(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 111917543 A
(43)申请公布日 2020.11.10

(21)申请号 202010820835.7

(22)申请日 2020.08.14

(71)申请人 国科量子通信网络有限公司
地址 201203 上海市浦东新区自由贸易试验区芳春路400号1幢3层

(72)发明人 李晋 杨勇华 张雪松 王家勇 方可燕

(74)专利代理机构 北京汉鼎理利专利代理事务所(特殊普通合伙) 11618
代理人 潘满根

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)
H04B 10/70(2013.01)

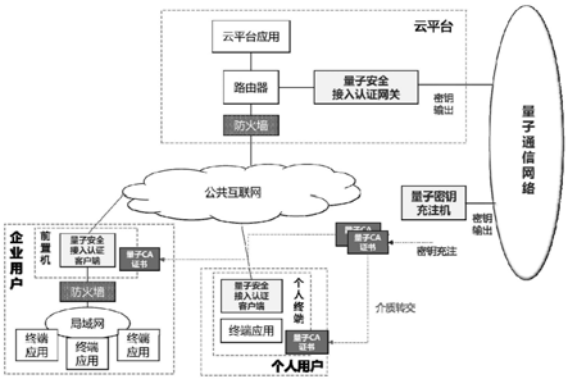
权利要求书2页 说明书5页 附图1页

(54)发明名称

用户接入云平台安全接入认证系统及其应用方法

(57)摘要

本发明提供用户接入云平台安全接入认证系统及其应用方法,本发明用户接入云平台安全接入认证系统包括量子保密通信装置,所述量子保密通信装置在用户端和云平台端原有数字认证基础上增加量子安全接入认证机制,数字认证中的用户端CA数字证书模块同时充当量子安全接入认证机制中的用户端量子CA证书模块。本发明将依托量子保密通信网络提供的安全的端到端对称密钥分发能力,设计了基于对称密钥的用户接入云平台应用量子安全接入认证系统,该系统可具备抗量子计算机破解攻击的能力,有效提升用户接入云平台的认证安全性。



CN 111917543 A

1.用户接入云平台安全接入认证系统,其特征在于,所述系统包括量子保密通信装置,所述量子保密通信装置在用户端和云平台端原有数字认证基础上增加量子安全接入认证机制,数字认证中的用户端CA数字证书模块同时充当量子安全接入认证机制中的用户端量子CA证书模块。

2.根据权利要求1所述的认证系统,其特征在于,所述量子保密通信装置包括量子通信网络,量子密钥充注机,设置在云平台端的量子安全接入认证网关,和设置在用户端的量子安全接入认证客户端和所述量子CA证书模块;

所述量子密钥充注机通过接入所述量子通信网络,从所述量子通信网络获取量子密钥,并向所述量子CA证书模块中充注量子密钥;

所述量子CA证书模块在证书内部加密安全保存量子密钥,并提供基于量子密钥的认证信息加解密运算功能;

所述量子安全接入认证客户端利用量子CA证书模块完成接入认证信息的生成、网关认证信息的解密;和

所述量子安全接入认证网关通过接入所述量子通信网络,获取与所述充注机所获取的量子密钥对称的量子密钥,并与所述量子安全接入认证客户端配合,实现基于量子CA证书模块中量子密钥的量子安全接入用户的身份认证。

3.根据权利要求2所述的认证系统,其特征在于,用户端的量子CA证书模块中充注的量子密钥编号与该用户端之间的对应关系,以及该用户端的账号有效期已在所述量子安全接入认证网关中记录并存储。

4.根据权利要求2所述的认证系统,其特征在于,用户端利用所述量子安全接入认证客户端读取所述量子CA证书模块中原有的用户端数字证书,并基于该用户端数字证书向所述量子安全接入认证网关进行接入认证。

5.根据权利要求2所述的认证系统,其特征在于,所述用户端是个人终端或者企业用户终端;企业用户终端中在其局域网前端设置有前置机,用于设置量子安全接入认证客户端和量子CA证书模块。

6.根据权利要求2-5任一所述的认证系统的应用方法,其特征在于,所述方法包括以下步骤:

步骤1,对所述量子CA证书模块充注量子密钥,与该充注量子密钥对称的量子密钥已通过量子通信网络安全分发至量子安全接入认证网关,并在网关中存储;每个用户端的量子CA证书模块中充注的量子密钥编号与该用户端之间的对应关系和/或用户端的账号有效期已在所述量子安全接入认证网关中记录并存储;

步骤2,将所述量子CA证书模块接入用户端,通过量子安全接入认证客户端,完成用户端登录,然后配置量子安全接入认证客户端和云平台端;

步骤3,用户端利用量子安全接入认证客户端,读取量子CA证书中原有的用户数字证书,并基于该数字证书向量子安全接入认证网关进行接入认证;

步骤4,用户端的量子安全接入认证客户端将该用户端的信息合成认证数据,并通过量子CA证书模块的量子安全认证信息生成接口提交给量子CA证书模块;

步骤5,量子CA证书模块从该证书模块中存储的量子密钥中随机选取一个量子密钥,利用该量子密钥和对称加密算法对所述合成认证数据加密,获得加密后的认证数据,将选取

的量子密钥的编号和加密后的认证数据返回给量子安全接入认证客户端;和

步骤6,用户端将选取的量子密钥的编号和加密后的认证数据合成一个认证数据包,通过公共互联网发送给量子安全接入认证网关进行认证,如核对无误,则通过认证。

7.根据权利要求6所述的方法,其特征在于,还包括步骤7,完成认证后,量子安全接入认证网关应向量子安全认证客户端发送认证通过确认信息。

8.根据权利要求6所述的方法,其特征在于,步骤2中,配置量子安全接入认证客户端和云平台端量包括配置量子安全接入认证客户端和云平台端的网关IP地址和端口号。

9.根据权利要求6所述的方法,其特征在于,步骤5中,所述量子CA证书模块从证书模块中存储的量子密中随机选取一个128bit的密钥,然后利用该密钥和对称加密算法对所述合成认证数据加密。

10.根据权利要求9所述的方法,其特征在于,步骤6中,所述量子安全接入认证网关从数据包中提取认证数据和量子密钥的编号,并按照量子密钥的编号从量子安全接入认证网关的密钥池中调取相应的密钥,然后使用对称解密算法将认证数据解密为认证数据明文认证数据。

用户接入云平台安全接入认证系统及其应用方法

技术领域

[0001] 本发明涉及云计算安全领域,具体涉及用户接入云平台安全接入认证系统及其应用方法。

背景技术

[0002] 目前用户接入云平台应用的身份认证方式主要有两种:基于账号密码的认证方式和基于CA证书的接入认证方式。

[0003] 账号密码认证方式通常是用户在应用系统中注册账号,并设置账号对应的密码。在后续登录时正确输入账号密码,即可登录云平台应用。在普通的账号密码的基础上,可进一步增加手机短信动态密码的方式增强接入的安全性。

[0004] 但账号密码的方式普遍存在安全防护性能不足的问题:一方面密码设置简单且长期不更换,则难以抵御暴力破解;而密码设置过于复杂且经常更换,则如何安全的记忆或保存这些密码又成为一个难题;而短信动态密码的方式也容易遭受伪基站的攻击,并不足够安全可靠。

[0005] 基于CA证书的认证方式,是目前比较常见的利用密码技术实现用户身份认证接入控制的方式。首先用户要利用合法的资质证明材料,在CA机构的证书注册单位(RA)进行注册,并获得相应的CA证书;其次云平台需部署身份认证网关设备,负责对需要登录的用户进行证书验证;用户在登录云平台时,需要向身份认证网关提交证书信息,身份认证网关通过在线或离线的方式向CA机构进行证书验证,只有通过认证的用户才能进一步访问相应的应用。

[0006] 基于CA证书的接入认证方式,其安全性基于PKI体制中非对称密钥的计算数学原理,也即密钥长度足够的前提下(一般不低于2048比特),通过经典计算机对公钥进行破解获得私钥的时间应比所保护信息安全的时间要求(一般是证书的有效期)要更长。但随着量子计算机技术的飞速发展,一旦具备成熟的、量子比特位数足够多的量子计算机,结合相应的破解算法(如shor算法),则通过破解公钥获得私钥的时间将降低为分钟数量级,CA证书的接入认证安全性基础将不复存在。

发明内容

[0007] 为了解决上述问题,本发明提供一种用户接入云平台安全接入认证系统,所述系统包括量子保密通信装置,所述量子保密通信装置在用户端和云平台端原有数字认证基础上增加量子安全接入认证机制,数字认证中的用户端CA数字证书模块同时充当量子安全接入认证机制中的用户端量子CA证书模块。

[0008] 在一种实施方式中,所述量子保密通信装置包括量子通信网络,量子密钥充注机,设置在云平台端的量子安全接入认证网关,和设置在用户端的量子安全接入认证客户端和所述量子CA证书模块;所述量子密钥充注机通过接入所述量子通信网络,从所述量子通信网络获取量子密钥,并向所述量子CA证书模块中充注量子密钥;所述量子CA证书模块在证

书内部加密安全保存量子密钥，并提供基于量子密钥的认证信息加解密运算功能；所述量子安全接入认证客户端利用量子CA证书模块完成接入认证信息的生成、网关认证信息的解密；和所述量子安全接入认证网关通过接入所述量子通信网络，获取与所述充注机所获取的量子密钥对称的量子密钥，并与所述量子安全接入认证客户端配合，实现基于量子CA证书模块中量子密钥的量子安全接入用户的身份认证。

[0009] 在一种实施方式中，用户端的量子CA证书模块中充注的量子密钥编号与该用户端之间的对应关系，以及该用户端的账号有效期已在所述量子安全接入认证网关中记录并存储。

[0010] 在一种实施方式中，用户端利用所述量子安全接入认证客户端读取所述量子CA证书模块中原有的用户端数字证书，并基于该用户端数字证书向所述量子安全接入认证网关进行接入认证。

[0011] 在一种实施方式中，所述用户端是个人终端或者企业用户终端；企业用户终端中在其局域网前端设置有前置机，用于设置量子安全接入认证客户端和量子CA证书模块。

[0012] 在一种实施方式中本发明提供上述用户接入云平台安全接入认证系统的应用方法，所述方法包括以下步骤：步骤1，对所述量子CA证书模块充注量子密钥，与该充注量子密钥对称的量子密钥已通过量子通信网络安全分发至量子安全接入认证网关，并在网关中存储；每个用户端的量子CA证书模块中充注的量子密钥编号与该用户端之间的对应关系和/或用户端的账号有效期已在所述量子安全接入认证网关中记录并存储；步骤2，将所述量子CA证书模块接入用户端，通过量子安全接入认证客户端，完成用户端登录，然后配置量子安全接入认证客户端和云平台端；步骤3，用户端利用量子安全接入认证客户端，读取量子CA证书中原有的用户数字证书，并基于该数字证书向量子安全接入认证网关进行接入认证；步骤4，用户端的量子安全接入认证客户端将该用户端的信息合成认证数据，并通过量子CA证书模块的量子安全认证信息生成接口提交给量子CA证书模块；步骤5，量子CA证书模块从该证书模块中存储的量子密钥中随机选取一个量子密钥，利用该量子密钥和对称加密算法对所述合成认证数据加密，获得加密后的认证数据，将选取的量子密钥的编号和加密后的认证数据返回给量子安全接入认证客户端；和步骤6，用户端将选取的量子密钥的编号和加密后的认证数据合成一个认证数据包，通过公共互联网发送给量子安全接入认证网关进行认证，如核对无误，则通过认证。

[0013] 在一种实施实施方式中，还包括步骤7，完成认证后，量子安全接入认证网关应向量子安全认证客户端发送认证通过确认信息。

[0014] 在一种实施方式中，步骤2中，配置量子安全接入认证客户端和云平台端量包括配置量子安全接入认证客户端和云平台端的网关IP地址和端口号。

[0015] 在一种实施方式中，步骤5中，所述量子CA证书模块从证书模块中存储的量子密中随机选取一个128bit的密钥，然后利用该密钥和对称加密算法对所述合成认证数据加密。

[0016] 在一种实施方式中，步骤6中，所述量子安全接入认证网关从数据包中提取认证数据和量子密钥的编号，并按照量子密钥的编号从量子安全接入认证网关的密钥池中调取相应的密钥，然后使用对称解密算法将认证数据解密为认证数据明文认证数据。

[0017] 在本发明中，各种术语含义如下。

[0018] CA证书模块：由CA(Certification Authority)机构签发的，用于证明用户身份的

数字信息及承载这些信息的载体，证书内容包含电子签证机关的信息、公钥用户信息、公钥、权威机构的签字和有效期等等。

[0019] PKI：公钥基础设施(Public Key Infrastructure)是一个包括硬件、软件、人员、策略和规程的集合，用来实现基于公钥密码体制的密钥和证书的产生、管理、存储、分发和撤销等功能。

[0020] 密钥：控制密码算法运算的关键信息或参数。

[0021] 对称加密：采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密。

[0022] 非对称密码体制：非对称密码体制又称为双密钥密码体制或公开密钥密码体制，是指加密和解密操作分别使用两个不同的密钥，并且不可能由加密密钥推导出解密密钥。

[0023] 量子通信网络：基于量子密钥分发技术构建的网络，可为网络内的终端节点间实现安全的对称的密钥分发生成，其安全性由量子力学特性保证。。

[0024] 在本发明中，用户接入云平台安全接入认证系统基于对称密码体制的接入认证与基于非对称密码体制的CA证书认证方式融合应用，在抗量子计算机破解方面具有优势，可在增加一倍密钥长度之后就防止量子计算机的破解仿冒。

[0025] 在本发明中，使用了量子通信网络来实现广域的对称密钥安全分发，解决了传统对称密码技术应用中密钥分发传递困难的问题，减少了人工参与的环节，提升了系统运行的效率，降低了系统运维成本。

[0026] 本发明将依托量子保密通信网络提供的安全的端到端对称密钥分发能力，设计了基于对称密钥的用户接入云平台应用量子安全接入认证系统，该系统可具备抗量子计算机破解攻击的能力，有效提升用户接入云平台的认证安全性。

附图说明

[0027] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例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仅是本申请中记载的一些实施例，对于本领域普通技术人员来说，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

[0028] 图1是本发明的用户接入云平台安全接入认证系统的结构示意图。

具体实施方式

[0029] 为了使本领域技术领域人员更好地理解本申请中的技术方案，下面将结合实施例对本发明作进一步说明，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都应当属于本申请保护的范围。下面结合附图及实施例对本发明作进一步描述。

[0030] 如图1所示，用户接入云平台安全接入认证系统，所述系统包括量子保密通信装置，量子保密通信装置在用户端和云平台端原有数字认证基础上增加量子安全接入认证机制，数字认证中的用户客户端CA数字证书模块同时充当量子安全接入认证机制中的量子CA证书模块。

[0031] 本发明量子保密通信装置包括量子通信网络,量子密钥充注机,设置在云平台端的量子安全接入认证网关,和设置在用户端的量子安全接入认证客户端和量子CA证书模块。

[0032] 量子密钥充注机通过接入量子通信网络,从所述量子通信网络获取量子密钥,并向所述量子CA证书模块中充注量子密钥。

[0033] 量子CA证书模块在在数字CA证书模块内部加密安全保存量子密钥,并提供基于量子密钥的认证信息加解密运算功能。量子CA证书模块是符合《GM/T0016-2012智能密码钥匙密码应用接口规范》的通用CA证书,可以为USB key、TF卡、软件模块等形式。

[0034] 量子安全接入认证客户端利用量子CA证书模块完成接入认证信息的生成、网关认证信息的解密。

[0035] 量子安全接入认证网关通过接入量子通信网络,获取与充注机所获取的量子密钥对称的量子密钥,并与量子安全接入认证客户端配合,实现基于量子CA证书模块中量子密钥的量子安全接入用户的身份认证。量子密钥充注机通过接入量子通信网络,从量子通信网络获取密钥,并向合法的量子CA证书中充注密钥。

[0036] 量子CA证书是符合《GM/T0016-2012智能密码钥匙密码应用接口规范》的通用CA证书,可以为USB key、TF卡、软件模块等形式,可在证书内部加密安全保存量子密钥,并提供基于量子密钥的认证信息加解密运算功能。

[0037] 量子安全接入认证网关通过接入量子通信网络,获取量子密钥(与量子密钥充注机所获取的密钥为对称密钥),并与量子安全接入认证客户端配合,实现基于量子CA证书中量子密钥的量子安全接入身份认证。

[0038] 量子安全接入认证客户端可利用量子CA证书完成接入认证信息的生成、网关认证信息的解密。

[0039] 本发明用户接入云平台安全接入认证系统的应用包含以下步骤:

[0040] (1)准备工作

[0041] 需要通过量子安全接入认证方式登录云平台的用户A已完成量子安全接入认证客户端设置,并已成功申领量子CA证书模块UkeyA,UkeyA在有效期内;

[0042] 量子CA证书模块UkeyA中已完成一定数量的量子密钥QKeys的充注,对称的量子密钥QKeys已通过量子通信网络安全分发至量子安全接入认证网关,并在网关中存储;需注意,量子密钥的充注,并不破坏基础CA证书模块中的相关数字证书信息;

[0043] 用户A所领取的量子CA证书模块UkeyA中充注的量子密钥编号UkeyA-Num与该用户A之间的对应关系,以及用户A的账号有效期已在量子安全接入认证网关中记录并存储。

[0044] (2)用户登录用户端

[0045] 用户A在个人终端(如计算机、智能手机等)或者企业的上网前置机上安装量子安全接入认证客户端,并将量子CA证书模块正常接入该终端或前置机,打开量子安全接入认证客户端,正确输入客户端的账号密码,正确输入量子CA证书模块的登录密码,完成用户端。

[0046] 在登录用户端后,用户A配置量子安全接入认证客户端的网关IP地址、端口号等信息,配置需访问的云平台应用访问IP地址、端口号等。

[0047] (3)CA证书模块接入认证

[0048] 用户A可利用量子安全接入认证客户端，读取量子CA证书模块中原有的用户A数字证书CertA，并基于CertA向量子安全接入认证网关进行接入认证，相关认证交互协议及流程符合商密的相关规范，基于非对称密钥加解密技术，不受本专利权利申请限制。

[0049] (4)量子安全接入认证

[0050] 在完成基于CA证书模块的接入认证后，启动基于量子密钥的接入认证，具体步骤包括：

[0051] 生成加密认证信息：用户A的量子安全接入认证客户端将用户A的身份信息、当前时间等拼合成本次认证数据UsrData，并通过量子CA证书模块的量子安全认证信息生成接口(函数调用接口)提交给量子CA证书模块；量子CA证书模块从证书中存储的量子密钥Qkeys中随机选取一个128bit的密钥QkeyA1，利用QkeyA1和对称加密算法(比如国密的SM4算法)对UsrData加密，获得加密后的认证数据Cr_UsrData，将Cr_UsrData和QkeyA1的编号A1返回给量子安全接入认证客户端；

[0052] 验证认证消息：用户A将Cr_UsrData和A1合成一个认证数据包，通过公共互联网发送给量子安全接入认证网关。认证网关从数据包中提取Cr_UsrData和A1，并按照A1从本地的密钥池中调取相应的密钥QkeyA1，然后使用对称解密算法(比如国密的SM4算法)将Cr_UsrData解密为认证数据明文UsrData，从UsrData中提取用户信息、时间信息等，与本地时间核对是否是过时信息，与本地数据库存储的用户信息列表核对该用户是否处于正常激活工作状态、该密钥编号与用户对应关系是否符合等。如核对无误，则表示该用户工作正常，通过认证。

[0053] 完成认证后，接入认证网关应向接入认证客户端发送认证通过确认信息，该确认新消息可使用A1对应的密钥QkeyA1进行加解密保护，确保整个接入认证的过程是安全的。

[0054] 本领域的技术人员容易理解的是，在不冲突的前提下，上述各有利方式可以自由地组合、叠加。

[0055] 以上仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。以上仅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技术人员来说，在不脱离本发明技术原理的前提下，还可以做出若干改进和变型，这些改进和变型也应视为本发明的保护范围。

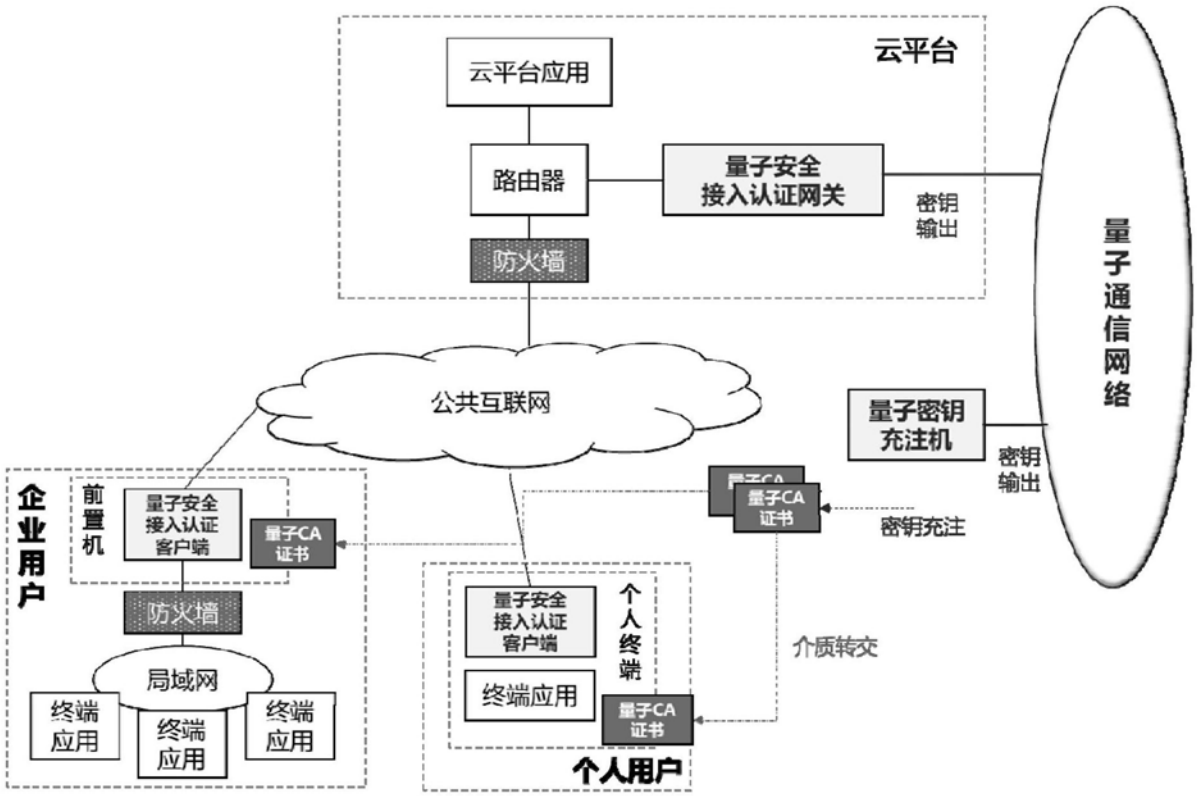

云平台
云平台应用
路由器
量子安全
接入认证网关
密钥
输出
防火墙
量子通信网络
公共互联网
量子密钥
充注机
密钥
输出
量子CA
证书
密钥充注
企业
用户
前置
机
量子安全
接入认证
客户端
量子CA
证书
防火墙
局域网
终端
应用
终端
应用
终端
应用
量子安全
接入认证
客户端
个人
终端
终端应用
量子CA
证书
介质转交
个人用户

图1