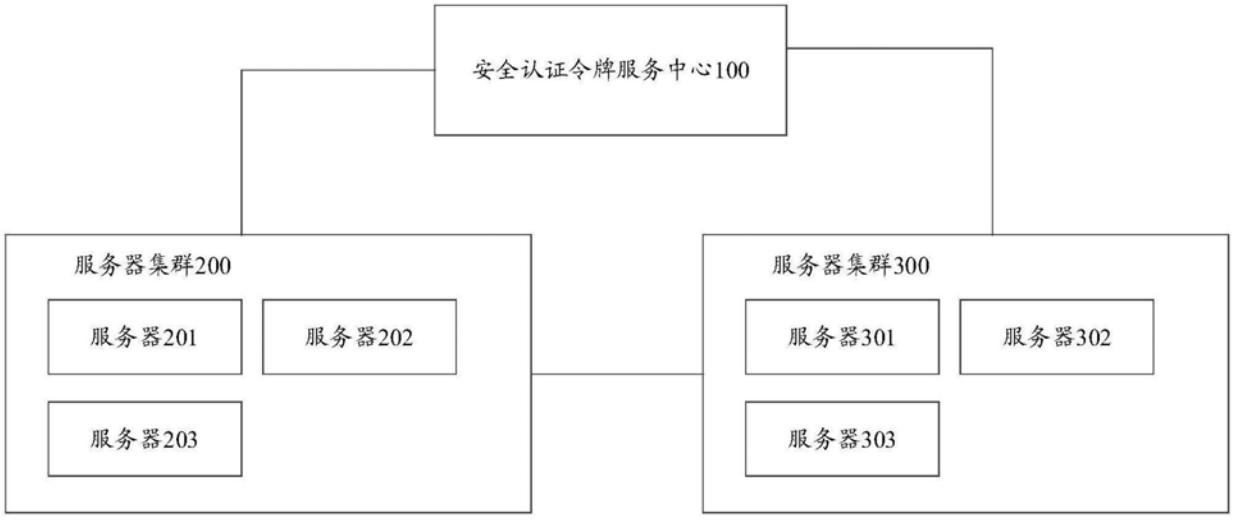

安全认证令牌服务中心100
服务器集群200
服务器201
服务器202
服务器203
服务器集群300
服务器301
服务器302
服务器303

图1

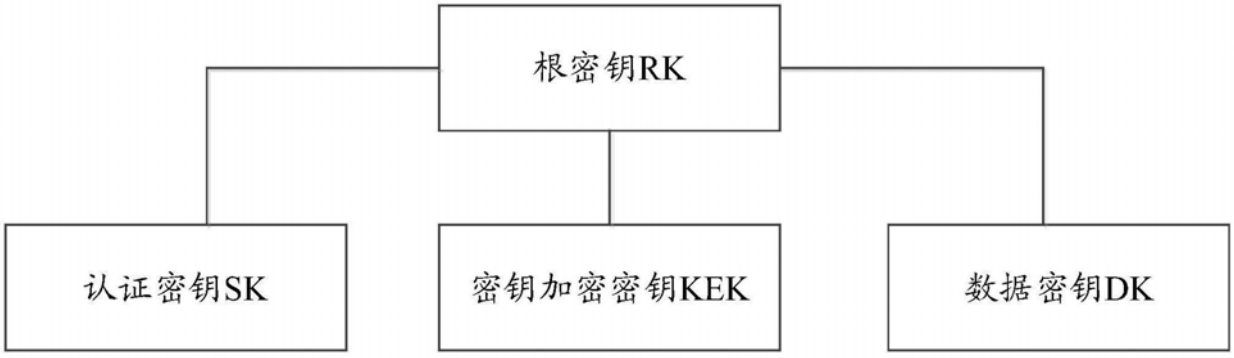

根密钥RK
认证密钥SK
密钥加密密钥KEK
数据密钥DK

图2

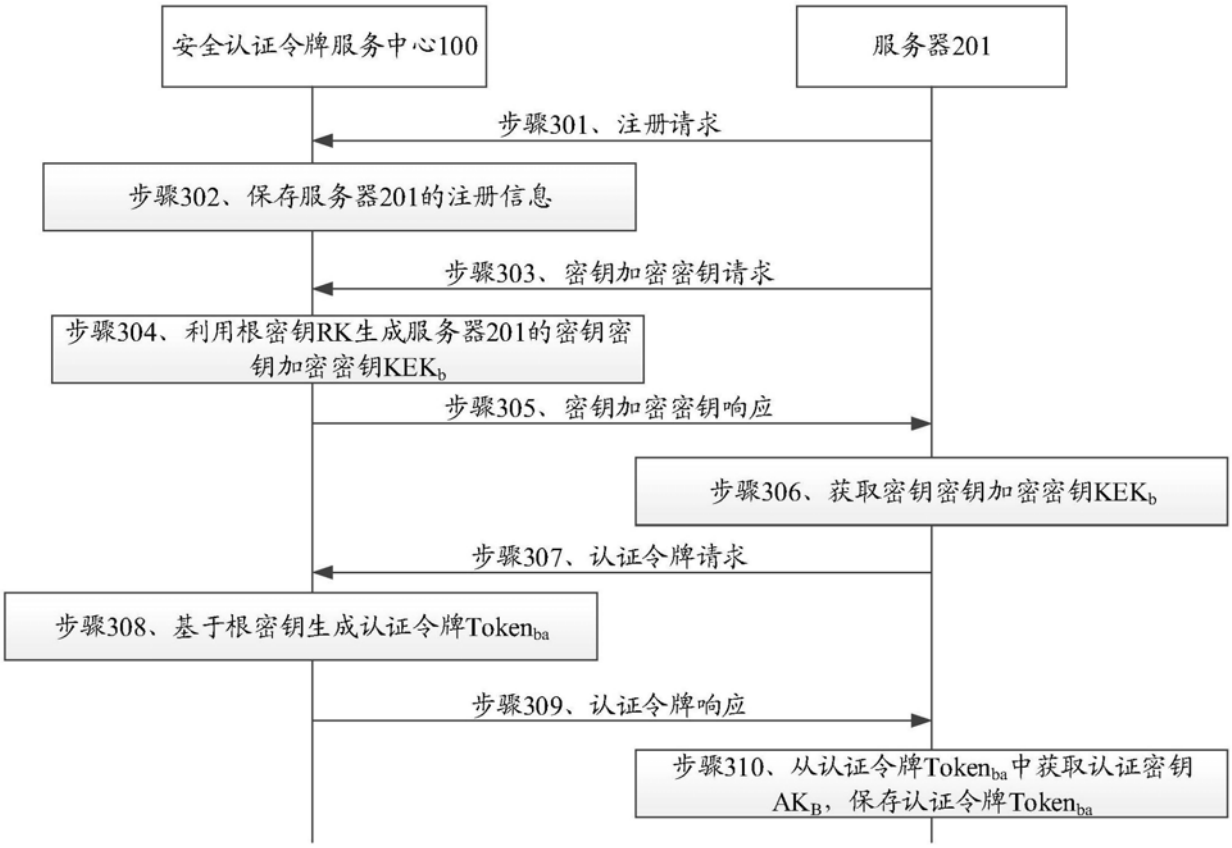

安全认证令牌服务中心100
服务器201
步骤301、注册请求
步骤302、保存服务器201的注册信息
步骤303、密钥加密密钥请求
步骤304、利用根密钥RK生成服务器201的密钥密钥加密密钥KEK$_b$
步骤305、密钥加密密钥响应
步骤306、获取密钥密钥加密密钥KEK$_b$
步骤307、认证令牌请求
步骤308、基于根密钥生成认证令牌Token$_{ba}$
步骤309、认证令牌响应
步骤310、从认证令牌Token$_{ba}$中获取认证密钥AK$_B$，保存认证令牌Token$_{ba}$

图3

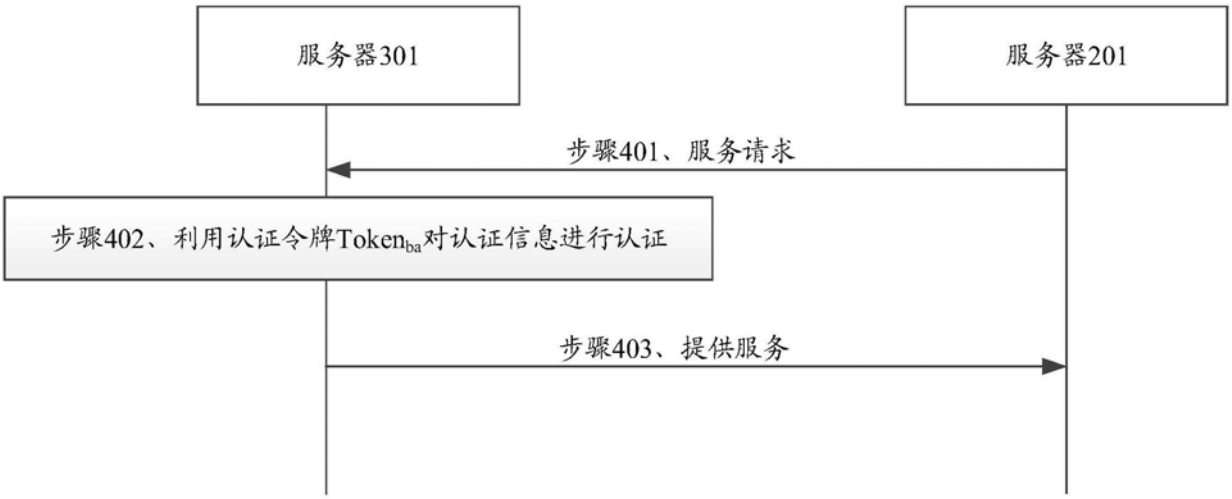

服务器301
服务器201
步骤401、服务请求
步骤402、利用认证令牌Token$_{ba}$对认证信息进行认证
步骤403、提供服务

图4

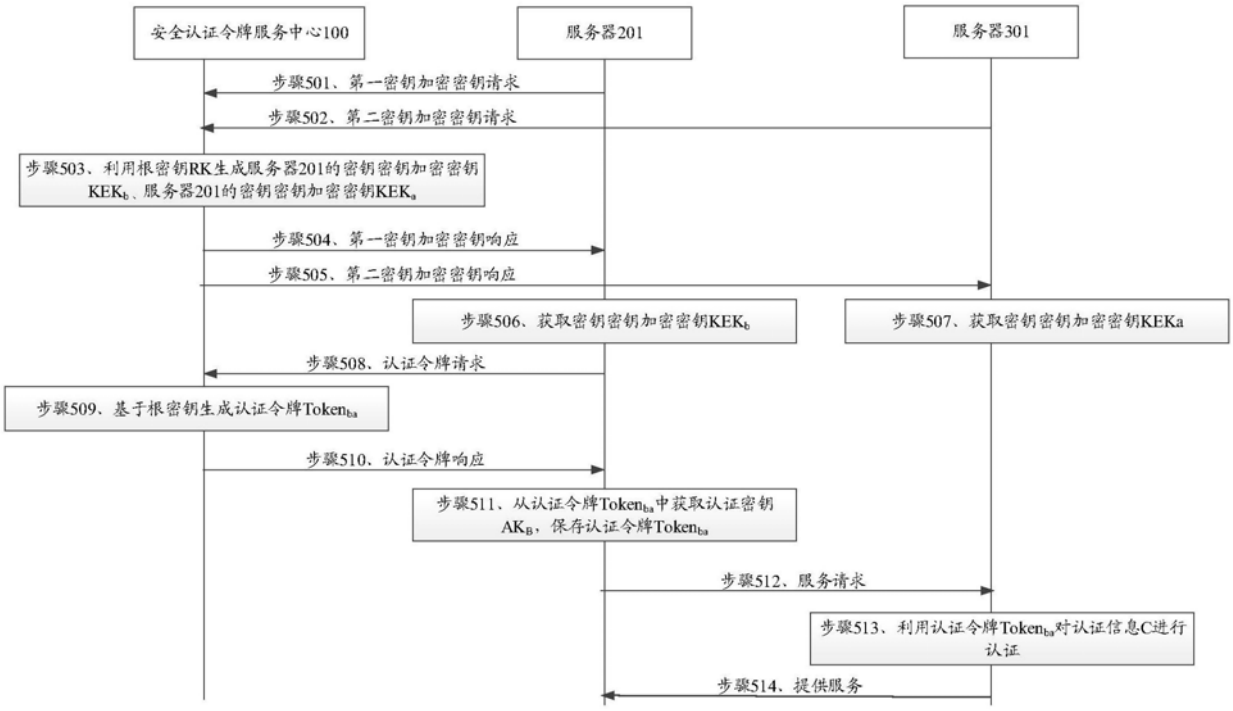

安全认证令牌服务中心100
服务器201
服务器301
步骤501、第一密钥加密密钥请求
步骤502、第二密钥加密密钥请求
步骤503、利用根密钥RK生成服务器201的密钥密钥加密密钥KEKb、服务器201的密钥密钥加密密钥KEKa
步骤504、第一密钥加密密钥响应
步骤505、第二密钥加密密钥响应
步骤506、获取密钥密钥加密密钥KEKb
步骤507、获取密钥密钥加密密钥KEKa
步骤508、认证令牌请求
步骤509、基于根密钥生成认证令牌Tokenba
步骤510、认证令牌响应
步骤511、从认证令牌Tokenba中获取认证密钥AKB，保存认证令牌Tokenba
步骤512、服务请求
步骤513、利用认证令牌Tokenba对认证信息C进行认证
步骤514、提供服务

图5

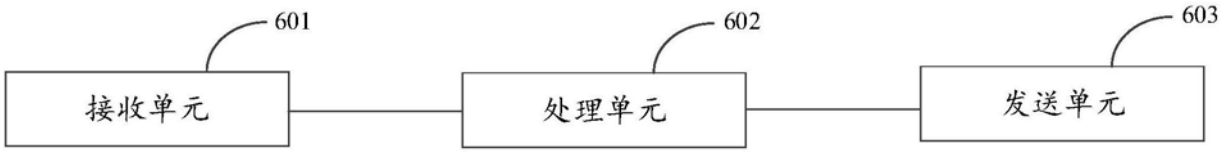

601
接收单元
602
处理单元
603
发送单元

图6


703
接收单元
701
生成单元
702
发送单元

图7

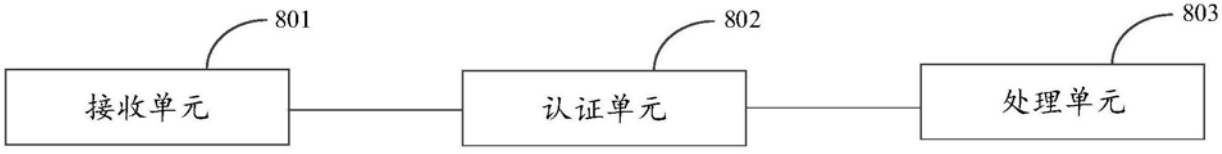

801
接收单元
802
认证单元
803
处理单元

图8

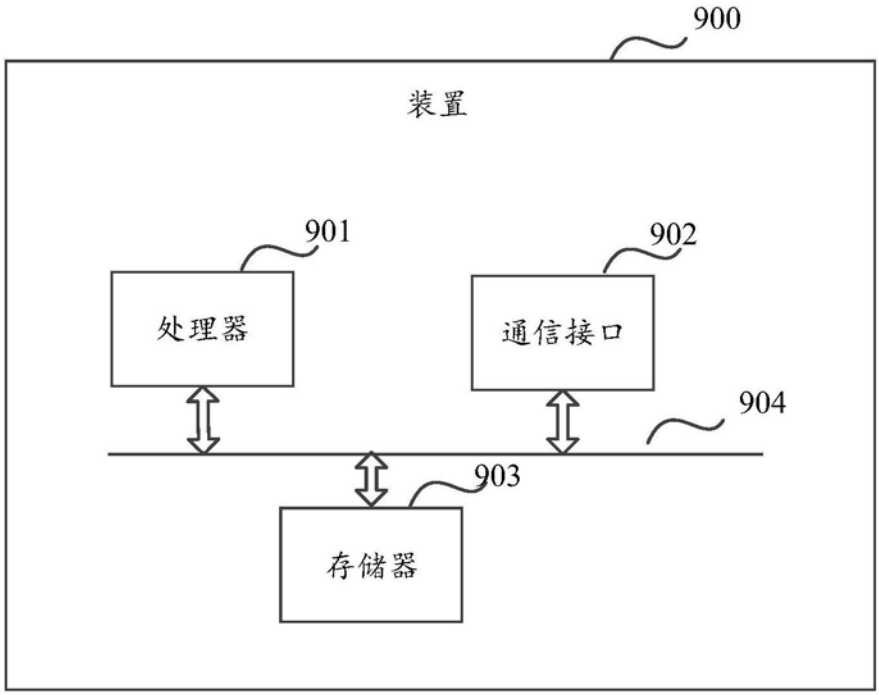


图9