(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 108737436 B
(45)授权公告日 2020.02.21

(21)申请号 201810548516.8

(22)申请日 2018.05.31

(65)同一申请的已公布的文献号
申请公布号 CN 108737436 A

(43)申请公布日 2018.11.02

(73)专利权人 西安电子科技大学
地址 710071 陕西省西安市雁塔区太白南路2号

(72)发明人 马文平 马晓婷

(74)专利代理机构 陕西电子工业专利中心 61205
代理人 田文英 王品华

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

(56)对比文件
CN 105516119 A,2016.04.20,全文.
CN 106789042 A,2017.05.31,全文.

审查员 赵颖

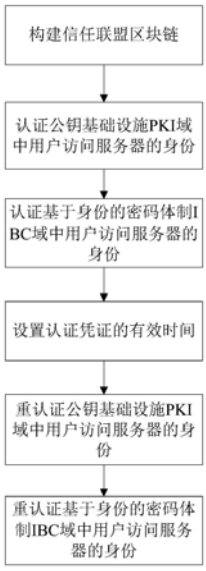
权利要求书3页 说明书7页 附图1页

(54)发明名称

基于信任联盟区块链的跨域服务器身份认证方法

(57)摘要

本发明公开了基于信任联盟区块链的跨域服务器身份认证方法,其步骤为:(1)构建信任联盟区块链;(2)认证公钥基础设施PKI域中用户访问服务器身份;(3)认证基于身份的密码体制IBC域中用户访问服务器的身份;(4)设置认证凭证的有效时间(5)重认证公钥基础设施PKI域中用户访问服务器身份;(6)重认证基于身份的密码体制IBC域中用户访问服务器的身份。本发明构建信任联盟区块链,通过信任联盟区块链中节点之间的相互认证实现域间相互认证,进而实现对服务器的跨域认证,减少了对桥中心系统的维护负担,降低了用户端的计算量和通信量,具有良好的实用性和可拓展性。



CN 108737436 B

1.一种基于信任联盟区块链的跨域服务器身份认证方法,其特征在于,构建信任联盟区块链,将所有信任联盟区块链中的节点服务器的证书和公钥基础设施PKI域内合法用户的证书,保存入信任联盟区块链,利用信任联盟区块链实现对服务器身份的跨域认证,将认证成功的信息作为认证凭证,保存入信任联盟区块链,利用认证凭证实现重认证;该方法的具体步骤包括如下:

(1)构建信任联盟区块链:

(1a)根据区块链通信能力可容纳的信任联盟中节点服务器的数量,分别设置公钥基础设施PKI域和基于身份的密码体制IBC域的数量;

(1b)将每个公钥基础设施PKI域中的证书服务器和每个基于身份的密码体制IBC域中的域代理服务器,作为信任联盟区块链的节点服务器;

(1c)公钥基础设施PKI域中的证书服务器为基于身份的密码体制IBC域中的域代理服务器颁发证书;

(1d)根据证书的大小选择哈希函数,生成证书的哈希值;

(1e)将证书的哈希值作为第一个区块,在区块体内保存,得到信任联盟区块链;

(2)认证公钥基础设施PKI域中用户访问服务器的身份:

(2a)基于身份的密码体制IBC域中请求访问的用户,利用自身私钥和国产标识密码SM9签名算法,对自身身份标识ID计算生成签名认证申请,将签名认证申请发送给域代理服务器;

(2b)基于身份的密码体制IBC域中的域代理服务器,验证请求访问的用户的身份是否合法,若是,则执行步骤(2c),否则,执行步骤(2f);

(2c)判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域中的域代理服务器是否满足相互信任条件,若是,则执行步骤(2d),否则,执行步骤(2f);

(2d)采用颁发临时身份的方法,构建公钥基础设施PKI域中用户请求服务器与访问用户的安全通信;

(2e)公钥基础设施PKI域中的证书服务器,采用将认证凭证写入信任联盟区块链的方法存储认证凭证;

(2f)结束认证;

(3)认证基于身份的密码体制IBC域中用户访问服务器的身份:

(3a)公钥基础设施PKI域中请求访问的用户,向证书服务器发送认证申请;

(3b)公钥基础设施PKI域中的证书服务器,在信任联盟区块链上查询访问用户的证书状态,如果证书状态为声明则执行步骤(3c),如果证书状态为撤销,则执行步骤(3f);

(3c)判断公钥基础设施PKI域中的证书服务器和基于身份的密码体制IBC域中的域代理服务器是否满足相互信任条件,若是,则执行步骤(3d),否则执行步骤(3f);

(3d)采用颁发临时证书的方法,构建公钥基础设施PKI域中用户访问服务器和申请访问用户的安全通信;

(3e)基于身份的密码体制IBC域中的域代理服务器,采用将认证凭证写入信任联盟区块链的方法存储认证凭证;

(3f)结束认证;

(4)设置认证凭证的有效时间:

(4a)根据公钥基础设施PKI域中用户访问服务器的安全等级,对应设置存储在信任联盟区块链上认证凭证的有效时间;

(4b)根据基于身份的密码体制IBC域中用户访问服务器的安全等级,对应设置存储在信任联盟区块链上认证凭证的有效时间;

(5)重认证公钥基础设施PKI域中用户访问服务器的身份;

(5a)基于身份的密码体制IBC域中的其他用户,向域代理服务器发送身份签名申请和访问申请;

(5b)判断公钥基础设施PKI域中的证书服务器和基于身份的密码体制IBC域中的域代理服务器是否满足相互信任条件,若是,则执行步骤(5c),否则,执行步骤(5g);

(5c)基于身份的密码体制IBC域中的域代理服务器,利用公钥基础设施PKI域中用户访问服务器的身份标识信息ID,生成认证凭证;

(5d)基于身份的密码体制IBC域中的域代理服务器,在信任联盟区块链上查询认证凭证,如果查询到认证凭证,认证凭证在有效时间内,则允许本次访问,执行步骤(5g),否则执行步骤(5e);

(5e)利用颁发临时身份的方法,构建公钥基础设施PKI域中用户访问服务器与访问用户的安全通信;

(5f)公钥基础设施PKI域中的证书服务器,采用将认证凭证写入信任联盟区块链的方法存储认证凭证;

(5g)结束认证;

(6)重认证基于身份的密码体制IBC域中用户访问服务器的身份:

(6a)公钥基础设施PKI域中的其他用户,向证书服务器发送访问请求;

(6b)判断公钥基础设施PKI域中的证书服务器和基于身份的密码体制IBC域中的域代理服务器是否满足相互信任条件,若是,则允许本次访问,执行步骤(6c),否则执行步骤(6g);

(6c)公钥基础设施PKI域中的证书服务器,利用密码体制IBC域中用户访问服务器的身份标识信息ID,生成认证凭证;

(6d)公钥基础设施PKI域中的证书服务器,在信任联盟区块链上查询认证凭证,如果查询到认证凭证,认证凭证在有效时间内,则允许本次访问,否则执行步骤(6e):

(6e)采用颁发临时证书的方法,构建基于身份的密码体制IBC域中用户访问服务器和访问用户的安全通信;

(6f)基于身份的密码体制IBC域中的域代理服务器,采用将认证凭证写入信任联盟区块链的方法存储认证凭证;

(6g)结束认证;

步骤(2e)、步骤(3e)、步骤(5f)和步骤(6f)中所述的将认证凭证写入信任联盟区块链的方法的具体步骤如下:

第一步,信任联盟区块链中节点服务器将成功认证用户访问服务器的身份标识信息ID生成认证凭证;

第二步,信任联盟区块链中节点服务器根据认证凭证的大小选择哈希函数,利用哈希运算,将认证凭证生成哈希值,将哈希值写入区块链。

2.根据权利要求1所述的基于信任联盟区块链的跨域服务器身份认证方法，其特征在于，步骤(2b)中所述的用户身份合法是指，利用请求访问的用户的公钥，由国产标识密码SM9签名验证算法对签名认证申请进行验证，通过验证的签名认证申请为用户身份合法。

3.根据权利要求1所述的基于信任联盟区块链的跨域服务器身份认证方法，其特征在于，步骤(2c)、步骤(3c)、步骤(5b)和步骤(6b)中所述的相互信任条件是指同时满足以下两个条件的情形：

条件1，公钥基础设施PKI域中的证书服务器，在信任联盟区块链上查询基于身份的密码体制IBC域中的域代理服务器的证书，证书状态为声明；

条件2，基于身份的密码体制IBC域中的域代理服务器，在信任联盟区块链上查询公钥基础设施PKI域中的证书服务器的证书，证书状态为声明。

4.根据权利要求1所述的基于信任联盟区块链的跨域服务器身份认证方法，其特征在于，步骤(2d)、步骤(5e)中所述的颁发临时身份的方法的具体步骤如下：

第一步，基于身份的密码体制IBC域中的域代理服务器，生成公钥基础设施PKI域中用户访问服务器的临时身份信息，将临时身份信息发送至公钥基础设施PKI域证书服务器；

第二步，公钥基础设施PKI域中的证书服务器转发临时身份信息给用户访问的服务器；

第三步，公钥基础设施PKI域中提供服务的服务器保存临时身份信息，利用临时身份信息与基于身份的密码体制IBC域中请求服务用户进行安全通信。

5.根据权利要求1所述的基于信任联盟区块链的跨域服务器身份认证方法，其特征在于，步骤(3d)、步骤(6e)中所述的颁发临时证书的方法的具体步骤如下：

第一步，公钥基础设施PKI域中的证书服务器，生成基于身份的密码体制IBC域中用户访问服务器的临时证书，将临时证书发送给基于身份的密码体制IBC域中的域代理服务器；

第二步，基于身份的密码体制IBC域中，域代理服务器将临时证书转发至用户访问服务器；

第三步，基于身份的密码体制IBC域中，用户访问服务器保存临时证书，利用临时证书中的身份信息与公钥基础设施PKI域中请求服务用户实现安全通信。

基于信任联盟区块链的跨域服务器身份认证方法

技术领域

[0001] 本发明属于网络通信技术领域，更进一步涉及网络安全技术领域中的一种基于信任联盟区块链的跨域认证服务器身份的方法。本发明可应用于基于证书的公钥基础设施PKI(Public Key Infrastructure)与基于身份的密码体制IBC(Identity-Based Cryptography)域中用户请求跨域访问服务器时，对所访问服务器的身份进行认证的方法。

背景技术

[0002] 目前基于公开密钥的信任域认证框架较多应用基于证书的公钥基础设施PKI和基于身份的密码体制IBC。当基于身份的密码体制IBC域用户访问公钥基础设施PKI域服务器、或公钥基础设施PKI域用户访问基于身份的密码体制IBC域服务器时，需要对所访问的服务器身份进行安全性认证，保证其提供安全的服务。此时会出现因公钥基础设施PKI与基于身份的密码体制IBC的认证结构不同，无法实现跨域身份认证等问题。

[0003] 北京迪曼森科技有限公司在其申请的专利文献“一种基于标识的组合密钥跨域认证方法”(申请号201710647789.3，公开号CN 107395364A)中提出了一种基于标识的组合密钥跨域认证方法。该方法在各个标识密钥基础设施IKI(Identity Key Infrastructure)系统之外建立一个IKI系统，称为桥IKI，各个IKI系统与桥IKI分别相互签发矩阵标识，系统用户利用用户标识以及所属系统与桥IKI相互签发的矩阵标识的相互交换实现跨域认证。以上的交互认证基于桥IKI系统的可信性，因此需要进行信任安全性维护；用户认证时进行本系统矩阵标识和桥IKI矩阵标识的相互交换，需要对以上矩阵标识进行存储。该方法存在的不足之处是：第一，桥IKI系统的身份需要信任维护，增加维护负担；第二，当IKI系统增多时，桥IKI系统存储负担增大，如果设置多个桥IKI系统，增大用户的存储负担。

[0004] 西南交通大学在其申请的专利文献“IBC域内的用户访问PKI域内的资源的认证密钥协商方法”(申请号201710081516.7，公开号CN 106789042 A)和“PKI域内的用户访问IBC域内的资源的认证密钥协商方法(申请号201710082835.X，公开号CN106877996A)”中公开了实现PKI与IBC域之间跨域访问的身份认证秘钥协商方法，以上系统包括用户、资源以及IBC和PKI域的认证服务器。在其实现方法中，用户需要首先向本域认证服务器发送验证申请，然后与外域认证服务器共同生成访问授权票据和会话秘钥，最后利用生成的授权票据申请资源端的身份验证。资源端验证用户身份合法后与用户实现安全通信。该方法存在的不足之处是：由于用户端在本次认证过程中，进行四次交互通信，通信前需要进行授权票据、会话秘钥和签名加密等运算，导致用户端承载的计算量和通信量较大，不适用于资源受限的轻量级移动用户终端。

发明内容

[0005] 本发明的目的在于针对上述已有技术的不足，提出一种基于信任联盟区块链的服务器跨域认证方法，公钥基础设施PKI与基于身份的密码体制IBC域在平级关系上实现对服务器的跨域认证和安全高效重认证。

[0006] 实现本发明目的的思路是:将公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域中域代理服务器作为节点,构建信任联盟区块链;将所有信任联盟区块链中的节点服务器的证书和公钥基础设施PKI域内合法用户的证书,保存入信任联盟区块链,通过联盟信任模型中节点之间的相互认证实现域间相互认证;利用联盟信任模型实现对服务器身份的跨域认证,认证成功的信息作为认证凭证写入信任联盟区块链,利用认证凭证实现快速重认证。

[0007] 本发明的具体步骤如下:

[0008] (1)构建信任联盟区块链:

[0009] (1a)根据区块链通信能力可容纳的信任联盟中节点服务器的数量,分别设置公钥基础设施PKI域和基于身份的密码体制IBC域的数量;

[0010] (1b)将每个公钥基础设施PKI域中的证书服务器和每个基于身份的密码体制IBC域中的域代理服务器,作为信任联盟区块链的节点服务器;

[0011] (1c)公钥基础设施PKI域中的证书服务器为基于身份的密码体制IBC域中域代理服务器颁发证书;

[0012] (1d)根据证书的大小选择哈希函数,生成证书的哈希值;

[0013] (1e)将证书的哈希值作为第一个区块,在区块体内保存,得到信任联盟区块链;

[0014] (2)认证公钥基础设施PKI域中用户访问服务器的身份:

[0015] (2a)基于身份的密码体制IBC域中请求访问的用户,利用自身私钥和国产标识密码SM9签名算法,对自身身份标识ID计算生成的签名认证申请,将签名认证申请发送给向域代理服务器;

[0016] (2b)基于身份的密码体制IBC域中域代理服务器,验证请求访问的用户的身份是否合法,若是,则执行步骤(2c),否则,执行步骤(2f);

[0017] (2c)判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件,若是,则执行步骤(2d),否则执行步骤(2f);

[0018] (2d)采用颁发临时身份的方法,构建公钥基础设施PKI域中用户请求服务器与访问用户的安全通信;

[0019] (2e)公钥基础设施PKI域中证书服务器,采用将认证凭证写入信任联盟区块链的方法存储认证凭证;

[0020] (2f)结束认证;

[0021] (3)认证基于身份的密码体制IBC域中用户访问服务器的身份:

[0022] (3a)公钥基础设施PKI域中请求访问的用户,向证书服务器发送认证申请;

[0023] (3b)公钥基础设施PKI域证书服务器,在信任联盟区块链上查询访问用户的证书状态,如果证书状态为声明则执行步骤(3c),如果证书状态为撤销,则执行步骤(3f);

[0024] (3c)判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件,若是,则执行步骤(3d),否则执行步骤(3f);

[0025] (3d)采用颁发临时证书的方法,构建公钥基础设施PKI域中用户访问服务器和申请访问用户的安全通信;

[0026] (3e)基于身份的密码体制IBC域域代理服务器,采用将认证凭证写入信任联盟区块链的方法存储认证凭证;

[0027] (3f)结束认证；

[0028] (4)设置认证凭证的有效时间：

[0029] (4a)根据公钥基础设施PKI域中用访问户服务器的安全等级，将其存储在信任联盟区块链上的认证凭证作为安全等级对应的有效时间；

[0030] (4b)根据基于身份的密码体制IBC域中用访问户服务器的安全等级，将其存储在信任联盟区块链上的认证凭证作为安全等级对应的有效时间；

[0031] (5)重认证公钥基础设施PKI域中用户访问服务器的身份；

[0032] (5a)基于身份的密码体制IBC域中的其他用户，向域代理服务器发送身份签名申请和访问申请；

[0033] (5b)判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件，若是，则执行(5c)，否则，执行步骤(5g)；

[0034] (5c)基于身份的密码体制IBC域域代理服务器，利用公钥基础设施PKI域中用户访问服务器的身份标识信息ID，生成认证凭证；

[0035] (5d)基于身份的密码体制IBC域域代理服务器，在信任联盟区块链上查询认证凭证，如果查询到认证凭证，认证凭证在有效时间内，则允许本次访问，执行步骤(5g)，否则执行步骤(5e)；

[0036] (5e)利用颁发临时身份的方法，构建公钥基础设施PKI域中用户访问服务器与访问用户的安全通信；

[0037] (5f)公钥基础设施PKI域中证书服务器，采用将认证凭证写入信任联盟区块链的方法存储认证凭证；

[0038] (5g)结束认证；

[0039] (6)重认证基于身份的密码体制IBC域中用户访问服务器的身份：

[0040] (6a)公钥基础设施PKI域中的其他用户，向证书服务器发送访问请求；

[0041] (6b)判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件，若是，则执行(6c)，否则执行步骤(6g)；

[0042] (6c)公钥基础设施PKI域中证书服务器，利用密码体制IBC域中用户访问服务器的身份标识信息ID，生成认证凭证；

[0043] (6d)公钥基础设施PKI域中证书服务器，在信任联盟区块链上查询认证凭证，如果查询到认证凭证，认证凭证在有效时间内，则允许本次访问，否则采用执行(6e)：

[0044] (6e)采用颁发临时证书的方法，构建基于身份的密码体制IBC域中用户访问服务器和访问用户的安全通信；

[0045] (6f)基于身份的密码体制IBC域域代理服务器，采用将认证凭证写入信任联盟区块链的方法存储认证凭证；

[0046] (6g)结束认证。

[0047] 本发明与现有技术相比具有以下优点：

[0048] 第一，由于本发明构建联盟信任区块链，通过联盟信任区块链中节点之间的相互信任实现域间相互认证，克服了现有技术因需要对桥中心系统进行信任维护，导致维护负担增加的问题，使得本发明在服务器跨域认证方法中具有更好的实用性和可扩展性的优点。

[0049] 第二，由于本发明保存用户访问服务器的认证凭证，通过联盟信任区块链中节点服务器查询用户访问服务器的认证凭证实现重认证，克服了现有技术因需要多次访问相同服务器，导致重复认证时节点服务器计算和通信负担增加的问题，使得本发明在服务器跨域认证方法中具有效率更快的优点。

[0050] 第三，由于本发明构建联盟信任区块链，通过联盟信任区块链中节点之间的相互信任实现域间相互认证，克服了现有技术因需对访问用户进行域间身份认证，导致访问用户端承载较大计算和通信负担的问题，使得本发明在服务器跨域认证方法中具有更适用于主流的、资源受限的移动用户终端的优点。

附图说明

[0051] 图1是本发明的流程图。

具体实施方式

[0052] 下面结合附图1对本发明做进一步描述。

[0053] 步骤1，构建信任联盟区块链。

[0054] 根据区块链通信能力可容纳的信任联盟中节点服务器的数量，分别设置公钥基础设施PKI域和基于身份的密码体制IBC域的数量。

[0055] 将每个公钥基础设施PKI域中的证书服务器和每个基于身份的密码体制IBC域中的域代理服务器，作为信任联盟区块链的节点服务器。

[0056] 公钥基础设施PKI域中的证书服务器为基于身份的密码体制IBC域中域代理服务器颁发证书。

[0057] 根据证书的大小选择哈希函数，生成证书的哈希值。

[0058] 将证书的哈希值作为第一个区块，在区块体内保存，得到信任联盟区块链。

[0059] 步骤2，认证公钥基础设施PKI域中用户访问服务器的身份。

[0060] 基于身份的密码体制IBC域中请求访问的用户，利用自身私钥和国产标识密码SM9签名算法，对自身身份标识ID计算生成的签名认证申请，将签名认证申请发送给向域代理服务器。

[0061] 基于身份的密码体制IBC域中域代理服务器，验证请求访问的用户的身份是否合法，若是，判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件，否则，认证结束。

[0062] 请求访问的用户的公钥，由国产标识密码SM9签名验证算法对签名认证申请进行验证，通过验证的签名认证申请为用户身份合法。

[0063] 判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件，若是，则采用颁发临时身份的方法，构建公钥基础设施PKI域中用户请求服务器与访问用户的安全通信，否则认证失败。

[0064] 所述的相互信任条件是指同时满足以下两个条件的情形：

[0065] 条件1，公钥基础设施PKI域证书服务器，在信任联盟区块链上查询基于身份的密码体制IBC域中域代理服务器的证书，证书状态为声明；

[0066] 条件2，基于身份的密码体制IBC域中域代理服务器，在信任联盟区块链上查询公

钥基础设施PKI域证书服务器的证书，证书状态为声明。

[0067] 公钥基础设施PKI域中证书服务器，采用将认证凭证写入信任联盟区块链的方法存储认证凭证。

[0068] 所述的颁发临时身份的方法的具体步骤如下：

[0069] 第1步，基于身份的密码体制IBC域的域代理服务器，生成公钥基础设施PKI域中用户访问服务器的临时身份信息，将临时身份信息发送至公钥基础设施PKI域证书服务器；

[0070] 第2步，公钥基础设施PKI域中证书服务器转发临时身份信息给用户访问的服务器；

[0071] 第3步，公钥基础设施PKI域中提供服务的服务器保存临时身份信息，利用临时身份信息与基于身份的密码体制IBC域中请求服务用户进行安全通信。

[0072] 所述的将认证凭证写入信任联盟区块链的方法的具体步骤如下：

[0073] 第1步，信任联盟区块链中节点服务器将成功认证用户访问服务器的身份标识信息ID生成认证凭证；

[0074] 第2步，信任联盟区块链中节点服务器根据认证凭证的大小选择哈希函数，利用哈希运算，将认证凭证生成哈希值，将哈希值写入区块链。

[0075] 结束认证。

[0076] 步骤3，认证基于身份的密码体制IBC域中用户访问服务器的身份。

[0077] 公钥基础设施PKI域中请求访问的用户，向证书服务器发送认证申请。

[0078] 公钥基础设施PKI域证书服务器，在信任联盟区块链上查询访问用户的证书状态，如果证书状态为声明则判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件，如果证书状态为撤销，则结束认证。

[0079] 判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件，若是，则采用颁发临时证书的方法，构建公钥基础设施PKI域中用户访问服务器和申请访问用户的安全通信，否则结束认证。

[0080] 所述的相互信任条件是指同时满足以下两个条件的情形：

[0081] 条件1，公钥基础设施PKI域证书服务器，在信任联盟区块链上查询基于身份的密码体制IBC域中域代理服务器的证书，证书状态为声明；

[0082] 条件2，基于身份的密码体制IBC域中域代理服务器，在信任联盟区块链上查询公钥基础设施PKI域证书服务器的证书，证书状态为声明。

[0083] 所述的颁发临时证书的方法的具体步骤如下：

[0084] 第1步，公钥基础设施PKI域证书服务器，生成基于身份的密码体制IBC域中用户访问服务器的临时证书，将临时证书发送给基于身份的密码体制IBC域域代理服务器；

[0085] 第2步，基于身份的密码体制IBC域中，域代理服务器将临时证书转发至用户访问服务器；

[0086] 第3步，基于身份的密码体制IBC域中，用户访问服务器保存临时证书，利用临时证书中的身份信息与公钥基础设施PKI域中请求服务用户实现安全通信。

[0087] 基于身份的密码体制IBC域域代理服务器，采用将认证凭证写入信任联盟区块链的方法存储认证凭证。

[0088] 所述的将认证凭证写入信任联盟区块链的方法的具体步骤如下：

[0089] 第1步，信任联盟区块链中节点服务器将成功认证用户访问服务器的身份标识信息ID生成认证凭证；

[0090] 第2步，信任联盟区块链中节点服务器根据认证凭证的大小选择哈希函数，利用哈希运算，将认证凭证生成哈希值，将哈希值写入区块链。

[0091] 结束认证。

[0092] 步骤4，设置认证凭证的有效时间。

[0093] 根据公钥基础设施PKI域中用访问户服务器的安全等级，将其存储在信任联盟区块链上的认证凭证作为安全等级对应的有效时间。

[0094] 根据基于身份的密码体制IBC域中用访问户服务器的安全等级，将其存储在信任联盟区块链上的认证凭证作为安全等级对应的有效时间。

[0095] 步骤5，重认证公钥基础设施PKI域中用户访问服务器的身份；

[0096] 基于身份的密码体制IBC域中的其他用户，向域代理服务器发送身份签名申请和访问申请。

[0097] 判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件，若是，基于身份的密码体制IBC域域代理服务器，利用公钥基础设施PKI域中用户访问服务器的身份标识信息ID，生成认证凭证，否则，结束认证。

[0098] 所述的相互信任条件是指同时满足以下两个条件的情形：

[0099] 条件1，公钥基础设施PKI域证书服务器，在信任联盟区块链上查询基于身份的密码体制IBC域中域代理服务器的证书，证书状态为声明；

[0100] 条件2，基于身份的密码体制IBC域中域代理服务器，在信任联盟区块链上查询公钥基础设施PKI域证书服务器的证书，证书状态为声明。

[0101] 基于身份的密码体制IBC域域代理服务器，在信任联盟区块链上查询认证凭证，如果查询到认证凭证，认证凭证在有效时间内，则允许本次访问，认证结束，否则利用颁发临时身份的方法，构建公钥基础设施PKI域中用户访问服务器与访问用户的安全通信。

[0102] 所述的颁发临时身份的方法的具体步骤如下：

[0103] 第1步，基于身份的密码体制IBC域域代理服务器，生成公钥基础设施PKI域中用户访问服务器的临时身份信息，将临时身份信息发送至公钥基础设施PKI域证书服务器；

[0104] 第2步，公钥基础设施PKI域中证书服务器转发临时身份信息给用户访问的服务器；

[0105] 第3步，公钥基础设施PKI域中提供服务的服务器保存临时身份信息，利用临时身份信息与基于身份的密码体制IBC域中请求服务用户进行安全通信。

[0106] 公钥基础设施PKI域中证书服务器，采用将认证凭证写入信任联盟区块链的方法存储认证凭证。

[0107] 所述的将认证凭证写入信任联盟区块链的方法的具体步骤如下：

[0108] 第1步，信任联盟区块链中节点服务器将成功认证用户访问服务器的身份标识信息ID生成认证凭证；

[0109] 第2步，信任联盟区块链中节点服务器根据认证凭证的大小选择哈希函数，利用哈希运算，将认证凭证生成哈希值，将哈希值写入区块链。

[0110] 结束认证。

[0111] 步骤6,重认证基于身份的密码体制IBC域中用户访问服务器的身份。

[0112] 公钥基础设施PKI域中的其他用户,向证书服务器发送访问请求。

[0113] 判断公钥基础设施PKI域中证书服务器和基于身份的密码体制IBC域域代理服务器是否满足相互信任条件,若是,则公钥基础设施PKI域中证书服务器,利用密码体制IBC域中用户访问服务器的身份标识信息ID,生成认证凭证,否则执行结束认证。

[0114] 所述的相互信任条件是指同时满足以下两个条件的情形:

[0115] 条件1,公钥基础设施PKI域证书服务器,在信任联盟区块链上查询基于身份的密码体制IBC域中域代理服务器的证书,证书状态为声明;

[0116] 条件2,基于身份的密码体制IBC域中域代理服务器,在信任联盟区块链上查询公钥基础设施PKI域证书服务器的证书,证书状态为声明。

[0117] 公钥基础设施PKI域中证书服务器,在信任联盟区块链上查询认证凭证,如果查询到认证凭证,认证凭证在有效时间内,则允许本次访问,认证结束,否则采用颁发临时证书的方法,构建基于身份的密码体制IBC域中用户访问服务器和访问用户的安全通信。

[0118] 所述的颁发临时证书的方法的具体步骤如下:

[0119] 第1步,公钥基础设施PKI域证书服务器,生成基于身份的密码体制IBC域中用户访问服务器的临时证书,将临时证书发送给基于身份的密码体制IBC域域代理服务器;

[0120] 第2步,基于身份的密码体制IBC域中,域代理服务器将临时证书转发至用户访问服务器;

[0121] 第3步,基于身份的密码体制IBC域中,用户访问服务器保存临时证书,利用临时证书中的身份信息与公钥基础设施PKI域中请求服务用户实现安全通信。

[0122] 基于身份的密码体制IBC域域代理服务器,采用将认证凭证写入信任联盟区块链的方法存储认证凭证。

[0123] 所述的将认证凭证写入信任联盟区块链的方法的具体步骤如下:

[0124] 第1步,信任联盟区块链中节点服务器将成功认证用户访问服务器的身份标识信息ID生成认证凭证;

[0125] 第2步,信任联盟区块链中节点服务器根据认证凭证的大小选择哈希函数,利用哈希运算,将认证凭证生成哈希值,将哈希值写入区块链。

[0126] 结束认证。

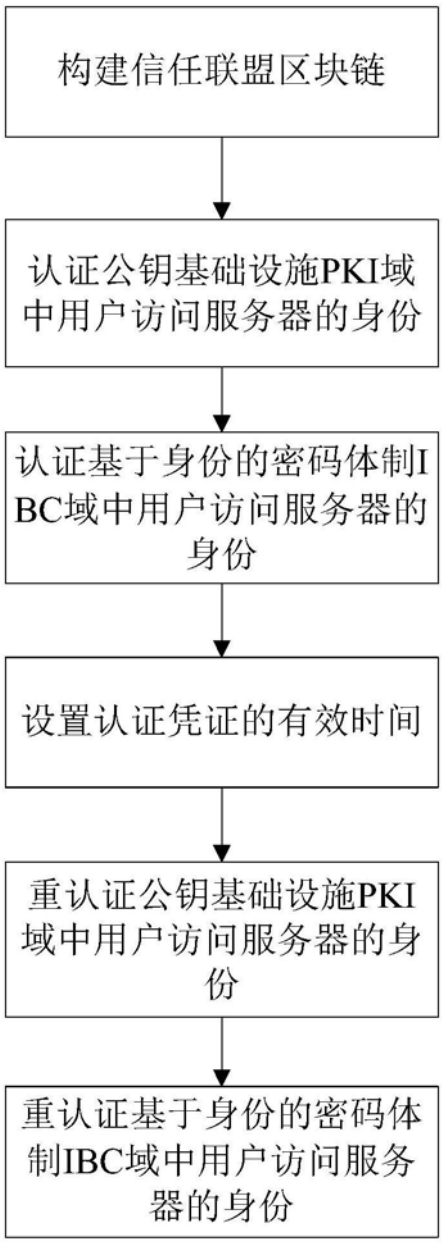

构建信任联盟区块链
认证公钥基础设施PKI域中用户访问服务器的身份
认证基于身份的密码体制IBC域中用户访问服务器的身份
设置认证凭证的有效时间
重认证公钥基础设施PKI域中用户访问服务器的身份
重认证基于身份的密码体制IBC域中用户访问服务器的身份

图1