(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114760029 A
(43)申请公布日 2022.07.15

(21)申请号 202011569190.0

(22)申请日 2020.12.26

(71)申请人 西安西电捷通无线网络通信股份有限公司
地址 710075 陕西省西安市高新区科技二路68号西安软件园秦风阁A201

(72)发明人 赖晓龙 曹军 铁满霞 赵晓荣 李琴 张变玲 黄振海

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 钱湾湾

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)

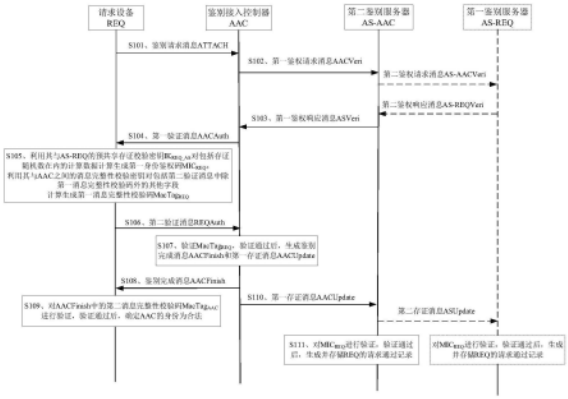
权利要求书11页 说明书25页 附图4页

(54)发明名称

一种身份鉴别方法和装置

(57)摘要

本申请实施例公开了一种身份鉴别方法，请求设备和鉴别接入控制器采用对称密钥的实体鉴别协议进行双向身份鉴别时，在传输消息的过程中以密文的形式传输请求设备的身份信息，由此保证身份鉴别过程中请求设备的真实身份信息的安全性。另外，鉴别接入控制器在验证请求设备的身份合法后，会相应地向请求设备信任的第一鉴别服务器发送第一存证消息，以利用该第一鉴别服务器记录请求设备请求访问网络的行为，为后续网络接入点计费提供客观证据，有效地防止网络接入点对没有在其服务区内尝试访问网络的用户恶意计费。



CN 114760029 A

1.一种身份鉴别方法,其特征在于,所述方法包括:

请求设备向鉴别接入控制器发送鉴别请求消息,所述鉴别请求消息中包括所述请求设备的身份信息密文;所述请求设备的身份信息密文是所述请求设备利用加密证书的公钥对包括所述请求设备的身份标识在内的加密数据加密得到的;

所述鉴别接入控制器向其信任的第二鉴别服务器发送携带有所述请求设备的身份信息密文的第一鉴权请求消息,接收所述第二鉴别服务器发送的第一鉴权响应消息,从所述第一鉴权响应消息中获得所述请求设备信任的第一鉴别服务器产生的存证随机数和所述第一鉴别服务器生成的身份鉴别密钥,其中,所述存证随机数和所述身份鉴别密钥是所述第一鉴别服务器在解密所述请求设备的身份信息密文并根据解密得到的所述请求设备的身份标识确定所述请求设备的身份合法后产生的;所述身份鉴别密钥是根据包括所述第一鉴别服务器与所述请求设备的预共享加密密钥在内的计算数据计算得到的;

所述请求设备接收所述鉴别接入控制器发送的第一验证消息,向所述鉴别接入控制器发送第二验证消息,所述第一验证消息中包括所述存证随机数,所述第二验证消息中包括第一身份鉴权码和第一消息完整性校验码;所述第一身份鉴权码是所述请求设备利用其与所述第一鉴别服务器的预共享存证校验密钥对包括所述存证随机数在内的信息计算生成的;所述第一消息完整性校验码是所述请求设备利用其与所述鉴别接入控制器之间的消息完整性校验密钥对包括所述第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的;其中,所述消息完整性校验密钥是根据包括所述身份鉴别密钥在内的信息计算生成的;

所述鉴别接入控制器对所述第一消息完整性校验码进行验证,验证通过后,确定所述请求设备的身份为合法,生成鉴别完成消息和第一存证消息;

所述请求设备对所述鉴别完成消息中的第二消息完整性校验码进行验证,验证通过后,确定所述鉴别接入控制器的身份为合法;所述第二消息完整性校验码是所述鉴别接入控制器利用所述消息完整性校验密钥对包括所述鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的;

所述第一鉴别服务器对所述第一存证消息中的所述第一身份鉴权码进行验证,验证通过后,生成并存储所述请求设备的请求通过记录。

2.根据权利要求1所述的方法,其特征在于,所述鉴别接入控制器先发送所述第一存证消息,所述第一鉴别服务器对所述第一存证消息中的所述第一身份鉴权码验证通过后,生成第一存证确认消息;

所述鉴别接入控制器接收所述第一存证确认消息后再向所述请求设备发送所述鉴别完成消息。

3.根据权利要求1所述的方法,其特征在于,所述消息完整性校验密钥是所述请求设备和所述鉴别接入控制器协商生成的,包括:

所述第一验证消息中还包括所述鉴别接入控制器根据所述身份鉴别密钥生成的第一密钥交换参数;

所述第二验证消息中还包括所述请求设备根据所述身份鉴别密钥生成的第二密钥交换参数;

所述请求设备根据包括所述第二密钥交换参数对应的临时私钥和所述第一密钥交换

参数所包括的临时公钥进行密钥交换计算生成第一密钥，根据包括所述第一密钥在内的信息利用密钥导出算法计算所述消息完整性校验密钥；所述鉴别接入控制器根据包括所述第一密钥交换参数对应的临时私钥和所述第二密钥交换参数所包括的临时公钥进行密钥交换计算生成所述第一密钥，根据包括所述第一密钥在内的信息利用所述密钥导出算法计算所述消息完整性校验密钥。

4.根据权利要求3所述的方法，其特征在于，所述鉴别接入控制器利用所述身份鉴别密钥，采用对称加密算法对包括所述鉴别接入控制器产生的临时公钥在内的信息进行加密生成所述第一密钥交换参数；

所述请求设备利用所述身份鉴别密钥，采用对称加密算法对包括所述请求设备产生的临时公钥在内的信息进行加密生成所述第二密钥交换参数；

则所述请求设备计算所述消息完整性校验密钥具体为，根据包括所述第二密钥交换参数对应的临时私钥和由所述第一密钥交换参数恢复出的临时公钥进行密钥交换计算生成所述第一密钥，再根据包括所述第一密钥在内的信息利用密钥导出算法计算所述消息完整性校验密钥；

所述鉴别接入控制器计算所述消息完整性校验密钥具体为，根据包括所述第一密钥交换参数对应的临时私钥和由所述第二密钥交换参数恢复出的临时公钥进行密钥交换计算生成所述第一密钥，再根据包括所述第一密钥在内的信息利用所述密钥导出算法计算所述消息完整性校验密钥。

5.根据权利要求4所述的方法，其特征在于，所述鉴别接入控制器计算所述身份鉴别密钥的杂凑值，对所述杂凑值和包括所述鉴别接入控制器产生的临时公钥在内的信息进行异或运算生成所述第一密钥交换参数；

所述请求设备计算所述身份鉴别密钥的杂凑值，对所述杂凑值和包括所述请求设备产生的临时公钥在内的信息进行异或运算生成所述第二密钥交换参数。

6.根据权利要求1所述的方法，其特征在于，所述鉴别请求消息中还包括所述请求设备生成的第一随机数；所述第一鉴权请求消息中还包括所述第一随机数和所述鉴别接入控制器生成的第二随机数；

则所述第一鉴权响应消息中还包括所述第一随机数和所述第二随机数；所述第一验证消息中还包括所述第一随机数和所述第二随机数，所述身份鉴别密钥的计算数据还包括所述第一随机数和所述第二随机数，所述第二验证消息中还包括所述第二随机数；

则所述鉴别接入控制器向所述请求设备发送第一验证消息之前，所述方法还包括：

所述鉴别接入控制器验证所述第一鉴权响应消息中的第二随机数和所述鉴别接入控制器生成的第二随机数的一致性；

则所述请求设备向所述鉴别接入控制器发送第二验证消息之前，所述方法还包括：

所述请求设备验证所述第一验证消息中的第一随机数和所述请求设备生成的第一随机数的一致性；

则在所述鉴别接入控制器确定所述请求设备的身份为合法之前，还包括：

所述鉴别接入控制器对所述第二验证消息中的第二随机数和所述鉴别接入控制器生成的第二随机数的一致性进行验证。

7.根据权利要求1所述的方法，其特征在于，所述鉴别请求消息中还包括所述请求设备

支持的安全能力参数信息，则所述方法还包括：

所述鉴别接入控制器根据所述安全能力参数信息确定所述鉴别接入控制器使用的特定安全策略，则所述第一验证消息中还包括所述特定安全策略。

8.根据权利要求1所述的方法，其特征在于，所述鉴别请求消息中还包括所述请求设备信任的至少一个鉴别服务器的身份标识，则所述方法还包括：

所述鉴别接入控制器根据所述鉴别请求消息中所述请求设备信任的至少一个鉴别服务器的身份标识和所述鉴别接入控制器信任的鉴别服务器的身份标识，确定所述第二鉴别服务器。

9.根据权利要求3所述的方法，其特征在于，所述请求设备的身份信息密文的加密数据还包括所述请求设备生成的身份标识加密密钥；

则所述第一鉴权响应消息中还包括所述请求设备的身份标识密文，所述请求设备的身份标识密文是所述第一鉴别服务器利用解密所述请求设备的身份信息密文所得的所述身份标识加密密钥对所述请求设备的身份标识加密得到的；所述第一验证消息中还包括所述请求设备的身份标识密文；

在所述请求设备向所述鉴别接入控制器发送第二验证消息之前，所述方法还包括：

所述请求设备根据自身的身份标识和所述身份标识加密密钥对所述第一验证消息中的所述请求设备的身份标识密文进行验证。

10.根据权利要求1所述的方法，其特征在于，在生成所述鉴别完成消息和所述第一存证消息之前，所述方法还包括：

所述鉴别接入控制器为所述请求设备分配临时身份标识，则所述鉴别完成消息和所述第一存证消息中还包括所述请求设备的临时身份标识；

所述请求设备确定所述鉴别接入控制器的身份合法时还保存所述请求设备的临时身份标识，所述第一鉴别服务器在生成和存储所述请求设备的请求通过记录时还保存所述请求设备的临时身份标识。

11.根据权利要求1所述的方法，其特征在于，所述鉴别接入控制器获得所述身份鉴别密钥，包括：所述鉴别接入控制器利用与所述第二鉴别服务器的预共享加密密钥解密身份鉴别密钥密文得到所述身份鉴别密钥；所述身份鉴别密钥密文是所述第二鉴别服务器利用与所述鉴别接入控制器的预共享加密密钥对包括所述身份鉴别密钥在内的信息加密生成的。

12.根据权利要求1所述的方法，其特征在于，所述第一存证消息中还包括第二身份鉴权码，所述第二身份鉴权码是所述鉴别接入控制器利用与所述第二鉴别服务器的预共享校验密钥对所述第一存证消息中所述第二身份鉴权码之前的其他字段计算生成的，则所述第一鉴别服务器在生成和存储所述请求设备的请求通过记录之前，所述方法还包括：

所述第二鉴别服务器利用与所述鉴别接入控制器的预共享校验密钥验证所述第二身份鉴权码的正确性。

13.根据权利要求1所述的方法，其特征在于，所述第一鉴权请求消息中还包括所述鉴别接入控制器的身份标识；则所述第一鉴权响应消息中还包括所述鉴别接入控制器的身份标识，所述鉴别接入控制器向所述请求设备发送第一验证消息之前，还包括：

所述鉴别接入控制器验证所述第一鉴权响应消息中的所述鉴别接入控制器的身份标

识和所述鉴别接入控制器自身的身份标识的一致性。

14.根据权利要求9所述的方法,其特征在于,所述第一验证消息中还包括所述鉴别接入控制器的身份标识,所述方法还包括:

当确定所述请求设备的身份为合法时,所述鉴别接入控制器根据包括所述第一密钥、所述请求设备的身份标识密文和所述鉴别接入控制器的身份标识在内的信息计算生成用于后续保密通信的会话密钥;

当确定所述鉴别接入控制器的身份为合法时,所述请求设备根据包括所述第一密钥、所述请求设备的身份标识密文和所述鉴别接入控制器的身份标识在内的信息计算生成用于后续保密通信的会话密钥。

15.根据权利要求1所述的方法,其特征在于,所述第一鉴别服务器和所述第二鉴别服务器不同时,则所述方法还包括:

所述第二鉴别服务器接收所述鉴别接入控制器发送的第一鉴权请求消息,根据所述第一鉴权请求消息生成第二鉴权请求消息,向第一鉴别服务器发送所述第二鉴权请求消息;所述第二鉴权请求消息中包括所述请求设备的身份信息密文;

所述第一鉴别服务器产生存证随机数,生成并向所述第二鉴别服务器发送第二鉴权响应消息;所述第二鉴权响应消息中包括所述身份鉴别密钥和所述存证随机数;

所述第二鉴别服务器根据所述第二鉴权响应消息生成所述第一鉴权响应消息,所述第一鉴权响应消息中包括所述身份鉴别密钥和所述存证随机数;

所述鉴别接入控制器生成所述第一存证消息之后,向所述第二鉴别服务器发送所述第一存证消息;

所述第二鉴别服务器根据所述第一存证消息生成第二存证消息,向所述第一鉴别服务器发送所述第二存证消息;所述第二存证消息中包括所述第一身份鉴权码;

则所述第一鉴别服务器对所述第一身份鉴权码进行验证,具体为所述第一鉴别服务器验证所述第二存证消息中的所述第一身份鉴权码。

16.根据权利要求15所述的方法,其特征在于,所述鉴别接入控制器先向所述第二鉴别服务器发送所述第一存证消息,所述第二鉴别服务器根据所述第一存证消息生成第二存证消息,向所述第一鉴别服务器发送所述第二存证消息,所述第一鉴别服务器验证所述第二存证消息中的所述第一身份鉴权码,验证通过后生成第二存证确认消息;

所述第二鉴别服务器接收所述第二存证确认消息后生成第一存证确认消息,并向所述鉴别接入控制器发送所述第一存证确认消息;

所述鉴别接入控制器接收所述第一存证确认消息后再向所述请求设备发送所述鉴别完成消息。

17.根据权利要求1至16任一项所述的方法,其特征在于,

所述第一消息完整性校验码是所述请求设备利用所述消息完整性校验密钥对包括所述第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的;

所述第二消息完整性校验码是所述鉴别接入控制器利用所述消息完整性校验密钥对包括所述鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的。

18.根据权利要求1至16任一项所述的方法,其特征在于,所述请求设备向所述鉴别接入控制器发送的消息还包括所述请求设备对接收到的所述鉴别接入控制器发送的最新前

序消息计算的杂凑值；

则所述鉴别接入控制器收到所述请求设备发送的消息时，先对接收到的消息中的杂凑值进行验证，验证通过后再执行后续操作；

所述鉴别接入控制器向所述请求设备发送的消息还包括所述鉴别接入控制器对接收到的所述请求设备发送的最新前序消息计算的杂凑值；

则所述请求设备收到所述鉴别接入控制器发送的消息时，先对接收到的消息中的杂凑值进行验证，验证通过后再执行后续操作；

所述鉴别接入控制器向所述第二鉴别服务器发送的消息还包括所述鉴别接入控制器对接收到的所述第二鉴别服务器发送的最新前序消息计算的杂凑值；

则所述第二鉴别服务器收到所述鉴别接入控制器发送的消息时，先对接收到的消息中的杂凑值进行验证，验证通过后再执行后续操作；

所述第二鉴别服务器向所述鉴别接入控制器发送的消息还包括所述第二鉴别服务器对接收到的所述鉴别接入控制器发送的最新前序消息计算的杂凑值；

则所述鉴别接入控制器收到所述第二鉴别服务器器发送的消息时，先对接收到的消息中的杂凑值进行验证，验证通过后再执行后续操作；

所述第一鉴别服务器向所述第二鉴别服务器发送的消息还包括所述第一鉴别服务器对接收到的所述第二鉴别服务器发送的最新前序消息计算的杂凑值；

则所述第二鉴别服务器收到所述第一鉴别服务器发送的消息时，先对接收到的消息中的杂凑值进行验证，验证通过后再执行后续操作；

所述第二鉴别服务器向所述第一鉴别服务器发送的消息还包括所述第二鉴别服务器对接收到的所述第一鉴别服务器发送的最新前序消息计算的杂凑值；

则所述第一鉴别服务器收到所述第二鉴别服务器发送的消息时，先对接收到的消息中的杂凑值进行验证，验证通过后再执行后续操作。

19.一种鉴别接入控制器，其特征在于，所述鉴别接入控制器包括：

接收单元，用于接收请求设备发送的鉴别请求消息，所述鉴别请求消息中包括所述请求设备的身份信息密文；所述请求设备的身份信息密文是所述请求设备利用加密证书的公钥对包括所述请求设备的身份标识在内的加密数据加密得到的；

发送单元，用于向所述鉴别接入控制器信任的第二鉴别服务器发送携带有所述请求设备的身份信息密文的第一鉴权请求消息；

所述接收单元还用于接收所述第二鉴别服务器发送的第一鉴权响应消息，并从所述第一鉴权响应消息中获得所述请求设备信任的第一鉴别服务器产生的存证随机数和所述第一鉴别服务器生成的身份鉴别密钥；所述身份鉴别密钥是根据包括所述第一鉴别服务器与所述请求设备的预共享加密密钥在内的计算数据计算得到的；

所述发送单元还用于向所述请求设备发送第一验证消息，所述第一验证消息中包括所述存证随机数；

所述接收单元还用于接收所述请求设备发送的第二验证消息，所述第二验证消息中包括第一身份鉴权码和第一消息完整性校验码；所述第一消息完整性校验码是所述请求设备利用其与所述鉴别接入控制器之间的消息完整性校验密钥对包括所述第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的；其中，所述消息完整性校验密钥是

根据包括所述身份鉴别密钥在内的信息计算生成的；

处理单元，用于对所述第一消息完整性校验码进行验证，验证通过后，确定所述请求设备的身份为合法，生成鉴别完成消息和第一存证消息；

所述发送单元还用于向所述请求设备发送所述鉴别完成消息，以及向所述第二鉴别服务器发送所述第一存证消息。

20.根据权利要求19所述的鉴别接入控制器，其特征在于，所述发送单元先发送所述第一存证消息，当所述接收单元接收到第一存证确认消息后，所述发送单元再向所述请求设备发送所述鉴别完成消息。

21.根据权利要求19所述的鉴别接入控制器，其特征在于，所述第一验证消息中还包括所述鉴别接入控制器根据所述身份鉴别密钥生成的第一密钥交换参数，所述第二验证消息中还包括所述请求设备根据所述身份鉴别密钥生成的第二密钥交换参数，则所述处理单元还用于：根据包括所述第一密钥交换参数对应的临时私钥和所述第二密钥交换参数所包括的临时公钥进行密钥交换计算生成第一密钥，根据包括所述第一密钥在内的信息利用密钥导出算法计算出所述消息完整性校验密钥。

22.根据权利要求21所述的鉴别接入控制器，其特征在于，所述处理单元还用于：利用所述身份鉴别密钥，采用对称加密算法对包括所述鉴别接入控制器产生的临时公钥在内的信息进行加密生成所述第一密钥交换参数；所述接收单元接收的第二验证消息中的第二密钥交换参数是所述请求设备利用所述身份鉴别密钥，采用对称加密算法对包括所述请求设备产生的临时公钥在内的信息进行加密生成的；

则所述处理单元计算所述消息完整性校验密钥具体为，根据包括所述第一密钥交换参数对应的临时私钥和由所述第二密钥交换参数恢复出的临时公钥进行密钥交换计算生成所述第一密钥，根据包括所述第一密钥在内的信息利用所述密钥导出算法计算出所述消息完整性校验密钥。

23.根据权利要求22所述的鉴别接入控制器，其特征在于，所述处理单元具体用于：计算所述身份鉴别密钥的杂凑值，对所述杂凑值和包括所述鉴别接入控制器产生的临时公钥在内的信息进行异或运算生成所述第一密钥交换参数。

24.根据权利要求19所述的鉴别接入控制器，其特征在于，所述接收单元接收的鉴别请求消息中还包括所述请求设备生成的第一随机数；所述发送单元发送的第一鉴权请求消息中还包括所述第一随机数和所述鉴别接入控制器生成的第二随机数；

则所述接收单元接收的第一鉴权响应消息中还包括所述第一随机数和所述第二随机数；所述发送单元发送的第一验证消息中还包括所述第一随机数和所述第二随机数，所述身份鉴别密钥的计算数据还包括所述第一随机数和所述第二随机数，所述接收单元接收的第二验证消息中还包括所述第二随机数；

则所述处理单元还用于：验证所述第一鉴权响应消息中的第二随机数和所述鉴别接入控制器生成的第二随机数的一致性；以及，对所述第二验证消息中的第二随机数和所述鉴别接入控制器生成的第二随机数的一致性进行验证。

25.根据权利要求19所述的鉴别接入控制器，其特征在于，所述接收单元接收的鉴别请求消息中还包括所述请求设备支持的安全能力参数信息；则所述处理单元还用于：根据所述安全能力参数信息确定所述鉴别接入控制器使用的特定安全策略，则所述第一验证消息

中还包括所述特定安全策略。

26.根据权利要求19所述的鉴别接入控制器，其特征在于，所述接收单元接收的鉴别请求消息中还包括所述请求设备信任的至少一个鉴别服务器的身份标识；则所述处理单元还用于：根据所述鉴别请求消息中所述请求设备信任的至少一个鉴别服务器的身份标识和所述鉴别接入控制器信任的鉴别服务器的身份标识，确定所述第二鉴别服务器。

27.根据权利要求19所述的鉴别接入控制器，其特征在于，所述处理单元还用于：为所述请求设备分配临时身份标识；则所述发送单元发送的鉴别完成消息和第一存证消息中还包括所述请求设备的临时身份标识。

28.根据权利要求19所述的鉴别接入控制器，其特征在于，所述接收单元具体通过以下方式获得所述身份鉴别密钥：利用与所述第二鉴别服务器的预共享加密密钥解密身份鉴别密钥密文得到所述身份鉴别密钥；所述身份鉴别密钥密文是所述第二鉴别服务器利用与所述鉴别接入控制器的预共享加密密钥对包括所述身份鉴别密钥在内的信息加密生成的。

29.根据权利要求19所述的鉴别接入控制器，其特征在于，所述发送单元发送的第一鉴权请求消息中还包括所述鉴别接入控制器的身份标识；所述接收单元接收的第一鉴权响应消息中还包括所述鉴别接入控制器的身份标识；

则所述处理单元还用于：验证所述第一鉴权响应消息中的所述鉴别接入控制器的身份标识和所述鉴别接入控制器自身的身份标识的一致性。

30.根据权利要求21所述的鉴别接入控制器，其特征在于，所述接收单元接收的第一鉴权响应消息中还包括所述请求设备的身份标识密文，所述发送单元发送的第一验证消息中还包括所述鉴别接入控制器的身份标识；则所述处理单元还用于：当确定所述请求设备的身份为合法时，根据包括所述第一密钥、所述请求设备的身份标识密文和所述鉴别接入控制器的身份标识在内的信息计算生成用于后续保密通信的会话密钥。

31.根据权利要求19至30任一项所述的鉴别接入控制器，其特征在于，所述接收单元接收的第二验证消息中的第一消息完整性校验码是所述请求设备利用所述消息完整性校验密钥对包括所述第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的。

32.根据权利要求19至30任一项所述的鉴别接入控制器，其特征在于，所述鉴别接入控制器向所述请求设备发送的消息还包括所述鉴别接入控制器对接收到的所述请求设备发送的最新前序消息计算的杂凑值；所述鉴别接入控制器向所述第二鉴别服务器发送的消息还包括所述鉴别接入控制器对接收到的所述第二鉴别服务器发送的最新前序消息计算的杂凑值。

33.一种请求设备，其特征在于，所述请求设备包括：

发送单元，用于向鉴别接入控制器发送鉴别请求消息，所述鉴别请求消息中包括所述请求设备的身份信息密文；所述请求设备的身份信息密文是所述请求设备利用加密证书的公钥对包括所述请求设备的身份标识在内的加密数据加密得到的；

接收单元，用于接收所述鉴别接入控制器发送的第一验证消息，所述第一验证消息中包括存证随机数；

处理单元，用于利用所述请求设备与其信任的第一鉴别服务器的预共享存证校验密钥对包括所述存证随机数在内的信息计算生成第一身份鉴权码；利用所述请求设备与所述鉴别接入控制器之间的消息完整性校验密钥对包括第二验证消息中除第一消息完整性校验

码外的其他字段计算生成第一消息完整性校验码;其中,所述消息完整性校验密钥是根据包括身份鉴别密钥在内的信息计算得到的,所述身份鉴别密钥是根据包括所述请求设备与所述第一鉴别服务器的预共享加密密钥在内的计算数据计算得到的;

所述发送单元还用于向所述鉴别接入控制器发送所述第二验证消息,所述第二验证消息中包括所述第一身份鉴权码和所述第一消息完整性校验码;

所述接收单元还用于接收所述鉴别接入控制器发送的鉴别完成消息;

所述处理单元还用于对所述鉴别完成消息中的第二消息完整性校验码进行验证,验证通过后,确定所述鉴别接入控制器的身份为合法;所述第二消息完整性校验码是所述鉴别接入控制器利用所述消息完整性校验密钥对包括所述鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的。

34.根据权利要求33所述的请求设备,其特征在于,所述第一验证消息中还包括所述鉴别接入控制器根据身份鉴别密钥生成的第一密钥交换参数;所述第二验证消息中还包括所述请求设备根据所述身份鉴别密钥生成的第二密钥交换参数,则所述处理单元还用于:根据包括所述第二密钥交换参数对应的临时私钥和所述第一密钥交换参数所包括的临时公钥进行密钥交换计算生成第一密钥,根据包括所述第一密钥在内的信息利用密钥导出算法计算出所述消息完整性校验密钥。

35.根据权利要求34所述的请求设备,其特征在于,所述接收单元接收的第一验证消息中所述第一密钥交接参数是所述鉴别接入控制器利用所述身份鉴别密钥,采用对称加密算法对包括所述鉴别接入控制器产生的临时公钥在内的信息进行加密生成的;所述处理单元还用于:利用所述身份鉴别密钥,采用对称加密算法对包括所述请求设备产生的临时公钥在内的信息进行加密生成所述第二密钥交换参数;

则所述处理单元计算所述消息完整性校验密钥具体为,根据包括所述第二密钥交换参数对应的临时私钥和由所述第一密钥交换参数恢复出的临时公钥进行密钥交换计算生成所述第一密钥,根据包括所述第一密钥在内的信息利用所述密钥导出算法计算出所述消息完整性校验密钥。

36.根据权利要求35所述的请求设备,其特征在于,所述处理单元具体用于:计算所述身份鉴别密钥的杂凑值,对所述杂凑值和包括所述请求设备产生的临时公钥在内的信息进行异或运算生成所述第二密钥交换参数。

37.根据权利要求34所述的请求设备,其特征在于,所述发送单元发送的鉴别请求消息中还包括所述请求设备生成的第一随机数;所述接收单元接收的第一验证消息中还包括所述第一随机数和所述鉴别接入控制器生成的第二随机数,所述身份鉴别密钥的计算数据还包括所述第一随机数和所述第二随机数,所述发送单元发送的第二验证消息中还包括所述第二随机数;则所述处理单元还用于:验证所述第一验证消息中的第一随机数和所述请求设备生成的第一随机数的一致性。

38.根据权利要求34所述的请求设备,其特征在于,所述请求设备的身份信息密文的加密数据还包括所述请求设备生成的身份标识加密密钥;

则所述接收单元接收的第一验证消息中还包括请求设备的身份标识密文;所述请求设备的身份标识密文是所述第一鉴别服务器利用解密所述请求设备的身份信息密文所得的所述身份标识加密密钥对所述请求设备的身份标识加密得到的;

则所述处理单元还用于:根据自身的身份标识和所述身份标识加密密钥对所述第一验证消息中的所述请求设备的身份标识密文进行验证。

39.根据权利要求33所述的请求设备,其特征在于,所述接收单元接收的鉴别完成消息中还包括所述鉴别接入控制器为所述请求设备分配的临时身份标识;则所述处理单元还用于确定所述鉴别接入控制器的身份合法时保存所述请求设备的临时身份标识。

40.根据权利要求38所述的请求设备,其特征在于,所述接收单元接收的第一验证消息中还包括所述鉴别接入控制器的身份标识,则所述处理单元还用于:当确定所述鉴别接入控制器的身份为合法时,根据包括所述第一密钥、所述请求设备的身份标识密文和所述鉴别接入控制器的身份标识在内的信息计算生成用于后续保密通信的会话密钥。

41.根据权利要求33至40任一项所述的请求设备,其特征在于,

所述处理单元还用于利用所述消息完整性校验密钥对包括所述第二验证消息中除第一消息完整性校验码外的其他字段计算生成第一消息完整性校验码;

所述接收单元接收的鉴别完成消息中的第二消息完整性校验码是所述鉴别接入控制器利用所述消息完整性校验密钥对包括所述鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的。

42.根据权利要求33至40任一项所述的请求设备,其特征在于,所述请求设备向所述鉴别接入控制器发送的消息还包括所述请求设备对接收到的所述鉴别接入控制器发送的最新前序消息计算的杂凑值。

43.一种第一鉴别服务器,其特征在于,所述第一鉴别服务器为请求设备信任的鉴别服务器,所述第一鉴别服务器包括:

处理单元,用于利用加密证书对应的私钥解密请求设备的身份信息密文得到请求设备的身份标识,根据请求设备的身份标识确定所述请求设备的合法性,在确定所述请求设备的身份合法后,产生存证随机数和身份鉴别密钥,所述身份鉴别密钥是根据包括所述第一鉴别服务器与所述请求设备的预共享加密密钥在内的计算数据计算得到的;

所述处理单元还用于对第一存证消息中的第一身份鉴权码进行验证,验证通过后,生成并存储所述请求设备的请求通过记录。

44.根据权利要求43所述的第一鉴别服务器,其特征在于,所述处理单元还用于对所述第一存证消息中的所述第一身份鉴权码验证通过后,生成第一存证确认消息。

45.根据权利要求43所述的第一鉴别服务器,其特征在于,所述处理单元还用于在生成和存储所述请求设备的请求通过记录时,保存所述鉴别接入控制器为所述请求设备分配的临时身份标识。

46.根据权利要求43所述的第一鉴别服务器,其特征在于,所述第一鉴别服务器与所述鉴别接入控制器信任的第二鉴别服务器不同时,所述第一鉴别服务器还包括:

接收单元,用于接收所述第二鉴别服务器发送的第二鉴权请求消息,所述第二鉴权请求消息中包括所述请求设备的身份信息密文;

发送单元,用于向所述第二鉴别服务器发送第二鉴权响应消息,所述第二鉴权响应消息中包括所述身份鉴别密钥和所述存证随机数;

所述接收单元还用于接收所述第二鉴别服务器发送的第二存证消息,所述第二存证消息中包括所述第一身份鉴权码;

所述处理单元具体用于验证所述第二存证消息中的所述第一身份鉴权码。

47.根据权利要求46所述的第一鉴别服务器,其特征在于,所述处理单元还用于在对所述第二存证消息中的所述第一身份鉴权码验证通过后,生成第二存证确认消息;所述发送单元还用于向所述第二鉴别服务器发送所述第二存证确认消息。

48.根据权利要求43至47任一项所述的第一鉴别服务器,其特征在于,所述第一鉴别服务器向所述第二鉴别服务器发送的消息还包括所述第一鉴别服务器对接收到的所述第二鉴别服务器发送的最新前序消息计算的杂凑值。

49.一种第二鉴别服务器,其特征在于,所述第二鉴别服务器为鉴别接入控制器信任的鉴别服务器,所述第二鉴别服务器包括:

接收单元,用于接收所述鉴别接入控制器发送的携带有请求设备的身份信息密文的第一鉴权请求消息;

发送单元,用于向所述鉴别接入控制器发送第一鉴权响应消息,所述第一鉴别响应消息中包括所述请求设备信任的第一鉴别服务器产生的存证随机数和所述第一鉴别服务器生成的身份鉴别密钥;

所述接收单元还用于接收所述鉴别接入控制器发送的第一存证消息,所述第一存证消息中包括第一身份鉴权码。

50.根据权利要求49所述的第二鉴别服务器,其特征在于,所述接收单元接收的第一存证消息中还包括第二身份鉴权码,所述第二身份鉴权码是所述鉴别接入控制器利用其与所述第二鉴别服务器的预共享校验密钥对所述第一存证消息中所述第二身份鉴权码之前的其他字段计算生成的;则所述第二鉴别服务器还包括:

验证单元,用于利用与所述鉴别接入控制器的预共享校验密钥验证所述第二身份鉴权码的正确性。

51.根据权利要求49所述的第二鉴别服务器,其特征在于,所述第二鉴别服务器与所述请求设备信任的第一鉴别服务器不同时,所述第二鉴别服务器还包括:

处理单元,用于根据所述第一鉴权请求消息生成第二鉴权请求消息,所述第二鉴权请求消息包括所述请求设备的身份信息密文;

所述发送单元还用于向所述第一鉴别服务器发送所述第二鉴权请求消息;

所述接收单元还用于接收所述第一鉴别服务器发送的第二鉴权响应消息,所述第二鉴权响应消息中包括所述身份鉴别密钥和所述存证随机数;

所述处理单元还用于根据所述第二鉴权响应消息生成所述第一鉴权响应消息;

所述处理单元还用于根据所述第一存证消息生成第二存证消息,所述第二存证消息包括所述第一身份鉴权码;

所述发送单元还用于向所述第一鉴别服务器发送所述第二存证消息。

52.根据权利要求51所述的第二鉴别服务器,其特征在于,所述接收单元还用于接收所述第一鉴别服务器生成的第二存证确认消息;所述处理单元还用于在所述接收单元接收到第二存证确认消息后,生成第一存证确认消息;所述发送单元还用于向所述鉴别接入控制器发送所述第一存证确认消息。

53.根据权利要求49至52所述的第二鉴别服务器,其特征在于,所述第二鉴别服务器向所述鉴别接入控制器发送的消息还包括所述第二鉴别服务器对接收到的所述鉴别接入控

制器发送的最新前序消息计算的杂凑值;所述第二鉴别服务器向所述第一鉴别服务器发送的消息还包括所述第二鉴别服务器对接收到的所述第一鉴别服务器发送的最新前序消息计算的杂凑值。

一种身份鉴别方法和装置

技术领域

[0001] 本申请涉及网络通信安全技术领域，特别是涉及一种身份鉴别方法和装置。

背景技术

[0002] 目前，通信网络通常要求在用户和网络接入点之间执行双向身份鉴别，确保合法用户能够与合法网络通信。但在已有的实体鉴别方案中，通常不能保护用户的隐私信息，且会存在网络接入点恶意计费，给用户造成异常收费的问题。

发明内容

[0003] 为了解决上述技术问题，本申请提供了一种身份鉴别方法和装置，采用对称密钥的实体鉴别协议，在保障实体身份和相关信息机密性的同时，实现了请求设备和鉴别接入控制器之间的双向身份鉴别，确保合法用户访问合法网络；并且可以防止网络接入点对没有在其服务区内尝试访问网络的用户恶意计费。同时，选择采用密钥交换计算并通过巧妙的细节及过程设计，增强了协议的抗量子计算攻击或者抗字典暴力破解攻击的能力。

[0004] 本申请实施例公开了如下技术方案：

[0005] 第一方面，本申请实施例提供了一种身份鉴别方法，包括：

[0006] 请求设备向鉴别接入控制器发送鉴别请求消息，所述鉴别请求消息中包括所述请求设备的身份信息密文；所述请求设备的身份信息密文是所述请求设备利用加密证书的公钥对包括所述请求设备的身份标识在内的加密数据加密得到的；

[0007] 所述鉴别接入控制器向其信任的第二鉴别服务器发送携带有所述请求设备的身份信息密文的第一鉴权请求消息，接收所述第二鉴别服务器发送的第一鉴权响应消息，从所述第一鉴权响应消息中获得所述请求设备信任的第一鉴别服务器产生的存证随机数和所述第一鉴别服务器生成的身份鉴别密钥，其中，所述存证随机数和所述身份鉴别密钥是所述第一鉴别服务器在解密所述请求设备的身份信息密文并根据解密得到的所述请求设备的身份标识确定所述请求设备的身份合法后产生的；所述身份鉴别密钥是根据包括所述第一鉴别服务器与所述请求设备的预共享加密密钥在内的计算数据计算得到的；

[0008] 所述请求设备接收所述鉴别接入控制器发送的第一验证消息，向所述鉴别接入控制器发送第二验证消息，所述第一验证消息中包括所述存证随机数，所述第二验证消息中包括第一身份鉴权码和第一消息完整性校验码；所述第一身份鉴权码是所述请求设备利用其与所述第一鉴别服务器的预共享存证校验密钥对包括所述存证随机数在内的信息计算生成的；所述第一消息完整性校验码是所述请求设备利用其与所述鉴别接入控制器之间的消息完整性校验密钥对包括所述第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的；其中，所述消息完整性校验密钥是根据包括所述身份鉴别密钥在内的信息计算得到的；

[0009] 所述鉴别接入控制器对所述第一消息完整性校验码进行验证，验证通过后，确定所述请求设备的身份为合法，生成鉴别完成消息和第一存证消息；

[0010] 所述请求设备对所述鉴别完成消息中的第二消息完整性校验码进行验证，验证通过后，确定所述鉴别接入控制器的身份为合法；所述第二消息完整性校验码是所述鉴别接入控制器利用所述消息完整性校验密钥对包括所述鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的；

[0011] 所述第一鉴别服务器对所述第一存证消息中的所述第一身份鉴权码进行验证，验证通过后，生成并存储所述请求设备的请求通过记录。

[0012] 第二方面，本申请实施例提供了一种鉴别接入控制器，包括：

[0013] 接收单元，用于接收请求设备发送的鉴别请求消息，所述鉴别请求消息中包括所述请求设备的身份信息密文；所述请求设备的身份信息密文是所述请求设备利用加密证书的公钥对包括所述请求设备的身份标识在内的加密数据加密得到的；

[0014] 发送单元，用于向所述鉴别接入控制器信任的第二鉴别服务器发送携带有所述请求设备的身份信息密文的第一鉴权请求消息；

[0015] 所述接收单元还用于接收所述第二鉴别服务器发送的第一鉴权响应消息，并从所述第一鉴权响应消息中获得所述请求设备信任的第一鉴别服务器产生的存证随机数和所述第一鉴别服务器生成的身份鉴别密钥；所述身份鉴别密钥是根据包括所述第一鉴别服务器与所述请求设备的预共享加密密钥在内的计算数据计算得到的；

[0016] 所述发送单元还用于向所述请求设备发送第一验证消息，所述第一验证消息中包括所述存证随机数；

[0017] 所述接收单元还用于接收所述请求设备发送的第二验证消息，所述第二验证消息中包括第一身份鉴权码和第一消息完整性校验码；所述第一消息完整性校验码是所述请求设备利用其与所述鉴别接入控制器之间的消息完整性校验密钥对包括所述第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的；其中，所述消息完整性校验密钥是根据包括所述身份鉴别密钥在内的信息计算生成的；

[0018] 处理单元，用于对所述第一消息完整性校验码进行验证，验证通过后，确定所述请求设备的身份为合法，生成鉴别完成消息和第一存证消息；

[0019] 所述发送单元还用于向所述请求设备发送所述鉴别完成消息，以及向所述第二鉴别服务器发送所述第一存证消息。

[0020] 第三方面，本申请实施例提供了一种请求设备，包括：

[0021] 发送单元，用于向鉴别接入控制器发送鉴别请求消息，所述鉴别请求消息中包括所述请求设备的身份信息密文；所述请求设备的身份信息密文是所述请求设备利用加密证书的公钥对包括所述请求设备的身份标识在内的加密数据加密得到的；

[0022] 接收单元，用于接收所述鉴别接入控制器发送的第一验证消息，所述第一验证消息中包括存证随机数；

[0023] 处理单元，用于利用所述请求设备与其信任的第一鉴别服务器的预共享存证校验密钥对包括所述存证随机数在内的信息计算生成第一身份鉴权码；利用所述请求设备与所述鉴别接入控制器之间的消息完整性校验密钥对包括第二验证消息中除第一消息完整性校验码外的其他字段计算生成第一消息完整性校验码；其中，所述消息完整性校验密钥是根据包括身份鉴别密钥在内的信息计算得到的，所述身份鉴别密钥是根据包括所述请求设备与所述第一鉴别服务器的预共享加密密钥在内的计算数据计算得到的；

[0024] 所述发送单元还用于向所述鉴别接入控制器发送所述第二验证消息，所述第二验证消息中包括所述第一身份鉴权码和所述第一消息完整性校验码；

[0025] 所述接收单元还用于接收所述鉴别接入控制器发送的鉴别完成消息；

[0026] 所述处理单元还用于对所述鉴别完成消息中的第二消息完整性校验码进行验证，验证通过后，确定所述鉴别接入控制器的身份为合法；所述第二消息完整性校验码是所述鉴别接入控制器利用所述消息完整性校验密钥对包括所述鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的。

[0027] 第四方面，本申请实施例提供了一种第一鉴别服务器，所述第一鉴别服务器为请求设备信任的鉴别服务器，包括：

[0028] 处理单元，用于利用加密证书对应的私钥解密请求设备的身份信息密文得到请求设备的身份标识，根据请求设备的身份标识确定所述请求设备的合法性，在确定所述请求设备的身份合法后，产生存证随机数和身份鉴别密钥，所述身份鉴别密钥是根据包括所述第一鉴别服务器与所述请求设备的预共享加密密钥在内的计算数据计算得到的；

[0029] 所述处理单元还用于对第一存证消息中的第一身份鉴权码进行验证，验证通过后，生成并存储所述请求设备的请求通过记录。

[0030] 第五方面，本申请实施例提供了一种第二鉴别服务器，所述第二鉴别服务器为鉴别接入控制器信任的鉴别服务器，包括：

[0031] 接收单元，用于接收所述鉴别接入控制器发送的携带有请求设备的身份信息密文的第一鉴权请求消息；

[0032] 发送单元，用于向所述鉴别接入控制器发送第一鉴权响应消息，所述第一鉴别响应消息中包括所述请求设备信任的第一鉴别服务器产生的存证随机数和所述第一鉴别服务器生成的身份鉴别密钥；

[0033] 所述接收单元还用于接收所述鉴别接入控制器发送的第一存证消息，所述第一存证消息中包括第一身份鉴权码。

[0034] 由上述技术方案可以看出，请求设备和鉴别接入控制器采用对称密钥的实体鉴别协议进行双向身份鉴别时，在传输消息的过程中以密文的形式传输请求设备的身份信息，由此保证身份鉴别过程中请求设备的真实身份信息的安全性。另外，鉴别接入控制器在验证请求设备的身份合法后，会相应地向请求设备信任的第一鉴别服务器发送第一存证消息，以利用该第一鉴别服务器记录请求设备请求访问网络的行为，为后续网络接入点计费提供客观证据，有效地防止网络接入点对没有在其服务区内尝试访问网络的用户恶意计费。

附图说明

[0035] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0036] 图1为本申请实施例提供的一种身份鉴别方法的示意图；

[0037] 图2为本申请实施例提供的非漫游情况下一种身份鉴别方法的示意图，其中“*”表

示可选的字段或可选的操作；

[0038] 图3为本申请实施例提供的漫游情况下一种身份鉴别方法的示意图，其中“*”表示可选的字段或可选的操作；

[0039] 图4为本申请实施例提供的一种鉴别接入控制器AAC的结构框图；

[0040] 图5为本申请实施例提供的一种请求设备REQ的结构框图；

[0041] 图6为本申请实施例提供的一种第一鉴别服务器AS-REQ的结构框图；

[0042] 图7为本申请实施例提供的一种第二鉴别服务器AS-AAC的结构框图。

具体实施方式

[0043] 在通信网络中，请求设备可以通过鉴别接入控制器访问网络，为了确保访问网络的请求设备为合法设备，以及用户所请求访问的网络为合法网络，鉴别接入控制器和请求设备之间通常需要进行双向的身份鉴别。

[0044] 例如，在请求设备通过鉴别接入控制器接入无线网络的场景下，请求设备可以为手机、个人数字助理(Personal Digital Assistant，简称PDA)、平板电脑等终端设备，鉴别接入控制器可以是无线接入点。在请求设备通过鉴别接入控制器接入有线网络的场景下，请求设备可以为台式机、笔记本电脑等终端设备，鉴别接入控制器可以是交换机或路由器等。在请求设备通过鉴别接入控制器接入第四/五代移动通信技术(the 4th/5th Generation mobile communication technology，简称4G/5G)网络的场景下，请求设备可以为手机，鉴别接入控制器可以为基站。当然，本申请同样适用于其他有线网络、近距离通信网络等各种数据通信场景。

[0045] 在请求设备进行身份鉴别的过程中，请求设备需要提供自身真实的身份信息，以便鉴别接入控制器对请求设备进行身份鉴别，例如该身份信息可以为请求设备的身份标识，身份标识中可能携带了身份证号、家庭住址、银行卡信息、地理位置等私密、敏感信息，若在身份鉴别过程中被攻击者截获用于非法用途，会对鉴别接入控制器、请求设备甚至网络造成极大的安全隐患。

[0046] 为了解决上述技术问题，本申请实施例提供了一种身份鉴别方法，在该方法中，请求设备向鉴别接入控制器发送鉴别请求消息，鉴别请求消息中包括请求设备的身份信息密文，身份信息密文是请求设备利用加密证书的公钥对包括请求设备的身份标识在内的加密数据加密得到的；鉴别接入控制器向其信任的第二鉴别服务器发送携带有请求设备的身份信息密文的第一鉴权请求消息，并接收第二鉴别服务器发送的第一鉴权响应消息，从第一鉴权响应消息中获得请求设备信任的第一鉴别服务器在确定请求设备的身份合法后产生的存证随机数和第一鉴别服务器生成的身份鉴别密钥，身份鉴别密钥是根据包括第一鉴别服务器与请求设备的预共享加密密钥在内的计算数据计算得到的；请求设备接收鉴别接入控制器发送的第一验证消息，第一验证消息中包括存证随机数，并向鉴别接入控制器发送第二验证消息，第二验证消息中包括第一身份鉴权码和第一消息完整性校验码，第一身份鉴权码是请求设备利用其与第一鉴别服务器的预共享存证校验密钥对包括存证随机数在内的信息计算生成的，第一消息完整性校验码是请求设备利用其与鉴别接入控制器之间的消息完整性校验密钥对包括第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的；鉴别接入控制器验证第一消息完整性校验码，验证通过后，确定请求设备的身

份合法,生成鉴别完成消息和第一存证消息;请求设备验证鉴别完成消息中的第二消息完整性校验码,验证通过后,确定鉴别接入控制器的身份为合法,第二消息完整性校验码是鉴别接入控制器利用所述消息完整性校验密钥对包括鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的;第一鉴别服务器验证第一存证消息中的第一身份鉴权码,验证通过后,生成并存储请求设备的请求通过记录。

[0047] 由此可见,请求设备和鉴别接入控制器采用对称密钥的实体鉴别协议进行双向身份鉴别时,以密文的形式传输请求设备的身份信息,由此保证身份鉴别过程中请求设备的真实身份信息的安全性。另外,鉴别接入控制器在验证请求设备的身份合法后,会相应地向请求设备信任的第一鉴别服务器发送包括请求设备生成的第一身份鉴权码的第一存证消息,以便第一鉴别服务器根据所述第一身份鉴权码生成并存储请求设备的请求访问网络的记录,为后续网络接入点计费提供客观证据,有效地防止网络接入点对没有在其服务区内尝试访问网络的用户恶意计费。

[0048] 需要说明的是,本申请实施例提供的身份鉴别方法用于实现鉴别接入控制器与请求设备的双向身份鉴别(Mutual Identity Authentication,简称MIA)。

[0049] 为便于介绍,在本申请实施例中,将以请求设备(REQuester,简称REQ)、鉴别接入控制器(Authentication Access Controller,简称AAC)和鉴别服务器(Authentication Server,简称AS)为例对一种身份鉴别方法进行介绍。

[0050] 其中,REQ信任的AS称为第一鉴别服务器AS-REQ,AAC信任的AS称为第二鉴别服务器AS-AAC。REQ可以为参与身份鉴别过程的一个端点,与AAC建立连接,访问AAC提供的服务,且通过AAC访问AS。AAC可以为参与身份鉴别过程的另一个端点,与REQ建立连接,提供服务,且可直接访问AS-AAC;AS-AAC可直接访问AS-REQ。当REQ与AAC信任的AS相同时,AS-AAC与AS-REQ可以为同一AS;当REQ与AAC信任的AS不同时,AS-AAC与AS-REQ为不同的AS,此时发生了漫游。

[0051] 在采用对称密钥的实体鉴别协议实现REQ与AAC之间的双向身份鉴别之前,REQ和AS-REQ之间具有预共享存证校验密钥K_{REQ_AS},K_{REQ_AS}为REQ和AS-REQ预置或分发的相同的静态密钥,REQ和AAC均具有能够标识自身身份的ID。证书解密服务器(Certificate Sever-Decrypt,简称CS-DEC)持有符合ISO/IEC 9594-8/ITU X.509、其他标准或其他技术体系规定的加密证书和加密证书对应的私钥,CS-DEC可以是独立的服务器,也可以驻留在AS-REQ中;且REQ知晓该加密证书或加密证书中的公钥。

[0052] 下面对图1示出的一种身份鉴别方法进行介绍,该方法包括:

[0053] S101、REQ向AAC发送鉴别请求消息ATTACH。

[0054] 该ATTACH中包括REQ的身份信息密文$EncPub_{AS}$。$EncPub_{AS}$是REQ利用加密证书的公钥对包括自身的身份标识ID_{REQ}在内的加密数据加密得到的。如此,在传输消息的过程中,防止非法分子获取REQ的真实身份标识,保证REQ的真实身份标识的安全性。本申请中,将被加密的对象称为加密数据。

[0055] 可选的,REQ计算$EncPub_{AS}$的加密数据中还可以包括REQ生成的身份标识加密密钥$Nonce_{REQID}$,即REQ还可以利用加密证书的公钥对包括ID_{REQ}和$Nonce_{REQID}$在内的加密数据加密得到身份信息密文$EncPub_{AS}$。

[0056] 可选的,ATTACH中还可以包括REQ支持的安全能力参数信息Security

capabilities$_{REQ}$,Security capabilities$_{REQ}$中包括REQ支持的身份鉴别套件(身份鉴别套件中包含一种或多种身份鉴别方法)、完整性校验算法、杂凑(HASH)算法、密钥交换算法和/或密钥导出算法等,以供AAC据以选择要使用的特定安全策略Security capabilities$_{AAC}$。

[0057] 可选的,ATTACH中还可以包括REQ信任的至少一个鉴别服务器的身份标识Route$_{AS}$,以便AAC根据Route$_{AS}$及自身信任的鉴别服务器的身份标识,确定第二鉴别服务器AS-AAC。

[0058] 可选的,ATTACH中还可以包括REQ生成的第一随机数Nonce$_{REQ}$。

[0059] S102、AAC向其信任的AS-AAC发送第一鉴权请求消息AACVeri。

[0060] 该AACVeri中包括ATTACH中携带的REQ的身份信息密文EncPub$_{AS}$。

[0061] 可选的,若ATTACH中包括REQ信任的至少一个鉴别服务器的身份标识Route$_{AS}$,则AAC在发送AACVeri之前,需要先根据ATTACH中的Route$_{AS}$和自身信任的鉴别服务器的身份标识,确定第二鉴别服务器AS-AAC。具体的,若REQ与AAC存在共同信任的鉴别服务器,则可以确定此时为非漫游情况,即AS-AAC与AS-REQ为同一鉴别服务器;若REQ与AAC之间不存在共同信任的鉴别服务器,则可以确定此时为漫游情况,即AS-AAC与AS-REQ为两个独立的鉴别服务器。

[0062] 可选的,AACVeri中还可以包括AAC的身份标识ID$_{AAC}$和/或AAC生成的第二随机数Nonce$_{AAC}$。若REQ向AAC发送的ATTACH中包括Nonce$_{REQ}$,则AAC向AS-AAC发送的AACVeri中也可以包括该Nonce$_{REQ}$。

[0063] S103、AAC接收AS-AAC发送的第一鉴权响应消息ASVeri。

[0064] 该ASVeri中包括AS-REQ在验证REQ的身份合法后产生的存证随机数和身份鉴别密钥IAK。

[0065] 需要说明的是,若AS-REQ与AS-AAC为同一个鉴别服务器,即非漫游情况,此时可以用AS-AAC(当然也可以用AS-REQ)表示REQ和AAC共同信任的鉴别服务器,则AAC向AS-AAC(也可以表示为AS-REQ)发送携带有EncPub$_{AS}$的AACVeri,AS-AAC(也可以表示为AS-REQ)接收到AACVeri后,获取利用加密证书对应的私钥解密EncPub$_{AS}$得到的ID$_{REQ}$,并根据ID$_{REQ}$判断REQ的身份是否合法,若合法,则生成存证随机数Nonce$_{AS_AAC}$(也可以表示为Nonce$_{AS_REQ}$)和身份鉴别密钥IAK,并将包括Nonce$_{AS_AAC}$(也可以表示为Nonce$_{AS_REQ}$)和IAK的ASVeri发送给AAC。其中,上述对EncPub$_{AS}$的解密可以由与AS-AAC(也可以表示为AS-REQ)有交互、信任关系的CS-DEC执行,也可以由AS-AAC(也可以表示为AS-REQ)执行。其中,IAK是AS-AAC(也可以表示为AS-REQ)采用与REQ约定的密钥导出算法对包括自身与REQ的预共享加密密钥K$_{REQ_AS}$在内的计算数据计算得到的。本申请中,将算法运算时采用的计算对象称为计算数据。

[0066] 若AS-REQ与AS-AAC为不同的鉴别服务器,即漫游情况,此时AAC先向AS-AAC发送携带有EncPub$_{AS}$的AACVeri,AS-AAC根据AACVeri生成第二鉴权请求消息AS-AACVeri,向AS-REQ发送AS-AACVeri,AS-AACVeri中携带有EncPub$_{AS}$。AS-REQ获取利用加密证书对应的私钥解密EncPub$_{AS}$得到的ID$_{REQ}$,根据ID$_{REQ}$判断REQ的身份是否合法,若合法,则生成存证随机数Nonce$_{AS_REQ}$和身份鉴别密钥IAK,将包括Nonce$_{AS_REQ}$和IAK在内的第二鉴权响应消息AS-REQVeri发送给AS-AAC,然后AS-AAC根据AS-REQVeri生成ASVeri,并将包括Nonce$_{AS_REQ}$和IAK的ASVeri发送给AAC。其中,上述对EncPub$_{AS}$的解密可以由与AS-REQ有交互、信任关系的CS-DEC执行,也可以由AS-REQ执行。IAK是AS-REQ采用与REQ约定的密钥导出算法对包括自身与REQ的预共享加密密钥K$_{REQ_AS}$在内的计算数据计算得到的。

[0067] 可选的，当AACVeri中包括$Nonce_{REQ}$和$Nonce_{AAC}$时，鉴别服务器计算IAK时的计算数据还包括$Nonce_{REQ}$和$Nonce_{AAC}$。

[0068] 可选的，当REQ的身份信息密文$EncPub_{AS}$的加密数据还包括身份标识加密密钥$Nonce_{REQID}$时，非漫游情况下，AS-AAC(当然也可以表示为AS-REQ)还可以利用解密$EncPub_{AS}$得到的$Nonce_{REQID}$对ID_{REQ}进行加密得到REQ的身份标识密文，则ASVeri中还可以包括REQ的身份标识密文；漫游情况下，AS-REQ还可以利用解密$EncPub_{AS}$得到的$Nonce_{REQID}$对ID_{REQ}进行加密得到REQ的身份标识密文，则AS-REQVeri和ASVeri中还可以包括REQ的身份标识密文；REQ的身份标识密文可以为利用$Nonce_{REQID}$对ID_{REQ}进行异或运算的结果，即$ID_{REQ} \oplus Nonce_{REQID}$。

[0069] 可选的，当AACVeri中包括ID_{AAC}和/或$Nonce_{AAC}$时，ASVeri中也可以包括ID_{AAC}和/或$Nonce_{AAC}$。相应地，AAC接收到ASVeri后，可以判断ASVeri中的ID_{AAC}与自身的身份标识ID_{AAC}是否一致，和/或，判断ASVeri中的$Nonce_{AAC}$与自身生成的$Nonce_{AAC}$是否一致，若一致，则继续执行后续操作，若不一致，则丢弃ASVeri。

[0070] 可选的，AAC和AS-AAC之间具有预共享加密密钥EK_{AAC_AS}，AS-AAC可以利用EK_{AAC_AS}对包括IAK在内的信息进行加密得到身份鉴别密钥密文$EncData_{AS_AAC}$，利用$EncData_{AS_AAC}$替换ASVeri中的IAK。

[0071] S104、AAC向REQ发送第一验证消息AACAuth。

[0072] 该AACAuth中包括存证随机数。

[0073] 可选的，AACAuth还可以包括第一密钥交换参数$KeyInfo_{AAC}$。$KeyInfo_{AAC}$是AAC利用身份鉴别密钥IAK采用对称加密算法对包括自身产生的临时公钥在内的信息加密计算得到的结果。AAC计算$KeyInfo_{AAC}$时，可以先计算IAK的杂凑值即HASH(IAK)，进而对HASH(IAK)和包括AAC产生的临时公钥在内的信息进行异或运算生成$KeyInfo_{AAC}$。或者，AAC计算$KeyInfo_{AAC}$时，可以先计算扩展身份鉴别密钥EIAK，再对EIAK和包括AAC产生的临时公钥在内的信息进行异或运算生成$KeyInfo_{AAC}$，其中，EIAK是AAC根据包括所述IAK及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算生成的。其中，AAC产生的所述临时公钥是AAC产生的临时公私钥对中的临时公钥。

[0074] 可选的，若ASVeri中携带有身份鉴别密钥密文$EncData_{AS_AAC}$，则AAC需要利用其与AS-AAC的预共享加密密钥EK_{AAC_AS}解密$EncData_{AS_AAC}$得到IAK。

[0075] 可选的，若ATTACH中包括$Security\ capabilities_{REQ}$，则AAC可以根据$Security\ capabilities_{REQ}$确定自身使用的特定安全策略$Security\ capabilities_{AAC}$，并将$Security\ capabilities_{AAC}$添加至AACAuth中发送给REQ。$Security\ capabilities_{AAC}$表示AAC确定使用的身份鉴别方法、完整性校验算法、杂凑算法、密钥交换算法和/或密钥导出算法等。

[0076] 可选的，当ASVeri中还包括REQ的身份标识密文时，AAC可以将REQ的身份标识密文添加至AACAuth中发送给REQ，即AACAuth中还可以包括$ID_{REQ} \oplus Nonce_{REQID}$。

[0077] 可选的，AAC还可以将ID_{AAC}、$Nonce_{AAC}$和$Nonce_{REQ}$中任意一项或多项添加至AACAuth中发送给REQ。

[0078] S105、REQ利用其与AS-REQ的预共享存证校验密钥IK_{REQ_AS}对包括存证随机数在内的计算数据计算生成第一身份鉴权码MIC_{REQ}，利用其与AAC之间的消息完整性校验密钥对包括第二验证消息中除第一消息完整性校验码外的其他字段计算生成第一消息完整性校验码$MacTag_{REQ}$。

[0079] 可选的，REQ可以生成第二密钥交换参数$KeyInfo_{REQ}$，例如REQ接收到AACAuth后，即可利用身份鉴别密钥IAK，采用对称加密算法对包括REQ产生的临时公钥在内的信息进行加密计算生成$KeyInfo_{REQ}$。简单的，REQ计算IAK的杂凑值即HASH(IAK)，对HASH(IAK)和包括REQ产生的临时公钥在内的信息进行异或运算生成$KeyInfo_{REQ}$；或者，REQ先计算扩展身份鉴别密钥EIAK，再对EIAK和包括REQ产生的临时公钥在内的信息进行异或运算生成$KeyInfo_{REQ}$，其中，EIAK是REQ根据包括所述IAK及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算生成的。其中，REQ利用的IAK是REQ采用与AS-REQ约定的密钥导出算法对包括自身与AS-REQ的预共享加密密钥K_{REQ_AS}在内的计算数据计算得到的。

[0080] 可选的，当AACAuth中包括$Nonce_{REQ}$和$Nonce_{AAC}$时，REQ计算IAK时的计算数据还可以包括$Nonce_{REQ}$和$Nonce_{AAC}$。

[0081] 其中，REQ和AAC之间的消息完整性校验密钥可以是REQ和AAC之间预先共享的，也可以是REQ和AAC协商生成的。REQ和AAC协商生成消息完整性校验密钥的方式包括：REQ可以根据包括$KeyInfo_{REQ}$对应的临时私钥和由$KeyInfo_{AAC}$恢复的临时公钥进行密钥交换计算得到第一密钥K1，将K1结合$Nonce_{AAC}$、$Nonce_{REQ}$及其他信息(REQ和AAC采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算消息完整性校验密钥。其中，密钥交换是指如迪菲·赫尔曼(Diffie-Hellman，简称DH)等密钥交换算法。$KeyInfo_{REQ}$对应的所述临时私钥是REQ产生的临时公私钥对中的临时私钥。

[0082] 可选的，当AACAuth中包括$Nonce_{REQ}$时，REQ可以验证AACAuth中的$Nonce_{REQ}$与REQ生成的$Nonce_{REQ}$的一致性，若一致，则继续执行后续操作，若不一致，则丢弃AACAuth。

[0083] 可选的，当AACAuth中包括$ID_{REQ} \oplus Nonce_{REQID}$时，计算$MIC_{REQ}$所采用的计算数据还可以包括$ID_{REQ} \oplus Nonce_{REQID}$，即REQ可以采用自身与AS-REQ约定的消息完整性校验算法，利用IK_{REQ_AS}对包括$ID_{REQ} \oplus Nonce_{REQID}$、存证随机数在内的计算数据计算生成$MIC_{REQ}$。

[0084] 可选的，当AACAuth中包括$ID_{REQ} \oplus Nonce_{REQID}$时，REQ可以根据$Nonce_{REQID}$和自身的身份标识$ID_{REQ}$对AACAuth中的$ID_{REQ} \oplus Nonce_{REQID}$进行验证；一种方式为，REQ可以利用$Nonce_{REQID}$与$ID_{REQ} \oplus Nonce_{REQID}$进行异或运算恢复$ID_{REQ}$，再对比恢复出的$ID_{REQ}$与REQ自身的$ID_{REQ}$是否一致，另一种方式为，REQ将$Nonce_{REQID}$和自身的$ID_{REQ}$进行异或运算，对比异或运算的结果与AACAuth中的$ID_{REQ} \oplus Nonce_{REQID}$是否一致；若一致，则继续执行后续操作，若不一致，则丢弃AACAuth。

[0085] S106、REQ向AAC发送第二验证消息REQAuth。

[0086] 该REQAuth中包括MIC_{REQ}和$MacTag_{REQ}$。

[0087] 可选的，REQAuth中还可以包括$KeyInfo_{REQ}$。可选的，当AACAuth中包括$Nonce_{AAC}$时，REQ可以将$Nonce_{AAC}$添加至REQAuth中。

[0088] S107、AAC对$MacTag_{REQ}$进行验证，验证通过后，生成鉴别完成消息AACFinish和第一存证消息AACUpdate。

[0089] $MacTag_{REQ}$的验证过程包括：若$MacTag_{REQ}$为REQ利用其与AAC之间的消息完整性校验密钥对包括REQAuth中除$MacTag_{REQ}$外的其他字段计算生成的，则AAC验证$MacTag_{REQ}$时，应利用其与REQ之间的消息完整性校验密钥对包括REQAuth中除$MacTag_{REQ}$外的其他字段计算生

成$MacTag_{REQ}$，将计算得到的$MacTag_{REQ}$与REQAuth中的$MacTag_{REQ}$进行比较，若一致，则验证通过，确定REQ的身份合法，若不一致，则根据本地策略执行如下操作，包括丢弃REQAuth或确定REQ的身份不合法。

[0090] 其中，AAC和REQ之间的消息完整性校验密钥可以是AAC和REQ之间预先共享的，也可以是AAC和REQ协商生成的。AAC和REQ协商生成消息完整性校验密钥的方式包括：AAC可以根据包括$KeyInfo_{AAC}$对应的临时私钥和由$KeyInfo_{REQ}$恢复的临时公钥进行密钥交换计算得到第一密钥K1，将K1结合$Nonce_{AAC}$、$Nonce_{REQ}$及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算消息完整性校验密钥。$KeyInfo_{AAC}$对应的所述临时私钥是AAC产生的临时公私钥对中的临时私钥，由$KeyInfo_{REQ}$恢复的所述临时公钥是REQ产生的临时公私钥对中的临时公钥。

[0091] 可选的，当REQAuth中包括$Nonce_{AAC}$时，AAC在验证$MacTag_{REQ}$之前，还可以先验证REQAuth中的$Nonce_{AAC}$与自身生成的$Nonce_{AAC}$是否一致，若一致，则继续执行后续操作，若不一致，则丢弃REQAuth。

[0092] 可选的，AAC还可以为REQ分配临时身份标识TID_{REQnew}，用于将TID_{REQnew}添加至AACFinish和AACUpdate中。

[0093] 此外，为了实现REQ对于AAC的身份鉴别，AAC还要生成第二消息完整性校验码$MacTag_{AAC}$，并将该$MacTag_{AAC}$添加至AACFinish中。$MacTag_{AAC}$可以为AAC利用其与REQ之间的消息完整性校验密钥对包括鉴别完成消息AACFinish中除$MacTag_{AAC}$外的其他字段计算生成的。

[0094] 可选的，AAC验证REQ的身份合法后，还可以计算用于保证REQ和AAC后续保密通信的会话密钥。具体的，AAC可以根据包括$KeyInfo_{AAC}$对应的临时私钥和由$KeyInfo_{REQ}$恢复的临时公钥进行密钥交换计算得到第一密钥K1，将K1结合$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算会话密钥(包括数据加密密钥和/或数据完整性校验密钥)。

[0095] 其中，AAC通过上述方式在计算会话密钥时，可以利用密钥导出算法计算出一串密钥数据，该密钥数据可以作为数据加密密钥和/或数据完整性校验密钥，或者，将该密钥数据中的一部分密钥数据作为数据加密密钥，将另一部分密钥数据作为数据完整性校验密钥。

[0096] S108、AAC向REQ发送鉴别完成消息AACFinish。

[0097] 该AACFinish中包括$MacTag_{AAC}$。若AAC为REQ分配了临时身份标识TID_{REQnew}，则AACFinish中还包括TID_{REQnew}。

[0098] S109、REQ对AACFinish中的$MacTag_{AAC}$进行验证，验证通过后，确定AAC的身份为合法。

[0099] $MacTag_{AAC}$的验证过程包括：若$MacTag_{AAC}$为AAC利用其与REQ之间的消息完整性校验密钥对包括AACFinish中除$MacTag_{AAC}$外的其他字段计算生成的，则REQ验证$MacTag_{AAC}$时，应利用其与AAC之间的消息完整性校验密钥对包括AACFinish中除$MacTag_{AAC}$外的其他字段计算生成$MacTag_{AAC}$，将计算得到的$MacTag_{AAC}$与AACFinish中的$MacTag_{AAC}$进行比较，若一致，则验证通过，确定AAC的身份合法，若不一致，则根据本地策略执行如下操作，包括丢弃AACFinish或确定AAC的身份不合法。

[0100] 可选的，REQ确定AAC的身份合法后，还可以保存TID_{REQnew}，以便在后续身份鉴别过程中，使用该TID_{REQnew}替代自身真实的身份标识。

[0101] 可选的，REQ验证AAC的身份合法后，还可以计算用于保证REQ和AAC后续保密通信的会话密钥。具体的，REQ可以根据包括$KeyInfo_{REQ}$对应的临时私钥和由$KeyInfo_{AAC}$恢复的临时公钥进行密钥交换计算得到第一密钥K1，将K1结合$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$及其他信息(REQ和AAC采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算会话密钥(包括数据加密密钥和/或数据完整性校验密钥)。由$KeyInfo_{AAC}$恢复的临时公钥是AAC产生的临时公私钥对中的临时公钥。

[0102] 其中，REQ通过上述方式在计算会话密钥时，可以利用密钥导出算法计算出一串密钥数据，该密钥数据可以作为数据加密密钥和/或数据完整性校验密钥，或者，将该密钥数据中的一部分密钥数据作为数据加密密钥，将另一部分密钥数据作为数据完整性校验密钥。

[0103] S110、AAC向AS-REQ发送第一存证消息AACUpdate。

[0104] 该AACUpdate中包括REQAuth中携带的MIC_{REQ}。

[0105] 在非漫游情况下，AAC直接将AACUpdate发送至AS-AAC(当然也可以表示为AS-REQ)即可。

[0106] 在漫游情况下，AAC生成AACUpdate后，先向AS-AAC发送AACUpdate；进而AS-AAC根据AACUpdate生成第二存证消息ASUpdate，ASUpdate中包括MIC_{REQ}，并将ASUpdate发送至AS-REQ。

[0107] 该AACUpdate中还可以包括AAC为REQ分配的临时身份标识TID_{REQnew}。

[0108] 可选的，AACUpdate中还可以包括第二身份鉴权码MIC_{AAC}。MIC_{AAC}是AAC利用与AS-AAC的预共享校验密钥IK_{AAC_AS}，采用预共享的消息完整性校验算法对AACUpdate中MIC_{AAC}之前的其他字段计算生成的。

[0109] S111、AS-REQ对MIC_{REQ}进行验证，验证通过后，生成并存储REQ的请求通过记录。

[0110] AS-REQ在生成和存储REQ的请求通过记录时还可以保存TID_{REQnew}。

[0111] 若AACUpdate中还包括MIC_{AAC}，则在非漫游情况下，AS-AAC(当然也可以表示为AS-REQ)对MIC_{REQ}和MIC_{AAC}进行验证，即AS-AAC(当然也可以表示为AS-REQ)利用其与AAC的预共享校验密钥IK_{AAC_AS}在本地计算MIC_{AAC}，以及利用其与REQ的预共享存证校验密钥IK_{REQ_AS}在本地计算MIC_{REQ}，再将计算得到的MIC_{AAC}与AACUpdate中的MIC_{AAC}进行比较，以及将计算得到的MIC_{REQ}与AACUpdate中的MIC_{REQ}进行比较，若均一致，则验证通过。

[0112] 若AACUpdate中还包括MIC_{AAC}，则在漫游情况下，先由AS-AAC对MIC_{AAC}进行验证，即AS-AAC先利用其与AAC的预共享校验密钥IK_{AAC_AS}在本地计算MIC_{AAC}，将计算得到的MIC_{AAC}与AACUpdate中的MIC_{AAC}进行比较，若一致，则验证通过，验证通过后，AS-AAC再生成ASUpdate，并向AS-REQ发送ASUpdate。进而，由AS-REQ对ASUpdate中的MIC_{REQ}进行验证，即由AS-REQ利用其与REQ的预共享存证校验密钥IK_{REQ_AS}在本地计算MIC_{REQ}，将计算得到的MIC_{REQ}与ASUpdate中的MIC_{REQ}进行比较，若一致，则验证通过，可以生成并保存REQ的请求通过记录。

[0113] 需要说明的是，在实际应用中，可以先执行S108后执行S110，也可以先执行S110后执行S108，还可以同时执行S108和S110。

[0114] 可选的，AAC可以先执行S110即发送所述第一存证消息，S111中对所述第一存证消

息中的第一身份鉴权码MIC_{REQ}验证通过后，生成第一存证确认消息，用于防止REQ有意发送错误的第一身份鉴权码MIC_{REQ}来逃避计费。AAC接收所述第一存证确认消息后再执行S108即向REQ发送所述鉴别完成消息。

[0115] 由上述技术方案可以看出，请求设备和鉴别接入控制器采用对称密钥的实体鉴别协议进行双向身份鉴别时，以密文的形式传输请求设备的身份信息，由此保证身份鉴别过程中请求设备的真实身份信息的安全性。另外，鉴别接入控制器在验证请求设备的身份合法后，会相应地向请求设备信任的第一鉴别服务器发送第一存证消息，以利用该第一鉴别服务器记录请求设备请求访问网络的行为，为后续网络接入点计费提供客观证据，有效地防止网络接入点对没有在其服务区内尝试访问网络的用户恶意计费。

[0116] 基于前述实施例，下面针对非漫游和漫游两种情况介绍本申请实施例提供的身份鉴别方法。

[0117] 参见图2，为非漫游情况下身份鉴别方法的一个实施例，此时可以用AS-AAC(当然也可以表示为AS-REQ)表示AAC和REQ共同信任的鉴别服务器，该身份鉴别方法包括：

[0118] S201、REQ生成$Nonce_{REQ}$、$Nonce_{REQID}$和$EncPub_{AS}$，根据需要生成$Security\ capabilities_{REQ}$。

[0119] S202、REQ向AAC发送鉴别请求消息ATTACH。

[0120] 该ATTACH中包括$Security\ capabilities_{REQ}$、$EncPub_{AS}$、$Route_{AS}$及$Nonce_{REQ}$。其中，$EncPub_{AS}$为REQ利用加密证书的公钥对包括$ID_{REQ}$、$Nonce_{REQID}$在内的加密数据计算得到的REQ的身份信息密文；$Route_{AS}$表示REQ信任的鉴别服务器的标识；$Security\ capabilities_{REQ}$为可选字段，表示REQ支持的安全能力参数信息，包括REQ支持的身份鉴别套件、完整性校验算法、杂凑(HASH)算法、密钥交换算法和/或密钥导出算法等(下文同)。

[0121] S203、AAC生成$Nonce_{AAC}$。

[0122] AAC根据$Route_{AS}$判断REQ信任的鉴别服务器与自身信任的鉴别服务器是否相同，若相同，确定为非漫游情况，此实施例中REQ与AAC存在共同信任的鉴别服务器。

[0123] S204、AAC向AS-AAC发送第一鉴权请求消息AACVeri。

[0124] 该AACVeri中包括$EncPub_{AS}$、$Nonce_{REQ}$、ID_{AAC}及$Nonce_{AAC}$。其中，$EncPub_{AS}$和$Nonce_{REQ}$应分别等于ATTACH中的相应字段；ID_{AAC}为可选字段。

[0125] S205、AS-AAC接收AACVeri后，执行下述操作(若无特别说明或逻辑上的关系，下述以(1)、(2)……编号的动作并不因为有编号而存在必然的先后顺序。全文同)，包括：

[0126] (1)、利用加密证书的私钥解密$EncPub_{AS}$得到ID_{REQ}和$Nonce_{REQID}$，根据ID_{REQ}判断REQ的身份是否合法，若合法，则继续执行后续操作，若不合法，则丢弃AACVeri；

[0127] (2)、计算生成IAK；

[0128] AS-AAC利用其与REQ之间的预共享加密密钥K_{REQ_AS}结合包括ID_{REQ}、$Nonce_{REQ}$、ID_{AAC}、$Nonce_{AAC}$在内的计算数据，采用与REQ预先约定的密钥导出算法计算得到IAK。

[0129] (3)、产生存证随机数$Nonce_{AS_AAC}$；

[0130] (4)、对ID_{REQ}和$Nonce_{REQID}$进行异或运算生成$ID_{REQ} \oplus Nonce_{REQID}$；

[0131] (5)、可选的，AS-AAC利用其与AAC之间的预共享加密密钥EK_{AAC_AS}对包括IAK在内的信息加密生成$EncData_{AS_AAC}$。

[0132] S206、AS-AAC向AAC发送第一鉴权响应消息ASVeri。

[0133] 该ASVeri中包括$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$、$Nonce_{AS_AAC}$及IAK。其中，$ID_{AAC}$为可选字段，当且仅当AACVeri中$ID_{AAC}$存在而存在；$ID_{AAC}$、$Nonce_{AAC}$应分别等于AACVeri中的相应字段；若存在$EncData_{AS_AAC}$时，AS-AAC利用$EncData_{AS_AAC}$替换ASVeri中的IAK。

[0134] S207、AAC接收ASVeri后，执行下述操作，包括：

[0135] (1)、检查ASVeri中的$Nonce_{AAC}$与AAC生成的$Nonce_{AAC}$是否一致，若ASVeri中存在ID_{AAC}，则检查ASVeri中的ID_{AAC}与AAC自身的身份标识ID_{AAC}是否一致；若任一项不一致，则丢弃ASVeri；

[0136] (2)、获得IAK；

[0137] 在ASVeri中包括$EncData_{AS_AAC}$的情况下，则利用其与AS-AAC之间的预共享加密密钥EK_{AAC_AS}解密$EncData_{AS_AAC}$得到IAK；

[0138] (3)、根据包括IAK及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算生成EIAK；

[0139] (4)、计算生成$KeyInfo_{AAC}$；

[0140] 其中，AAC将EIAK和包括AAC产生的临时公钥在内的信息进行异或运算生成$KeyInfo_{AAC}$。

[0141] S208、AAC向REQ发送第一验证消息AACAuth。

[0142] 该AACAuth中包括Security capabilities$_{AAC}$、$KeyInfo_{AAC}$、$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$及$Nonce_{AS_AAC}$。其中，$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$Nonce_{AAC}$、$Nonce_{AS_AAC}$应分别等于ASVeri中的相应字段。Security capabilities$_{AAC}$为可选字段，表示AAC根据Security capabilities$_{REQ}$做出的特定安全策略的选择，即AAC确定使用的身份鉴别方法、完整性校验算法、杂凑(HASH)算法、密钥交换算法和/或密钥导出算法等(下文同)，当且仅当ATTACH中存在Security capabilities$_{REQ}$时才存在Security capabilities$_{AAC}$。

[0143] S209、REQ接收AACAuth后，执行下述操作，包括：

[0144] (1)、利用$Nonce_{REQID}$与$ID_{REQ} \oplus Nonce_{REQID}$进行异或运算恢复出$ID_{REQ}$；

[0145] (2)、检查恢复出的ID_{REQ}与REQ自身的身份标识ID_{REQ}是否一致，检查AACAuth中的$Nonce_{REQ}$与REQ生成的$Nonce_{REQ}$是否一致；若任一项不一致，则丢弃AACAuth；

[0146] (3)、计算IAK；

[0147] REQ利用与AS-AAC之间的预共享加密密钥K_{REQ_AS}结合包括ID_{REQ}、$Nonce_{REQ}$、ID_{AAC}、$Nonce_{AAC}$在内的计算数据，采用预先与AS-AAC约定的密钥导出算法计算IAK。REQ计算IAK所采用的计算数据与S205中AS-AAC计算IAK所采用的计算数据相同。

[0148] (4)、根据包括IAK及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算生成EIAK；

[0149] (5)、计算生成$KeyInfo_{REQ}$；

[0150] REQ将EIAK和包括REQ产生的临时公钥在内的信息进行异或运算生成$KeyInfo_{REQ}$。

[0151] (6)、计算消息完整性校验密钥；

[0152] REQ根据包括$KeyInfo_{REQ}$对应的临时私钥和由$KeyInfo_{AAC}$恢复出的临时公钥进行密钥交换计算得到第一密钥K1，将K1结合$Nonce_{REQ}$、$Nonce_{AAC}$及其他信息(REQ和AAC采用的其他

信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算消息完整性校验密钥。

[0153] (7)、计算MIC_{REQ}；

[0154] (8)、计算$MacTag_{REQ}$。

[0155] S210、REQ向AAC发送第二验证消息REQAuth。

[0156] 该REQAuth中包括$Nonce_{AAC}$、$KeyInfo_{REQ}$、MIC_{REQ}及$MacTag_{REQ}$。其中，$Nonce_{AAC}$应等于AACAuth中的$Nonce_{AAC}$；MIC_{REQ}是REQ利用自身与AS-AAC之间的预共享存证校验密钥IK_{REQ_AS}，采用与AS-AAC之间预共享的消息完整性校验算法对包括$Nonce_{AS_AAC}$在内的计算数据计算得到的。$MacTag_{REQ}$是REQ利用消息完整性校验密钥对包括REQAuth中除$MacTag_{REQ}$外的其他字段在内的信息计算得到的。

[0157] S211、AAC接收REQAuth后，执行下述操作，包括：

[0158] (1)、检查REQAuth中的$Nonce_{AAC}$与AAC生成的$Nonce_{AAC}$是否一致，若不一致，则丢弃REQAuth；

[0159] (2)、计算消息完整性校验密钥；

[0160] AAC根据包括$KeyInfo_{AAC}$对应的临时私钥和由$KeyInfo_{REQ}$恢复出的临时公钥进行密钥交换计算得到第一密钥K1，将K1结合$Nonce_{REQ}$、$Nonce_{AAC}$及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算消息完整性校验密钥。

[0161] (3)、验证$MacTag_{REQ}$；

[0162] AAC利用消息完整性校验密钥对包括REQAuth中除$MacTag_{REQ}$外的其他字段在内的信息在本地计算得到$MacTag_{REQ}$(该计算方式与REQ计算$MacTag_{REQ}$的方式相同)，对比计算出的$MacTag_{REQ}$与REQAuth中的$MacTag_{REQ}$是否一致，若一致，则确定REQ的身份合法，若不一致，则丢弃REQAuth。

[0163] (4)、为REQ分配生成的临时身份标识TID_{REQnew}；

[0164] (5)、可选的，计算MIC_{AAC}。

[0165] S212、AAC向AS-AAC发送第一存证消息AACUpdate。

[0166] 该AACUpdate中包括$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$、$Nonce_{AAC}$、$TID_{REQnew}$、$MIC_{REQ}$及$MIC_{AAC}$。其中，$ID_{AAC}$、$MIC_{AAC}$为可选字段；$MIC_{AAC}$是AAC利用自身与AS-AAC之间的预共享校验密钥IK_{AAC_AS}，采用与AS-AAC之间预共享的消息完整性校验算法对AACUpdate中MIC_{AAC}之前的其他字段计算得到的。例如，当AACUpdate中依次包括$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$、$Nonce_{AAC}$、$TID_{REQnew}$、$MIC_{REQ}$及$MIC_{AAC}$时，$MIC_{AAC}$是AAC利用所述$IK_{AAC_AS}$，采用所述消息完整性校验算法对AACUpdate中的字段$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$、$Nonce_{AAC}$、$TID_{REQnew}$及$MIC_{REQ}$计算得到的。

[0167] S213、AS-AAC接收AACUpdate后，执行下述操作，包括：

[0168] (1)、若AACUpdate中存在MIC_{AAC}，则验证MIC_{AAC}；

[0169] AS-AAC利用与AAC之间的预共享校验密钥IK_{AAC_AS}，采用与AAC之间预共享的消息完整性校验算法对AACUpdate中MIC_{AAC}之前的其他字段计算得到MIC_{AAC}，对比计算出的MIC_{AAC}与AACUpdate中的MIC_{AAC}是否一致，若不一致，则丢弃AACUpdate。

[0170] (2)、验证MIC_{REQ}；

[0171] AS-AAC利用与REQ之间的预共享存证校验密钥IK_{REQ_AS}，采用预共享的消息完整性校验算法对包括$Nonce_{AS_AAC}$在内的计算数据计算得到MIC_{REQ}，对比计算出的MIC_{REQ}与AACUpdate中的MIC_{REQ}是否一致，若不一致，则丢弃AACUpdate。

[0172] (3)、生成并保存REQ的请求通过记录，保存TID_{REQnew}；

[0173] (4)、可选的，计算MIC_{AS_AAC}。

[0174] S214、AS-AAC向AAC发送第一存证确认消息ASAck。

[0175] 该ASAck中包括ID_{AAC}、$Nonce_{AAC}$及MIC_{AS_AAC}。其中，ID_{AAC}、MIC_{AS_AAC}为可选字段；MIC_{AS_AAC}是AS-AAC利用自身与AAC之间的预共享校验密钥IK_{AAC_AS}，采用与AAC之间预共享的消息完整性校验算法对ASAck中MIC_{AS_AAC}之前的其他字段计算得到的。

[0176] S215、AAC接收到ASAck后，执行下述操作，包括：

[0177] (1)、若ASAck中存在ID_{AAC}，则检查ID_{AAC}是否与AAC自身的身份标识ID_{AAC}相同；

[0178] (2)、检查$Nonce_{AAC}$是否与AAC生成的$Nonce_{AAC}$相同；

[0179] (3)、若ASAck中存在MIC_{AS_AAC}，则验证MIC_{AS_AAC}；

[0180] AAC利用与AS-AAC之间的预共享校验密钥IK_{AAC_AS}，采用与AS-AAC之间预共享的消息完整性校验算法对ASAck中MIC_{AS_AAC}之前的其他字段计算得到MIC_{AS_AAC}，对比计算出的MIC_{AS_AAC}与ASAck中的MIC_{AS_AAC}是否一致。

[0181] (4)、上述检查与验证通过后，计算$MacTag_{AAC}$；上述检查与验证中任一步不通过，则立即丢弃ASAck；

[0182] (5)、计算会话密钥；

[0183] AAC将S211中计算的K1结合$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算出会话密钥，用于REQ和AAC后续的保密通信。

[0184] S216、AAC向REQ发送鉴别完成消息AACFinish。

[0185] 该AACFinish中包括TID_{REQnew}和$MacTag_{AAC}$。其中，$MacTag_{AAC}$是AAC利用消息完整性校验密钥对包括AACFinish中除$MacTag_{AAC}$外的其他字段在内的信息在本地计算得到的；TID_{REQnew}应与AACUpdate中的TID_{REQnew}相同。

[0186] S217、REQ接收到AACFinish后，执行下述操作，包括：

[0187] (1)、验证$MacTag_{AAC}$；

[0188] REQ利用消息完整性校验密钥对包括AACFinish中除$MacTag_{AAC}$外的其他字段在内的信息在本地计算得到$MacTag_{AAC}$(该计算方式与AAC计算$MacTag_{AAC}$的方式相同)，对比计算出的$MacTag_{AAC}$与AACFinish中的$MacTag_{AAC}$是否一致，若一致，则确定AAC身份合法，若不一致，则丢弃AACFinish。

[0189] (2)、保存TID_{REQnew}；

[0190] (3)、计算会话密钥；

[0191] REQ将在S209中计算得到的K1结合$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$及其他信息(REQ和AAC采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算出会话密钥，用于REQ和AAC后续的保密通信。

[0192] 由此在S211和S217分别实现对REQ和对AAC的身份鉴别，即实现REQ和AAC的双向身份鉴别。

[0193] 参见图3,为漫游情况下身份鉴别方法的实施例,该身份鉴别方法包括:

[0194] S301、REQ生成$Nonce_{REQ}$、$Nonce_{REQID}$和$EncPub_{AS}$,根据需要生成Security capabilities$_{REQ}$。

[0195] S302、REQ向AAC发送鉴别请求消息ATTACH。

[0196] 该ATTACH中包括Security capabilities$_{REQ}$、$EncPub_{AS}$、$Route_{AS}$及$Nonce_{REQ}$。其中,$EncPub_{AS}$为REQ利用加密证书的公钥对包括ID_{REQ}、$Nonce_{REQID}$在内的加密数据计算得到的REQ的身份信息密文。$Route_{AS}$表示REQ信任的鉴别服务器的标识;Security capabilities$_{REQ}$为可选字段。

[0197] S303、AAC生成$Nonce_{AAC}$。

[0198] AAC根据$Route_{AS}$判断REQ信任的鉴别服务器与自身信任的鉴别服务器是否相同,若不相同,确定为漫游情况,此实施例中REQ信任的AS-REQ与AAC信任的AS-AAC为两个独立的鉴别服务器。

[0199] S304、AAC向AS-AAC发送第一鉴权请求消息AACVeri。

[0200] 该AACVeri中包括$EncPub_{AS}$、$Nonce_{REQ}$、ID_{AAC}、$Nonce_{AAC}$及$Route_{AS}$。其中,$EncPub_{AS}$、$Nonce_{REQ}$和$Route_{AS}$应分别等于ATTACH中的相应字段;ID_{AAC}为可选字段。

[0201] S305、AS-AAC接收到AACVeri后,根据$Rout_{AS}$确定AS-REQ,向AS-REQ发送第二鉴权请求消息AS-AACVeri。

[0202] 其中,AS-AACVeri是根据AACVeri生成的,AS-AACVeri中包括$EncPub_{AS}$、$Nonce_{REQ}$、ID_{AAC}及$Nonce_{AAC}$。$EncPub_{AS}$、$Nonce_{REQ}$、ID_{AAC}和$Nonce_{AAC}$应分别等于AACVeri中的相应字段。

[0203] S306、AS-REQ接收AS-AACVeri后,执行下述操作,包括:

[0204] (1)、利用加密证书的私钥解密$EncPub_{AS}$得到ID_{REQ}和$Nonce_{REQID}$,根据ID_{REQ}判断REQ的身份是否合法,若合法,则继续执行后续操作,若不合法,丢弃AAC-ASVeri;

[0205] (2)、产生存证随机数$Nonce_{AS_REQ}$。

[0206] (3)、对ID_{REQ}和$Nonce_{REQID}$进行异或运算得到$ID_{REQ} \oplus Nonce_{REQID}$;

[0207] (4)、计算IAK;

[0208] AS-REQ利用其与REQ之间的预共享加密密钥K_{REQ_AS}结合包括ID_{REQ}、$Nonce_{REQ}$、ID_{AAC}、$Nonce_{AAC}$在内的计算数据,采用与REQ预先约定的密钥导出算法计算得到IAK。

[0209] (5)、可选的,AS-REQ利用其与AS-AAC之间的预共享加密密钥EK_{AS}对包括IAK在内的信息加密生成$EncData_{AS_REQ}$。

[0210] S307、AS-REQ向AS-AAC发送第二鉴权响应消息AS-REQVeri。

[0211] 该AS-REQVeri中包括$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$、$Nonce_{AAC}$、$Nonce_{AS_REQ}$及IAK。其中,$ID_{AAC}$、$Nonce_{AAC}$应分别等于AS-AACVeri中的相应字段;若存在$EncData_{AS_REQ}$时,AS-REQ利用$EncData_{AS_REQ}$替代AS-REQVeri中的IAK。

[0212] S308、AS-AAC接收AS-REQVeri后,执行下述操作,包括:

[0213] (1)、获得IAK;当AS-REQVeri中存在$EncData_{AS_REQ}$时,利用其与AS-REQ之间的预共享加密密钥EK_{AS}对$EncData_{AS_REQ}$解密得到IAK;

[0214] (2)、可选的,AS-AAC利用其与AAC之间的预共享加密密钥EK_{AAC_AS}对包括IAK在内的信息加密生成$EncData_{AS_AAC}$。

[0215] S309、AS-AAC向AAC发送第一鉴权响应消息ASVeri。

[0216] 该ASVeri中包括$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$、$Nonce_{AS_REQ}$及IAK。其中，$ID_{AAC}$为可选字段，且$Nonce_{REQ}$、$ID_{AAC}$和$Nonce_{AAC}$应分别等于AACVeri中的相应字段；若存在$EncData_{AS_AAC}$时，AS-AAC将利用$EncData_{AS_AAC}$替换ASVeri中的IAK。

[0217] S310、AAC接收ASVeri后，执行下述操作，包括：

[0218] (1)、检查ASVeri中的$Nonce_{AAC}$与AAC生成的$Nonce_{AAC}$是否一致，若ASVeri中存在ID_{AAC}，则检查ASVeri中的ID_{AAC}与AAC自身的身份标识ID_{AAC}是否一致；若任一项不一致，则丢弃ASVeri；

[0219] (2)、获得IAK；

[0220] 在ASVeri中包括$EncData_{AS_AAC}$的情况下，则利用其与AS-AAC之间的预共享加密密钥EK_{AAC_AS}解密$EncData_{AS_AAC}$得到IAK；

[0221] (3)、根据包括IAK及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算生成EIAK；

[0222] (4)、计算$KeyInfo_{AAC}$；

[0223] 其中，AAC将EIAK和包括AAC产生的临时公钥在内的信息进行异或运算生成$KeyInfo_{AAC}$。

[0224] S311、AAC向REQ发送第一验证消息AACAuth。

[0225] 该AACAuth中包括Security capabilities$_{AAC}$、$KeyInfo_{AAC}$、$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$及$Nonce_{AS_REQ}$。其中，$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$、$Nonce_{AS_REQ}$应分别等于ASVeri中的相应字段；Security capabilities$_{AAC}$为可选字段，当且仅当ATTACH中存在Security capabilities$_{REQ}$时才存在Security capabilities$_{AAC}$。

[0226] S312、REQ接收AACAuth后，执行下述操作，包括：

[0227] (1)、利用$Nonce_{REQID}$与$ID_{REQ} \oplus Nonce_{REQID}$进行异或运算恢复出$ID_{REQ}$；

[0228] (2)、检查恢复出的ID_{REQ}与REQ自身的身份标识ID_{REQ}是否一致，检查AACAuth中的$Nonce_{REQ}$与REQ生成的$Nonce_{REQ}$是否一致；若任一项不一致，则丢弃AACAuth；

[0229] (3)、计算IAK；

[0230] REQ利用与AS-REQ之间的预共享加密密钥K_{REQ_AS}结合包括ID_{REQ}、$Nonce_{REQ}$、ID_{AAC}、$Nonce_{AAC}$在内的计算数据，采用预先与AS-REQ约定的密钥导出算法计算IAK。REQ计算IAK所采用的计算数据与S306中AS-REQ计算IAK所采用的计算数据相同。

[0231] (4)、根据包括IAK及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算生成EIAK；

[0232] (5)、计算$KeyInfo_{REQ}$；其计算方式与图2实施例中的相关描述相同；

[0233] (6)、计算消息完整性校验密钥；

[0234] REQ根据包括$KeyInfo_{REQ}$对应的临时私钥和由$KeyInfo_{AAC}$恢复出的临时公钥进行密钥交换计算得到第一密钥K1，将K1结合$Nonce_{REQ}$、$Nonce_{AAC}$及其他信息(REQ和AAC采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算消息完整性校验密钥。

[0235] (7)、计算MIC_{REQ}；

[0236] (8)、计算$MacTag_{REQ}$。

[0237] S313、REQ向AAC发送第二验证消息REQAuth。

[0238] 该REQAuth中包括$Nonce_{AAC}$、$KeyInfo_{REQ}$、MIC_{REQ}及$MacTag_{REQ}$。其中，$Nonce_{AAC}$应等于AACAuth中的$Nonce_{AAC}$；MIC_{REQ}是REQ利用自身与AS-REQ之间的预共享存证校验密钥IK_{REQ_AS}，采用与AS-REQ之间预共享的消息完整性校验算法对包括$Nonce_{AS_REQ}$在内的计算数据计算得到的。$MacTag_{REQ}$是REQ利用消息完整性校验密钥对包括REQAuth中除$MacTag_{REQ}$外的其他字段在内的信息在本地计算得到的。

[0239] S314、AAC接收REQAuth后，执行下述操作，包括：

[0240] (1)、检查REQAuth中的$Nonce_{AAC}$与AAC生成的$Nonce_{AAC}$是否一致，若不一致，则丢弃REQAuth；

[0241] (2)、计算消息完整性校验密钥；

[0242] AAC根据包括$KeyInfo_{AAC}$对应的临时私钥和由$KeyInfo_{REQ}$恢复出的临时公钥进行密钥交换计算得到第一密钥K1，将K1结合$Nonce_{REQ}$、$Nonce_{AAC}$及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算消息完整性校验密钥。

[0243] (3)、验证$MacTag_{REQ}$；

[0244] AAC利用消息完整性校验密钥对包括REQAuth中除$MacTag_{REQ}$外的其他字段在内的信息在本地计算得到$MacTag_{REQ}$，对比计算出的$MacTag_{REQ}$与REQAuth中的$MacTag_{REQ}$是否一致，若一致，则确定REQ的身份合法，若不一致，则丢弃REQAuth。

[0245] (4)、为REQ分配生成的临时身份标识TID_{REQnew}；

[0246] (5)、可选的，AAC计算生成MIC_{AAC}。

[0247] S315、AAC向AS-AAC发送第一存证消息AACUpdate。

[0248] 该AACUpdate中包括$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$、$Nonce_{AAC}$、$TID_{REQnew}$、$MIC_{REQ}$及$MIC_{AAC}$。其中，$ID_{AAC}$为可选字段；$ID_{REQ} \oplus Nonce_{REQID}$应等于ASVeri中的相应字段；$MIC_{REQ}$应等于REQAuth中的相应字段；$MIC_{AAC}$为可选字段，$MIC_{AAC}$是AAC利用自身与AS-AAC之间的预共享校验密钥IK_{AAC_AS}，采用与AS-AAC之间预共享的消息完整性校验算法对AACUpdate中MIC_{AAC}之前的其他字段计算得到的。

[0249] S316、AS-AAC接收AACUpdate后，执行下述操作，包括：

[0250] (1)、当AACUpdate中存在MIC_{AAC}时，验证MIC_{AAC}；

[0251] AS-AAC利用与AAC之间的预共享校验密钥IK_{AAC_AS}，采用与AAC之间预共享的消息完整性校验算法对AACUpdate中MIC_{AAC}之前的其他字段计算得到MIC_{AAC}，将计算出的MIC_{AAC}与AACUpdate中的MIC_{AAC}进行对比，若不一致，则丢弃AACUpdate。

[0252] (2)、可选的，AS-AAC计算生成MIC_{AS_AAC}。

[0253] S317、AS-AAC向AS-REQ发送第二存证消息ASUpdate。

[0254] 该ASUpdate中包括$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$、$TID_{REQnew}$、$MIC_{REQ}$及$MIC_{AS_AAC}$。其中，$ID_{REQ} \oplus Nonce_{REQID}$、$ID_{AAC}$、$TID_{REQnew}$、$MIC_{REQ}$应分别等于AACUpdate中的相应字段；$MIC_{AS_AAC}$为可选字段，$MIC_{AS_AAC}$是AS-AAC利用自身与AS-REQ之间的预共享校验密钥IK_{AS}对ASUpdate中MIC_{AS_AAC}之前的其他字段在本地计算得到的。

[0255] S318、AS-REQ接收ASUpdate之后，执行下述操作，包括：

[0256] (1)、当ASUpdate中存在MIC_{AS}时，验证MIC_{AS_AAC}；

[0257] AS-REQ利用与AS-AAC之间的预共享校验密钥IK_{AS}对ASUpdate中MIC_{AS_AAC}之前的其他字段在本地计算得到MIC_{AS_AAC}，对比计算出的MIC_{AS_AAC}与ASUpdate中的MIC_{AS_AAC}是否一致，若不一致，则丢弃ASUpdate。

[0258] (2)、验证MIC_{REQ}；

[0259] AS-REQ利用与REQ之间的预共享存证校验密钥IK_{REQ_AS}，采用预共享的消息完整性校验算法对包括$Nonce_{AS_REQ}$在内的计算数据计算得到MIC_{REQ}，对比计算出的MIC_{REQ}与ASUpdate中的MIC_{REQ}是否一致，若不一致，则丢弃ASUpdate。

[0260] (3)、生成并保存REQ的请求通过记录，保存ASUpdate中的TID_{REQnew}；

[0261] (4)、可选的，计算MIC_{AS_REQ}。

[0262] S319、AS-REQ向AS-AAC发送第二存证确认消息AS-REQAck。

[0263] 该AS-REQAck中包括ID_{AAC}和MIC_{AS_REQ}。其中，ID_{AAC}应等于ASUpdate中的相应字段；MIC_{AS_REQ}为可选字段，是AS-REQ利用其与AS-AAC之间的预共享校验密钥IK_{AS}，采用其与AS-AAC之间预共享的消息完整性校验算法对AS-REQAck中MIC_{AS_REQ}之前的其他字段计算得到的。

[0264] S320、AS-AAC收到AS-REQAck后，执行下述操作，包括：

[0265] (1)、若AS-REQAck中存在MIC_{AS_REQ}，则验证MIC_{AS_REQ}；

[0266] AS-AAC利用与AS-REQ之间的预共享存证校验密钥IK_{AS}，采用与AS-REQ预共享的消息完整性校验算法对AS-REQAck中MIC_{AS_REQ}之前的其他字段计算得到MIC_{AS_REQ}，对比计算出的MIC_{AS_REQ}与AS-REQAck中的MIC_{AS_REQ}是否一致，若不一致，则丢弃AS-REQAck。

[0267] (2)、可选的，计算MIC_{AS}。

[0268] S321、AS-AAC向AAC发送第一存在确认消息AS-AACAck。

[0269] 该AS-AACAck中包括ID_{AAC}、$Nonce_{AAC}$及MIC_{AS}。其中，ID_{AAC}、MIC_{AS}为可选字段；MIC_{AS}是AS-AAC利用自身与AAC之间的预共享校验密钥IK_{AAC_AS}，采用与AAC之间预共享的消息完整性校验算法对AS-AACAck中MIC_{AS}之前的其他字段计算得到的。

[0270] S322、AAC收到AS-AACAck后，执行下述操作，包括：

[0271] (1)、若AS-AACAck中存在ID_{AAC}，则检查ID_{AAC}是否与AAC自身的身份标识ID_{AAC}相同；

[0272] (2)、检查$Nonce_{AAC}$是否与AAC生成的$Nonce_{AAC}$相同；

[0273] (3)、若AS-AACAck中存在MIC_{AS}，则验证MIC_{AS}；

[0274] AAC利用与AS-AAC之间的预共享校验密钥IK_{AAC_AS}，采用与AS-AAC之间预共享的消息完整性校验算法对AS-AACAck中MIC_{AS}之前的其他字段计算得到MIC_{AS}，对比计算出的MIC_{AS}与AS-AACAck中的MIC_{AS}是否一致。

[0275] (4)、上述检查与验证通过后，计算$MacTag_{AAC}$；上述检查与验证中任一步不通过，则立即丢弃AS-AACAck；

[0276] (5)、计算会话密钥；

[0277] AAC将S314中计算的K1结合$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$及其他信息(AAC和REQ采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算会话密钥，用于REQ和AAC后续的保密通信。

[0278] S323、AAC向REQ发送鉴别完成消息AACFinish。

[0279] 该AACFinish中包括TID_{REQnew}和$MacTag_{AAC}$。其中，TID_{REQnew}应与AACUpdate中的TID_{REQnew}相同；$MacTag_{AAC}$是AAC利用消息完整性校验密钥对包括AACFinish中除$MacTag_{AAC}$外的其他字段在内的信息在本地计算得到的。

[0280] S324、REQ接收AACFinish后，执行下述操作，包括：

[0281] (1)、验证$MacTag_{AAC}$；

[0282] REQ利用消息完整性校验密钥对包括AACFinish中除$MacTag_{AAC}$外的其他字段在内的信息在本地计算得到$MacTag_{AAC}$，对比计算出的$MacTag_{AAC}$与AACFinish中的$MacTag_{AAC}$是否一致，若一致，则确定AAC身份合法，若不一致，则丢弃AACFinish。

[0283] (2)、保存TID_{REQnew}；

[0284] (3)、计算会话密钥；

[0285] REQ将在S312中计算得到的K1结合$ID_{REQ} \oplus Nonce_{REQID}$、$Nonce_{REQ}$、$ID_{AAC}$、$Nonce_{AAC}$及其他信息(REQ和AAC采用的其他信息是相同的且可选的，譬如特定字符串等)，利用密钥导出算法计算出会话密钥，用于REQ和AAC后续的保密通信。

[0286] 由此在S314和S324分别实现对REQ和对AAC的身份鉴别，即实现REQ和AAC的双向身份鉴别。

[0287] 在上述各实施例中，每条消息还可以携带一个杂凑值$HASH_{X_Y}$，该杂凑值$HASH_{X_Y}$是该消息的发送方实体X利用杂凑算法对接收到的对端实体Y发送的最新前序消息计算得到的，用于对端实体Y来验证实体X是否接收到完整的最新前序消息。其中，$HASH_{REQ_AAC}$表示REQ对接收到的AAC发送的最新前序消息计算的杂凑值，$HASH_{AAC_REQ}$表示AAC对接收到的REQ发送的最新前序消息计算的杂凑值，$HASH_{AAC_AS\text{-}AAC}$表示AAC对接收到的AS-AAC发送的最新前序消息计算的杂凑值，$HASH_{AS\text{-}AAC_AAC}$表示AS-AAC对接收到的AAC发送的最新前序消息计算的杂凑值，$HASH_{AS\text{-}AAC_AS\text{-}REQ}$表示AS-AAC对接收到的AS-REQ发送的最新前序消息计算的杂凑值，$HASH_{AS\text{-}REQ_AS\text{-}AAC}$表示AS-REQ对接收到的AS-AAC发送的最新前序消息计算的杂凑值。若发送方实体X当前发送的消息为实体X和实体Y之间交互的首条消息，意味着实体X未曾收到对端实体Y发送的前序消息，则该条消息中$HASH_{X_Y}$可以不存在或者无意义。

[0288] 对应的，对端实体Y接收到实体X发送的消息后，若该条消息中包含$HASH_{X_Y}$，则当实体Y未曾向实体X发送过前序消息时，实体Y忽略$HASH_{X_Y}$；当实体Y曾向实体X发送过前序消息时，实体Y利用杂凑算法对之前向实体X发送的最新前序消息在本地计算杂凑值，并与接收到的消息中携带的杂凑值$HASH_{X_Y}$比较，若一致，则执行后续步骤，否则丢弃或者结束本次鉴别过程。

[0289] 本发明中，对实体X而言，对端实体Y向实体X发送的前序消息指的是：实体X向对端实体Y发送消息M之前，接收过的对端实体Y向实体X发送的消息；对端实体Y向实体X发送的最新前序消息指的是：实体X向对端实体Y发送消息M之前，接收的对端实体Y向实体X发送的最新一条消息。若实体X向其对端实体Y发送的消息M是实体X和实体Y之间交互的第一条消息，则实体X向其对端实体Y发送消息M之前，不存在对端实体Y向实体X发送的前序消息。

[0290] 上述图2和图3对应实施例中的可选字段和可选操作，在说明书附图的图2和图3中用“*”表示。以上所有实施例涉及的消息中包括的各个内容不限定顺序，且在没有特别说明的情况下，不限定消息接收方收到消息后对相关消息的操作顺序以及对消息中所包括的内容进行处理的顺序。

[0291] 基于图1至图3所对应的方法实施例，参见图4，本申请实施例提供了一种鉴别接入控制器，所述鉴别接入控制器包括：

[0292] 接收单元401，用于接收请求设备发送的鉴别请求消息，所述鉴别请求消息中包括所述请求设备的身份信息密文；所述请求设备的身份信息密文是所述请求设备利用加密证书的公钥对包括所述请求设备的身份标识在内的加密数据加密得到的；

[0293] 发送单元402，用于向所述鉴别接入控制器信任的第二鉴别服务器发送携带有所述请求设备的身份信息密文的第一鉴权请求消息；

[0294] 接收单元401还用于接收所述第二鉴别服务器发送的第一鉴权响应消息，并从所述第一鉴权响应消息中获得所述请求设备信任的第一鉴别服务器产生的存证随机数和所述第一鉴别服务器生成的身份鉴别密钥；所述身份鉴别密钥是根据包括所述第一鉴别服务器与所述请求设备的预共享加密密钥在内的计算数据计算得到的；

[0295] 发送单元402还用于向所述请求设备发送第一验证消息，所述第一验证消息中包括所述存证随机数；

[0296] 接收单元401还用于接收所述请求设备发送的第二验证消息，所述第二验证消息中包括第一身份鉴权码和第一消息完整性校验码；所述第一消息完整性校验码是所述请求设备利用其与所述鉴别接入控制器之间的消息完整性校验密钥对包括所述第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的；其中，所述消息完整性校验密钥是根据包括所述身份鉴别密钥在内的信息计算得到的；

[0297] 处理单元403，用于对所述第一消息完整性校验码进行验证，验证通过后，确定所述请求设备的身份为合法，生成鉴别完成消息和第一存证消息；

[0298] 发送单元402还用于向所述请求设备发送所述鉴别完成消息，以及向所述第二鉴别服务器发送所述第一存证消息。

[0299] 可选的，发送单元402先发送所述第一存证消息，当接收单元401接收到第一存证确认消息后，发送单元402再向所述请求设备发送所述鉴别完成消息。

[0300] 可选的，所述第一验证消息中还包括所述鉴别接入控制器根据所述身份鉴别密钥生成的第一密钥交换参数，所述第二验证消息中还包括所述请求设备根据所述身份鉴别密钥生成的第二密钥交换参数，则处理单元403还用于：根据包括所述第一密钥交换参数对应的临时私钥和所述第二密钥交换参数所包括的临时公钥进行密钥交换计算生成第一密钥，根据包括所述第一密钥在内的信息利用密钥导出算法计算出所述消息完整性校验密钥。

[0301] 可选的，处理单元403还用于：利用所述身份鉴别密钥，采用对称加密算法对包括所述鉴别接入控制器产生的临时公钥在内的信息进行加密生成所述第一密钥交换参数；接收单元401接收的第二验证消息中的第二密钥交换参数是所述请求设备利用所述身份鉴别密钥，采用对称加密算法对包括所述请求设备产生的临时公钥在内的信息进行加密生成的；

[0302] 则处理单元403计算所述消息完整性校验密钥具体为，根据包括所述第一密钥交换参数对应的临时私钥和由所述第二密钥交换参数恢复出的临时公钥进行密钥交换计算生成所述第一密钥，根据包括所述第一密钥在内的信息利用所述密钥导出算法计算出所述消息完整性校验密钥。

[0303] 可选的，处理单元403具体用于：计算所述身份鉴别密钥的杂凑值，对所述杂凑值

和包括所述鉴别接入控制器产生的临时公钥在内的信息进行异或运算生成所述第一密钥交换参数。

[0304] 可选的，接收单元401接收的鉴别请求消息中还包括所述请求设备生成的第一随机数；发送单元402发送的第一鉴权请求消息中还包括所述第一随机数和所述鉴别接入控制器生成的第二随机数；

[0305] 则接收单元401接收的第一鉴权响应消息中还包括所述第一随机数和所述第二随机数；发送单元402发送的第一验证消息中还包括所述第一随机数和所述第二随机数，所述身份鉴别密钥的计算数据还包括所述第一随机数和所述第二随机数，接收单元401接收的第二验证消息中还包括所述第二随机数；

[0306] 则处理单元403还用于：验证所述第一鉴权响应消息中的第二随机数和所述鉴别接入控制器生成的第二随机数的一致性；以及，对所述第二验证消息中的第二随机数和所述鉴别接入控制器生成的第二随机数的一致性进行验证。

[0307] 可选的，接收单元401接收的鉴别请求消息中还包括所述请求设备支持的安全能力参数信息，则处理单元403还用于：根据所述安全能力参数信息确定所述鉴别接入控制器使用的特定安全策略，则所述第一验证消息中还包括所述特定安全策略。

[0308] 可选的，接收单元401接收的鉴别请求消息中还包括所述请求设备信任的至少一个鉴别服务器的身份标识，则处理单元403还用于：根据所述鉴别请求消息中所述请求设备信任的至少一个鉴别服务器的身份标识和所述鉴别接入控制器信任的鉴别服务器的身份标识，确定所述第二鉴别服务器。

[0309] 可选的，处理单元403还用于：为所述请求设备分配临时身份标识；则发送单元402发送的鉴别完成消息和第一存证消息中还包括所述请求设备的临时身份标识。

[0310] 可选的，接收单元401具体通过以下方式获得所述身份鉴别密钥：

[0311] 利用与所述第二鉴别服务器的预共享加密密钥解密身份鉴别密钥密文得到所述身份鉴别密钥；所述身份鉴别密钥密文是所述第二鉴别服务器利用与所述鉴别接入控制器的预共享加密密钥对包括所述身份鉴别密钥在内的信息加密生成的。

[0312] 可选的，发送单元402发送的第一鉴权请求消息中还包括所述鉴别接入控制器的身份标识；接收单元401接收的第一鉴权响应消息中还包括所述鉴别接入控制器的身份标识；

[0313] 则处理单元403还用于：验证所述第一鉴权响应消息中的所述鉴别接入控制器的身份标识和所述鉴别接入控制器自身的身份标识的一致性。

[0314] 可选的，接收单元401接收的第一鉴权响应消息中还包括所述请求设备的身份标识密文，发送单元402发送的第一验证消息中还包括所述鉴别接入控制器的身份标识，则处理单元403还用于：当确定所述请求设备的身份为合法时，根据包括所述第一密钥、所述请求设备的身份标识密文和所述鉴别接入控制器的身份标识在内的信息计算生成用于后续保密通信的会话密钥。

[0315] 可选的，接收单元401接收的第二验证消息中的第一消息完整性校验码是所述请求设备利用所述消息完整性校验密钥对包括所述第二验证消息中除所述第一消息完整性校验码外的其他字段计算生成的。

[0316] 可选的，所述鉴别接入控制器向所述请求设备发送的消息还包括所述鉴别接入控

制器对接收到的所述请求设备发送的最新前序消息计算的杂凑值;所述鉴别接入控制器向所述第二鉴别服务器发送的消息还包括所述鉴别接入控制器对接收到的所述第二鉴别服务器发送的最新前序消息计算的杂凑值。

[0317] 参见图5,本申请实施例还提供了一种请求设备,所述请求设备包括:

[0318] 发送单元501,用于向鉴别接入控制器发送鉴别请求消息,所述鉴别请求消息中包括所述请求设备的身份信息密文;所述请求设备的身份信息密文是所述请求设备利用加密证书的公钥对包括所述请求设备的身份标识在内的加密数据加密得到的;

[0319] 接收单元502,用于接收所述鉴别接入控制器发送的第一验证消息,所述第一验证消息中包括存证随机数;

[0320] 处理单元503,用于利用所述请求设备与其信任的第一鉴别服务器的预共享存证校验密钥对包括所述存证随机数在内的信息计算生成第一身份鉴权码;利用所述请求设备与所述鉴别接入控制器之间的消息完整性校验密钥对包括第二验证消息中除第一消息完整性校验码外的其他字段计算生成第一消息完整性校验码;其中,所述消息完整性校验密钥是根据包括身份鉴别密钥在内的信息计算得到的,所述身份鉴别密钥是根据包括所述请求设备与所述第一鉴别服务器的预共享加密密钥在内的计算数据计算得到的;

[0321] 发送单元501还用于向所述鉴别接入控制器发送所述第二验证消息,所述第二验证消息中包括所述第一身份鉴权码和所述第一消息完整性校验码;

[0322] 接收单元502还用于接收所述鉴别接入控制器发送的鉴别完成消息;

[0323] 处理单元503还用于对所述鉴别完成消息中的第二消息完整性校验码进行验证,验证通过后,确定所述鉴别接入控制器的身份为合法;所述第二消息完整性校验码是所述鉴别接入控制器利用所述消息完整性校验密钥对包括所述鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的。

[0324] 可选的,所述第一验证消息中还包括所述鉴别接入控制器根据身份鉴别密钥生成的第一密钥交换参数;所述第二验证消息中还包括所述请求设备根据所述身份鉴别密钥生成的第二密钥交换参数,则处理单元503还用于:根据包括所述第二密钥交换参数对应的临时私钥和所述第一密钥交换参数所包括的临时公钥进行密钥交换计算生成第一密钥,根据包括所述第一密钥在内的信息利用密钥导出算法计算出所述消息完整性校验密钥。

[0325] 可选的,接收单元502接收的第一验证消息中所述第一密钥交接参数是所述鉴别接入控制器利用所述身份鉴别密钥,采用对称加密算法对包括所述鉴别接入控制器产生的临时公钥在内的信息进行加密生成的;处理单元503还用于:利用所述身份鉴别密钥,采用对称加密算法对包括所述请求设备产生的临时公钥在内的信息进行加密生成所述第二密钥交换参数;

[0326] 则处理单元503计算所述消息完整性校验密钥具体为,根据包括所述第二密钥交换参数对应的临时私钥和由所述第一密钥交换参数恢复出的临时公钥进行密钥交换计算生成所述第一密钥,根据包括所述第一密钥在内的信息利用所述密钥导出算法计算出所述消息完整性校验密钥。

[0327] 可选的,处理单元503具体用于:计算所述身份鉴别密钥的杂凑值,对所述杂凑值和包括所述请求设备产生的临时公钥在内的信息进行异或运算生成所述第二密钥交换参数。

[0328] 可选的，发送单元501发送的鉴别请求消息中还包括所述请求设备生成的第一随机数；接收单元502接收的第一验证消息中还包括所述第一随机数和所述鉴别接入控制器生成的第二随机数，所述身份鉴别密钥的计算数据还包括所述第一随机数和所述第二随机数，发送单元501发送的第二验证消息中还包括所述第二随机数；

[0329] 则处理单元503还用于：验证所述第一验证消息中的第一随机数和所述请求设备生成的第一随机数的一致性。

[0330] 可选的，所述请求设备的身份信息密文的加密数据还包括所述请求设备生成的身份标识加密密钥；则接收单元502接收的第一验证消息中还包括请求设备的身份标识密文；所述请求设备的身份标识密文是所述第一鉴别服务器利用解密所述请求设备的身份信息密文所得的所述身份标识加密密钥对所述请求设备的身份标识加密得到的；

[0331] 则处理单元503还用于：根据自身的身份标识和所述身份标识加密密钥对所述第一验证消息中的所述请求设备的身份标识密文进行验证。

[0332] 可选的，接收单元502接收的鉴别完成消息中还包括所述鉴别接入控制器为所述请求设备分配的临时身份标识；则处理单元503还用于确定所述鉴别接入控制器的身份合法时保存所述请求设备的临时身份标识。

[0333] 可选的，接收单元502接收的第一验证消息中还包括所述鉴别接入控制器的身份标识，则处理单元503还用于：当确定所述鉴别接入控制器的身份为合法时，根据包括所述第一密钥、所述请求设备的身份标识密文和所述鉴别接入控制器的身份标识在内的信息计算生成用于后续保密通信的会话密钥。

[0334] 可选的，处理单元503还用于利用所述消息完整性校验密钥对包括所述第二验证消息中除第一消息完整性校验码外的其他字段计算生成第一消息完整性校验码；

[0335] 接收单元502接收的鉴别完成消息中的第二消息完整性校验码是所述鉴别接入控制器利用所述消息完整性校验密钥对包括所述鉴别完成消息中除所述第二消息完整性校验码外的其他字段计算生成的。

[0336] 可选的，所述请求设备向所述鉴别接入控制器发送的消息还包括所述请求设备对接收到的所述鉴别接入控制器发送的最新前序消息计算的杂凑值。

[0337] 参见图6，本申请实施例还提供了一种第一鉴别服务器，所述第一鉴别服务器为请求设备信任的鉴别服务器，包括：

[0338] 处理单元601，用于利用加密证书对应的私钥解密请求设备的身份信息密文得到请求设备的身份标识，根据请求设备的身份标识确定所述请求设备的合法性，在确定所述请求设备的身份合法后，产生存证随机数和身份鉴别密钥；所述身份鉴别密钥是根据包括所述第一鉴别服务器与所述请求设备的预共享加密密钥在内的计算数据计算得到的；

[0339] 处理单元601还用于对第一存证消息中的第一身份鉴权码进行验证，验证通过后，生成并存储所述请求设备的请求通过记录。

[0340] 可选的，处理单元601还用于对所述第一存证消息中的所述第一身份鉴权码验证通过后，生成第一存证确认消息。

[0341] 可选的，处理单元601还用于：在生成和存储所述请求设备的请求通过记录时，保存所述鉴别接入控制器为所述请求设备分配的临时身份标识。

[0342] 可选的，所述第一鉴别服务器与所述鉴别接入控制器信任的第二鉴别服务器不同

时，所述第一鉴别服务器还包括：

[0343] 接收单元，用于接收所述第二鉴别服务器发送的第二鉴权请求消息；所述第二鉴权请求消息中包括所述请求设备的身份信息密文；

[0344] 发送单元，用于向所述第二鉴别服务器发送第二鉴权响应消息，所述第二鉴权响应消息中包括所述身份鉴别密钥和所述存证随机数；

[0345] 所述接收单元还用于接收所述第二鉴别服务器发送的第二存证消息，所述第二存证消息中包括所述第一身份鉴权码；

[0346] 处理单元601具体用于验证所述第二存证消息中的所述第一身份鉴权码。

[0347] 可选的，处理单元601还用于在对所述第二存证消息中的所述第一身份鉴权码验证通过后，生成第二存证确认消息；所述发送单元还用于向所述第二鉴别服务器发送所述第二存证确认消息。

[0348] 可选的，所述第一鉴别服务器向所述第二鉴别服务器发送的消息还包括所述第一鉴别服务器对接收到的所述第二鉴别服务器发送的最新前序消息计算的杂凑值。

[0349] 参见图7，本申请实施例还提供了一种第二鉴别服务器，所述第二鉴别服务器为鉴别接入控制器信任的鉴别服务器，包括：

[0350] 接收单元701，用于接收所述鉴别接入控制器发送的携带有请求设备的身份信息密文的第一鉴权请求消息；

[0351] 发送单元702，用于向所述鉴别接入控制器发送第一鉴权响应消息，所述第一鉴别响应消息中包括所述请求设备信任的第一鉴别服务器产生的存证随机数和所述第一鉴别服务器生成的身份鉴别密钥；

[0352] 接收单元701还用于接收所述鉴别接入控制器发送的第一存证消息，所述第一存证消息中包括第一身份鉴权码。

[0353] 可选的，接收单元701接收的第一存证消息中还包括第二身份鉴权码，所述第二身份鉴权码是所述鉴别接入控制器利用其与所述第二鉴别服务器的预共享校验密钥对所述第一存证消息中所述第二身份鉴权码之前的其他字段计算生成的；则所述第二鉴别服务器还包括：

[0354] 验证单元，用于利用与所述鉴别接入控制器的预共享校验密钥验证所述第二身份鉴权码的正确性。

[0355] 可选的，所述第二鉴别服务器与所述请求设备信任的第一鉴别服务器不同时，所述第二鉴别服务器还包括：

[0356] 处理单元，用于根据所述第一鉴权请求消息生成第二鉴权请求消息，所述第二鉴权请求消息包括所述请求设备的身份信息密文；

[0357] 发送单元702还用于向所述第一鉴别服务器发送所述第二鉴权请求消息；

[0358] 接收单元701还用于接收所述第一鉴别服务器发送的第二鉴权响应消息，所述第二鉴权响应消息中包括所述身份鉴别密钥和所述存证随机数；

[0359] 所述处理单元还用于根据所述第二鉴权响应消息生成所述第一鉴权响应消息；

[0360] 所述处理单元还用于根据所述第一存证消息生成第二存证消息，所述第二存证消息包括所述第一身份鉴权码；

[0361] 发送单元702还用于向所述第一鉴别服务器发送所述第二存证消息。

[0362] 可选的，接收单元701还用于接收所述第一鉴别服务器生成的第二存证确认消息；所述处理单元还用于在接收单元701接收到第二存证确认消息后，生成第一存证确认消息；发送单元702还用于向所述鉴别接入控制器发送所述第一存证确认消息。

[0363] 可选的，所述第二鉴别服务器向所述鉴别接入控制器发送的消息还包括所述第二鉴别服务器对接收到的所述鉴别接入控制器发送的最新前序消息计算的杂凑值；所述第二鉴别服务器向所述第一鉴别服务器发送的消息还包括所述第二鉴别服务器对接收到的所述第一鉴别服务器发送的最新前序消息计算的杂凑值。

[0364] 上述请求设备和鉴别接入控制器采用对称密钥的实体鉴别协议进行双向身份鉴别时，以密文的形式传输请求设备的身份信息，由此保证身份鉴别过程中请求设备的真实身份信息的安全性。另外，鉴别接入控制器在验证请求设备的身份合法后，会相应地向请求设备信任的第一鉴别服务器发送第一存证消息，以利用该第一鉴别服务器记录请求设备请求访问网络的行为，为后续网络接入点计费提供客观证据，有效地防止网络接入点对没有在其服务区内尝试访问网络的用户恶意计费。

[0365] 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，前述程序可以存储于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；而前述的存储介质可以是下述介质中的至少一种：只读存储器(英文：Read-Only Memory，缩写：ROM)、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0366] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于设备及系统实施例而言，由于其与方法实施例相一致和对应，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的设备及系统实施例仅是示意性的，其中作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者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模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可理解并实施。

[0367] 以上所述，仅为本申请的一种具体实施方式，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，可轻易想到的变化或替换，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该以权利要求的保护范围为准。

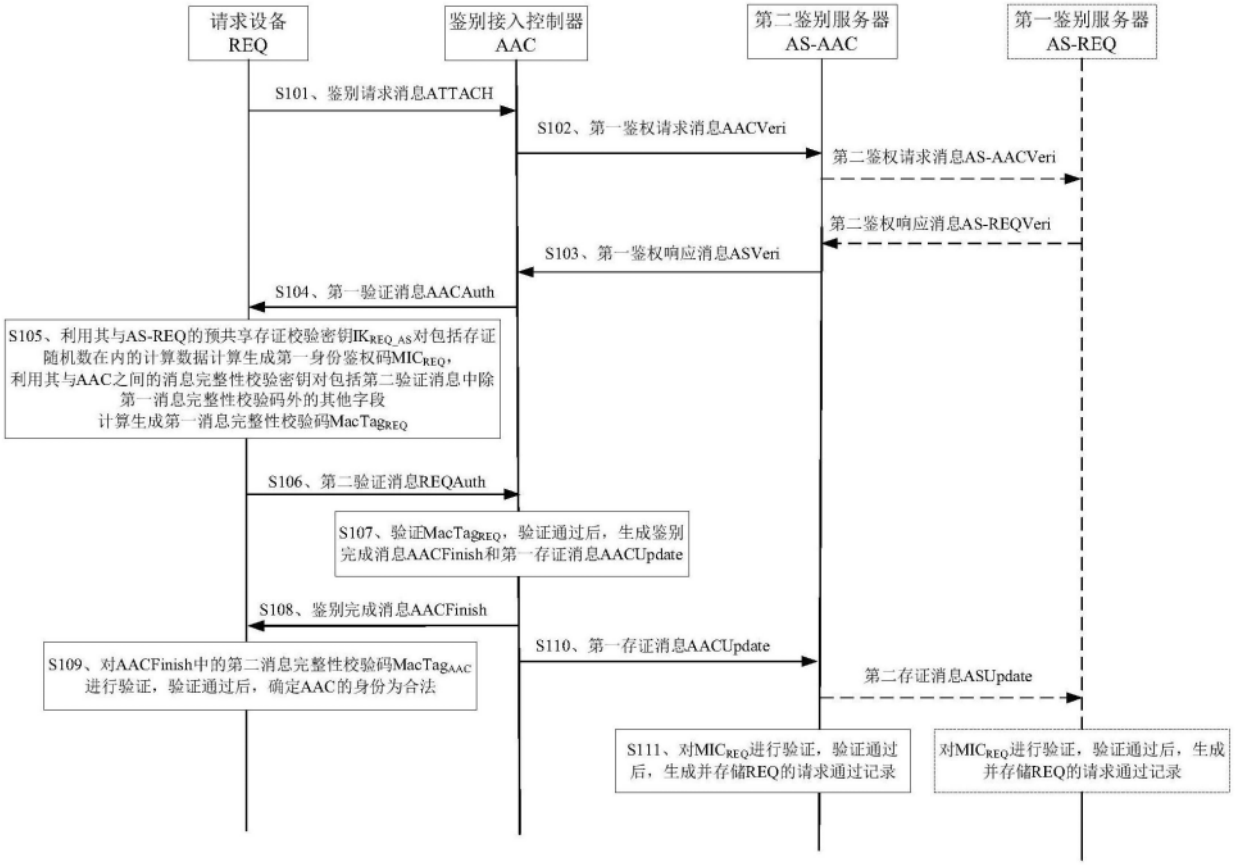

请求设备
REQ
鉴别接入控制器
AAC
第二鉴别服务器
AS-AAC
第一鉴别服务器
AS-REQ
S101、鉴别请求消息ATTACH
S102、第一鉴权请求消息AACVeri
第二鉴权请求消息AS-AACVeri
第二鉴权响应消息AS-REQVeri
S103、第一鉴权响应消息ASVeri
S104、第一验证消息AACAuth
S105、利用其与AS-REQ的预共享存证校验密钥IK_REQ_AS对包括存证随机数在内的计算数据计算生成第一身份鉴权码MIC_REQ，利用其与AAC之间的消息完整性校验密钥对包括第二验证消息中除第一消息完整性校验码外的其他字段计算生成第一消息完整性校验码MacTag_REQ
S106、第二验证消息REQAuth
S107、验证MacTag_REQ，验证通过后，生成鉴别完成消息AACFinish和第一存证消息AACUpdate
S108、鉴别完成消息AACFinish
S109、对AACFinish中的第二消息完整性校验码MacTag_AAC进行验证，验证通过后，确定AAC的身份为合法
S110、第一存证消息AACUpdate
第二存证消息ASUpdate
S111、对MIC_REQ进行验证，验证通过后，生成并存储REQ的请求通过记录
对MIC_REQ进行验证，验证通过后，生成并存储REQ的请求通过记录

图1

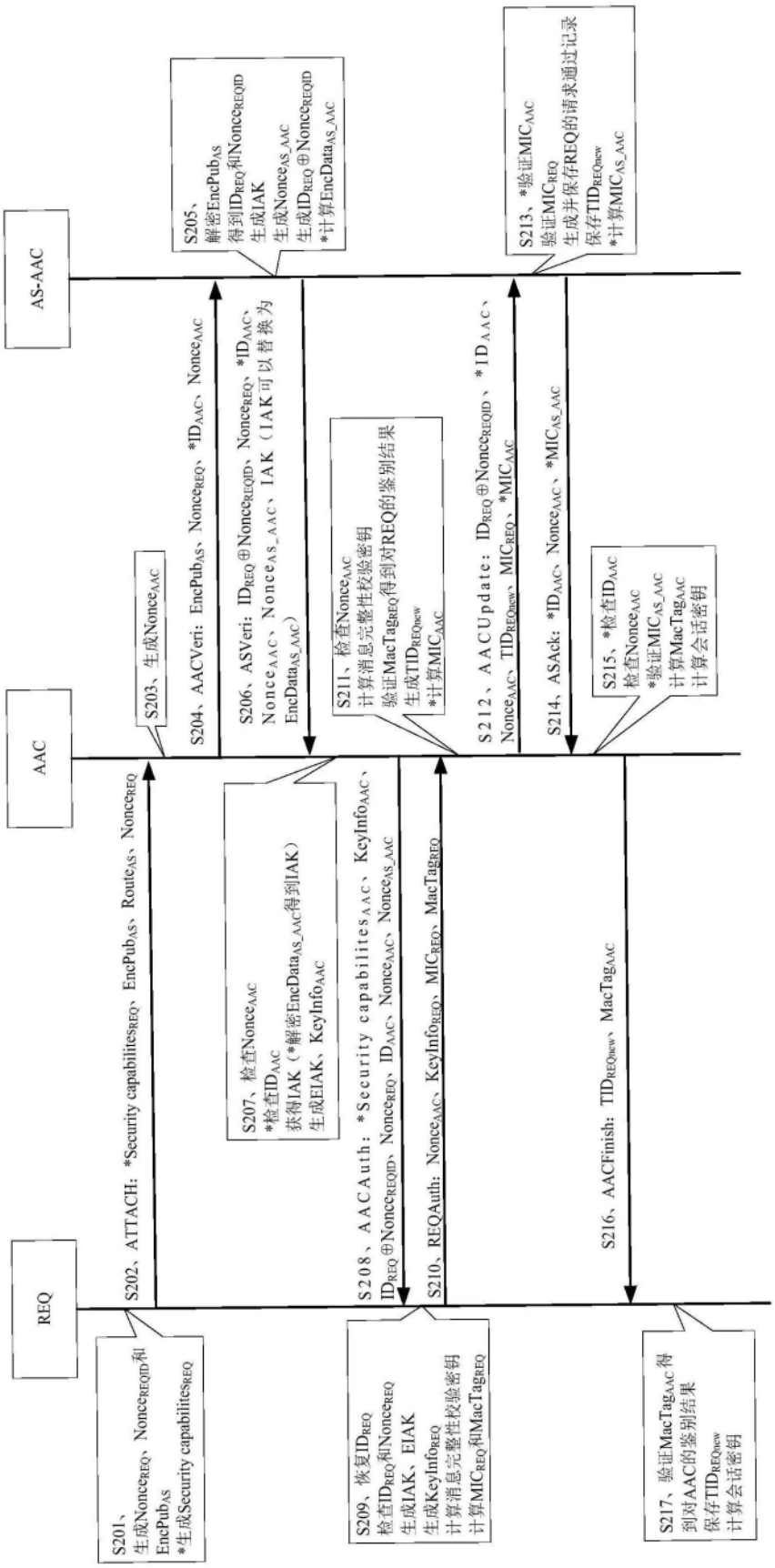

AS-AAC
AAC
REQ
S201、
生成Nonce$_{REQ}$、Nonce$_{REQID}$和EncPub$_{AS}$
*生成Security capabilites$_{REQ}$
S202、ATTACH：*Security capabilites$_{REQ}$、EncPub$_{AS}$、Route$_{AS}$、Nonce$_{REQ}$
S203、生成Nonce$_{AAC}$
S204、AACVeri：EncPub$_{AS}$、Nonce$_{REQ}$、*ID$_{AAC}$、Nonce$_{AAC}$
S205、
解密EncPub$_{AS}$
得到ID$_{REQ}$和Nonce$_{REQID}$
生成IAK
生成Nonce$_{AS_AAC}$
生成ID$_{REQ}$⊕Nonce$_{REQID}$
*计算EncData$_{AS_AAC}$
S206、ASVeri：ID$_{REQ}$⊕Nonce$_{REQID}$、Nonce$_{REQ}$、*ID$_{AAC}$、Nonce$_{AAC}$、Nonce$_{AS_AAC}$、IAK（IAK可以替换为EncData$_{AS_AAC}$）
S207、检查Nonce$_{AAC}$
*检查ID$_{AAC}$
获得IAK（*解密EncData$_{AS_AAC}$得到IAK）
生成EIAK、KeyInfo$_{AAC}$
S208、AACAuth：*Security capabilites$_{AAC}$、KeyInfo$_{AAC}$、ID$_{REQ}$⊕Nonce$_{REQID}$、Nonce$_{REQ}$、ID$_{AAC}$、Nonce$_{AAC}$、Nonce$_{AS_AAC}$
S209、恢复ID$_{REQ}$
检查ID$_{REQ}$和Nonce$_{REQ}$
生成IAK、EIAK
生成KeyInfo$_{REQ}$
计算消息完整性校验密钥
计算MIC$_{REQ}$和MacTag$_{REQ}$
S210、REQAuth：Nonce$_{AAC}$、KeyInfo$_{REQ}$、MIC$_{REQ}$、MacTag$_{REQ}$
S211、检查Nonce$_{AAC}$
计算消息完整性校验密钥
验证MacTag$_{REQ}$得到对REQ的鉴别结果
生成TID$_{REQnew}$
*计算MIC$_{AAC}$
S212、AACUpdate：ID$_{REQ}$⊕Nonce$_{REQID}$、*ID$_{AAC}$、Nonce$_{AAC}$、TID$_{REQnew}$、MIC$_{REQ}$、*MIC$_{AAC}$
S213、*验证MIC$_{AAC}$
验证MIC$_{REQ}$
生成并保存REQ的请求通过记录
保存TID$_{REQnew}$
*计算MIC$_{AS_AAC}$
S214、ASAck：*ID$_{AAC}$、Nonce$_{AAC}$、*MIC$_{AS_AAC}$
S215、*检查ID$_{AAC}$
检查Nonce$_{AAC}$
*验证MIC$_{AS_AAC}$
计算MacTag$_{AAC}$
计算会话密钥
S216、AACFinish：TID$_{REQnew}$、MacTag$_{AAC}$
S217、验证MacTag$_{AAC}$得到对AAC的鉴别结果
保存TID$_{REQnew}$
计算会话密钥

图2

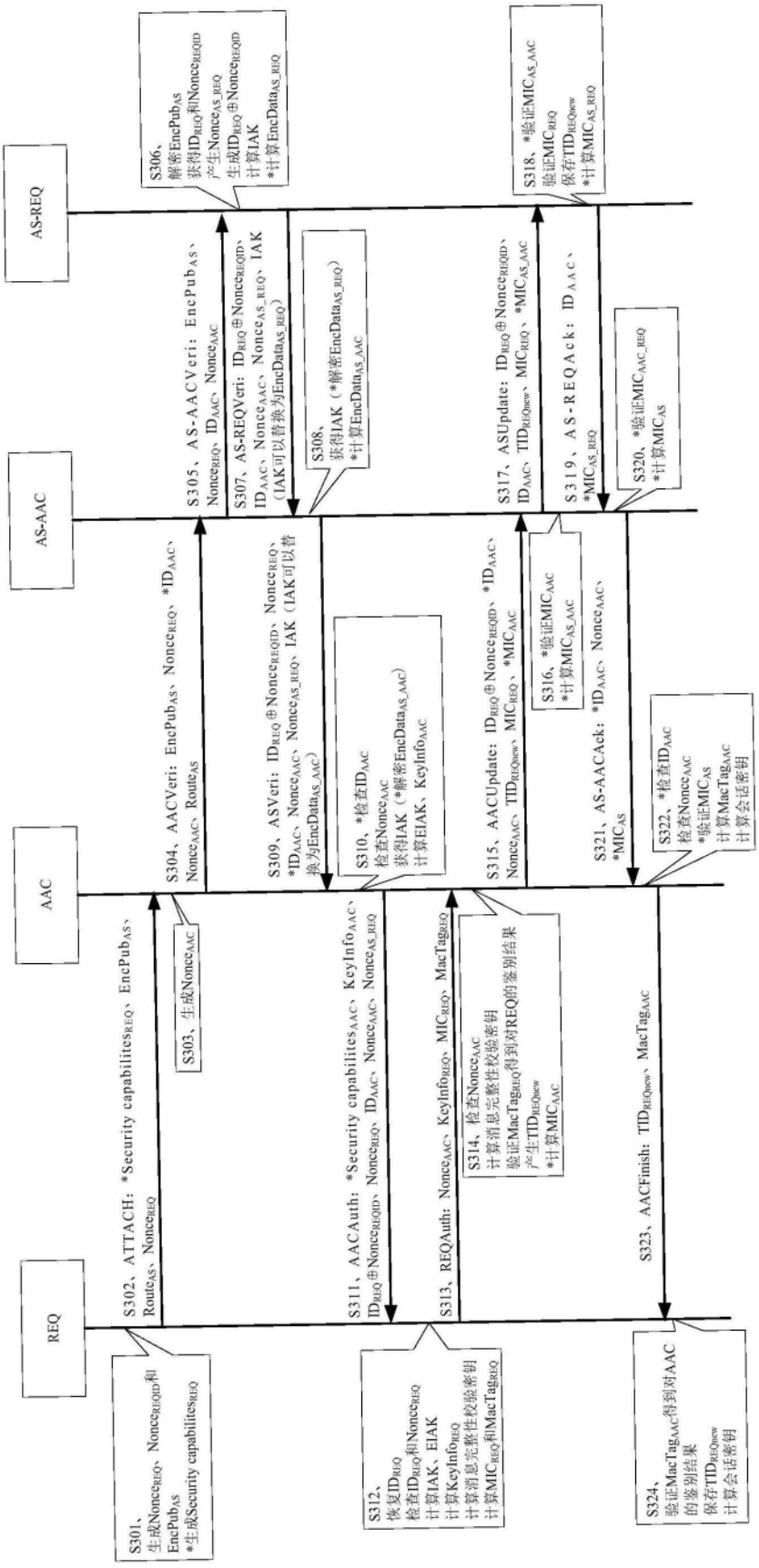

REQ
AAC
AS-AAC
AS-REQ
S301、生成Nonce$_{REQ}$、Nonce$_{REQID}$和EncPub$_{AS}$ *生成Security capabilites$_{REQ}$
S302、ATTACH: *Security capabilites$_{REQ}$、EncPub$_{AS}$、Route$_{AS}$、Nonce$_{REQ}$
S303、生成Nonce$_{AAC}$
S304、AACVeri: EncPub$_{AS}$、Nonce$_{REQ}$、*ID$_{AAC}$、Nonce$_{AAC}$、Route$_{AS}$
S305、AS-AACVeri: EncPub$_{AS}$、Nonce$_{REQ}$、ID$_{AAC}$、Nonce$_{AAC}$
S306、解密EncPub$_{AS}$ 获得ID$_{REQ}$和Nonce$_{REQID}$ 产生Nonce$_{AS_REQ}$ 生成ID$_{REQ}$⊕Nonce$_{REQID}$ 计算IAK *计算EncData$_{AS_REQ}$
S307、AS-REQVeri: ID$_{REQ}$⊕Nonce$_{REQID}$、ID$_{AAC}$、Nonce$_{AAC}$、Nonce$_{AS_REQ}$、IAK（IAK可以替换为EncData$_{AS_REQ}$）
S308、获得IAK（*解密EncData$_{AS_REQ}$） *计算EncData$_{AS_AAC}$
S309、ASVeri: ID$_{REQ}$⊕Nonce$_{REQID}$、Nonce$_{REQ}$、*ID$_{AAC}$、Nonce$_{AAC}$、Nonce$_{AS_REQ}$、IAK（IAK可以替换为EncData$_{AS_AAC}$）
S310、*检查ID$_{AAC}$ 检查Nonce$_{AAC}$ 获得IAK（*解密EncData$_{AS_AAC}$） 计算EIAK、KeyInfo$_{AAC}$
S311、AACAuth: *Security capabilites$_{AAC}$、KeyInfo$_{AAC}$、ID$_{REQ}$⊕Nonce$_{REQID}$、Nonce$_{REQ}$、ID$_{AAC}$、Nonce$_{AAC}$、Nonce$_{AS_REQ}$
S312、恢复ID$_{REQ}$ 检查ID$_{REQ}$和Nonce$_{REQ}$ 计算IAK、EIAK 计算KeyInfo$_{REQ}$ 计算消息完整性校验密钥 计算MIC$_{REQ}$和MacTag$_{REQ}$
S313、REQAuth: Nonce$_{AAC}$、KeyInfo$_{REQ}$、MIC$_{REQ}$、MacTag$_{REQ}$
S314、检查Nonce$_{AAC}$ 计算消息完整性校验密钥 验证MacTag$_{REQ}$得到对REQ的鉴别结果 产生TID$_{REQnew}$ *计算MIC$_{AAC}$
S315、AACUpdate: ID$_{REQ}$⊕Nonce$_{REQID}$、*ID$_{AAC}$、Nonce$_{AAC}$、TID$_{REQnew}$、MIC$_{REQ}$、*MIC$_{AAC}$
S316、*验证MIC$_{AAC}$ *计算MIC$_{AS_AAC}$
S317、ASUpdate: ID$_{REQ}$⊕Nonce$_{REQID}$、ID$_{AAC}$、TID$_{REQnew}$、MIC$_{REQ}$、*MIC$_{AS_AAC}$
S318、*验证MIC$_{AS_AAC}$ 验证MIC$_{REQ}$ 保存TID$_{REQnew}$ *计算MIC$_{AS_REQ}$
S319、AS-REQAck: ID$_{AAC}$、*MIC$_{AS_REQ}$
S320、*验证MIC$_{AAC_REQ}$ *计算MIC$_{AS}$
S321、AS-AACAck: *ID$_{AAC}$、Nonce$_{AAC}$、*MIC$_{AS}$
S322、*检查ID$_{AAC}$ 检查Nonce$_{AAC}$ *验证MIC$_{AS}$ 计算MacTag$_{AAC}$ 计算会话密钥
S323、AACFinish: TID$_{REQnew}$、MacTag$_{AAC}$
S324、验证MacTag$_{AAC}$得到对AAC的鉴别结果 保存TID$_{REQnew}$ 计算会话密钥

图3

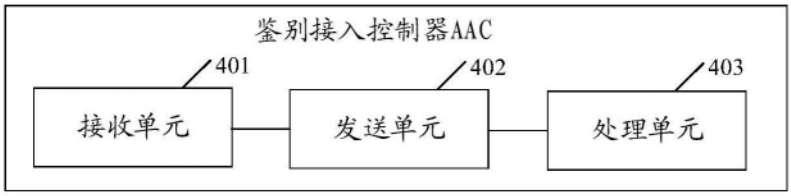

鉴别接入控制器AAC
401
402
403
接收单元
发送单元
处理单元

图4

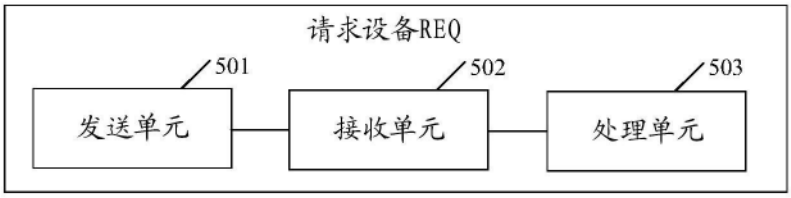

请求设备REQ
501
502
503
发送单元
接收单元
处理单元

图5

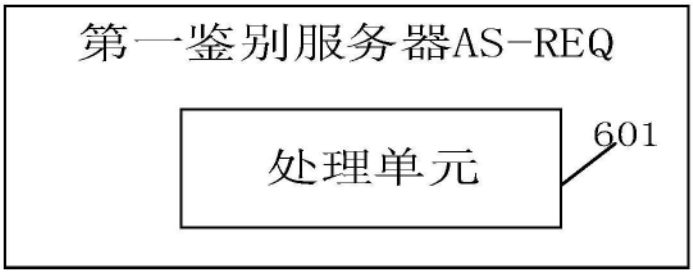

第一鉴别服务器AS-REQ
处理单元
601

图6

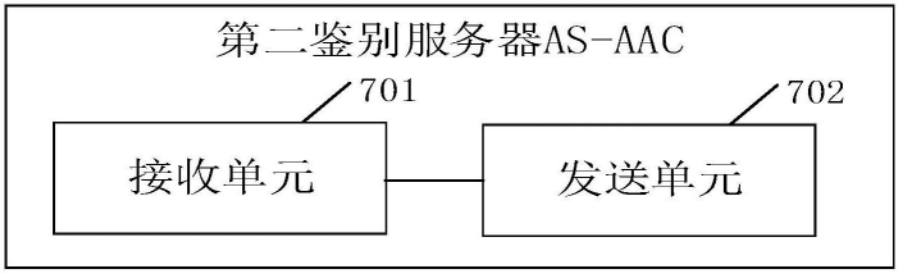

第二鉴别服务器AS-AAC
701
702
接收单元
发送单元

图7