(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107295510 B
(45)授权公告日 2020.01.03

(21)申请号 201610197304.0
(22)申请日 2016.03.31
(65)同一申请的已公布的文献号
申请公布号 CN 107295510 A
(43)申请公布日 2017.10.24
(73)专利权人 中国移动通信有限公司研究院
地址 100053 北京市西城区宣武门西大街32号
专利权人 中国移动通信集团公司
(72)发明人 阎军智 杭小勇
(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静 安利霞
(51)Int.Cl.
H04W 12/06(2009.01)
H04W 48/02(2009.01)
(56)对比文件
CN 101002420 A,2007.07.18,
US 2002184182 A1,2002.12.05,
审查员 李淼

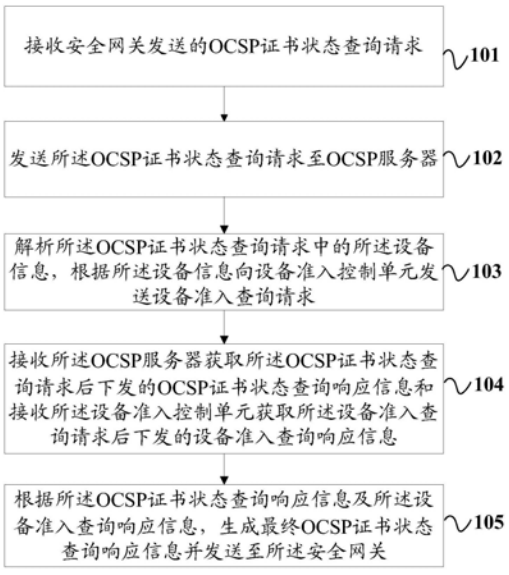
权利要求书3页 说明书11页 附图4页

(54)发明名称

基于OCSP实现家庭基站准入控制的方法、设备及系统

(57)摘要

本发明提供了一种基于OCSP实现家庭基站准入控制的方法、设备及系统，涉及家庭基站认证领域，其中方法包括：接收安全网关发送的OCSP证书状态查询请求，其中OCSP证书状态查询请求包括待验证的基站证书，且基站证书中包括待验证家庭基站的设备信息；发送OCSP证书状态查询请求至OCSP服务器；解析OCSP证书状态查询请求中的设备信息，根据设备信息向设备准入控制单元发送设备准入查询请求；接收OCSP证书状态查询响应信息和设备准入查询响应信息；生成最终OCSP证书状态查询响应信息并发送至安全网关。



CN 107295510 B

1.一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的方法,应用于OCSP代理服务器,其特征在于,所述方法包括:

接收安全网关发送的OCSP证书状态查询请求,其中所述OCSP证书状态查询请求包括待验证的基站证书,且所述基站证书中包括待验证家庭基站的设备信息;

发送所述OCSP证书状态查询请求至OCSP服务器;

解析所述OCSP证书状态查询请求中的所述设备信息,根据所述设备信息向设备准入控制单元发送设备准入查询请求;

接收所述OCSP服务器获取所述OCSP证书状态查询请求后下发的OCSP证书状态查询响应信息和接收所述设备准入控制单元获取所述设备准入查询请求后下发的设备准入查询响应信息;

根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息,生成最终OCSP证书状态查询响应信息并发送至所述安全网关。

2.根据权利要求1所述的方法,其特征在于,所述根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息,生成最终OCSP证书状态查询响应信息,包括:

解析所述设备准入查询响应信息,获取设备准入查询结果;

添加所述设备准入查询结果至所述OCSP证书状态查询响应信息,根据向证书授权中心CA机构申请得到的签名证书,替换所述OCSP证书状态查询响应信息的签名信息为一新的签名信息,得到最终OCSP证书状态查询响应信息。

3.根据权利要求2所述的方法,其特征在于,所述获取设备准入查询结果的步骤之后,所述方法还包括:

判断所述设备准入查询结果是否为不允许接入;

当判断结果为是时,根据所述设备准入查询响应信息,获取不允许接入的产生原因;

其中,在所述添加所述设备准入查询结果至所述OCSP证书状态查询响应信息的步骤中,同时添加所述产生原因至所述OCSP证书状态查询响应信息中。

4.根据权利要求1所述的方法,其特征在于,所述设备信息至少包括:设备名称及设备序列号。

5.一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的方法,应用于安全网关,其特征在于,所述方法包括:

发送OCSP证书状态查询请求至OCSP代理服务器,其中所述OCSP证书状态查询请求包括待验证的基站证书,且所述基站证书中包括待验证家庭基站的设备信息;

接收所述OCSP代理服务器下发的最终OCSP证书状态查询响应信息,其中所述最终OCSP证书状态查询响应信息为所述OCSP代理服务器根据从所述OCSP服务器接收的证书状态查询响应信息和从设备准入控制单元接收的设备准入查询响应信息生成;

根据所述最终OCSP证书状态查询响应信息,判断待验证家庭基站是否满足准入条件。

6.根据权利要求5所述的方法,其特征在于,所述根据所述最终OCSP证书状态查询响应信息,判断待验证家庭基站是否满足准入条件,包括:

当所述最终OCSP证书状态查询响应信息中记录的待验证的基站证书处于有效状态且设备准入查询结果为允许接入时,判断所述家庭基站满足准入条件。

7.一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的方法,应用于设备准

入控制单元，其特征在于，所述方法包括：

接收OCSP代理服务器发送的设备准入查询请求，所述设备准入查询请求中包括：待验证家庭基站的设备信息；

根据所述设备信息，按预设的准入规则，对所述待验证家庭基站进行设备准入查询并生成设备准入查询响应信息，包括：根据所述设备信息，按照根据所述预设的准入规则设置的黑名单或白名单，对所述待验证家庭基站进行设备准入查询；当所述设备信息不存在于所述黑名单或所述设备信息存在于所述白名单中时，生成允许接入的设备准入查询响应信息；当所述设备信息存在于所述黑名单或所述设备信息不存在于所述白名单中时，生成不允许接入的设备准入查询响应信息；

发送所述设备准入查询响应信息至所述OCSP代理服务器。

8.根据权利要求7所述的方法，其特征在于，所述生成设备准入查询响应信息的步骤中，所生成的所述设备准入查询响应信息包括：查询响应时间、设备准入查询结果及当所述设备准入查询结果为不允许接入时的产生原因。

9.一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，其特征在于，所述设备包括：

第一接收模块，用于接收安全网关发送的OCSP证书状态查询请求，其中所述OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息；

第一发送模块，用于发送所述OCSP证书状态查询请求至OCSP服务器；

第二发送模块，用于解析所述OCSP证书状态查询请求中的所述设备信息，根据所述设备信息向设备准入控制单元发送设备准入查询请求；

第二接收模块，用于接收所述OCSP服务器获取所述OCSP证书状态查询请求后下发的OCSP证书状态查询响应信息和接收所述设备准入控制单元获取所述设备准入查询请求后下发的设备准入查询响应信息；

生成模块，用于根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息，生成最终OCSP证书状态查询响应信息并发送至所述安全网关。

10.根据权利要求9所述的设备，其特征在于，所述生成模块，用于：

解析所述设备准入查询响应信息，获取设备准入查询结果；

添加所述设备准入查询结果至所述OCSP证书状态查询响应信息，根据向证书授权中心CA机构申请得到的签名证书，替换所述OCSP证书状态查询响应信息的签名信息为一新的签名信息，得到最终OCSP证书状态查询响应信息。

11.根据权利要求10所述的设备，其特征在于，所述生成模块还用于：

判断所述设备准入查询结果是否为不允许接入；

当判断结果为是时，根据所述设备准入查询响应信息，获取不允许接入的产生原因；

其中，在所述添加所述设备准入查询结果至所述OCSP证书状态查询响应信息的步骤中，同时添加所述产生原因至所述OCSP证书状态查询响应信息中。

12.根据权利要求9所述的设备，其特征在于，所述设备信息至少包括：设备名称及设备序列号。

13.一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，其特征在于，

所述设备包括：

第三发送模块，用于发送OCSP证书状态查询请求至OCSP代理服务器，其中所述OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息；

第三接收模块，用于接收所述OCSP代理服务器下发的最终OCSP证书状态查询响应信息，其中所述最终OCSP证书状态查询响应信息为所述OCSP代理服务器根据从所述OCSP服务器接收的证书状态查询响应信息和从设备准入控制单元接收的设备准入查询响应信息生成；

判断模块，用于根据所述最终OCSP证书状态查询响应信息，判断待验证家庭基站是否满足准入条件。

14.根据权利要求13所述的设备，其特征在于，所述判断模块，用于：

当所述最终OCSP证书状态查询响应信息中记录的待验证的基站证书处于有效状态且设备准入查询结果为允许接入时，判断所述家庭基站满足准入条件。

15.一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，其特征在于，所述设备包括：

第四接收模块，用于接收OCSP代理服务器发送的设备准入查询请求，所述设备准入查询请求中包括：待验证家庭基站的设备信息；

查询处理模块，用于根据所述设备信息，按预设的准入规则，对所述待验证家庭基站进行设备准入查询并生成设备准入查询响应信息；

第四发送模块，用于发送所述设备准入查询响应信息至所述OCSP代理服务器；

所述查询处理模块用于：

根据所述设备信息，按照根据所述预设的准入规则设置的黑名单或白名单，对所述待验证家庭基站进行设备准入查询；

当所述设备信息不存在于所述黑名单或所述设备信息存在于所述白名单中时，生成允许接入的设备准入查询响应信息；

当所述设备信息存在于所述黑名单或所述设备信息不存在于所述白名单中时，生成不允许接入的设备准入查询响应信息。

16.根据权利要求15所述的设备，其特征在于，所述查询处理模块所生成的所述设备准入查询响应信息包括：查询响应时间、设备准入查询结果及当所述设备准入查询结果为不允许接入时的产生原因。

17.一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的系统，其特征在于，所述系统包括：如权利要求9-权利要求12任一项所述的基于OCSP实现家庭基站准入控制的设备、如权利要求13-权利要求14任一项所述的基于OCSP实现家庭基站准入控制的设备及如权利要求15-如权利要求16任一项所述的基于OCSP实现家庭基站准入控制的设备。

基于OCSP实现家庭基站准入控制的方法、设备及系统

技术领域

[0001] 本发明主要涉及家庭基站认证领域，尤其是一种基于OCSP实现家庭基站准入控制的方法、设备及系统。

背景技术

[0002] 家庭基站，又称HeNB(Home evolved Node B，家庭演进基站)，是一种小型化、低功率蜂窝技术，通过固网宽带接入到移动核心网，为用户提供包括传统蜂窝移动通信基础业务在内的固定移动融合业务。目前3GPP HeNB安全规范TS 33.320已经定义了HeNB的认证方式，HeNB与安全网关之间采用数字证书进行设备双向认证。

[0003] 在安全网关接收到HeNB基站发送的因特网密匙交换-认证IKE_AUTH消息后，安全网关验证设备证书的有效性，仅当设备持有自己的合法证书时，安全网关才允许基站接入。通常情况下，只要基站持有合法的设备证书就可成功完成与安全网关之间的认证。而该方案通过证书是否被吊销实现证书的准入控制，即为只要给基站颁发了合法的证书就表示该基站具备接入权限，而若需要限制基站接入，则需吊销基站持有的证书。

[0004] 在部分可能由于一些其他原因导致基站不能接入的情况下，例如某基站设备被入侵或频繁攻击网络时，需要阻止该设备接入网络，按照上述方案，需要将基站设备的证书进行吊销处理来防止其接入到移动核心网，由于证书吊销之后不可恢复，因此当基站设备修复之后，基站需要重新向证书授权中心CA申请设备证书，尤其在CA机构不支持设备在线申请数字证书的情况下，还需要人工介入进行设备证书配置，流程复杂，效率低下。且在对基站进行准入控制时，往往还由于如资费等其他因素不允许其接入，在相似的该类情况下进行设备证书吊销来阻止其接入显然不是一种合理的解决措施，现有家庭基站准入控制方案不能灵活实现设备准入控制，限制了设备的应用规模。

发明内容

[0005] 本发明提供一种基于OCSP实现家庭基站准入控制的方法、设备及系统，用来解决现有家庭基站准入控制方案不能灵活实现设备准入控制，限制设备的应用规模的问题。

[0006] 为了解决上述技术问题，本发明采用如下技术方案：

[0007] 一方面，本发明提供了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的方法，应用于OCSP代理服务器，所述方法包括：

[0008] 接收安全网关发送的OCSP证书状态查询请求，其中所述OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息；

[0009] 发送所述OCSP证书状态查询请求至OCSP服务器；

[0010] 解析所述OCSP证书状态查询请求中的所述设备信息，根据所述设备信息向设备准入控制单元发送设备准入查询请求；

[0011] 接收所述OCSP服务器获取所述OCSP证书状态查询请求后下发的OCSP证书状态查询响应信息和接收所述设备准入控制单元获取所述设备准入查询请求后下发的设备准入

查询响应信息；

[0012] 根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息，生成最终OCSP证书状态查询响应信息并发送至所述安全网关。

[0013] 可选地，所述根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息，生成最终OCSP证书状态查询响应信息，包括：

[0014] 解析所述设备准入查询响应信息，获取设备准入查询结果；

[0015] 添加所述设备准入查询结果至所述OCSP证书状态查询响应信息，根据向证书授权中心CA机构申请得到的签名证书，替换所述OCSP证书状态查询响应信息的签名信息为一新的签名信息，得到最终OCSP证书状态查询响应信息。

[0016] 可选地，所述获取设备准入查询结果的步骤之后，所述方法还包括：

[0017] 判断所述设备准入查询结果是否为不允许接入；

[0018] 当判断结果为是时，根据所述设备准入查询响应信息，获取不允许接入的产生原因；

[0019] 其中，在所述添加所述设备准入查询结果至所述OCSP证书状态查询响应信息的步骤中，同时添加所述产生原因至所述OCSP证书状态查询响应信息中。

[0020] 可选地，所述设备信息至少包括：设备名称及设备序列号。

[0021] 另一方面，本发明还提供了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的方法，应用于安全网关，所述方法包括：

[0022] 发送OCSP证书状态查询请求至OCSP代理服务器，其中所述OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息；

[0023] 接收所述OCSP代理服务器下发的最终OCSP证书状态查询响应信息，其中所述最终OCSP证书状态查询响应信息为所述OCSP代理服务器根据从所述OCSP服务器接收的证书状态查询响应信息和从设备准入控制单元接收的设备准入查询响应信息生成；

[0024] 根据所述最终OCSP证书状态查询响应信息，判断待验证家庭基站是否满足准入条件。

[0025] 可选地，所述根据所述最终OCSP证书状态查询响应信息，判断待验证家庭基站是否满足准入条件，包括：

[0026] 当所述最终OCSP证书状态查询响应信息中记录的待验证的基站证书处于有效状态且设备准入查询结果为允许接入时，判断所述家庭基站满足准入条件。

[0027] 另一方面，本发明还提供了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的方法，应用于设备准入控制单元，所述方法包括：

[0028] 接收OCSP代理服务器发送的设备准入查询请求，所述设备准入查询请求中包括：待验证家庭基站的设备信息；

[0029] 根据所述设备信息，按预设的准入规则，对所述待验证家庭基站进行设备准入查询并生成设备准入查询响应信息；

[0030] 发送所述设备准入查询响应信息至所述OCSP代理服务器。

[0031] 可选地，所述根据所述设备信息，按预设的准入规则，对所述待验证家庭基站进行设备准入查询并生成设备准入查询响应信息，包括：

[0032] 根据所述设备信息，按照根据所述预设的准入规则设置的黑名单或白名单，对所

述待验证家庭基站进行设备准入查询；

[0033] 当所述设备信息不存在于所述黑名单或所述设备信息存在于所述白名单中时，生成允许接入的设备准入查询响应信息；

[0034] 当所述设备信息存在于所述黑名单或所述设备信息不存在于所述白名单中时，生成不允许接入的设备准入查询响应信息。

[0035] 可选地，所述生成设备准入查询响应信息的步骤中，所生成的所述设备准入查询响应信息包括：查询响应时间、设备准入查询结果及当所述设备准入查询结果为不允许接入时的产生原因。

[0036] 另一方面，本发明还提供了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，所述设备包括：

[0037] 第一接收模块，用于接收安全网关发送的OCSP证书状态查询请求，其中所述OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息；

[0038] 第一发送模块，用于发送所述OCSP证书状态查询请求至OCSP服务器；

[0039] 第二发送模块，用于解析所述OCSP证书状态查询请求中的所述设备信息，根据所述设备信息向设备准入控制单元发送设备准入查询请求；

[0040] 第二接收模块，用于接收所述OCSP服务器获取所述OCSP证书状态查询请求后下发的OCSP证书状态查询响应信息和接收所述设备准入控制单元获取所述设备准入查询请求后下发的设备准入查询响应信息；

[0041] 生成模块，用于根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息，生成最终OCSP证书状态查询响应信息并发送至所述安全网关。

[0042] 可选地，所述生成模块，用于：

[0043] 解析所述设备准入查询响应信息，获取设备准入查询结果；

[0044] 添加所述设备准入查询结果至所述OCSP证书状态查询响应信息，根据向证书授权中心CA机构申请得到的签名证书，替换所述OCSP证书状态查询响应信息的签名信息为一新的签名信息，得到最终OCSP证书状态查询响应信息。

[0045] 可选地，所述生成模块还用于：

[0046] 判断所述设备准入查询结果是否为不允许接入；

[0047] 当判断结果为是时，根据所述设备准入查询响应信息，获取不允许接入的产生原因；

[0048] 其中，在所述添加所述设备准入查询结果至所述OCSP证书状态查询响应信息的步骤中，同时添加所述产生原因至所述OCSP证书状态查询响应信息中。

[0049] 可选地，所述设备信息至少包括：设备名称及设备序列号。

[0050] 另一方面，本发明还提供了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，所述设备包括：

[0051] 第三发送模块，用于发送OCSP证书状态查询请求至OCSP代理服务器，其中所述OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息；

[0052] 第三接收模块，用于接收所述OCSP代理服务器下发的最终OCSP证书状态查询响应

信息，其中所述最终OCSP证书状态查询响应信息为所述OCSP代理服务器根据从所述OCSP服务器接收的证书状态查询响应信息和从设备准入控制单元接收的设备准入查询响应信息生成；

[0053] 判断模块，用于根据所述最终OCSP证书状态查询响应信息，判断待验证家庭基站是否满足准入条件。

[0054] 可选地，所述判断模块，用于：

[0055] 当所述最终OCSP证书状态查询响应信息中记录的待验证的基站证书处于有效状态且设备准入查询结果为允许接入时，判断所述家庭基站满足准入条件。

[0056] 另一方面，本发明还提供了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，所述设备包括：

[0057] 第四接收模块，用于接收OCSP代理服务器发送的设备准入查询请求，所述设备准入查询请求中包括：待验证家庭基站的设备信息；

[0058] 查询处理模块，用于根据所述设备信息，按预设的准入规则，对所述待验证家庭基站进行设备准入查询并生成设备准入查询响应信息；

[0059] 第四发送模块，用于发送所述设备准入查询响应信息至所述OCSP代理服务器。

[0060] 可选地，所述查询处理模块，用于：

[0061] 根据所述设备信息，按照根据所述预设的准入规则设置的黑名单或白名单，对所述待验证家庭基站进行设备准入查询；

[0062] 当所述设备信息不存在于所述黑名单或所述设备信息存在于所述白名单中时，生成允许接入的设备准入查询响应信息；

[0063] 当所述设备信息存在于所述黑名单或所述设备信息不存在于所述白名单中时，生成不允许接入的设备准入查询响应信息。

[0064] 可选地，所述查询处理模块所生成的所述设备准入查询响应信息包括：查询响应时间、设备准入查询结果及当所述设备准入查询结果为不允许接入时的产生原因。

[0065] 另一方面，本发明还提供了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的系统，所述系统包括：如上所述的基于OCSP实现家庭基站准入控制的设备、如上所述的另一种基于OCSP实现家庭基站准入控制的设备及如上所述的又一种基于OCSP实现家庭基站准入控制的设备。

[0066] 本发明的有益效果是：

[0067] 上述方案，需要结合OCSP证书状态查询响应信息及设备准入查询响应信息两方面计算生成最终OCSP查询响应信息，并将该最终响应信息返回给安全网关，该过程在结合原有的OCSP服务器查询处理过程，对OCSP证书状态查询请求进行查询处理时加入了设备准入查询过程，将基站证书的有效认证控制与对设备本身其他因素相关的设备准入控制结合起来，综合两者对基站进行准入控制，无需频繁吊销证书，避免了大量的重新申请证书的过程，实现灵活的设备准入控制，且OCSP服务器不需做出改变，仅需遵循现有技术规范即可，容易实施。

附图说明

[0068] 图1表示本发明第一实施例中的流程示意图；

[0069] 图2表示本发明第二实施例中的流程示意图；

[0070] 图3表示本发明第三实施例中的流程示意图；

[0071] 图4表示本发明第四实施例中的示意框图；

[0072] 图5表示本发明第五实施例中的示意框图；

[0073] 图6表示本发明第六实施例中的示意框图；

[0074] 图7表示本发明中基于OCSP实现家庭基站准入控制的整体时序图。

具体实施方式

[0075] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0076] 第一实施例

[0077] 如图1、图7所示，本发明公开了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的方法，应用于OCSP代理服务器。该方法包括：

[0078] 步骤101，接收安全网关发送的OCSP证书状态查询请求。

[0079] 其中，该OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息。

[0080] 步骤102，发送所述OCSP证书状态查询请求至OCSP服务器。

[0081] 该步骤中，在接收到安全网关发来的查询请求之后，将该查询请求转发给OCSP服务器，此处主要是对家庭基站证书的有效状态进行查询，具体内容包括对基站证书的名称、用途、有效期等信息的查询。

[0082] 步骤103，解析所述OCSP证书状态查询请求中的所述设备信息，根据所述设备信息向设备准入控制单元发送设备准入查询请求。

[0083] 该步骤中，在接收到安全网关发来的查询请求之后，将OCSP证书状态查询请求中的设备信息解析出来并根据该设备信息发送设备准入查询请求至设备准入控制单元，此处主要是对考虑进其他因素的是否允许家庭基站进入的结果进行查询。该设备信息可以是如设备名称、设备序列号等信息。

[0084] 其中，该其他因素包括但不限于是家庭基站设备的安全性、设备的资费缴纳情况、准入时限情况等。

[0085] 步骤104，接收所述OCSP服务器获取所述OCSP证书状态查询请求后下发的OCSP证书状态查询响应信息和接收所述设备准入控制单元获取所述设备准入查询请求后下发的设备准入查询响应信息。

[0086] 该步骤中，在分别向OCSP服务器发送OCSP证书状态查询请求、向设备准入控制单元发送设备准入查询请求之后，对应地，接收OCSP服务器反馈的OCSP证书状态查询响应信息及设备准入控制单元反馈的设备准入查询响应信息两方面的响应内容。

[0087] 步骤105，根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息，生成最终OCSP证书状态查询响应信息并发送至所述安全网关。

[0088] 该步骤中，在根据步骤104中，获取得到的OCSP证书状态查询响应信息及设备准入

查询响应信息，对该两个信息进行整合，获取到一个最终OCSP证书状态查询响应信息，将其发送至安全网关，以最终实现对安全网关的OCSP证书状态查询请求进行回应。其中，具体为对OCSP证书状态查询响应信息中的证书状态查询结果及设备准入查询响应信息中的准入查询进行封装整合形成一新的响应信息。

[0089] 上述方法中，需要分别向OCSP服务器和设备准入控制单元发送查询请求，并接收和处理查询响应结果，结合两方面的查询响应信息计算生成一最终OCSP查询响应信息，并将该最终响应信息返回给安全网关，该过程构造了一个OCSP服务器的代理角色，以响应安全网关的OCSP证书状态查询请求，该过程在结合原有的OCSP服务器查询处理过程，对OCSP证书状态查询请求进行查询处理时加入了设备准入查询过程，将基站证书的有效认证控制与对设备本身其他因素相关的设备准入控制结合起来，综合两者对基站进行准入控制，无需频繁吊销证书，避免了大量的重新申请证书的过程，实现灵活的设备准入控制，且OCSP服务器不需做出改变，仅需遵循现有技术规范即可，容易实施。

[0090] 进一步地，这里对根据OCSP证书状态查询响应信息及设备准入查询响应信息，生成最终OCSP证书状态查询响应信息的优选实施过程做出描述。

[0091] 其中，根据OCSP证书状态查询响应信息及设备准入查询响应信息，生成最终OCSP证书状态查询响应信息，包括：

[0092] 解析设备准入查询响应信息，获取设备准入查询结果；添加该设备准入查询结果至OCSP证书状态查询响应信息，根据向证书授权中心CA机构申请得到的签名证书，替换该OCSP证书状态查询响应信息的签名信息为一新的签名信息，得到最终OCSP证书状态查询响应信息。

[0093] 该过程中，需结合来自设备准入控制单元的设备准入查询结果与来自OCSP服务器的OCSP证书状态查询响应信息，重新计算以产生最终的查询响应信息。其中，重新计算生成最终OCSP查询响应信息的过程如下：首先需要向CA机构申请一张签名证书，用于签发OCSP查询响应，此处对签名证书进行一次申请即可，在OCSP证书状态查询响应信息中添加设备准入查询结果，对其进行重新封装整合。其中，在封装整合过程中，该设备准入查询结果，可以使用0、1进行表示，具体可以以0表示设备准入查询结果为不允许接入，1表示设备准入查询结果为允许接入，在得到签名证书之后，即可使用申请得到的签名证书对封装整合后的新的OCSP证书状态查询响应信息进行签名，替换原有的签名信息，该签名信息包含签名主体、签名算法等属性，以得到最终OCSP证书状态查询响应信息。

[0094] 更进一步地，其中，在上述的获取设备准入查询结果的步骤之后，该方法还包括：判断设备准入查询结果是否为不允许接入；当判断结果为是时，根据设备准入查询响应信息，获取不允许接入的产生原因；其中，在添加设备准入查询结果至OCSP证书状态查询响应信息的同时添加该产生原因至OCSP证书状态查询响应信息中。在当设备准入查询响应信息中的设备准入查询结果为不允许接入时，在最终证书状态查询响应信息中同时携带不允许接入的原因，以对安全网关侧及家庭基站侧做出提醒。

[0095] 具体地，上述的设备信息至少包括：设备名称及设备序列号，以此作为设备准入控制单元进行设备准入查询的关键字和查询依据。

[0096] 第二实施例

[0097] 如图2、图7所示，本实施例公开了另一种基于在线证书状态查询协议OCSP实现家

庭基站准入控制的方法，应用于安全网关。该方法包括：

[0098] 步骤201：发送OCSP证书状态查询请求至OCSP代理服务器。

[0099] 其中OCSP证书状态查询请求包括待验证的基站证书，且该待验证的基站证书中包括待验证家庭基站的设备信息。

[0100] 该步骤之前，安全网关需要先接收家庭基站发送的IKE_AUTH报文，从报文中解析出基站证书，根据基站证书生成OCSP证书状态查询请求。

[0101] 在步骤201过程中，发送查询请求要用到OCSP代理服务器的地址信息，基站证书中通常会携带OCSP服务器地址，但不会携带OCSP代理服务器地址。安全网关可预先配置OCSP代理服务器的地址，若基站证书中未携带OCSP代理服务器地址，则使用预先配置的OCSP代理服务器地址。在接收到家庭基站发送的IKE_AUTH报文后，从报文中解析出基站证书，然后向OCSP代理服务器发起OCSP证书状态查询请求。其中基站证书中需含有设备信息，如设备名称、设备序列号等。

[0102] 步骤202：接收所述OCSP代理服务器下发的最终OCSP证书状态查询响应信息。

[0103] 其中该最终OCSP证书状态查询响应信息为OCSP代理服务器根据从OCSP服务器接收的证书状态查询响应信息和从设备准入控制单元接收的设备准入查询响应信息生成。该最终OCSP证书状态查询响应信息中结合了基站证书的有效状态及由其他因素决定的是否允许基站接入两方面的信息。

[0104] 步骤203：根据所述最终OCSP证书状态查询响应信息，判断待验证家庭基站是否满足准入条件。

[0105] 安全网关向OCSP代理服务器发送OCSP证书状态查询请求，接收最终OCSP证书状态查询响应信息，根据最终OCSP证书状态查询响应信息中的两方面内容判断是否允许设备接入，将结果信息发送给家庭基站，设备认证流程结束。

[0106] 一般基站证书的状态分为“有效”、“未知”、“吊销”三种，该方法中，安全网关不再只针对家庭基站的基站证书的有效状态，来对家庭基站进行准入判断及控制，因此不需要总是通过吊销证书来实现禁止基站接入网络的控制过程，当因为其他因素导致基站不允许接入网络时，无需重复进行证书申请，节省时间及资源。

[0107] 具体地，其中根据最终OCSP证书状态查询响应信息，判断待验证家庭基站是否满足准入条件，包括：当最终OCSP证书状态查询响应信息中记录的待验证的基站证书处于有效状态且设备准入查询结果为允许接入时，判断该家庭基站满足准入条件。

[0108] 安全网关根据最终OCSP证书状态查询响应信息，可以获知家庭基站证书的状态信息，以及设备准入控制单元的设备准入信息，如果基站证书有效，且设备准入控制单元允许设备接入，那么安全网关继续处理并对IKE_AUTH报文进行响应，认证成功，否则设备认证失败，结束认证流程。

[0109] 第三实施例

[0110] 如图3、图7所示，本实施例公开了另一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的方法，应用于设备准入控制单元。该方法包括：

[0111] 步骤301：接收OCSP代理服务器发送的设备准入查询请求。

[0112] 该设备准入查询请求中包括：待验证家庭基站的设备信息。

[0113] 步骤302：根据所述设备信息，按预设的准入规则，对所述待验证家庭基站进行设

备准入查询并生成设备准入查询响应信息。

[0114] 该步骤中，根据接收到的设备准入查询请求中的设备信息，按预设的准入规则进行查询判断，得到设备准入查询结果，并生成设备准入查询响应信息。其中预设的准入规则可以是根据如套餐、资费等设备准入信息制定的白名单或黑名单模式，但不限于这两种模式。

[0115] 这里，主要是进行与家庭基站设备相关的由其他因素导致的准入限制的查询管理，该其他因素包括但不限于是家庭基站设备的安全性、设备的资费缴纳情况、准入时限情况等。其中，当基站设备被入侵或频繁攻击网络时，即认为该基站安全性差，通过对该家庭基站的设备信息进行记录，通过设备准入控制单元的查询得到相关准入查询结果限制其进入。

[0116] 步骤303：发送所述设备准入查询响应信息至所述OCSP代理服务器。

[0117] 该方法，可减少证书吊销需求，当基站设备被入侵或频繁攻击网络时或资费不足时，除基站证书被盗情形以外，无需吊销证书，只需要将对应的设备信息同步至设备准入控制单元，那么设备在接入认证时就会被拒绝接入；如果设备已经过修复准许接入，那么只需将修复的设备信息同步至设备准入控制单元，设备在接入认证时就可成功接入，可实现灵活的设备准入控制。基站设备无需改造，仅需遵循现有标准。

[0118] 进一步地，根据设备信息，按预设的准入规则，对待验证家庭基站进行设备准入查询并生成设备准入查询响应信息，包括：根据该设备信息，按照根据预设的准入规则设置的黑名单或白名单，对待验证家庭基站进行设备准入查询。当设备信息不存在于该黑名单或设备信息存在于该白名单中时，生成允许接入的设备准入查询响应信息；当设备信息存在于黑名单或设备信息不存在于白名单中时，生成不允许接入的设备准入查询响应信息。

[0119] 其中，如果采用白名单方式，白名单中每条记录含有设备信息、设备有效期、设备加入白名单的时间等数据，若设备准入查询请求中的设备信息在白名单中，则允许设备接入，否则不允许设备接入。如果采用黑名单方式，黑名单中每条记录含有设备信息、设备加入黑名单的时间和原因等数据，若查询请求中的设备信息在黑名单中，则不允许设备接入，否则允许设备接入。该白名单或黑名单可以根据家庭基站的具体情况进行维护更新，该更新维护可以由管理员进行或通过信息接口进行同步。

[0120] 具体地，在生成设备准入查询响应信息的步骤中，所生成的设备准入查询响应信息包括：查询响应时间、设备准入查询结果及当所述设备准入查询结果为不允许接入时的产生原因。

[0121] 具体地，上述的设备信息至少包括：设备名称及设备序列号，以此作为设备准入控制单元进行设备准入查询的关键字和查询依据。

[0122] 第四实施例

[0123] 如图4所示，本实施例中公开了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，该设备包括：第一接收模块401、第一发送模块402、第二发送模块403、第二接收模块404和生成模块405。

[0124] 第一接收模块401，用于接收安全网关发送的OCSP证书状态查询请求，其中所述OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息。

[0125] 第一发送模块402，用于发送所述OCSP证书状态查询请求至OCSP服务器。

[0126] 第二发送模块403，用于解析所述OCSP证书状态查询请求中的所述设备信息，根据所述设备信息向设备准入控制单元发送设备准入查询请求。

[0127] 第二接收模块404，用于接收所述OCSP服务器获取所述OCSP证书状态查询请求后下发的OCSP证书状态查询响应信息和接收所述设备准入控制单元获取所述设备准入查询请求后下发的设备准入查询响应信息。

[0128] 生成模块405，用于根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息，生成最终OCSP证书状态查询响应信息并发送至所述安全网关。

[0129] 其中，该生成模块405，用于：解析所述设备准入查询响应信息，获取设备准入查询结果；添加所述设备准入查询结果至所述OCSP证书状态查询响应信息，根据向证书授权中心CA机构申请得到的签名证书，替换所述OCSP证书状态查询响应信息的签名信息为一新的签名信息，得到最终OCSP证书状态查询响应信息。

[0130] 其中，该生成模块405，还用于：判断所述设备准入查询结果是否为不允许接入；当判断结果为是时，根据所述设备准入查询响应信息，获取不允许接入的产生原因；其中，在所述添加所述设备准入查询结果至所述OCSP证书状态查询响应信息的步骤中，同时添加所述产生原因至所述OCSP证书状态查询响应信息中。

[0131] 其中，该设备信息至少包括：设备名称及设备序列号。

[0132] 上述设备，需要分别向OCSP服务器和设备准入控制单元发送查询请求，并接收和处理查询响应结果，结合两方面的查询响应信息计算生成一最终OCSP查询响应信息，并将该最终响应信息返回给安全网关，该过程构造了一个OCSP服务器的代理角色，以响应安全网关的OCSP证书状态查询请求，该设备在结合原有的OCSP服务器查询处理过程，对OCSP证书状态查询请求进行查询处理时加入了设备准入查询过程，将基站证书的有效认证控制与对设备本身其他因素相关的设备准入控制结合起来，综合两者对基站进行准入控制，无需频繁吊销证书，避免了大量的重新申请证书的过程，实现灵活的设备准入控制，且OCSP服务器不需做出改变，仅需遵循现有技术规范即可，容易实施。

[0133] 本实施例中所涉及的基于OCSP实现家庭基站准入控制的设备具体为OCSP代理服务器。

[0134] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的设备的具体工作过程，可以参考前述方法实施例中第一实施例的对应过程，在此不再赘述。

[0135] 第五实施例

[0136] 如图5所示，本实施例中公开了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，该设备包括：第三发送模块501、第三接收模块502和判断模块503。

[0137] 第三发送模块501，用于发送OCSP证书状态查询请求至OCSP代理服务器，其中所述OCSP证书状态查询请求包括待验证的基站证书，且所述基站证书中包括待验证家庭基站的设备信息。

[0138] 第三接收模块502，用于接收所述OCSP代理服务器下发的最终OCSP证书状态查询响应信息，其中所述最终OCSP证书状态查询响应信息为所述OCSP代理服务器根据从所述OCSP服务器接收的证书状态查询响应信息和从设备准入控制单元接收的设备准入查询响应信息生成。

[0139] 判断模块503，用于根据所述最终OCSP证书状态查询响应信息，判断待验证家庭基站是否满足准入条件。

[0140] 其中，该判断模块503，用于：当所述最终OCSP证书状态查询响应信息中记录的待验证的基站证书处于有效状态且设备准入查询结果为允许接入时，判断所述家庭基站满足准入条件。

[0141] 本实施例中所涉及的基于OCSP实现家庭基站准入控制的设备具体为安全网关。

[0142] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的设备的具体工作过程，可以参考前述方法实施例中第二实施例的对应过程，在此不再赘述。

[0143] 第六实施例

[0144] 如图6所示，本实施例中公开了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的设备，该设备包括：第四接收模块601、查询处理模块602和第四发送模块603。

[0145] 第四接收模块601，用于接收OCSP代理服务器发送的设备准入查询请求，所述设备准入查询请求中包括：待验证家庭基站的设备信息。

[0146] 查询处理模块602，用于根据所述设备信息，按预设的准入规则，对所述待验证家庭基站进行设备准入查询并生成设备准入查询响应信息。

[0147] 第四发送模块603，用于发送所述设备准入查询响应信息至所述OCSP代理服务器。

[0148] 其中，该查询处理模块602，用于：根据所述设备信息，按照根据所述预设的准入规则设置的黑名单或白名单，对所述待验证家庭基站进行设备准入查询；当所述设备信息不存在于所述黑名单或所述设备信息存在于所述白名单中时，生成允许接入的设备准入查询响应信息；当所述设备信息存在于所述黑名单或所述设备信息不存在于所述白名单中时，生成不允许接入的设备准入查询响应信息。

[0149] 其中，查询处理模块602所生成的设备准入查询响应信息包括：查询响应时间、设备准入查询结果及当所述设备准入查询结果为不允许接入时的产生原因。

[0150] 本实施例中所涉及的基于OCSP实现家庭基站准入控制的设备具体为设备准入控制单元。

[0151] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的设备的具体工作过程，可以参考前述方法实施例中第三实施例的对应过程，在此不再赘述。

[0152] 本发明还公开了一种基于在线证书状态查询协议OCSP实现家庭基站准入控制的系统，该系统包括：如第四实施例中所述的基于OCSP实现家庭基站准入控制的设备、如第五实施例中所述的基于OCSP实现家庭基站准入控制的设备及如本实施例中所述的基于OCSP实现家庭基站准入控制的设备。

[0153] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

[0154] 以上所述的是本发明的优选实施方式，应当指出对于本技术领域的普通人员来

说,在不脱离本发明所述的原理前提下还可以作出若干改进和润饰,这些改进和润饰也在本发明的保护范围内。

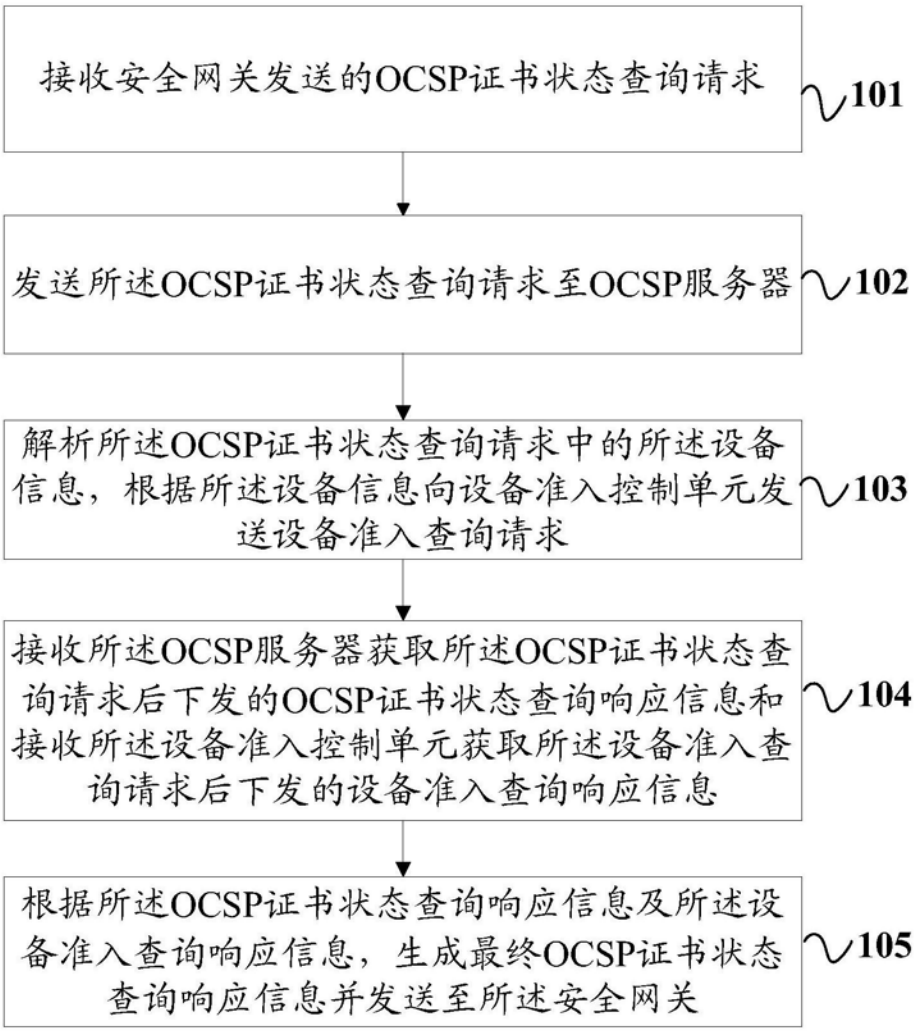

接收安全网关发送的OCSP证书状态查询请求
101
发送所述OCSP证书状态查询请求至OCSP服务器
102
解析所述OCSP证书状态查询请求中的所述设备信息，根据所述设备信息向设备准入控制单元发送设备准入查询请求
103
接收所述OCSP服务器获取所述OCSP证书状态查询请求后下发的OCSP证书状态查询响应信息和接收所述设备准入控制单元获取所述设备准入查询请求后下发的设备准入查询响应信息
104
根据所述OCSP证书状态查询响应信息及所述设备准入查询响应信息，生成最终OCSP证书状态查询响应信息并发送至所述安全网关
105

图1

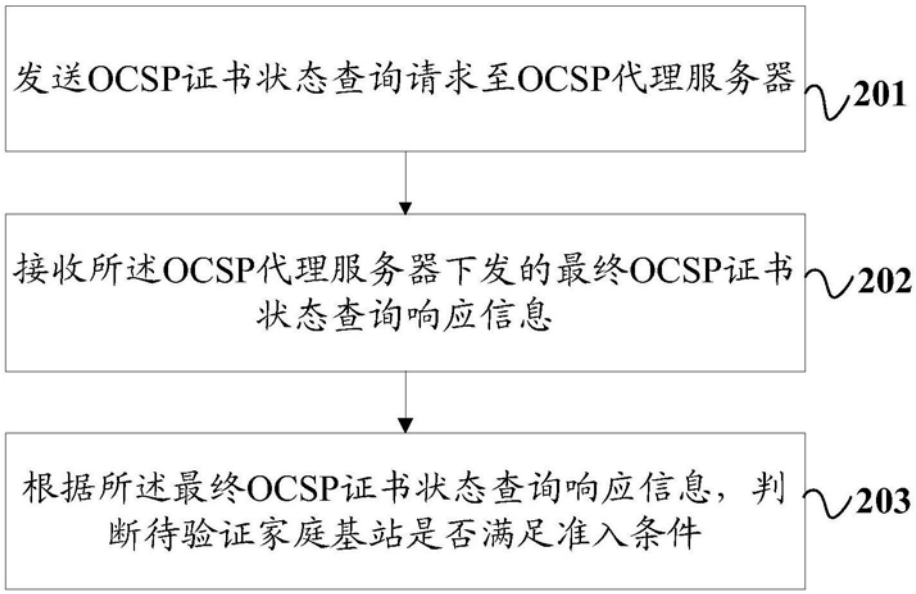

发送OCSP证书状态查询请求至OCSP代理服务器
201
接收所述OCSP代理服务器下发的最终OCSP证书状态查询响应信息
202
根据所述最终OCSP证书状态查询响应信息，判断待验证家庭基站是否满足准入条件
203

图2

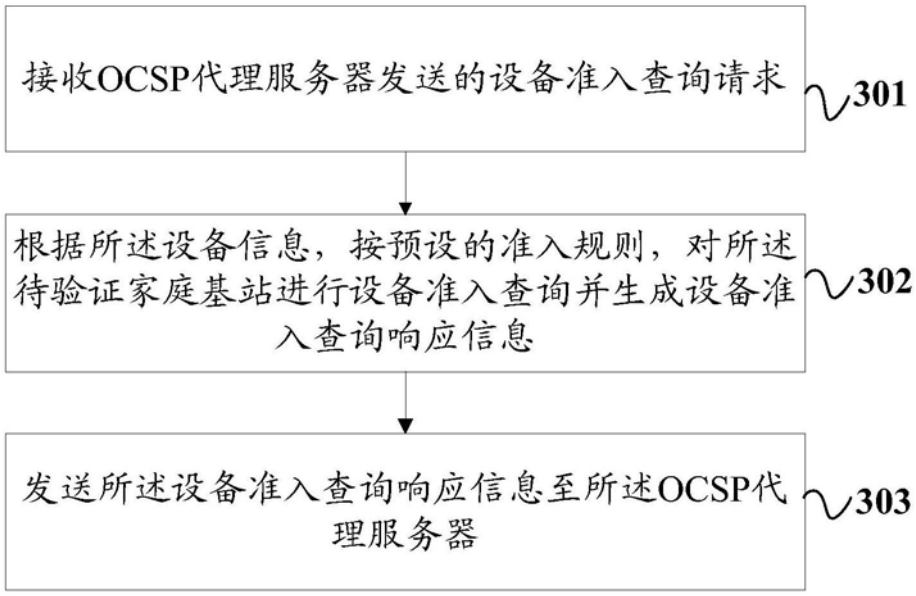

接收OCSP代理服务器发送的设备准入查询请求
301
根据所述设备信息，按预设的准入规则，对所述待验证家庭基站进行设备准入查询并生成设备准入查询响应信息
302
发送所述设备准入查询响应信息至所述OCSP代理服务器
303

图3

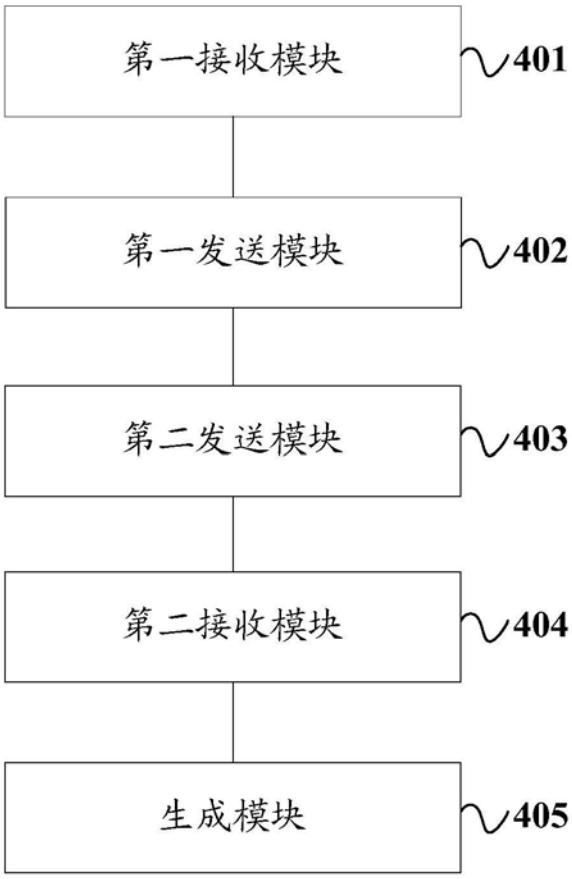

第一接收模块
401
第一发送模块
402
第二发送模块
403
第二接收模块
404
生成模块
405

图4

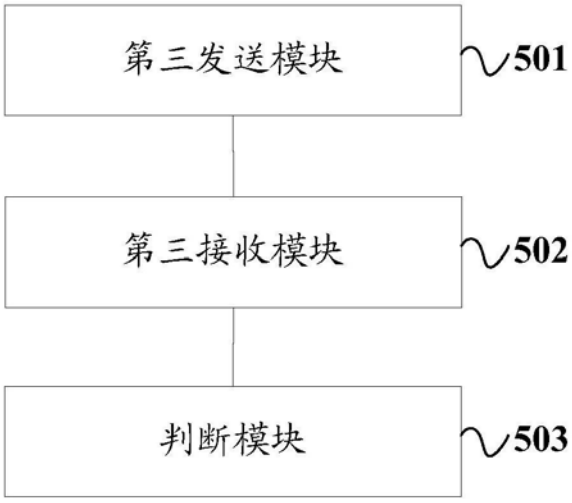

第三发送模块
501
第三接收模块
502
判断模块
503

图5

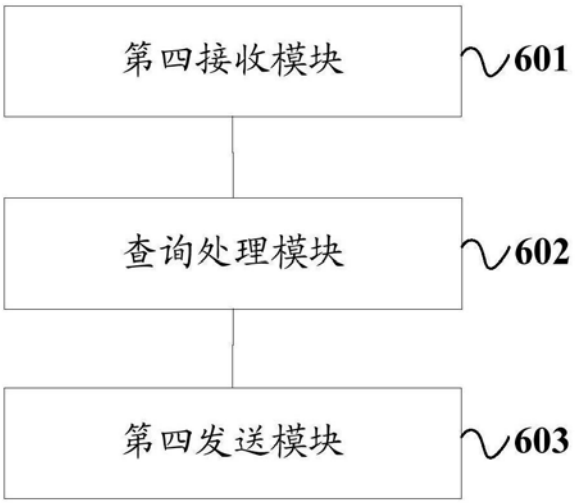

第四接收模块
601
查询处理模块
602
第四发送模块
603

图6

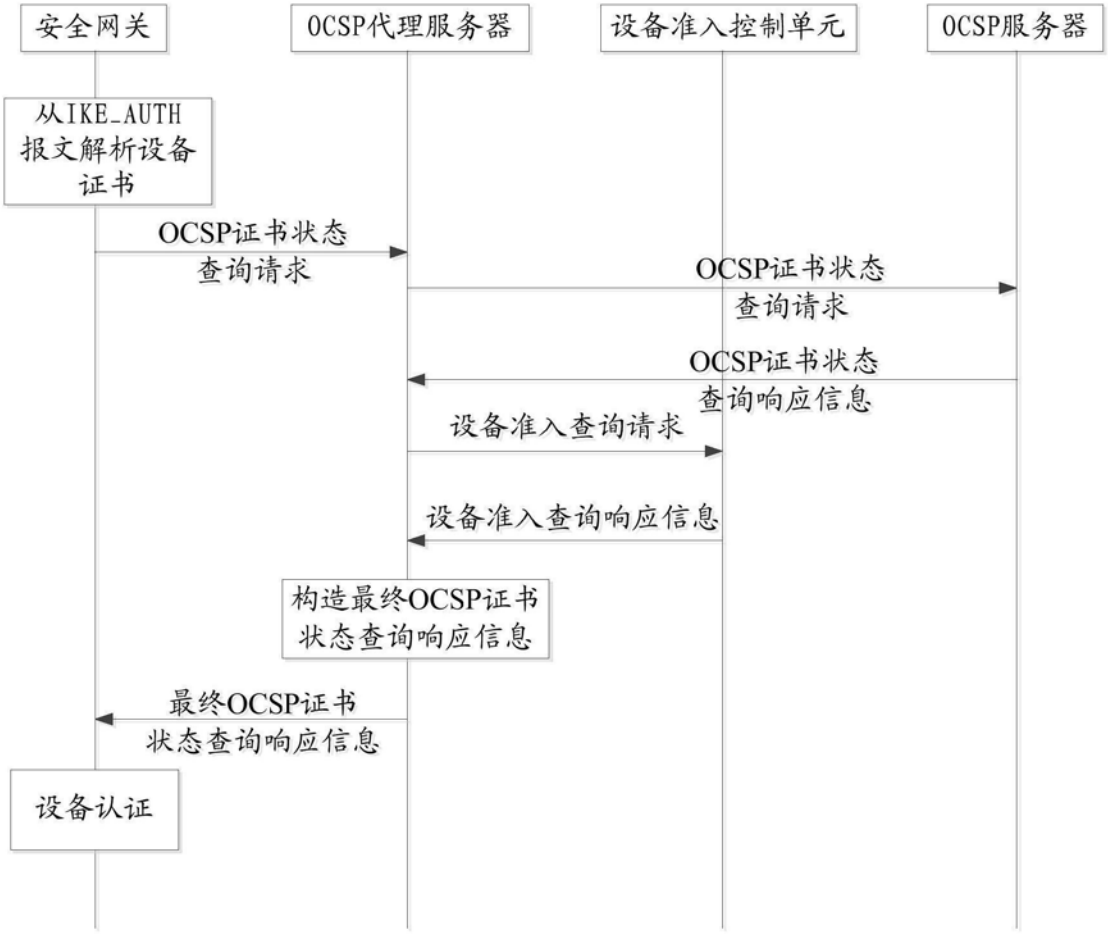

安全网关
OCSP代理服务器
设备准入控制单元
OCSP服务器
从IKE_AUTH报文解析设备证书
OCSP证书状态查询请求
OCSP证书状态查询请求
OCSP证书状态查询响应信息
设备准入查询请求
设备准入查询响应信息
构造最终OCSP证书状态查询响应信息
最终OCSP证书状态查询响应信息
设备认证

图7