(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 110061991 A
(43)申请公布日 2019.07.26

(21)申请号 201910321731.9

(22)申请日 2019.04.22

(71)申请人 陈喆
地址 510000 广东省广州市海珠区君雅街35号1402房

(72)发明人 陈喆

(74)专利代理机构 广州市南锋专利事务所有限公司 44228
代理人 罗晓聪

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 12/40(2006.01)
H04L 12/66(2006.01)

权利要求书1页 说明书7页 附图2页

(54)发明名称

一种实现高速公路收费专网安全接入互联网的网关设置方法

(57)摘要

本发明公开了一种实现高速公路收费专网安全接入互联网的网关设置方法。该方法中数锁卡基于PCIe总线与安全网关主机上的API进行数据交换，数锁卡与安全网关主机使用的私有数据交换协议是采用基于国产密码算法的数字证书进行保护，通过双向认证握手协议和“一次一密”的数据加密传输方式。同时，该安全机制建立在双安全模块(SE)的硬件级密码运算的基础之上，通过数锁卡实现。为高速公路收费专网接入互联网提供一种不可路由的数据交换私，实现安全、高效隔离网络攻击，并可进行高速通信。

CN 110061991 A

1.一种实现高速公路收费专网安全接入互联网的网关设置方法,其特征在于:所述的高速公路专网通过一安全网关主机与位于互联网的云平台连接,该安全网关主机中具有一数锁卡,数锁卡基于PCIe总线与安全网关主机上的API进行数据交换,包括以下步骤:

第一步:数锁卡从内嵌的安全模块(SE1)获得芯片编号sn,并生成随机数r1,设置算法标识A1,从网关主机获取时间戳T1,设置M1＝sn||r1||A1||T1,最后使用安全模块(SE1)私钥对M1签名,得到签名值S1;

第二步:数锁卡通过PCIe向安全网关主机发送请求R1(R1＝M1||S1),安全网关主机部署的授权应用通过数锁卡API解释PCIe私有协议数据,并向云平台透传握手请求数据;

第三步:云平台对握手请求进行验证,如果验证通过则继续,否则发送出错消息,结束握手;

第四步:验证通过后,云平台生成工作密钥密文K1_Enc及校验值K1_Mac、MAC密钥密文K2_Enc及校验值K2_Mac、随机数r2,设置M2＝K1_Enc||K1_Mac||K2_Enc||K1_Mac||r2,最后使用私钥对M2||M1进行签名,得到签名值S2;

第五步:云平台发送响应R2给授权应用,授权应用通过数锁卡API按照PCIe私有协议编码格式发送握手相应数据;

第六步:数锁卡使用云平台证书对签名S2进行验证,如果验证通过则继续,否则产生错误,同时退出握手;

第七步:数锁卡将K1_Enc、K1_Mac、K2_Enc、K2_Mac导入安全模块(SE1),安全模块(SE1)在内部计算工作密钥的校验值和MAC密钥的校验值,分别进行比较,如果生成的校验值和从处理中心收到的校验值一致,则将K1、K2存储在SE的安全区域中,否则产生错误、结束握手;如果一致,则握手过程正常完成。

2.根据权利要求1所述的一种实现高速公路收费专网安全接入互联网的网关设置方法,其特征在于:所述的第三步中,云平台对握手请求进行验证,包括以下验证过程:

(1)云平台安全接入安全网关主机,根据芯片编码sn查找终端证书,如果找到则继续,否则发送出错消息,结束握手;

(2)云平台使用终端证书对S1验签,如果通过则继续,否则发送出错消息,结束握手;

(3)云平台提取随机数r1,并判断时间戳,在同一时间窗口进行验重,如果该时间窗口内随机数重复,则认为存在重放攻击的风险,发送出错消息,结束握手,否则继续。

3.根据权利要求1所述的一种实现高速公路收费专网安全接入互联网的网关设置方法,其特征在于:所述的安全网关主机内嵌安全模块(SE2),并且所述的数锁卡内嵌安全模块(SE1)与安全网关主机内嵌安全模块(SE2)的数字证书使用国密非对称算法进行握手,双向认证通过后实现加密通信。

4.根据权利要求3所述的一种实现高速公路收费专网安全接入互联网的网关设置方法,其特征在于:所述的数锁卡内嵌的安全模块(SE1)装载有交通运输部路网监测与应急处置中心收费公路联网结算管理中心注册的国密数字证书;安全网关主机内嵌安全模块(SE2)内装载同根的国密数字证书,实现数锁卡内嵌的安全模块(SE1)安全网关主机内嵌安全模块(SE2)的双向认证与加密通信。

5.根据权利要求1所述的一种实现高速公路收费专网安全接入互联网的网关设置方法,其特征在于:数锁卡通过网络接口接入高速公路联网收费系统专网。

一种实现高速公路收费专网安全接入互联网的网关设置方法

技术领域：

[0001] 本发明涉及高速公路收费联网技术领域，特指一种实现高速公路收费专网安全接入互联网的网关设置方法。

背景技术：

[0002] 近年来，随着“互联网+”的蓬勃发展，高速公路行业拥抱互联网开创“智慧高速”的时代已经来临。然而，高速公路收费系统涉及每年数千亿的高速公路收费资金信息，一直以来均采用与外网(特别是互联网)隔离的专网体系。ETC被认定为交通运输行业国家关键信息基础设施以后，依据《中华人民共和国网络安全法》对于国家关键信息基础设施的运行安全的相关规定和要求，如何在保障ETC这一国家关键信息基础设施安全运行的前提下，实现基于互联网的应用，已成为高速公路运营者必须重点应对的问题。

[0003] 随着取消省界收费站，高速公路联网区域将由省域扩大到全国，对专网安全性和可靠性更提出了苛刻的保障要求。为了保障这张遍及全国的高速公路收费系统网络实时、持续、不间断可靠运行，ETC国家联网中心提出建设一套扁平化、高可靠性的备用网络链路，支撑取消省界收费站后的全国高速公路收费联网运行。然而，为节省投资、提高可用性，能否通过互联网实现部-站网络链路备份，同步为“智慧高速”提供互联网服务?首先要解决安全性问题，同时要保证效率、兼顾成本。目前，高速公路收费系统接入互联网的方法主要有以下几种：

[0004] 第一种为直接接入。即或多或少采购一些网络安全产品进行防护。这种方式安全性非常低，曾经出现过大面积中木马和“勒索病毒”的情况。这种方案的致命缺陷就是：不安全。

[0005] 第二种是采用外接设备连接互联网，通过串口与专网主机进行数据交换。这种方式受串口传输速率制约，通信速度慢，而且对设备也没有认证机制，并不能保证外接设备就是安全的。这种方案的主要问题就是：效率低、不够安全。

[0006] 第三种是使用网闸隔离内外网。这种方式成本高、效率低，而且对运维、管理能力都有很高的要求。这种方案的最大问题就是：成本高、效率低。

[0007] 以上方案，都不符合构建部-站网络链路备份的要求，这就需要有一种安全、高速、低成本地为高速公路收费专网接入互联网方法。

[0008] 另外一方面，以下技术经过发展已经得到广泛的应用。

[0009] 数字证书技术：数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。以数字证书为核心的加密技术(加密传输、数字签名、数字信封等安全技术)可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性及交易的不可抵赖性。

[0010] 最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。

[0011] 证书授权中心(Certificate Authority)，简称CA中心，作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。CA中心为每个使用公开密钥的用

户发放一个数字证书,数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA机构的数字签名使得攻击者不能伪造和篡改证书。

[0012] 证书注册中心(Registration Authority),简称RA中心,是CA中心证书发放、管理的承担机构,主要负责证书申请者的信息录入、审核以及证书发放等工作,同时,对发放的证书完成相应的管理功能。

[0013] 交通运输部路网监测与应急处置中心收费公路联网结算管理中心,作为全国高速公路联网收费的运营管理机构,目前已对接交通运输行业CA中心建设了服务于全国高速公路联网收费的RA中心。这样,高速公路联网收费专网就基本具备了应用数字证书技术保障与外部网络进行数据传输的安全性的能力。

[0014] 国产密码算法:密码技术是信息安全保障的核心,我国绝大部分行业核心领域长期以来都是沿用国际通用的密码算法体系,主要包括RSA、SHA-1、3DES、MD5等密码算法。为确保密码算法的自主可控,降低敏感信息泄露和信息系统遭受攻击的风险,国家密码管理局制定并发布了国产密码算法及相关密码行业标准,统称“国产密码算法”。国产密码算法是我国自主研制、具有自主知识产权的一系列密码算法,享有较高安全性,主要包括SM2、SM3、SM4等一系列密码算法和标准。

[0015] SM2算法:SM2椭圆曲线公钥密码算法是一种非对称加密算法,替代RSA算法,适用于数字签名等高强度加解密运算。

[0016] SM3算法:SM3杂凑算法是一种摘要算法,替代SHA-1或MD5算法,适用于数字签名和验证消息认证码的生成与验证以及随机数的生成。

[0017] SM4算法:SM4分组密码算法是一种对称加密算法,替代3DES算法,适用于对速度要求高的较高强度加解密运算。

[0018] 为了这保证安全性的前提下提高运算性能,一般采用SM2、SM3、SM4三种算法组合使用的方式。

[0019] PCIE高速总线:PCI-Express(PCIe)是一种高速串行计算机扩展总线标准,最新的接口是PCIe3.0,信号频率达到8GT/s,数据带宽达到10GB/s。

[0020] PCIe的主要优势在于其减少延迟的能力,基于点到点拓扑,单独的串行链路将每个设备连接到根系统(主机)。由于其共享总线拓扑,可以对单个方向上的PCI总线进行仲裁(在多个主机的情况下),支持任何两个端点之间的全双工通信,同时跨多个端点的并发访问没有固有的限制。基本的PCI Express链路由两个低电压,差分驱动信号对组成:发送对和接收对,使用编码方案嵌入数据时钟以实现非常高的数据速率。

[0021] 本发明人基于上述技术,经过长期的实验,克服现有技术的不同,提出了以下技术方案。

发明内容:

[0022] 本发明所要解决的技术问题在于克服现有技术的不足,提供一种实现高速公路收费专网安全接入互联网的网关设置方法。该方法具有安全、高速,并且成本低等诸多优点。

[0023] 为了解决上述技术问题,本发明采用了下述技术方案:一种实现高速公路收费专网安全接入互联网的网关设置方法,其特征在于:所述的高速公路专网通过一安全网关主机与位于互联网的云平台连接,该安全网关主机中具有一数锁卡,数锁卡基于PCIe总线与

安全网关主机上的API进行数据交换，包括以下步骤：第一步：数锁卡从内嵌的安全模块(SE1)获得芯片编号sn，并生成随机数r1，设置算法标识A1，从网关主机获取时间戳T1，设置M1＝sn||r1||A1||T1，最后使用安全模块(SE1)私钥对M1签名，得到签名值S1；第二步：数锁卡通过PCIe向安全网关主机发送请求R1(R1＝M1||S1)，安全网关主机部署的授权应用通过数锁卡API解释PCIe私有协议数据，并向云平台透传握手请求数据；第三步：云平台对握手请求进行验证，如果验证通过则继续，否则发送出错消息，结束握手；第四步：验证通过后，云平台生成工作密钥密文K1_Enc及校验值K1_Mac、MAC密钥密文K2_Enc及校验值K2_Mac、随机数r2，设置M2＝K1_Enc||K1_Mac||K2_Enc||K1_Mac||r2，最后使用私钥对M2||M1进行签名，得到签名值S2；第五步：云平台发送响应R2给授权应用，授权应用通过数锁卡API按照PCIe私有协议编码格式发送握手相应数据；第六步：数锁卡使用云平台证书对签名S2进行验证，如果验证通过则继续，否则产生错误，同时退出握手；第七步：数锁卡将K1_Enc、K1_Mac、K2_Enc、K2_Mac导入安全模块(SE1)，安全模块(SE1)在内部计算工作密钥的校验值和MAC密钥的校验值，分别进行比较，如果生成的校验值和从处理中心收到的校验值一致，则将K1、K2存储在SE的安全区域中，否则产生错误、结束握手；如果一致，则握手过程正常完成。

[0024] 进一步而言，上述技术方案中，所述的第三步中，云平台对握手请求进行验证，包括以下验证过程：(1)云平台安全接入安全网关主机，根据芯片编码sn查找终端证书，如果找到则继续，否则发送出错消息，结束握手；(2)云平台使用终端证书对S1验签，如果通过则继续，否则发送出错消息，结束握手；(3)云平台提取随机数r1，并判断时间戳，在同一时间窗口进行验重，如果该时间窗口内随机数重复，则认为存在重放攻击的风险，发送出错消息，结束握手，否则继续。

[0025] 进一步而言，上述技术方案中，所述的安全网关主机内嵌安全模块SE2，并且所述的数锁卡内嵌安全模块SE1与安全网关主机内嵌安全模块SE2的数字证书使用国密非对称算法进行握手，双向认证通过后实现加密通信。

[0026] 进一步而言，上述技术方案中，所述的数锁卡内嵌的安全模块SE1装载有交通运输部路网监测与应急处置中心收费公路联网结算管理中心注册的国密数字证书；安全网关主机内嵌安全模块SE2内装载同根的国密数字证书，实现数锁卡内嵌的安全模块SE1安全网关主机内嵌安全模块SE2的双向认证与加密通信。

[0027] 进一步而言，上述技术方案中，数锁卡通过网络接口接入高速公路联网收费系统专网。

[0028] 本发明为一种一种实现高速公路收费专网安全接入互联网的网关设置方法，该方法是所使用的私有数据交换协议是采用基于国产密码算法的数字证书进行保护，符合交通行业数字证书认证相关标准规范，开发专用的双向认证握手协议和“一次一密”的数据加密传输协议。整套协议的安全机制建立在双安全模块(SE)的硬件级密码运算的基础之上，通过数锁卡实现。为高速公路收费专网接入互联网提供一种不可路由的数据交换私，实现安全、高效隔离网络攻击，并可进行高速通信。

附图说明：

[0029] 图1是本发明应用于安全网关的系统原理图；

[0030] 图2是本发明方法流程图。

具体实施方式：

[0031] 下面结合具体实施例和附图对本发明进一步说明。

[0032] 为了保障高速公路专网接入互联网的安全性和高性能，所以本发明提供了一种方法，通过一台安全网关将威胁隔离，并实现数据交换。本发明的技术方案是一种基于PCIe数锁卡的解决方案，其核心是通过PCIe高速总线建立一套不可路由的数据交换私有协议，实现安全、高效隔离网络攻击并进行高速通信。

[0033] 结合图1所示，这是本发明所应用的安全网关的架构图，其核心通过数锁卡实现，结合对应的辅助硬件设备。所有的硬件可以采用成熟产品，应用软件根据标准化接口进行开发。

[0034] 所述的数锁卡是一块PCIe接口的集成电路板卡，可使用ARM嵌入式平台，Linux操作系统。

[0035] 数锁卡可直接通过PCIe插槽插接在安全网关的主机上。数锁卡内嵌的安全模块SE1应当装载交通运输部路网监测与应急处置中心收费公路联网结算管理中心注册的国密数字证书1。同样的，安全网关的主机也内嵌安全模块SE2，并装载同根的国密数字证书2，实现与SE1的双向认证与加密通信。

[0036] 数锁卡通过RJ45接口接入高速公路联网收费系统专网，从高速公路联网收费专网的角度看，数锁卡就是专网内的一个IP化设备，数锁卡为高速公路专网提供Web Service服务，采用HTTPS协议通信，通过数锁卡提供互联网接入服务。

[0037] 数锁卡预制了基于PCIe总线的专有通讯协议，能与安装在安全网关的主机上的专用API进行数据交换。此通讯协议通过拼装底层的TLP事务层包，根据高速公路应用的电信特性选择合适的链路速度和数据带宽、合理设定最大有效载荷、启用最大数量的DMA通道，最大限度地发挥PCIe总线的传输效率。

[0038] 此通讯协议应用数锁卡上的SE1与安全网关主机上的SE2的数字证书，使用国密非对称算法进行握手，双向认证通过后实现加密通信。这样，就保证了数锁卡与安全网关主机之间，只有经过授权认证的数据，可以以加密的方式进行通信，而且使用的通讯协议是基于PCIe高速差分总线规格的非IP化私有协议，掐断了不符合此私有协议、未经管理部门授权的所有攻击，保障了内外网数据交换的安全性。

[0039] 任何新授权的应用下载和证书更新，都必须在SE1数字证书的保护下，通过双向认证授权和非对称加密传输方可完成。

[0040] 在线应用经过授权后，可以在安全网关主机上安装基于互联网的应用，其与通过互联网与服务后台进行数据交换以后，经本地API通过PCIe高速差分总线传送到数锁卡的授权应用数据缓存中，数锁卡的Web Service服务在授权应用数据缓存中存取数据。这样，从高速公路联网收费专网的角度看，数锁卡就是一个提供数据服务的互联网网站。

[0041] 结合图2所示，所述的高速公路专网通过一安全网关主机与位于互联网的云平台连接，该安全网关主机中具有一数锁卡，数锁卡基于PCIe总线与安全网关主机上的API进行数据交换。所述的安全网关主机内嵌安全模块SE2，并且所述的数锁卡内嵌安全模块SE1与安全网关主机内嵌安全模块SE2的数字证书使用国密非对称算法进行握手，双向认证通过

后实现加密通信。

[0042] 数锁卡通过网络接口接入高速公路联网收费系统专网。如图1所示的通过RJ45接口与高速公路联网收费系统专网

[0043] 本发明实现高速公路收费专网安全接入互联网的网关设置方法具体包括以下步骤：

[0044] 第一步：数锁卡从内嵌的安全模块(SE1)获得芯片编号sn，并生成随机数r1，设置算法标识A1，从安全网关主机获取时间戳T1，设置M1＝sn||r1||A1||T1，最后使用安全模块(SE1)私钥对M1签名，得到签名值S1。

[0045] 例如：具体实施时，随机生成的随机数r1设置为16字节，算法标识A1设置1字节。

[0046] 第二步：数锁卡通过PCIe向安全网关主机发送请求R1(R1＝M1||S1)，安全网关主机部署的授权应用通过数锁卡API解释PCIe私有协议数据，并向云平台透传握手请求数据。

[0047] 第三步：云平台对握手请求进行验证，如果验证通过则继续，否则发送出错消息，结束握手。

[0048] 该第三步中，云平台对握手请求进行验证，包括以下验证过程：

[0049] (1)云平台安全接入安全网关主机，根据芯片编码sn查找终端证书，如果找到则继续，否则发送出错消息，结束握手；

[0050] (2)云平台使用终端证书对S1验签，如果通过则继续，否则发送出错消息，结束握手；

[0051] (3)云平台提取随机数r1，并判断时间戳，在同一时间窗口进行验重，如果该时间窗口内随机数重复，则认为存在重放攻击的风险，发送出错消息，结束握手，否则继续。

[0052] 第四步：验证通过后，云平台生成工作密钥密文K1_Enc及校验值K1_Mac、MAC密钥密文K2_Enc及校验值K2_Mac、随机数r2，设置M2＝K1_Enc||K1_Mac||K2_Enc||K1_Mac||r2，最后使用私钥对M2||M1进行签名，得到签名值S2。

[0053] 例如：具体实施时，工作密钥密文K1_Enc设置为32字节，对应的校验值K1_Mac设置为8字节。MAC密钥密文K2_Enc设置为32字节，对应的校验值K2_Mac设置为8字节。随机数r2设置为16字节。K1_Enc和K2_Enc都是由对应的SE终端证书公钥进行非对称加密，密钥生成过程必须在硬件密码设备内部完成，校验值是工作密钥明文对系统保密因子做SM4加密，取前8字节。

[0054] 第五步：云平台发送响应R2给授权应用，授权应用通过数锁卡API按照PCIe私有协议编码格式发送握手相应数据；

[0055] 第六步：数锁卡使用云平台证书对签名S2进行验证，如果验证通过则继续，否则产生错误，同时退出握手；

[0056] 第七步：数锁卡将K1_Enc、K1_Mac、K2_Enc、K2_Mac导入安全模块(SE1)，安全模块(SE1)在内部计算工作密钥的校验值和MAC密钥的校验值，分别进行比较，如果生成的校验值和从处理中心收到的校验值一致，则将K1、K2存储在SE的安全区域中，否则产生错误、结束握手；如果一致，则握手过程正常完成。

[0057] 本发明中之所以采用PCIe总线，这是因为：PCIe链路协议使用“端到端的数据传送方式”，分为事务层、数据链路层和物理层三层结构，发送端和接收端中都含有TX(发送逻辑)和RX(接收逻辑)。其中事务层、数据链路层和物理层三层结构各自特点如下：

[0058] 1、物理层(PhysicalLayer):电气特性,使用两个单向的低电压差分对信号实现数据传输,同时也承担8b/10b的数据编解码(即每10bit链路数据中含8bit有效数据)。

[0059] 2、数据链路层(DataLink Layer):对该层传输的TLP进行组装和分拆,作为中间层为上下两层服务。

[0060] 3、事务层(Transaction Layer):接受从软件方送来的请求,并生成请求包传输到数据链路层。同时接受从数据链路层传来的数据包传递给软件,也就是对TLP进行分装和组装。

[0061] PCIe通信协议使用事务的方式通信,事务通过事务包(TLP)具体实现。PCIe通信协议所传送的数据报文首先通过事务层被封装为一个或者多个TLP,并通过PCIe总线的各个层次发送出去。事务层TLP的数据组织方法如下:TLP主要由三部分组成:Header,Data和CRC。

[0062] 1.Header域。事务层根据上层请求内容,生成TLP Header。Header内容包括发送者的相关信息、目标地址(该TLP要发给谁)、TLP类型(前面提到的诸如Memory read,Memory Write之类的)、数据长度(如果有的话)等等。

[0063] 2.Data Payload域。用以放有效载荷数据。但不是每个TLP都必须携带数据,是否携带数据是由Header域决定的。一个TLP最大载重是4KB,数据长度大于4KB的话,就需要分几个TLP传输。

[0064] 3.ECRC检验域。用于校验数据正确性。发送端对Header和Data生成一个CRC,接收端对收到的TLP,重新生成Header和Data的CRC,和收到的CRC比较,结果一样则说明数据在传输过程中没有出错,否则就有错。

[0065] 按上述则对数据进行编解码打包,通过事务层TLP实现PCIe高速通信。

[0066] 采用本发明的技术放哪后,可以对现有的高速公路收费系统进行进一步的优化。首先,本发明所采用的PCIe通信私有协议具有最优的传输效能。

[0067] 其次,SE芯片规范完全符合全国高速公路联网收费RA中心的数字证书应用要求,所有高速公路行业数字证书保护的双向认证技术,所有应用数据授权完全符合官方规定。

[0068] 综上所述,本发明采用的技术方案具备“网闸”的安全特性,支持数字证书电子签名,对接行业CA、RA中心受《电子签名法》保护;基于PCIe高速总线协议的不可路由私有通信协议效率极高,理论数据带宽可达10GB/s,远高于“网闸”、“串口”方案;采用PCIe集成电路板卡,成本略高于“串口”方案,但远低于“网闸”方案。

[0069] 本发明所采用的技术方案,将其应用于现有的高速公路收费系统,还可进一步进行其他应用,包括:

[0070] 1、在线费率计算:车辆在高速公路行驶中,如果出现标识点漏标的情况,这样到了出口,收费系统将无法还原车辆行驶路径,容易导致通行费计算偏差,多收车辆通行费或者造成高速公路经营单位损失。而通过本发明的技术方案后,高速公路联网收费管理部门可在云上提供在线还原车辆行驶路径的服务,高速公路收费车道通过数锁卡访问经授权的路径在线还原服务,即可正确计算漏标路径车辆的通行费。

[0071] 2、在线状态名单:目前的高速公路网络,状态名单是通过多级离线下载的,常常出现名单下载不及时导致误操作(如黑名单下载不及时,放跑了黑名单车辆;黑名单撤销不及时,误拦了已恢复正常的车辆)。而且状态名单种类有限,导致名单应用灵活性受限,极难实

现全网名单应用。通过本发明的技术方案，高速公路联网收费管理部门可在云上提供实时状态名单服务，高速公路收费车道通过数锁卡访问经授权的实时状态名单，即可实时判定当前车辆的状态，同时也为更多类型的状态名单的全网应用提供了入口。

[0072] 3、移动支付：近年来，随着“互联网+”的蓬勃发展，以微信支付、支付宝等为代表的手机支付迅速渗透至人们的日常生活当中。在这交通运输与信息化逐渐深度融合的时代，用户已形成手机支付的使用习惯，高速公路运营者也有为MTC用户解决现金不足问题、以及解决现金收费带来零钞、假钞、清点等问题的迫切需求。目前高速公路移动支付的接入模式，大多处于“裸奔”状态，存在极大的安全风险。通过本发明的技术方案，高速公路联网收费管理部门可在云上提供统一的移动支付接入服务，提供多支付渠道的聚合支付能力，高速公路收费车道通过数锁卡访问经授权的移动支付接入服务，即可实现移动支付的接入。此外，数锁卡的安全模块，还能为移动支付交易提供数字签名功能，确保交易的安全性，并受《电子签名法》保障。

[0073] 4、专网安全态势感知：由于高速公路联网收费专网分布广、终端数量庞大，尽管有关部门做了很多安全防范各种，但可能仍存在许多网络安全风险：例如未知的安全泄密通道、已经中毒或者被植入木马程序的主机等。通过本发明技术方案，高速公路联网收费管理部门可统一发布专网安全态势感知程序，安装到高速公路联网收费专网的主机上。该探针对机器是否安装了指定安全软件、是否开启了主机防火墙、是否采用了弱密码、是否有违规外联行为、是否开启网络共享(打开数据传输途径)、是否存在系统漏洞、是否私用违规外设、是否开启违规端口等安全漏洞进行扫描。一旦发现存在安全漏洞，立即通过数锁卡上传漏洞报警信息，高速公路联网收费管理部门即可采取相应措施及时防范安全风险蔓延。

[0074] 5、联合打逃治超：为治理超载、打击逃费，各省高速公路经营单位提出各种方式，也取得了一些成效。但是取消省界收费站以后，全网联通，打逃治超工作非一省之力可以完成。然而目前，各省打逃治超方式并不一致，而近期全国取消省界收费站工作压力山大，各省已无法抽出精力开展联合打逃治超工作。通过本发明技术方案，高速公路联网收费管理部门可在云上提供统一的联合打逃治超数据查询服务，高速公路收费车道通过数锁卡访问经授权的联合打逃治超数据查询服务，即可同步外省打逃治超工作成果，并采取相应措施。

[0075] 6、投诉取证：ETC全国联网以来，投诉跨省取证难一直是制约提升处理效率的主要问题。全国取消省界收费站以后，跨省投诉数量将剧增，提高投诉取证效率势所必然。通过本发明技术方案，高速公路联网收费管理部门可在云上提供统一的全网投诉取证采集、查询服务，收费现场发生争议时，高速公路收费车道通过数锁卡上传收费现场证据数据；用户事后投诉的，处理人可以通过云平台的投诉取证服务，向车道现场发起提取证据请求，高速公路收费车道通过数锁卡接收到提取证据请求，采集证据后再通过数锁卡上传收费现场证据数据。

[0076] 当然，以上所述仅为本发明的具体实施例而已，并非来限制本发明实施范围，凡依本发明申请专利范围所述构造、特征及原理所做的等效变化或修饰，均应包括于本发明申请专利范围内。

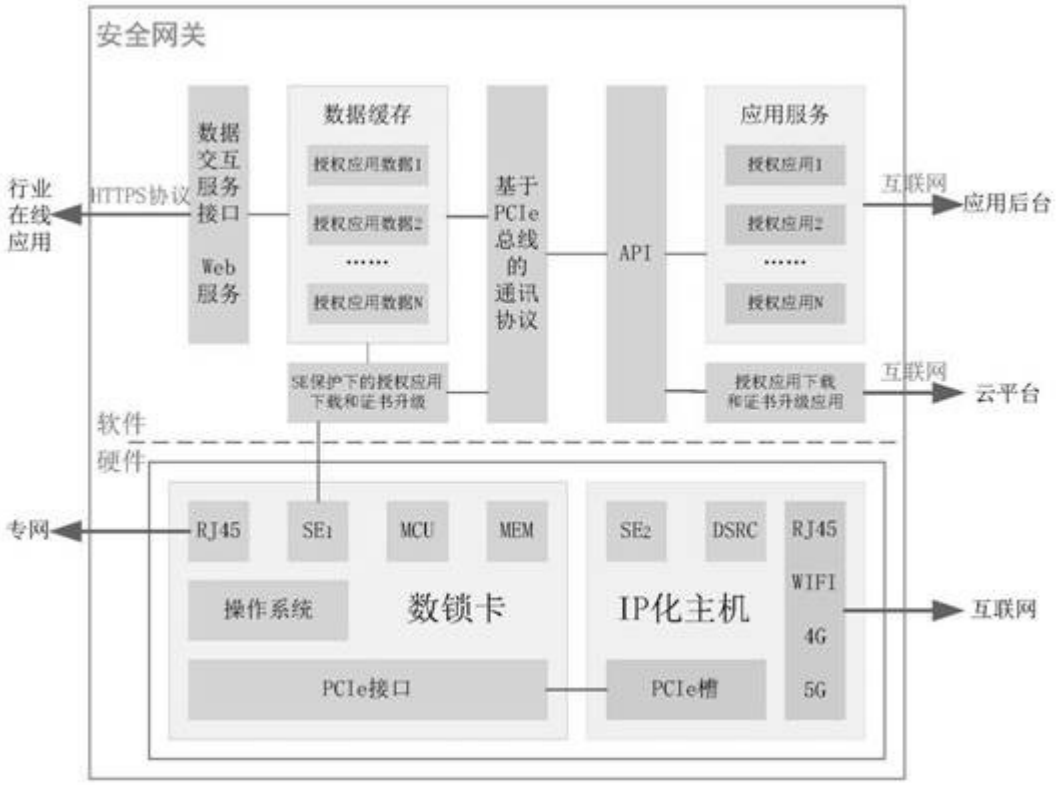
安全网关
数据交互服务接口
Web服务
数据缓存
授权应用数据1
授权应用数据2
.....
授权应用数据N
基于PCIe总线的通讯协议
API
应用服务
授权应用1
授权应用2
.....
授权应用N
行业在线应用
HTTPS协议
互联网
应用后台
SE保护下的授权应用下载和证书升级
授权应用下载和证书升级应用
互联网
云平台
软件
硬件
专网
RJ45
SE1
MCU
MEM
SE2
DSRC
RJ45
WIFI
4G
5G
操作系统
数锁卡
IP化主机
PCIe接口
PCIe槽
互联网

图1

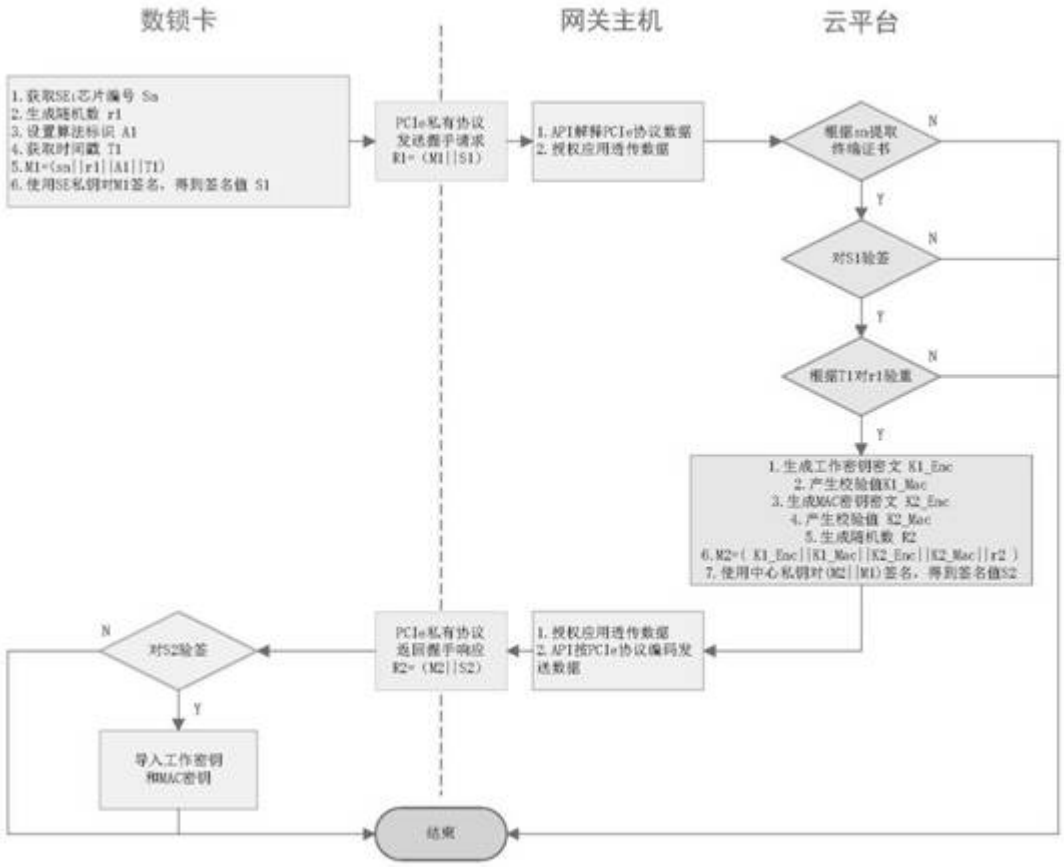
数锁卡
网关主机
云平台
1.获取SE(芯片编号 Sn
2.生成随机数 r1
3.设置算法标识 A1
4.获取时间戳 T1
5.M1=(sn||r1||A1||T1)
6.使用SE私钥对M1签名，得到签名值 S1
PCIe私有协议
发送握手请求
R1=（M1||S1）
1.API解释PCIe协议数据
2.授权应用透传数据
根据sn提取
终端证书
N
Y
对S1验签
N
Y
根据T1对r1验重
N
Y
1.生成工作密钥密文 K1_Enc
2.产生校验值K1_Mac
3.生成MAC密钥密文 K2_Enc
4.产生校验值 K2_Mac
5.生成随机数 R2
6.M2=(K1_Enc||K1_Mac||K2_Enc||K2_Mac||r2)
7.使用中心私钥对(M2||M1)签名，得到签名值S2
1.授权应用透传数据
2.API按PCIe协议编码发
送数据
PCIe私有协议
返回握手响应
R2=（M2||S2）
对S2验签
N
Y
导入工作密钥
和MAC密钥
结束

图2