(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 101997880 A
(43)申请公布日 2011.03.30

(21)申请号 201010569400.6

(22)申请日 2010.12.01

(71)申请人 湖南智源信息网络技术开发有限公司
地址 100007 北京市东城区东直门南大街 1 号来福士中心办公楼 9 层

(72)发明人 王伟

(74)专利代理机构 隆天国际知识产权代理有限公司 72003
代理人 张浴月 刘文意

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

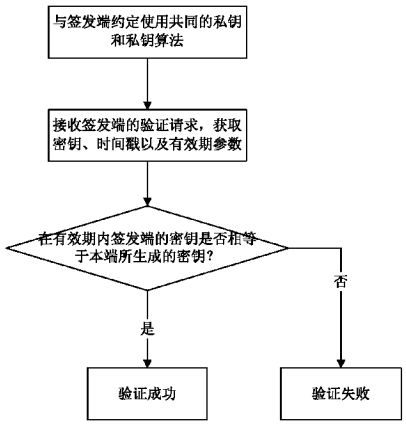
权利要求书 2 页 说明书 7 页 附图 4 页

(54)发明名称

一种用于网络页面或接口的安全验证方法及其装置

(57)摘要

本发明公开了一种用于网络页面或接口的安全验证方法及装置，所述方法为：授权给发起页面或接口验证请求的签发端使用共同的私钥、私钥的更新周期、更新计划以及私钥算法；接收所述签发端的参数，获取所述签发端的密钥参数、时间戳参数以及有效期参数；根据所述获取的密钥参数、时间戳参数以及有效期参数，在所述验证请求的有效期内采用所述共同的私钥和私钥算法进行运算，并将运算结果与所述签发端的密钥参数进行比较，若相同，则表明验证成功，否则返回验证失败。本发明能够实现了在互信验证的两端唯一可信的通信传输，并且满足通用性。



CN 101997880 A

1. 一种用于网络页面或接口的安全验证方法，其特征在于，所述方法为：

S1：与给发起页面或接口验证请求的签发端约定使用共同的私钥、私钥的更新周期、更新计划以及私钥算法；

S2：接收所述签发端的验证请求，获取所述签发端的密钥参数、时间戳参数以及有效期参数，其中所述密钥参数是所述签发端使用所述共同的私钥算法对其私钥进行运算所生成的密钥，所述时间戳参数标注有所述签发端发起验证请求的时间，其中所述有效期参数标注有所述签发端发起验证请求的最大有效期；

S3：根据所述获取的密钥参数、时间戳参数以及有效期参数，在所述验证请求的有效期内采用本端的所述共同的私钥和私钥算法进行运算，并将运算结果与所述签发端的密钥参数进行比较，若相同，则表明验证成功，否则返回验证失败。

2. 根据权利要求 1 所述的安全验证方法，其特征在于，所述步骤 S2 进一步包括：

S21：接收所述签发端的参数，在所述签发端的参数中查找密钥参数，若查找到则获取所述密钥参数并转入步骤 S22，否则返回验证失败；

S22：获取所述签发端的时间戳参数和有效期参数。

3. 根据权利要求 1 所述的安全验证方法，其特征在于，所述步骤 S3 进一步包括：

S31：根据所述获取的时间戳参数和有效期参数，验证所述签发端的验证请求是否在有效期内，是则转入步骤 S32，否则返回验证失败；

S32：判断所述密钥参数是否在所述有效期内使用过，是则，转入步骤 S33，否则返回验证失败；

S33：采用所述共同的私钥和私钥算法对所述私钥进行运算，并将运算的结果与所接收到的密钥参数进行比较，若相等，则表明验证成功，否则返回验证失败。

4. 根据权利要求 1 所述的安全验证方法，其特征在于，所述密钥参数、时间戳参数以及有效期参数放置在所述签发端的统一资源定位符 URL 中或者封装在所述签发端的 HTTP host 中。

5. 根据权利要求 1 所述的安全验证方法，其特征在于，所述步骤 S1 还包括：与所述签发端进行所述私钥的交换并确认。

6. 根据权利要求 1 所述的安全验证方法，其特征在于，在步骤 S1 和 S2 之间还包括步骤 S1'：与计时服务中心进行服务器校时，其中所述签发端采用与所述计时服务中心相同的时间。

7. 根据权利要求 1 所述的安全验证方法，其特征在于，所述私钥算法为采用 SHA 算法，所述密钥参数生成方法具体为：cak = SHA(cat+var1+var2+.....+varN+key)，其中 cak 为所述密钥参数，cat 为所述时间戳参数，var1、var2.....varN 为 cak 的因子，所述 key 为所述共同的私钥。

8. 根据权利要求 7 所述的安全验证方法，其特征在于，所述私钥算法还包括对采用 SHA 算法生成的密钥参数进行截短、替换或者异或。

9. 一种用于网络页面或接口的安全验证装置，其特征在于，所述装置包括：

授权模块，用于与给发起页面或接口验证请求的签发端约定使用共同的私钥、私钥的更新周期、更新计划以及私钥算法；

获取参数模块，用于接收所述签发端的参数，并获取所述签发端的密钥参数、时间戳参

数以及有效期参数，其中所述密钥参数是所述签发端使用所述共同的私钥算法对其私钥进行运算所生成的密钥，所述时间戳参数标注有所述签发端发起验证请求的时间，其中所述有效期参数标注有所述签发端发起验证请求的最大有效期；

验证模块，用于根据所述获取参数模块所获取到的密钥参数、时间戳参数以及有效期参数，在所述验证请求的有效期内采用所述共同的私钥和私钥算法进行运算，并将运算结果与所述签发端的密钥参数进行比较，若相同，则表明验证成功，否则返回验证失败。

10. 根据权利要求 9 所述的安全验证装置，其特征在于，所述获取参数模块进一步包括：

获取密钥参数模块，用于接收所述签发端的参数，在所述签发端的参数中查找密钥参数，若查找到则获取所述密钥参数，否则返回验证失败；

获取时间戳参数和有效期参数模块，用于在所述获取密钥参数模块获取到密钥参数之后获取所述签发端的时间戳参数和有效期参数；

11. 根据权利要求 9 所述的安全验证方法，其特征在于，所述验证模块还包括：

验证有效期模块，用于根据所述获取的时间戳参数和有效期参数，验证所述签发端的验证请求是否在有效期内，是则转入到再使用判断模块中，否则返回验证失败；

再使用判断模块，用于判断所述密钥参数是否在所述有效期内使用过，是则转入到比较密钥参数模块，否则返回验证失败；

比较密钥参数模块，用于采用所述共同的私钥和私钥算法对所述私钥进行运算，并将运算的结果与所述获取到的密钥参数进行比较，若相等，则表明验证成功，否则返回验证失败。

12. 一种发起页面或接口安全验证请求的方法，其特征在于，所述方法为：

设定用来验证页面或接口安全信任关系的验证端所授权的私钥、私钥的更新周期、更新计划以及私钥算法；

采用所述私钥算法生成密钥参数，同时生成标注有发起页面或接口安全验证请求时间的时间戳参数，以及标注有所述验证请求的最大有效期的有效期参数；

将所述密钥参数、时间戳参数以及有效期参数传递给所述验证端。

13. 一种发起页面或接口安全验证请求的装置，其特征在于，所述装置包括：

设定模块，用于设定验证页面或接口安全信任关系的验证端所授权的私钥、私钥的更新周期、更新计划以及私钥算法；

参数生成模块，用于采用所述私钥算法生成密钥参数，同时生成标注有发起页面或接口安全验证请求时间的时间戳参数，以及标注有所述验证请求的最大有效期的有效期参数；

发送模块，用于将所述密钥参数、时间戳参数以及有效期参数传递给所述验证端。

一种用于网络页面或接口的安全验证方法及其装置

技术领域

[0001] 本发明涉及通信安全验证，尤其涉及一种用于网络页面或接口的安全验证方法及装置。

背景技术

[0002] 现有技术在网页页面（或接口）间要实现安全或合法性验证，通常使用http(Hyper Text Transfer Protocol，超文本传输协议）头部refer字段作为来源判断，或者专有的自定义字段在URL(Uniform/Universal ResourceLocator，统一资源定位符）中拼入或者也放在http的头部。

[0003] 现有技术的问题是，http中的refer或者其他自定义字段很容易伪造，URL中的自定义参数也会被复制冒用等问题，其主要原因是因为：1、明文传输、易被截获、冒用；2、没有加密算法或者加密算法简单易被破解、复制、篡改；3、不可靠性，网络中refer因终端浏览器的问题会丢失，尤其是手机浏览器中情况更因千差万别的浏览器和网络环境而表现各异；拼入url中的自定义字段受url长度限制（255字节）；4、没有通用性。

[0004] 在日益增长的业务系统中，公司内各个模块之间，各个公司之间需要安全可靠的通信，在涉及到计费的情况下，需要确保是合法来源的用户（需确知用户的上一步来自哪个页面或者接口），同时要满足其通用性，一次设计，全局通用。

发明内容

[0005] 为了解决上述问题，本发明提供一种能够满足通用性且安全可靠的用于网络页面或接口的安全验证方法及装置，从而实现了在互信验证的两端唯一可信的通信传输。

[0006] 为实现上述目的，本发明提供了一种用于网络页面或接口的安全验证方法，所述方法为：

[0007] S1：与给发起页面或接口验证请求的签发端约定使用共同的私钥、私钥的更新周期、更新计划以及私钥算法；

[0008] S2：接收所述签发端的参数，获取所述签发端的密钥参数、时间戳参数以及有效期参数，其中所述密钥参数是所述签发端使用所述共同的私钥算法对其私钥进行运算所生成的密钥，所述时间戳参数标注有所述签发端发起验证请求的时间，其中所述有效期参数标注有所述签发端发起验证请求的最大有效期；

[0009] S3：根据所述获取的密钥参数、时间戳参数以及有效期参数，在所述验证请求的有效期内采用所述共同的私钥和私钥算法进行运算，并将运算结果与所述签发端的密钥参数进行比较，若相同，则表明验证成功，否则返回验证失败。

[0010] 进一步地，所述步骤S2进一步包括：

[0011] S21：接收所述签发端的参数，在所述签发端的参数中查找密钥参数，若查找到则获取所述密钥参数并转入步骤S22，否则返回验证失败；

[0012] S22：获取所述签发端的时间戳参数和有效期参数；

[0013] 进一步地，所述步骤 S3 进一步包括：

[0014] S31：根据所述获取的时间戳参数和有效期参数，验证所述签发端的验证请求是否在有效期内，是则转入步骤 S32，否则返回验证失败；

[0015] S32：判断所述密钥参数是否在所述有效期内使用过，是则，转入步骤 S33，否则返回验证失败；

[0016] S33：采用所述共同的私钥和私钥算法对所述私钥进行运算，并将运算的结果与所接收到的密钥参数进行比较，若相等，则表明验证成功，否则返回验证失败。

[0017] 优选地，所述密钥参数、时间戳参数以及有效期参数放置在所述签发端的统一资源定位符 URL 中或者封装在所述签发端的 HTTP host 中。

[0018] 进一步地，所述步骤 S1 还包括：与所述签发端进行所述私钥的交换并确认。

[0019] 进一步地，在步骤 S1 和 S2 之间还包括步骤 S1'：与计时服务中心进行服务器校时，其中所述签发端采用与所述计时服务中心相同的时间。

[0020] 优选地，所述私钥算法为采用 SHA 算法，所述密钥参数生成方法具体为：cak = SHA(cat+var1+var2+.....+varN+key)，其中 cak 为所述密钥参数，cat 为所述时间戳参数，var1、var2.....varN 为 cak 的因子，所述 key 为所述共同的私钥。

[0021] 进一步地，所述私钥算法还包括对采用 SHA 算法生成的密钥参数进行截短、替换或者异或。

[0022] 本发明还提供一种用于网络页面或接口的安全验证装置，所述装置包括：

[0023] 授权模块，用于与给发起页面或接口验证请求的签发端约定使用共同的私钥、私钥的更新周期、更新计划以及私钥算法；

[0024] 获取参数模块，用于接收所述签发端的参数，并获取所述签发端的密钥参数、时间戳参数以及有效期参数，其中所述密钥参数是所述签发端使用所述共同的私钥算法对其私钥进行运算所生成的密钥，所述时间戳参数标注有所述签发端发起验证请求的时间，其中所述有效期参数标注有所述签发端发起验证请求的最大有效期；

[0025] 验证模块，用于根据所述获取参数模块所获取到的密钥参数、时间戳参数以及有效期参数，在所述验证请求的有效期内采用所述共同的私钥和私钥算法进行运算，并将运算结果与所述签发端的密钥参数进行比较，若相同，则表明验证成功，否则返回验证失败。

[0026] 进一步地，所述获取参数模块还包括：

[0027] 获取密钥参数模块，用于接收所述签发端的参数，在所述签发端的参数中查找密钥参数，若查找到则获取所述密钥参数，否则返回验证失败；

[0028] 获取时间戳参数和有效期参数模块，用于在所述获取密钥参数模块获取到密钥参数之后获取所述签发端的时间戳参数和有效期参数；

[0029] 进一步地，所述验证模块还包括：

[0030] 验证有效期模块，用于根据所述获取的时间戳参数和有效期参数，验证所述签发端的验证请求是否在有效期内，是则转入到再使用判断模块中，否则返回验证失败；

[0031] 再使用判断模块，用于判断所述密钥参数是否在所述有效期内使用过，是则转入到比较密钥参数模块，否则返回验证失败；

[0032] 比较密钥参数模块，用于采用所述共同的私钥和私钥算法对所述私钥进行运算，并将运算的结果与所述获取到的密钥参数进行比较，若相等，则表明验证成功，否则返回验

证失败。

[0033] 相应地，本发明还提供一种发起页面或接口安全验证请求的方法，所述方法为：

[0034] 设定验证页面或接口安全信任关系的验证端所授权的私钥、私钥的更新周期、更新计划以及私钥算法；

[0035] 采用所述私钥算法生成密钥参数，同时生成标注有发起页面或接口安全验证请求时间的时间戳参数，以及标注有所述验证请求的最大有效期的有效期参数；

[0036] 将所述密钥参数、时间戳参数以及有效期参数传递给所述验证端。

[0037] 同时，本发明还一种发起页面或接口安全验证请求的装置，所述装置包括：

[0038] 设定模块，用于设定验证页面或接口安全信任关系的验证端所授权的私钥、私钥的更新周期、更新计划以及私钥算法；

[0039] 参数生成模块，用于采用所述私钥算法生成密钥参数，同时生成标注有发起页面或接口安全验证请求时间的时间戳参数，以及标注有所述验证请求的最大有效期的有效期参数；

[0040] 发送模块，用于将所述密钥参数、时间戳参数以及有效期参数传递给所述验证端。

[0041] 由上述技术方案可知，本发明的技术方案通过授权也即约定好的私钥和私钥算法，规避了被截获、破解、篡改的问题，同时在验证端对密钥是否占用做了排重，消除了除了冒用、重用的问题；从而在在互信验证的两端实现了唯一、可信的传输，实现了不可抵赖的签名效果。

[0042] 通过以下参照附图对优选实施例的说明，本发明的上述以及其它目的、特征和优点将更加明显。

附图说明

[0043] 图 1 为本发明的实现两网络页面或接口互信验证的方法示意流程图；

[0044] 图 2 为本发明的在签发端发起安全验证的方法示意流程图；

[0045] 图 3 为本发明的在验证端的网络页面或接口安全验证的方法示意流程图；

[0046] 图 4 为本发明在验证端的一种实施例的网络页面或接口安全验证的方法示意流程图；

[0047] 图 5 为本发明的在验证端的网络页面或接口安全验证的装置结构示意图；

[0048] 图 6 为本发明的在签发端的发起网络页面或接口安全验证的装置结构示意图。

具体实施方式

[0049] 下面将详细描述本发明的具体实施例。应当注意，这里描述的实施例只用于举例说明，并不用于限制本发明。

[0050] 基于规范描述和方便阅读的考虑，逐一定义本发明专利申请文件中出现的术语如下：签发端：是应用本发明身份互信验证技术方案的发起一方，也即指网络通信中发起网页页面或验证请求的发起方；验证端，是指应用本发明身份互信验证技术方案的接收一方，也即指网络通信中接收签发端所发起的验证请求的接收方。需要说明的是，上述各术语仅作为指称其意指的名称之一，因此凡意指与其相同或近似的名称均应视为其等价物。

[0051] 本发明涉及到一种网络页面或接口之间的互信验证方法，该方法能够实现验证端

的网络页面或接口对签发端的网络页面或接口的安全可靠的信任关系，如图 1 所示，该方法主要思路为：

[0052] 在签发端和验证端网络页面或接口中都约定双方共用的私钥和私钥算法，并约定私钥的更新周期和更新计划；

[0053] 签发端将标注有发起请求时间的时间戳 cat、使用私钥算法所生成的新密钥以及请求有效期发送给验证端；其中在签发端使用私钥算法对私钥进行运算所生成新密钥，优选地，可根据新密钥的长短将该新密钥放在签发端的 URL 或者 http post 主体本身；

[0054] 而在验证端在接收到签发端发送来的参数之后，采用共用的私钥算法对其约定好的私钥进行运算，将运算结果与所接收到的签发端的密钥进行比较，根据比较结果来表明验证成功或失败。

[0055] 下面结合附图分别以签发端和验证端为例，来主要描述本发明的安全验证方法。

[0056] (1) 签发端

[0057] 如图 2 所示，在签发端，需要生成密钥、时间戳以及有效期三个参数，在生成这三个参数之前，首先将与验证端约定好共同的私钥、私钥算法的更新周期、更新计划以及私钥算法设定好，优选地，这里所述共同的私钥可在签发端和验证端通过可信赖的方式进行交换并经过双方确认，这样某一方的私钥发生变化时，则可对另一方进行同步更新。

[0058] 然后在签发端生成发起请求时的时间戳 cat(ChinaM AuthenticatingTimestamp) 参数，一般来说，该时间戳参数取签发端发起请求时的时间值即可，优选地，可以当前时间的秒数，或者千分之一秒为单位选取，这样可便于在各种语言中实现。由于在验证端需要根据时间戳参数判断验证请求是否在有效期内，因而所述验证端和签发端需要进行校时，比如说向计时服务中心 pool.ntp.org 进行校时，并做定期校时的时间更新计划。

[0059] 接着，采用设定好的私钥算法对私钥进行运算，生成新密钥 cak(ChinaM Authenticating Key)，这里所述的私钥算法可为 MD5 算法或者 SHA 算法，由于 MD5 的碰撞较容易实现，在本发明中推荐使用 SHA。举例来说：

[0060] cak = SHA(cat+var1+var2+var3+.....+varN+key)

[0061] 其中 cat 是上述时间戳参数，var1，var2，var3，....varN 是需要传输和验证的 cak 的因子，key 是预先约定的私钥。

[0062] 在得到上述 cak 之后，还可以根据需要对其进行更进一步的操作，增加其复杂度，比如说对上述生成的 cak 进行截短、替换或者异或等操作，例如：

[0063] cak = cak.substring(2)，对上述生成的密钥 cak 作二次处理，该式子表示从密钥 cak 的第三位开始截取（丢弃前二个字符），将截取后的密钥作为新的密钥来使用。

[0064] 或者

[0065] cak = cak.replaceAll(“6”,“9”)，这里将上述生成的密钥 cak 中的字符“6”统一替换为字符“9”，将替换后的密钥作为新的密钥来使用。

[0066] 上述举例的 relaceAll 也可采用 replace 表达式来进行二次处理，如 cak = cak.replace(“6”,“9”)，与替换所有的 relaceAll 不同的是，replace 是替换首先被找到的一个。因此，本发明中实际的二次处理方法可能千变万化，归结大概是三类：截短（加长）、替换和异或（二次 MD5、SHA 等）。

[0067] 二次处理的目的在于，随着信息技术的进步，在信息摘要算法 MD5 能够快速产生

“碰撞”之后，SHA 也面临同样的问题，而对按公开已知算法的结果做二次“私有”处理后，避免了未来可能“碰撞”技术对本方法的影响。也即，在传输中看到的 cak，不能够通过反向的 SHA 操作还原出“原文”，因为所看到 cak 已经被“二次处理”了。

[0068] 继续，在签发端所生成的有效期参数 cam(ChinaM AuthenticatingMaximum)，该有效期参数表明的是签发端所发起验证请求的最大请求有效期，该有效期参数可根据网络情况约定一个数值，用来限定该次通信色时效性，比如 60 秒或者 43200 秒 (12 小时)。

[0069] 签发端生成上述密钥、时间戳以及有效期三个参数之后，可根据密钥的长度将其拼入签发端的 URL 或者放在 HTTP Post 本身，连同时间戳 cat 和有效期 cam，一起传递给验证端的页面 / 接口。比如说，这三个参数可附加在 http 地址 URL 中 :

[0070] http://site/file.jsp ? a = 1&b = 2...&cat = 12435832882&cak = a5128e2780785817c821&cam = 43200

[0071] 也可放在 HTTP Post 本身中，例如 :

[0072] <xml>

[0073] ….

[0074] <cat>12435832882</cat>

[0075] <cak>a5128e2780785817c821</cak>

[0076] <cam>43200</cam>

[0077] ….

[0078] </xml>

[0079] 其他在 Socket 通信中的传输，可自行封装。

[0080] (2) 验证端

[0081] 如图 3 所示，正如在签发端部分所述的，在验证端需要事先与签发端约定好，也即授权给发起页面或接口验证请求的签发端使用共同的私钥、私钥的更新周期、更新计划以及私钥算法 ;

[0082] 验证端接收到签发端所发起的验证请求，获取所述签发端的密钥参数、时间戳参数以及有效期参数，然后将密钥 cat、时间戳 cak 和有效期 cam 三个参数采用约定的私钥和私钥算法进行合法性验证，在所述验证请求的有效期内采用所述共同的私钥和私钥算法进行运算，并将运算结果与所述签发端的密钥参数进行比较，若相同，则表明验证成功，否则返回验证失败。由于采取的是不可逆的算法，因此在验证端是重现签发端的算法过程，然后再比对结果。

[0083] 如图 4 所示，验证端具体的验证过程如下 :

[0084] 1.1. 首先在签发端发送的验证请求参数中是否携带有密钥 cak 参数，如果有 cak 则进行 1.2，没有的话，直接返回失败 ;

[0085] 1.2. 判断 1.1 之后，获得时间戳 cat 和有效期 cam 参数，根据这两个参数判断，该次通信的时效是否过期，也即进行 cak+cam ＞ NOW ? 判断，如果没有过期进行 1.3，如果已经过期，直接返回失败 ;

[0086] 1.3. 判断 1.2 之后，获得 cak，判断该 cak 在 (cat+cam) 约定的时效内是否已经被使用过，也即进行 cak.req occupied ? ，如果还没有被使用过，则判断 1.4，否则直接返回失败 ;

[0087] 1.4. 判断 1.3 之后，根据预先约定好的私钥算法和私钥，代入传来的 cat 和其他因子参数，模拟签发端对私钥的运算过程，取得新的 cak.new，比对 cak 和 cak.new，如果相等，则返回验证成功，否则返回失败。

[0088] 通过上面的判断，有效期 cam 的作用在判断通信的时效性，而在验证端需同时生成一个临时的容器，用以保存已经通过验证且在有效期内的 cak，以防被重用。

[0089] 从上述的描述中可以看出，在互信验证的两端实现了唯一、可信的传输，实现了不可抵赖的签名效果。由于算法和密钥都是私有的，规避了被截获、破解、篡改的问题；由于在验证端对 cak 是否占用做排重，消除了冒用、重用的问题；由于在 HTTP Post 里封装，回避了 refer 不可靠和 url 地址长度限制的问题。

[0090] 本发明相应地，提供一种用于网络页面或接口的安全验证装置，如图 5 所示，所述装置包括：

[0091] 授权模块，用于授权给发起页面或接口验证请求的签发端使用共同的私钥、私钥的更新周期、更新计划以及私钥算法；

[0092] 获取参数模块，用于接收所述签发端的参数，并获取所述签发端的密钥参数、时间戳参数以及有效期参数，其中所述密钥参数是所述签发端使用所述共同的私钥算法对其私钥进行运算所生成的密钥，所述时间戳参数标注有所述签发端发起验证请求的时间；其中所述有效期参数标注有所述签发端发起验证请求的最大有效期；

[0093] 验证模块，用于根据所述获取参数模块所获取到的密钥参数、时间戳参数以及有效期参数，在所述验证请求的有效期内采用所述共同的私钥和私钥算法进行运算，并将运算结果与所述签发端的密钥参数进行比较，若相同，则表明验证成功，否则返回验证失败。

[0094] 优选地，所述获取参数模块进一步包括：

[0095] 获取密钥参数模块，用于接收所述签发端的参数，在所述签发端的参数中查找密钥参数，若查找到则获取所述密钥参数，否则返回验证失败；

[0096] 获取时间戳参数和有效期参数模块，用于在所述获取密钥参数模块获取到密钥参数之后获取所述签发端的时间戳参数和有效期参数。

[0097] 优选地，所述验证模块还包括：

[0098] 验证有效期模块，用于根据所述获取的时间戳参数和有效期参数，验证所述签发端的验证请求是否在有效期内，是则转入到再使用判断模块中，否则返回验证失败；

[0099] 再使用判断模块，用于判断所述密钥参数是否在所述有效期内使用过，是则转入到比较密钥参数模块，否则返回验证失败；

[0100] 比较密钥参数模块，用于采用所述共同的私钥和私钥算法对所述私钥进行运算，并将运算的结果与所述获取到的密钥参数进行比较，若相等，则表明验证成功，否则返回验证失败。

[0101] 同样，本发明还提供一种发起页面或接口安全验证请求的装置，如图 6 所示，所述装置包括：

[0102] 设定模块，用于设定验证页面或接口安全信任关系的验证端所授权的私钥、私钥的更新周期、更新计划以及私钥算法；

[0103] 参数生成模块，用于采用所述私钥算法生成密钥参数，同时生成标注有发起页面或接口安全验证请求时间的时间戳参数，以及标注有所述验证请求的最大有效期的有效期

参数；

[0104] 发送模块，用于将所述密钥参数、时间戳参数以及有效期参数传递给所述验证端。

[0105] 虽然已参照几个典型实施例描述了本发明，但应当理解，所用的术语是说明和示例性、而非限制性的术语。由于本发明能够以多种形式具体实施而不脱离发明的精神或实质，所以应当理解，上述实施例不限于任何前述的细节，而应在随附权利要求所限定的精神和范围内广泛地解释，因此落入权利要求或其等效范围内的全部变化和改型都应为随附权利要求所涵盖。

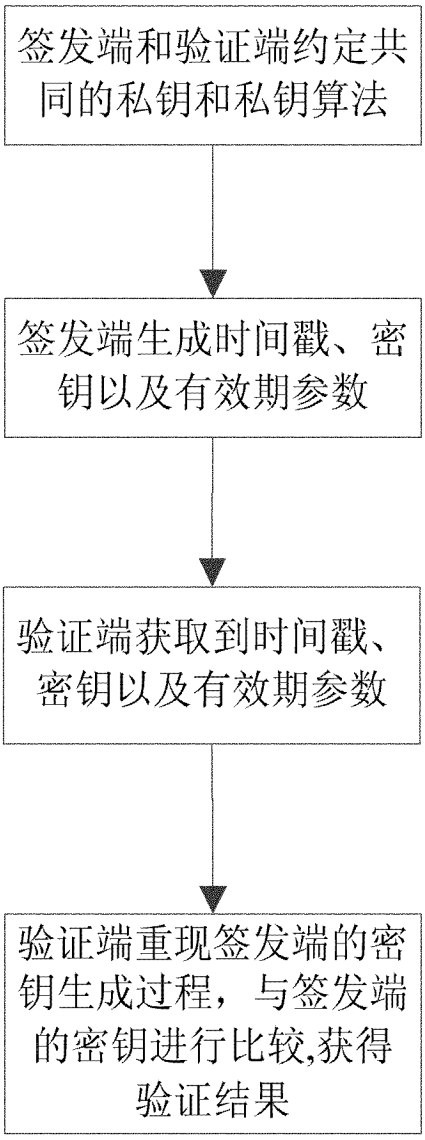

签发端和验证端约定共同的私钥和私钥算法
签发端生成时间戳、密钥以及有效期参数
验证端获取到时间戳、密钥以及有效期参数
验证端重现签发端的密钥生成过程，与签发端的密钥进行比较,获得验证结果

图 1

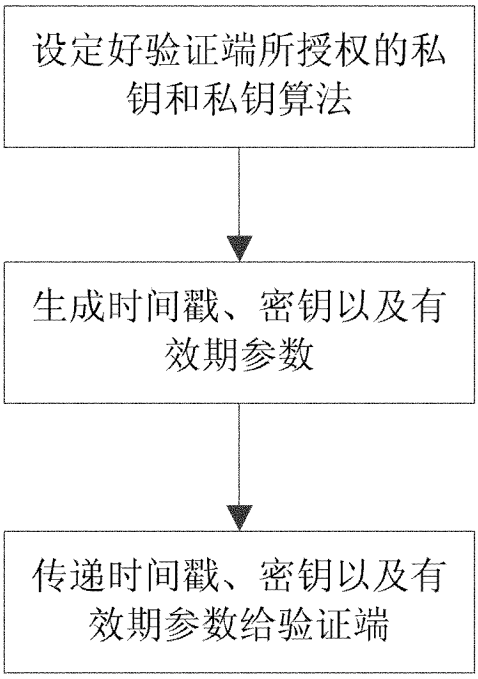

设定好验证端所授权的私钥和私钥算法
生成时间戳、密钥以及有效期参数
传递时间戳、密钥以及有效期参数给验证端

图 2

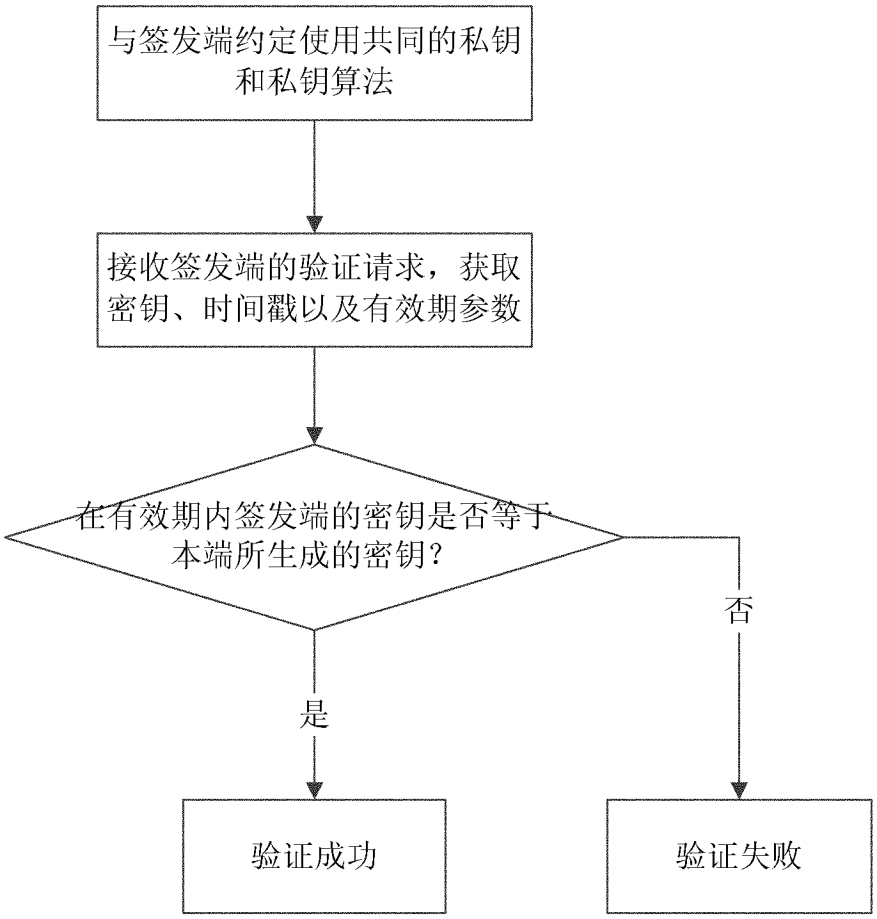

与签发端约定使用共同的私钥和私钥算法
接收签发端的验证请求，获取密钥、时间戳以及有效期参数
在有效期内签发端的密钥是否等于本端所生成的密钥？
否
是
验证成功
验证失败

图 3

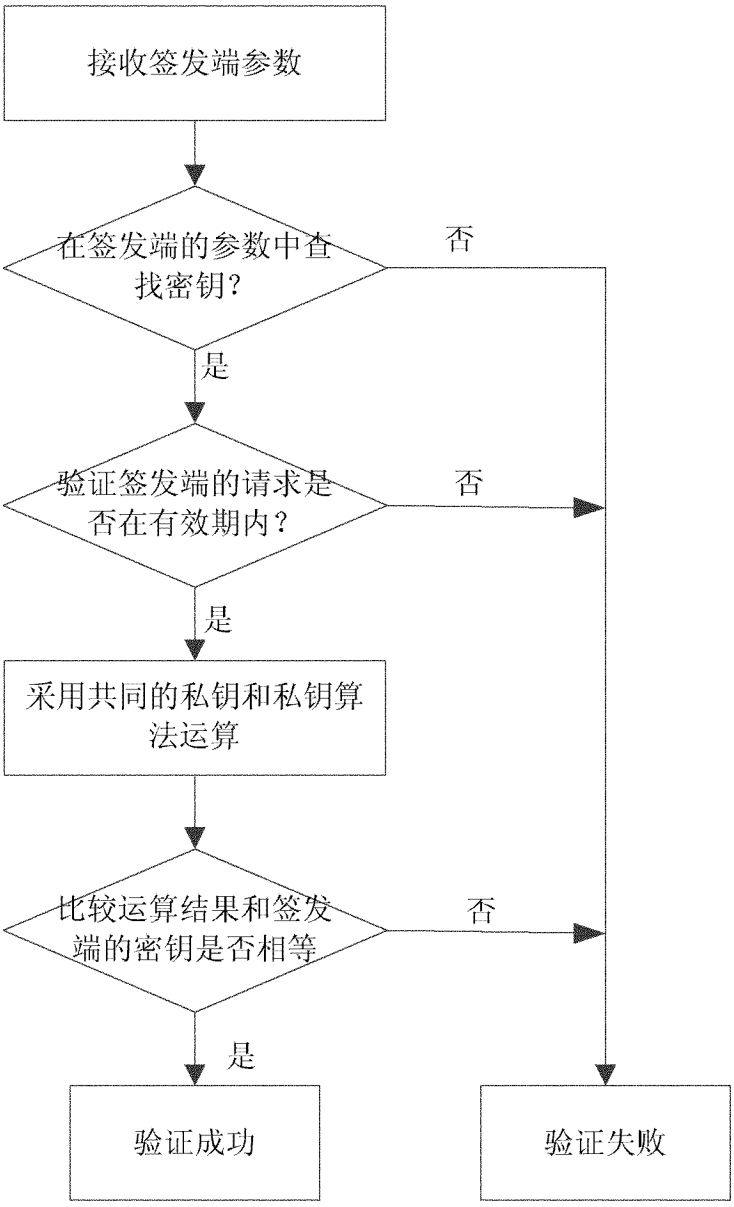

接收签发端参数
在签发端的参数中查找密钥?
否
是
验证签发端的请求是否在有效期内?
否
是
采用共同的私钥和私钥算法运算
比较运算结果和签发端的密钥是否相等
否
是
验证成功
验证失败

图 4

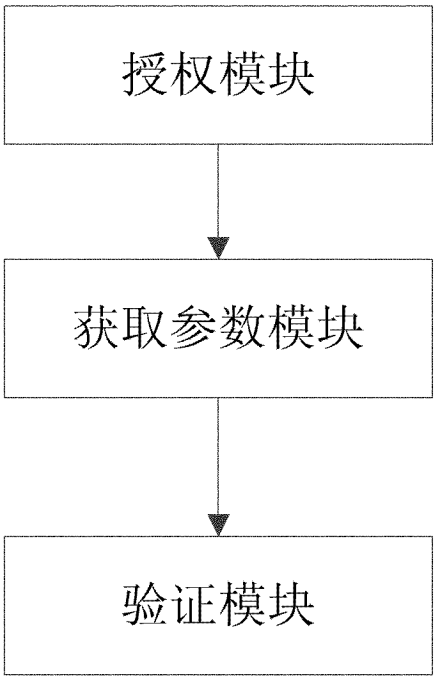

授权模块
获取参数模块
验证模块

图 5

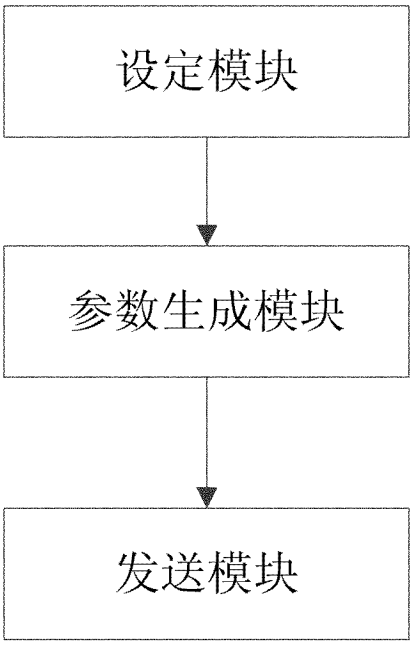


图 6