(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 111162902 A
(43)申请公布日 2020.05.15

(21)申请号 201911406286.2

(22)申请日 2019.12.31

(71)申请人 航天信息股份有限公司
地址 100195 北京市海淀区杏石口路甲18号

(72)发明人 李继 张平 李利 解军伟 吕志刚

(74)专利代理机构 北京工信联合知识产权代理有限公司 11266
代理人 白晓晰

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/08(2006.01)
G06Q 40/00(2012.01)

权利要求书1页 说明书3页 附图3页

(54)发明名称

一种基于税务证书的云签服务器

(57)摘要

本发明公开一种基于税务证书的云签服务器,包括:标准接口单元,用于提供多种云签设备的标准接口,所述接口通过加密的方式完成签名验证单元数据的传输;签名验证单元,用于通过标准接口单元接收云签设备发送的签名请求,读取云签设备的证书,完成云签设备的签名与验证;多用户远程使用单元,支持多用户通过客户端访问所述云签服务器,解决对国产数字签名功能和数字验签功能的签名验签服务器的需求问题。

CN 111162902 A

1.一种基于税务证书的云签服务器,其特征在于,包括:

标准接口单元,用于提供多种云签设备的标准接口,所述接口通过加密的方式完成签名验证单元数据的传输;

签名验证单元,用于通过标准接口单元接收云签设备发送的签名请求,读取云签设备的证书,完成云签设备的签名与验证;

多用户远程使用单元,支持多用户通过客户端访问所述云签服务器。

2.根据权利要求1所述的服务器,其特征在于,标准接口单元,用于提供多种云签设备的标准接口,包括:

安全客户端接口、国密接口、CSP接口、PKCS#11接口。

3.根据权利要求1所述的服务器,其特征在于,所述云签服务器,适用于A9\A10型号服务器。

4.根据权利要求1所述的服务器,其特征在于,所述云签设备,包括;

多税号密盘和PCIE密码卡。

5.根据权利要求4所述的服务器,其特征在于,所述多税号密盘和PCIE密码卡,支持不低于65535Slot,每个Slot可存储Default、RSA1024、RSA2048、SM2四个应用。

6.根据权利要求5所述的服务器,其特征在于,所述Defalut,用于P11证书应用,RSA1024、RSA2048、SM2用于国密接口证书应用。

7.根据权利要求6所述的服务器,其特征在于,还包括:

RSA1024、RSA2048、SM2分别对应于rsa1024算法、rsa2048算法、sm2算法的数字证书。

8.根据权利要求1所述的服务器,其特征在于,所述接口通过加密的方式完成签名验证单元数据的传输,包括:

云签设备调用云签服务器所提供的函数进行签名验证,函数名称和函数参数以密文形式传输给云签服务器,服务器执行签名验证并返回结果。

一种基于税务证书的云签服务器

技术领域

[0001] 本申请涉及云服务领域，具体涉及一种基于税务证书的云签服务器

背景技术

[0002] 随着信息资源数字化、网络化的加快，基于PKI体系和数字证书支撑的需求也日益增大，但当前商用密码基础设施，包括数字证书认证系统、密钥管理系统、密码设备及密码服务等环节中存在缺少顶层设计，产品各自为政、缺少统一接口的问题。所以迫切需要在密码基础设施技术体系及标准规范研究成果的基础上开发一种能够提供数字签名功能和数字验签功能的签名验签服务，来解决上述问题。而目前的数字验签功能的签名验签服务的成本太高、接口不统一，更重要的一点是核心技术采用的是国外的芯片。因此研究适合国内需求的国产数字签名功能和数字验签功能的签名验签服务器是非常迫切的。

发明内容

[0003] 本申请提供一种基于税务证书的云签服务器，解决对国产数字签名功能和数字验签功能的签名验签服务器的需求问题。

[0004] 本申请提供一种基于税务证书的云签服务器，包括：

[0005] 标准接口单元，用于提供多种云签设备的标准接口，所述接口通过加密的方式完成签名验证单元数据的传输；

[0006] 签名验证单元，用于通过标准接口单元接收云签设备发送的签名请求，读取云签设备的证书，完成云签设备的签名与验证；

[0007] 多用户远程使用单元，支持多用户通过客户端访问所述云签服务器。

[0008] 优选的，标准接口单元，用于提供多种云签设备的标准接口，包括：

[0009] 安全客户端接口、国密接口、CSP接口、PKCS#11接口。

[0010] 优选的，所述云签服务器，适用于A9\A10型号服务器。

[0011] 优选的，所述云签设备，包括；

[0012] 多税号密盘和PCIE密码卡。

[0013] 优选的，所述多税号密盘和PCIE密码卡，支持不低于65535Slot，每个Slot可存储Default、RSA1024、RSA2048、SM2四个应用。

[0014] 优选的，所述Defalut，用于P11证书应用，RSA1024、RSA2048、SM2用于国密接口证书应用。

[0015] 优选的，还包括：

[0016] RSA1024、RSA2048、SM2分别对应于rsa1024算法、rsa2048算法、sm2算法的数字证书。

[0017] 优选的，所述接口通过加密的方式完成签名验证单元数据的传输，包括：

[0018] 云签设备调用云签服务器所提供的函数进行签名验证，函数名称和函数参数以密文形式传输给云签服务器，服务器执行签名验证并返回结果。

[0019] 本申请提供一种基于税务证书的云签服务器，包括：标准接口单元，用于提供多种云签设备的标准接口，所述接口通过加密的方式完成签名验证单元数据的传输；签名验证单元，用于通过标准接口单元接收云签设备发送的签名请求，读取云签设备的证书，完成云签设备的签名与验证；多用户远程使用单元，支持多用户通过客户端访问所述云签服务器，解决对国产数字签名功能和数字验签功能的签名验签服务器的需求问题。

附图说明

[0020] 图1是本申请提供的基于税务证书的小型云签服务器架构图；

[0021] 图2是本申请提供的基于税务证书的中型云签服务器架构图；

[0022] 图3是本申请提供的基于税务证书的大型云签服务器架构图；

[0023] 图4是本申请涉及的多税号密盘硬件架构图；

[0024] 图5是本申请涉及的PCIE密码卡硬件架构图；

[0025] 图6是本申请涉及的基于税务证书的云签服务器软件架构图；

[0026] 图7是本申请涉及的基于税务证书的云签服务器安全客户端接口签名流程图；

[0027] 图8是本申请涉及的基于税务证书的云签服务器云签服务制证流程图；

具体实施方式

[0028] 在下面的描述中阐述了很多具体细节以便于充分理解本申请。但是本申请能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本申请内涵的情况下做类似推广，因此本申请不受下面公开的具体实施的限制。

[0029] 本申请提供一种基于税务证书的云签服务器，包括：标准接口单元，用于提供多种云签设备的标准接口，所述接口通过加密的方式完成签名验证单元数据的传输；签名验证单元，用于通过标准接口单元接收云签设备发送的签名请求，读取云签设备的证书，完成云签设备的签名与验证；多用户远程使用单元，支持多用户通过客户端访问所述云签服务器，适用于低成本的小型、中型、大型云签服务器。小型云签服务器架构图如图1所示，中型云签服务器架构图如图2所示，大型云签服务器架构图如图3所示，具体的适用于A9\A10型号服务器。

[0030] 标准接口单元，用于提供多种云签设备的标准接口，所述接口通过加密的方式完成签名验证单元数据的传输，具有很强的安全防御性能。客户端通过访问标准接口即可以完成制证、签名、验签等操作，标准接口包括：安全客户端接口、国密接口、CSP接口、PKCS#11接口。云签设备，包括：多税号密盘和PCIE密码卡。多税号密盘的硬件架构如图4所示，PCIE密码卡的硬件架构如图5所示。证书存放在多税号密盘中或PCIE密码卡中。多税号密盘和PCIE密码卡，支持不低于65535Slot，每个Slot可存储Default、RSA1024、RSA2048、SM2四个应用。Defalut，用于P11证书应用，RSA1024、RSA2048、SM2用于国密接口证书应用。RSA1024、RSA2048、SM2分别对应于rsa1024算法、rsa2048算法、sm2算法的数字证书。

[0031] 基于税务证书的云签服务器软件架构如图5所示，从图中可以看出，云签服务器提供多种软件标准接口，能守接口函数客户端接口进行数据的加密传输。通过所述这云签服务器软件可以完成安全客户端的签名，其签名流程如图7所示，首先是连接云签设备，然后打开云签设备的slot，获取slot证书，根据slot证书对云签设备进行签名。

[0032] 云签服务制证流程如图8所示，首先，连接包含slot的云签设备并获取设备信息，根据设备信息对设备进行初始化，初始化后产生密钥对，将密钥对导入证书，完云签服务的制证。制证完成后，可以打开应用，对应用进行操作。

[0033] 本申请提供的一种基于税务证书的云签服务器，包括：标准接口单元，用于提供多种云签设备的标准接口，所述接口通过加密的方式完成签名验证单元数据的传输；签名验证单元，用于通过标准接口单元接收云签设备发送的签名请求，读取云签设备的证书，完成云签设备的签名与验证；多用户远程使用单元，支持多用户通过客户端访问所述云签服务器，解决对国产数字签名功能和数字验签功能的签名验签服务器的需求问题。同时支持低成本的小型、中型、大型云签服务器，使万元级的签名验签服务器降至百元级。同时具有很强的安全防御性能，实现了低成本、标准、兼容、安全等特点。

[0034] 最后应该说明的是：以上实施例仅用以说明本发明的技术方案而非对其限制，尽管参照上述实施例对本发明进行了详细的说明，所属领域的普通技术人员应当理解依然可以对本发明的具体实施方式进行修改或者等同替换，而未脱离本发明精神和范围的任何修改或者等同替换，其均应涵盖在本发明的权利要求范围当中。


网络接口
Arm9 核心平台
多税号密盘

图1


网络接口
X86 平台 linux 服务器
多税号密盘

图2


网络接口
高性能 X86 平台 linux 服务器
PCIE 密码卡

图3


USB 接口
智能卡芯片 AC4
密文存储
NAND FLASH

图4

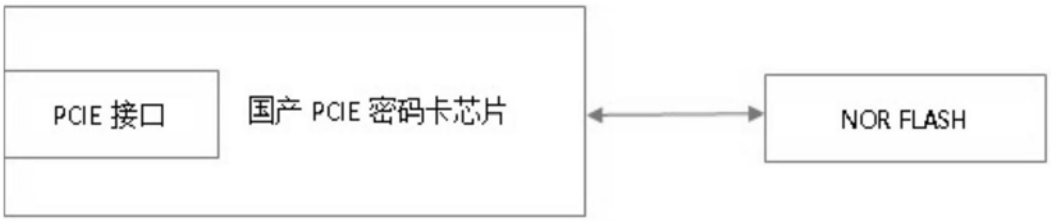
PCIE 接口
国产 PCIE 密码卡芯片
NOR FLASH

图5

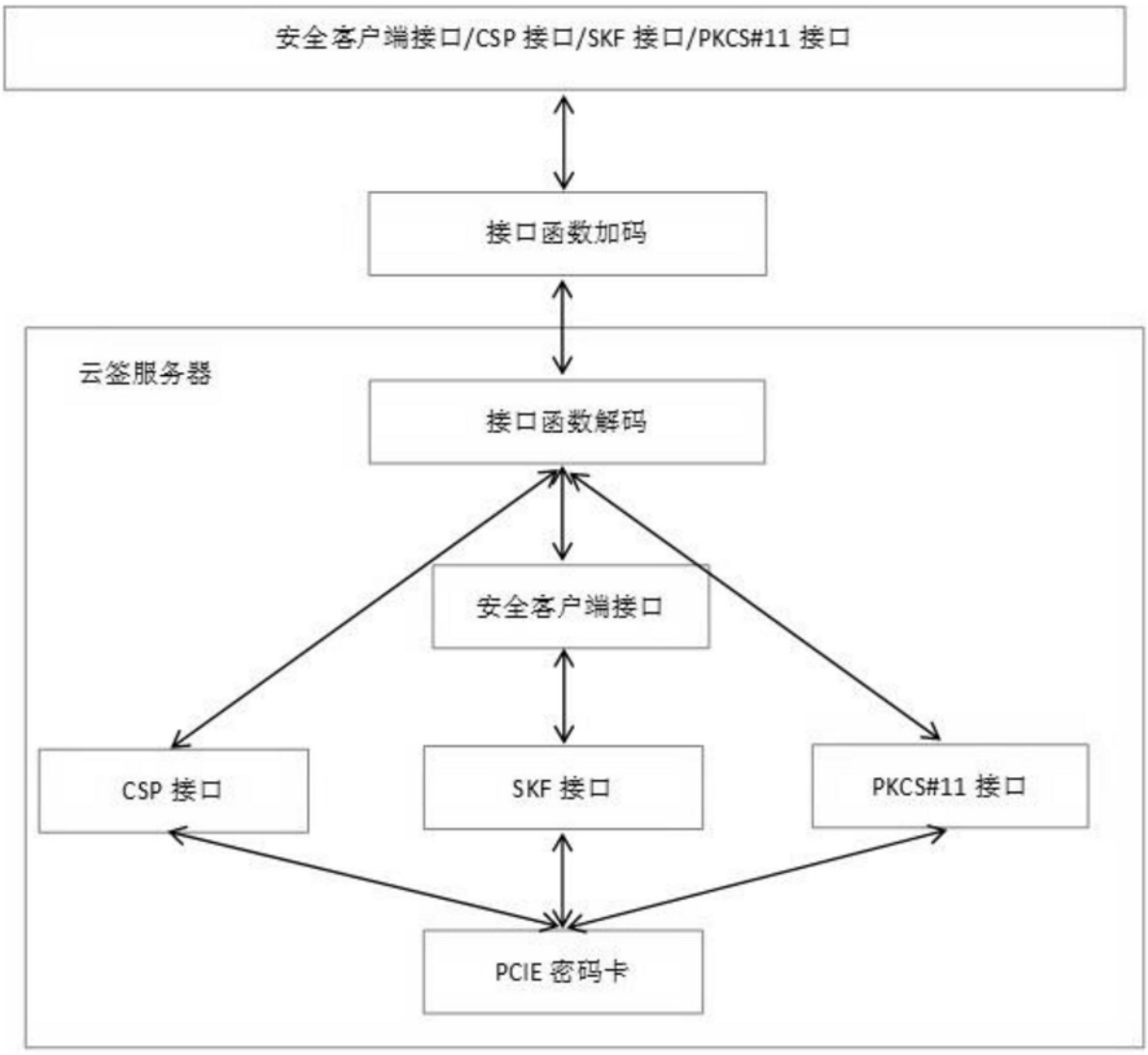
安全客户端接口/CSP 接口/SKF 接口/PKCS#11 接口
接口函数加码
云签服务器
接口函数解码
安全客户端接口
CSP 接口
SKF 接口
PKCS#11 接口
PCIE 密码卡

图6

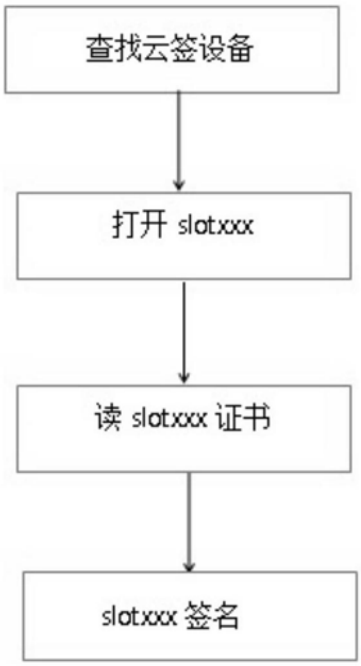
查找云签设备
打开 slotxxx
读 slotxxx 证书
slotxxx 签名

图7

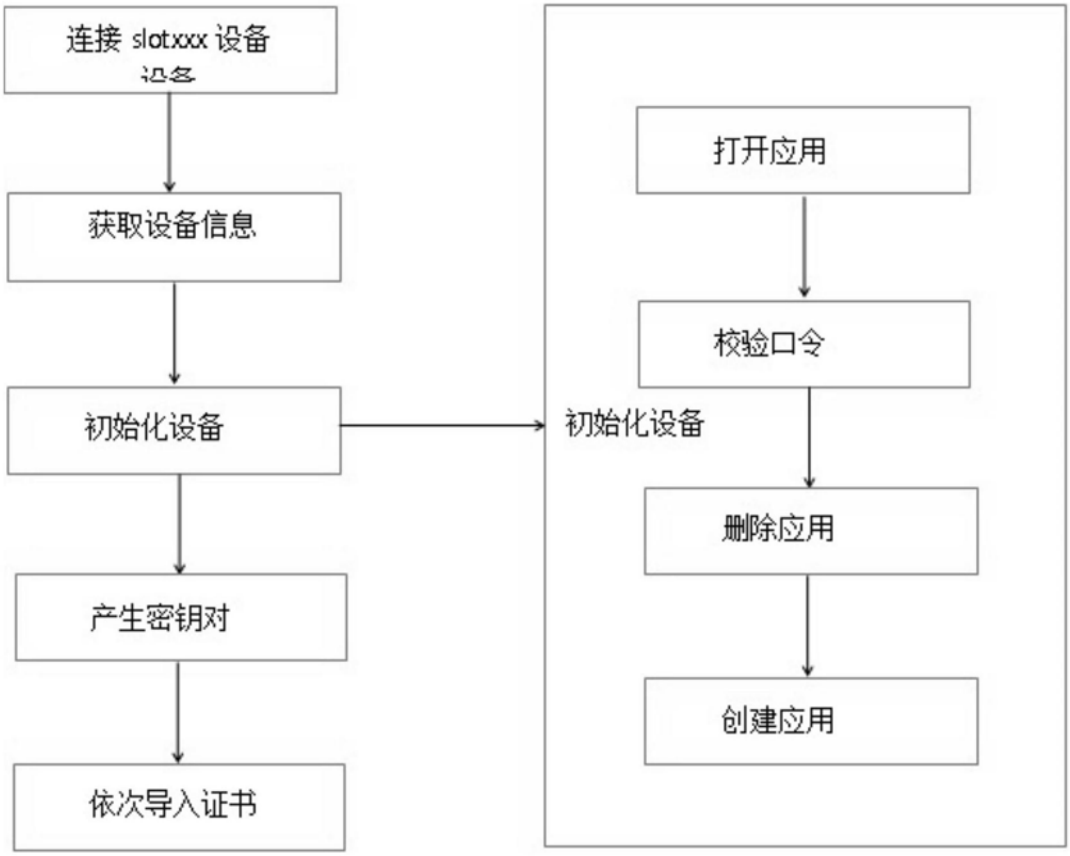
连接 slotxxx 设备
获取设备信息
初始化设备
产生密钥对
依次导入证书
初始化设备
打开应用
校验口令
删除应用
创建应用

图8