(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 106533659 A
(43)申请公布日 2017.03.22

(21)申请号 201510582456.8

(22)申请日 2015.09.14

(71)申请人 北京中质信维科技有限公司
地址 100088 北京市海淀区马甸东路7号9号楼4层412室、428、429室
申请人 国家质量监督检验检疫总局信息中心
北京明朝万达科技股份有限公司

(72)发明人 于毅 王志海 李宣 邢双秋 孙飞 喻波 廖黄河

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

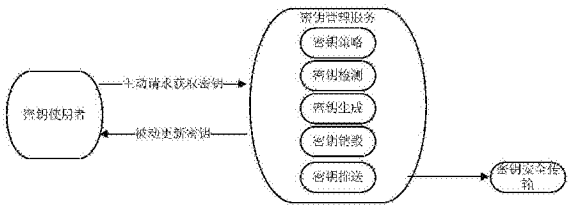
权利要求书2页 说明书5页 附图4页

(54)发明名称

一种密钥更新方法和系统

(57)摘要

本发明公开了一种密钥更新方法和系统，该系统包括：密钥管理服务端，用于配置安全通道密钥策略，实现对密钥的管理；终端，将所述密钥加载于安全通道中，实现安全通信；其中，所述密钥管理服务端根据所述安全通道密钥策略实时检测所述密钥是否失效，如果所述密钥失效，则生成新密钥，并将所述新密钥加密签名后生成的密钥数据推送给所述终端；所述终端等待接收所述密钥数据，签名验证，并解密后得到所述新密钥，启动所述新密钥，在安全通道中启用所述新密钥。



CN 106533659 A

1. 一种密钥更新方法，该方法包括如下步骤：

1) 密钥管理服务端实时对使用的密钥进行检测；

2) 判断所述密钥是否有效；

3) 如果有效，返回步骤 1)，否则生成新密钥；

4) 将生成的所述新密钥发送给通道服务和终端；

5) 所述通道服务和终端协商所述新密钥；

6) 在安全通道中启用所述新密钥；

7) 销毁旧密钥。

2. 根据权利要求 1 所述的方法，所述步骤 4) 中使用所述终端的公钥对所述新密钥进行加密，同时使用所述密钥管理服务端的私钥对包含经加密的新密钥的密钥数据进行签名。

3. 根据权利要求 2 所述的方法，所述步骤 6) 中启用所述新密钥之前：使用所述密钥管理服务端的所述私钥对接收的所述密钥数据进行验证签名，验证通过后使用所述终端的私钥解密所述密钥数据。

4. 根据权利要求 1 所述的方法，在所述步骤 1) 之前所述终端需要根据身份凭证进行登录，登录成功之后才能获得所述密钥，并开启所述通道服务。

5. 一种密钥更新方法，该方法包括如下步骤：

1) 终端对实时使用的密钥进行检测；

2) 判断所述密钥是否有效；

3) 如果有效，返回到步骤 1)，否则向密钥管理服务端请求新密钥；

4) 所述密钥管理服务端判断是否存在所述新密钥；

5) 如果存在所述新密钥，则向通道服务和所述终端发送所述新密钥；

6) 否则生成所述新密钥，然后向所述通道服务和所述终端发送所述新密钥；

7) 所述通道服务和所述终端协商使用所述新密钥；

8) 在安全通道中启用新密钥；

9) 销毁旧密钥。

6. 根据权利要求 5 所述的方法，所述步骤 5)-6) 中使用所述终端的公钥对所述新密钥进行加密，同时使用所述密钥管理终端的私钥对包含经加密的新密钥的密钥数据进行签名。

7. 根据权利要求 6 所述的方法，所述步骤 8) 中启用所述新密钥之前：使用所述密钥管理服务端的所述私钥对接收的所述密钥数据进行验证签名，验证通过后使用所述终端的私钥解密所述密钥数据。

8. 一种密钥更新系统，该系统包括：

密钥管理服务端，用于配置安全通道密钥策略，实现对密钥的管理；

终端，将所述密钥加载于安全通道中，实现安全通信；

其中，所述密钥管理服务端根据所述安全通道密钥策略实时检测所述密钥是否失效，如果所述密钥失效，则生成新密钥，并将所述新密钥加密签名后生成的密钥数据推送给所述终端；

所述终端等待接收所述密钥数据，签名验证，并解密后得到所述新密钥，启动所述新密钥，在安全通道中启用所述新密钥。

9. 根据权利要求 8 所述的系统，所述密钥管理服务端使用所述终端的公钥对所述新密钥进行加密，同时使用所述密钥管理终端的私钥对加密后的新密钥数据进行签名，生成所述密钥数据；

所述终端启用所述新密钥之前：使用所述密钥管理服务端的所述私钥对接收的所述密钥数据进行验证签名，验证通过后使用终端的私钥解密所述密钥数据。

10. 根据权利要求 8 或 9 所述的系统，所述终端端登录成功之后，依据身份凭证获取对应的所述密钥，并开启通道服务，如果客户端没有登录或登录失败，则无法获取所述密钥。

一种密钥更新方法和系统

技术领域

[0001] 本发明涉及一种网络安全领域，尤其涉及一种网络通信中的密钥更新方法和系统。

背景技术

[0002] 随着国家信息化建设的不断推进，对信息安全提出了更高的要求，在信息安全方面除了采取必要的保护措施和相关的法规、政策外，努力掌握核心技术则更为重要。在保证像信息的机密性、真实性、完整性这些必要的信息安全中，公钥加密技术扮演着非常重要的角色。为了增强互联网的安全机制，主要采用防火墙技术、公开密钥加密技术、数据加密技术、数字签名、数字时间戳技术、身份认证和安全协议等。

[0003] 移动网络安全接入需提供移动终端与接入设备之间的数据传输加密功能。移动终端安全组件在收到上层应用传输请求数据时，通过算法加密数据传输到接入设备，接入设备解密数据转发给后台应用；后台应用接收请求返回响应，接入设备对响应结果进行加密转发给移动终端安全组件，安全组件解密响应数据反馈给上层应用。

[0004] 通过安全组件的密码传输协议形成加密数据并传输，达到一包一密，防重放、可校验的安全要求。完全支持使用国家保密局认可的算法进行加密，并具有商用密码产品资质。

[0005] 目前市场上针对网络传输数据的保护，主要采用端对端的密钥协商机制，通过协商达到两端密钥一致，使用协商好的相同密钥进行传输数据安全加密，另一端安全解密。

[0006] 现有的技术主要是由客户端主动向服务器端获取密钥，并且对密钥的有效期和长度限定灵活性不足。

[0007] 附图 1 是现有技术中的密钥分发方案。

[0008] 该密钥更新机制首先由密钥使用者主动发起获取或更新密钥请求包给密钥管理服务提供者，提供者校验发起者身份合法后，根据密钥配置策略生成密钥；将密钥使用对称算法加密，然后组成密钥响应包将密钥返回给密钥使用者。

[0009] 上述技术密钥更新主要依靠使用方主动发起，对密钥安全控制措施较弱，并且在密钥安全传输上安全性较弱。

[0010] 本发明中安全通道密钥的使用和分发并不是保护重点，重点是提出通信密钥根据策略实时更新机制。此机制将 PKI 安全技术与推送技术结合，实现通信密钥安全可靠即时更新。

发明内容

[0011] 为了解决现有技术中密钥更新主要依靠使用方主动发起，对密钥安全控制措施较弱，并且在密钥安全传输上安全性较弱的安全问题，本发明公开了一种实施方式，具体为：

[0012] 一种密钥更新方法，该方法包括如下步骤：

[0013] 1) 密钥管理服务端实时对使用的密钥进行检测；

[0014] 2) 判断所述密钥是否有效；

[0015] 3) 如果有效，返回步骤 1)，否则生成新密钥；

[0016] 4) 将生成的所述新密钥发送给通道服务和终端；

[0017] 5) 所述通道服务和终端协商所述新密钥；

[0018] 6) 在安全通道中启用所述新密钥；

[0019] 7) 销毁旧密钥。

[0020] 进一步，所述步骤 4) 中使用所述终端的公钥对所述新密钥进行加密，同时使用所述密钥管理终端的私钥对包含经加密的新密钥的密钥数据进行签名。

[0021] 进一步，所述步骤 6) 中启用所述新密钥之前：使用所述密钥管理服务端的所述私钥对接收的所述密钥数据进行验证签名，验证通过后使用所述终端的私钥解密所述密钥数据。

[0022] 进一步，在所述步骤 1) 之前所述终端需要根据身份凭证进行登录，登录成功之后才能获得所述密钥，并开启所述通道服务。

[0023] 为解决上述技术问题，本发明还公开了另一实施方式，具体为：

[0024] 一种密钥更新方法，该方法包括如下步骤：

[0025] 1) 终端对实时使用的密钥进行检测；

[0026] 2) 判断所述密钥是否有效；

[0027] 3) 如果有效，返回到步骤 1)，否则向密钥管理服务端请求新密钥；

[0028] 4) 所述密钥管理服务端判断是否存在所述新密钥；

[0029] 5) 如果存在所述新密钥，则向通道服务和所述终端发送所述新密钥；

[0030] 6) 否则生成所述新密钥，然后向所述通道服务和所述终端发送所述新密钥；

[0031] 7) 所述通道服务和所述终端协商使用所述新密钥；

[0032] 8) 在安全通道中启用新密钥；

[0033] 9) 销毁旧密钥。

[0034] 进一步，所述步骤 5)-6) 中使用所述终端的公钥对所述新密钥进行加密，同时使用所述密钥管理终端的私钥对包含经加密的新密钥的密钥数据进行签名。

[0035] 进一步，所述步骤 8) 中启用所述新密钥之前：使用所述密钥管理服务端的所述私钥对接收的所述密钥数据进行验证签名，验证通过后使用所述终端的私钥解密所述密钥数据。

[0036] 为解决上述技术问题，本发明还公开了另一实施方式，具体为：

[0037] 一种密钥更新系统，该系统包括：

[0038] 密钥管理服务端，用于配置安全通道密钥策略，实现对密钥的管理；

[0039] 终端，将所述密钥加载于安全通道中，实现安全通信；

[0040] 其中，所述密钥管理服务端根据所述安全通道密钥策略实时检测所述密钥是否失效，如果所述密钥失效，则生成新密钥，并将所述新密钥加密签名后生成的密钥数据推送给所述终端；

[0041] 所述终端等待接收所述密钥数据，签名验证，并解密后得到所述新密钥，启动所述新密钥，在安全通道中启用所述新密钥。

[0042] 进一步，所述密钥管理服务端使用所述终端的公钥对所述新密钥进行加密，同时使用所述密钥管理终端的私钥对加密后的新密钥数据进行签名，生成所述密钥数据；

[0043] 所述终端启用所述新密钥之前：使用所述密钥管理服务端的所述私钥对接收的所述密钥数据进行验证签名，验证通过后使用终端的私钥解密所述密钥数据。

[0044] 进一步，所述终端端登录成功之后，依据身份凭证获取对应的所述密钥，并开启通道服务，如果客户端没有登录或登录失败，则无法获取所述密钥。

[0045] 通过本发明提出的方案，取得了以下技术效果：

[0046] 根据策略配置，控制密钥更新灵活性，不同的角色采用不同的密钥策略，并确保策略实时更新到终端，提高网络数据传输的安全性。

附图说明

[0047] 图 1 是现有技术中密钥更新架构图。

[0048] 图 2 是本发明的密钥更新架构图。

[0049] 图 3 是本发明的密钥安全传输流程图。

[0050] 图 4 是本发明的密钥下发流程图。

[0051] 图 5 是本发明的密钥主动更新流程图。

具体实施方式

[0052] 图 2 是本发明的密钥更新架构图。

[0053] 密钥使用者可以主动向密钥管理服务端请求更新密钥，也可以由密钥管理服务端向密钥使用者推送更新的密钥，管理管理服务端主要包括以下功能：密钥更新策略，密钥有效检测，新密钥生成，旧密钥销毁，新密钥的推送。所述的密钥使用者可以为网络移动终端等各种密钥使用终端，而密钥管理服务端可以为密钥管理服务器，鉴权中心等设施。

[0054] 附图 3 是本发明的密钥安全传输流程图。

[0055] 密钥安全传输流程如下：

[0056] 密钥管理服务端获取密钥请求者的证书公钥；使用密钥请求者的证书公钥加密密钥，再对密钥加密数据信息使用密钥管理服务端证书私钥进行私钥签名；

[0057] 将公钥加密数据和私钥签名数据进行组成响应包，然后发送给密钥请求者；

[0058] 请求者接收到响应包后使用密钥管理服务端证书进行验证签名，再使用密钥请求者的私钥进行私钥解密；

[0059] 获取解密后的密钥，将密钥加载到安全通道中。

[0060] 也就是说，无论是密钥管理服务端向密钥使用者主动推送更新的密钥，还是密钥请求者主动向密钥管理服务端请求新的密钥，都会通过上述密钥安全传输流程传输更新密钥，以保证更新密钥的安全。

[0061] 附图 4 是是密钥管理服务端向密钥使用者主动推送更新密钥的流程图。

[0062] 密钥下发流程如下：

[0063] 密钥管理服务端实时检测密钥是否过期；如果过期则生成新的密钥；

[0064] 将新的密钥采用密钥安全传输流程下发到通道服务和终端（密钥使用者）；

[0065] 通道服务和终端双方协商确认新密钥启用；

[0066] 新密钥启用后，将密钥加载到安全通道中，密钥管理服务端和终端（密钥使用者）销毁旧密钥。

[0067] 附图 5 是终端（密钥使用者）主动请求更新密钥的流程图。

[0068] 密钥主动更新流程如下：

[0069] 终端（密钥使用者）实时检测密钥是否过期；如果过期则向密钥管理服务端发送密钥更新请求；

[0070] 密钥管理服务接收请求后，判断在服务器端是否存在新的密钥，如果没有，则创建新的密钥；

[0071] 将新的密钥采用密钥安全传输流程下发到通道服务和终端（密钥使用者）；

[0072] 通道服务和终端双方协商确认新密钥启用；

[0073] 新密钥启用后，将密钥加载到安全通道中，密钥管理服务端和终端（密钥使用者）销毁旧密钥。

[0074] 技术实现过程中主要涉及以下几个关键技术：

[0075] 1) 密钥策略：密钥策略配置与解析

[0076] 负责设置密钥有效期、密钥长度、复杂度等配置，负责密钥策略按照用户、角色进行分发。

[0077] 2) 密钥推送：密钥实时推送

[0078] 为了保证密钥能即时生效，提供新密钥实时推送。

[0079] 3) 安全通道：安全通道服务管理

[0080] 提供安全通道服务，密钥实时更新加载。

[0081] 4) 身份认证：客户端身份信息验证

[0082] 客户端登录成功之后，依据身份凭证获取对应的安全通道加密密钥。如果客户端没有登录或登录失败，则无法开启通道服务。

[0083] 5) 终端加解密模块

[0084] 为了保护数据，用户发出的数据经过终端加密模块进行加密，加密后的数据在公网上传输后到达安全网关，安全网关使用解密模块进行解密。

[0085] 为了保护安全通道密钥在网络中传输的安全，在密钥管理服务端生成安全通道密钥时，将安全通道密钥采用用户证书进行加密并签名；将加密数据签名后的数据传送给终端，终端接收后先使用密钥管理服务的证书进行验证签名，在使用用户私钥进行解密操作，获取安全通道密钥数据。

[0086] 附图 6 是将本发明的密钥更新方案用于 VPN 网络时的一个实施例。

[0087] 部署安全方案后，首先在 VPN 安全网关策略模块中配置安全通道密钥策略，配置密钥长度、有效期、复杂度等信息。

[0088] VPN 客户端登录进行身份认证，身份认证成功后，在 VPN 网关生成安全通道密钥数据，将密钥数据采用登录用户证书进行加密，并采用 VPN 网关密钥证书进行签名；然后将签名数据发送到 VPN 客户端。

[0089] VPN 客户端接收到数据后，先使用网关证书对数据进行验证签名，在使用登录用户证书私钥进行解密，获取解密后的安全通道密钥；将安全通道密钥加载到安全通道模块，要加密的数据就采用此密钥进行加解密操作。

[0090] 网关密钥管理服务在后台实时检测用户密钥是否失效，如果密钥失效，则生成新的密钥，通过推送模块，推送给 VPN 客户端；另外同时 VPN 客户端密钥管理模块在后台等待

接收新密钥并加载到安全通道服务。

[0091] 通过本发明的实施例，可以实现根据策略配置，控制密钥更新灵活性，不同的角色采用不同的密钥策略，并确保策略实时更新到终端，提高网络数据传输的安全性。。

[0092] 以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换以及改进等，均应保护在本发明的保护范围之内。

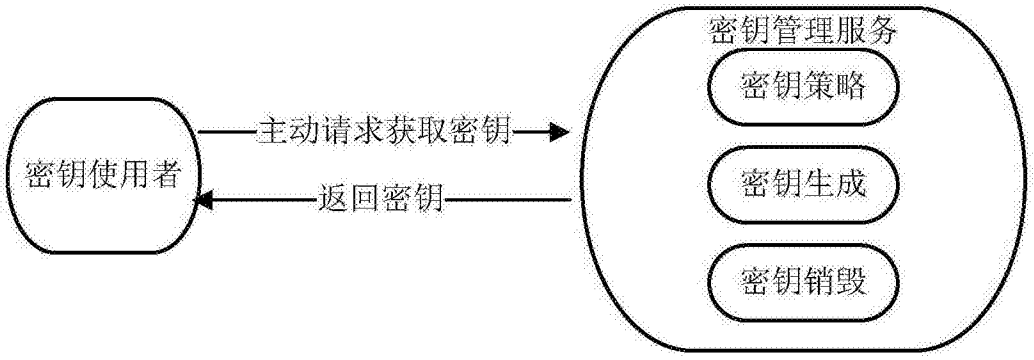

密钥管理服务
密钥策略
密钥生成
密钥销毁
密钥使用者
主动请求获取密钥
返回密钥

图 1

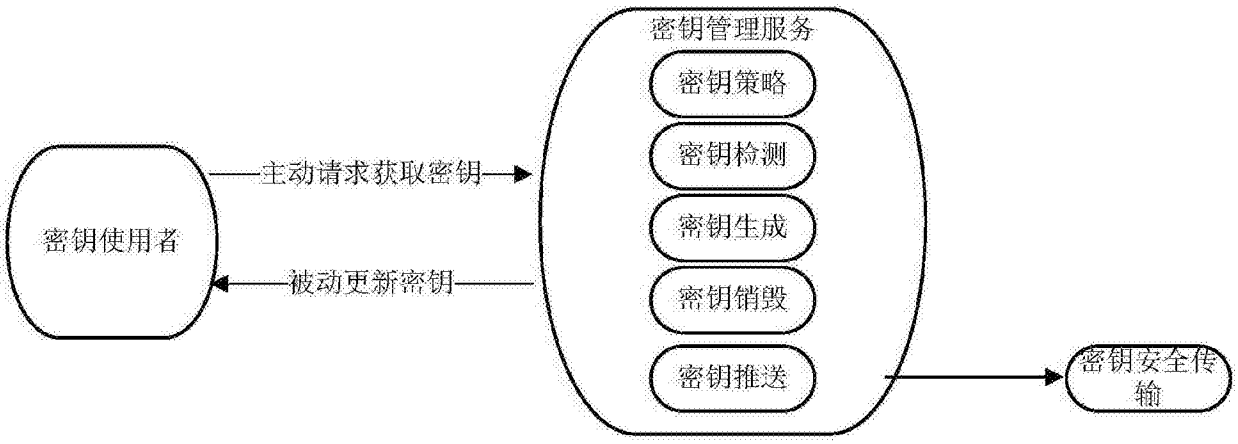

密钥管理服务
密钥策略
密钥检测
密钥生成
密钥销毁
密钥推送
密钥安全传输
密钥使用者
主动请求获取密钥
被动更新密钥

图 2

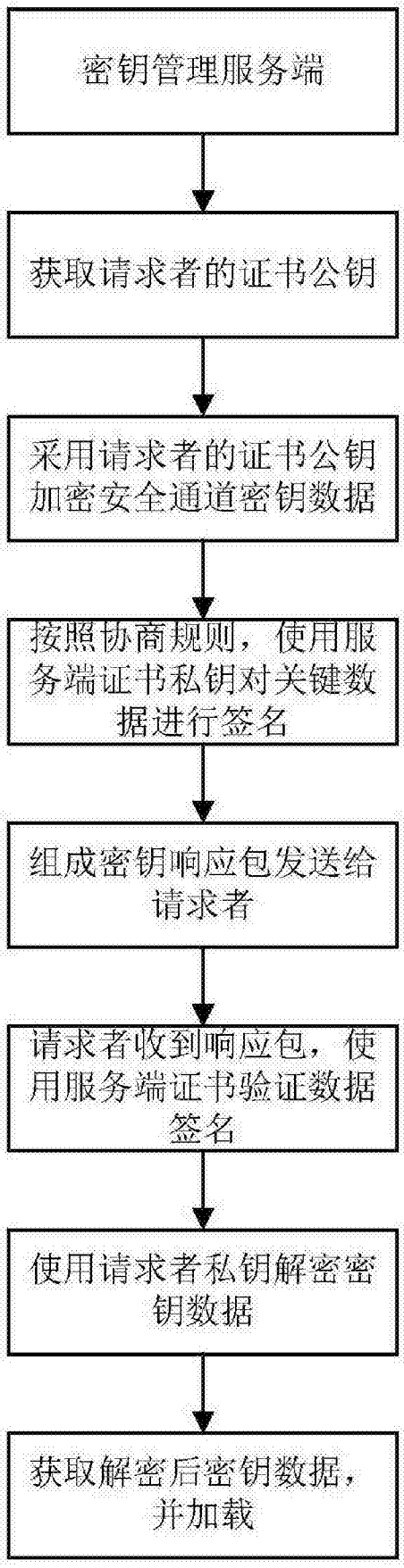

密钥管理服务端
获取请求者的证书公钥
采用请求者的证书公钥加密安全通道密钥数据
按照协商规则，使用服务端证书私钥对关键数据进行签名
组成密钥响应包发送给请求者
请求者收到响应包，使用服务端证书验证数据签名
使用请求者私钥解密密钥数据
获取解密后密钥数据，并加载

图 3

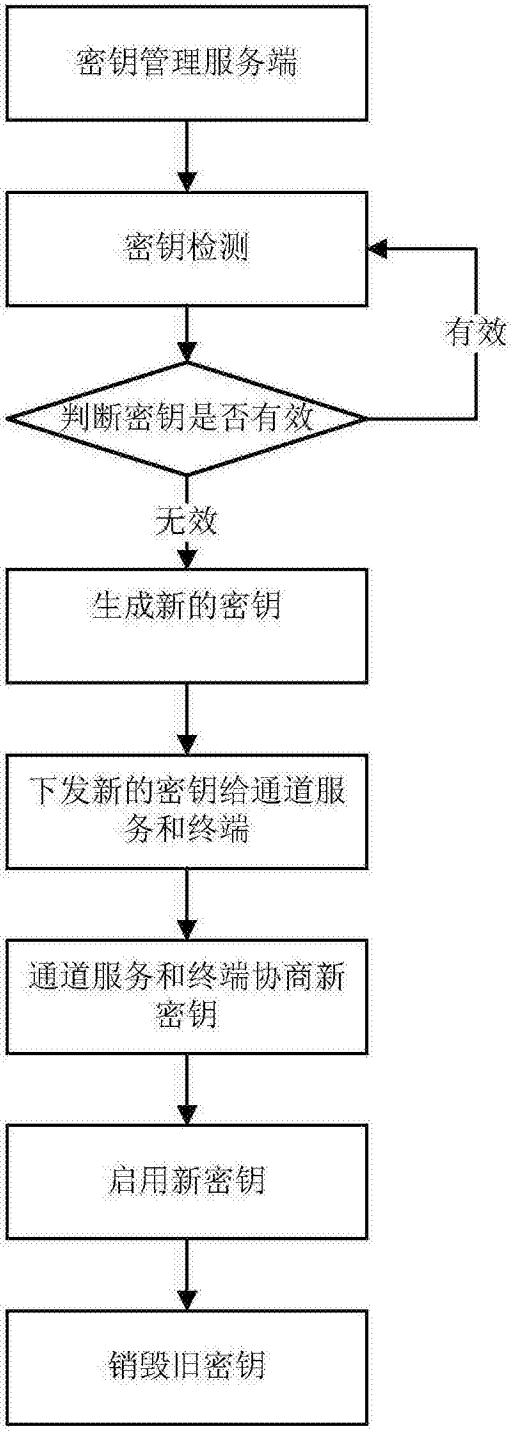

密钥管理服务端
密钥检测
有效
判断密钥是否有效
无效
生成新的密钥
下发新的密钥给通道服务和终端
通道服务和终端协商新密钥
启用新密钥
销毁旧密钥

图 4

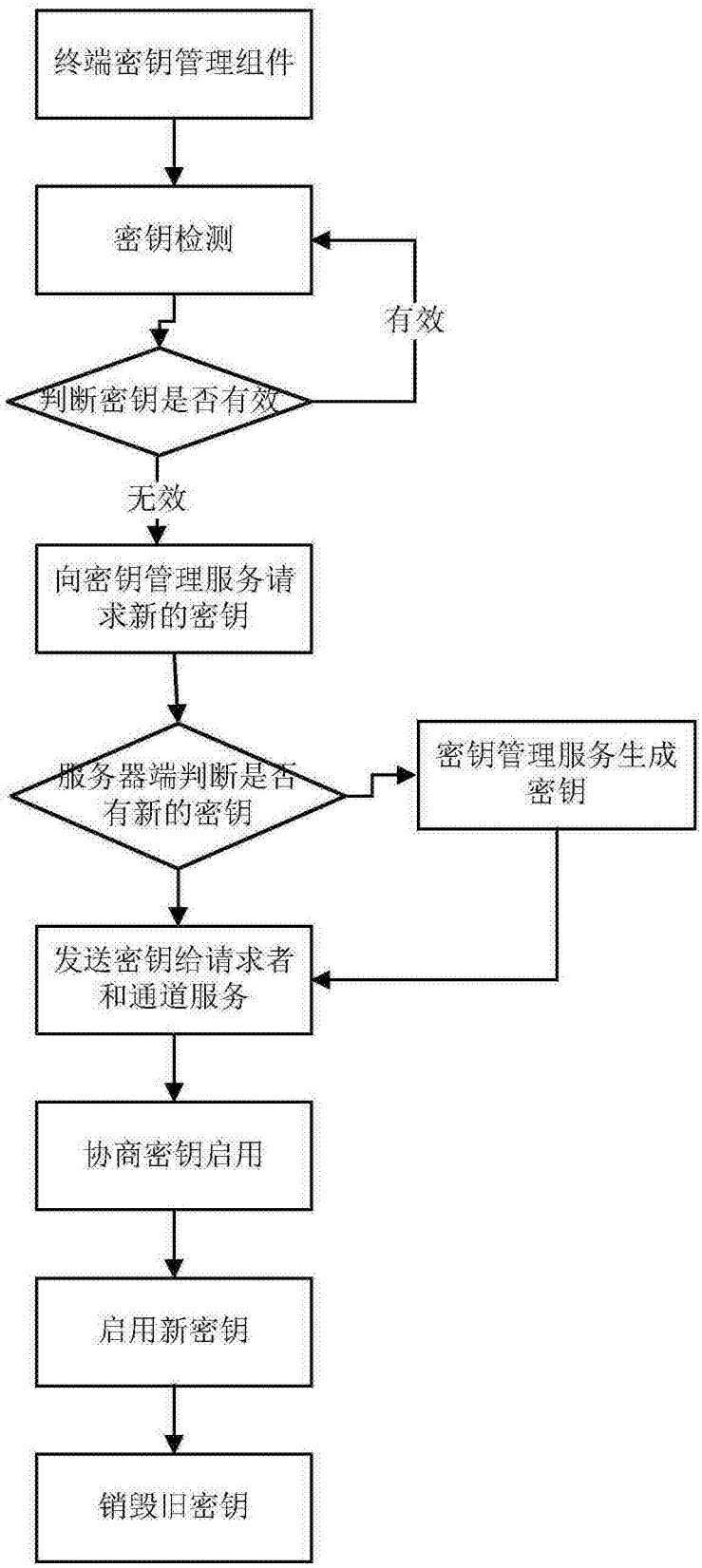

终端密钥管理组件
密钥检测
有效
判断密钥是否有效
无效
向密钥管理服务请求新的密钥
服务器端判断是否有新的密钥
密钥管理服务生成密钥
发送密钥给请求者和通道服务
协商密钥启用
启用新密钥
销毁旧密钥

图 5

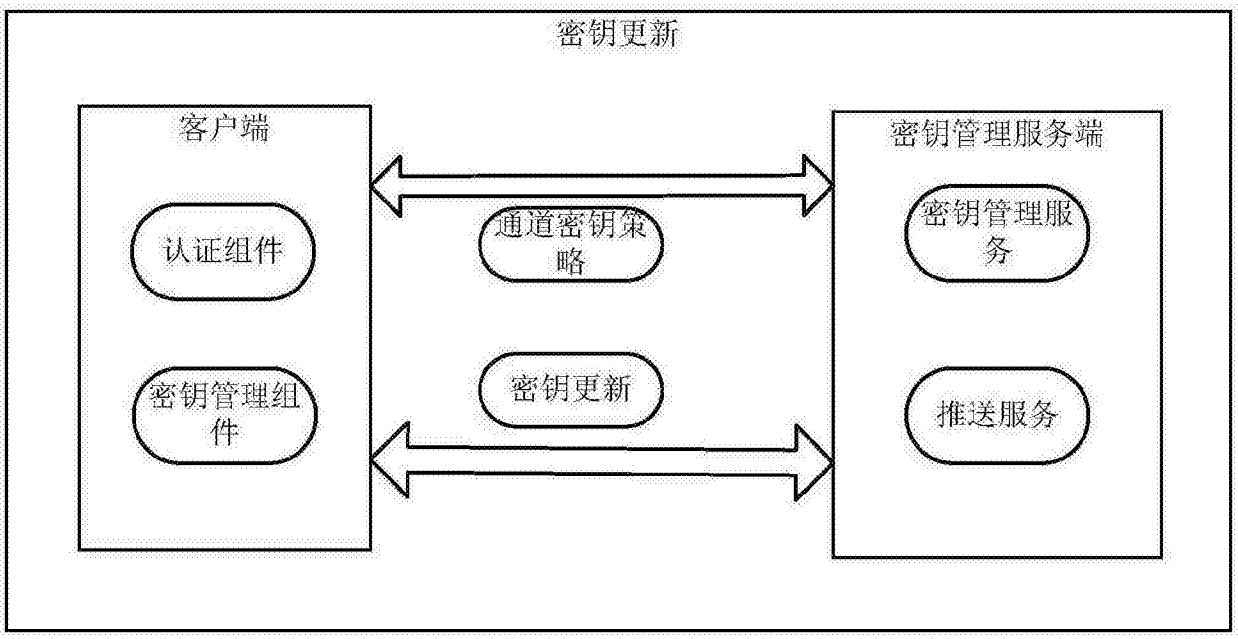


图 6