doi:10.3969/j.issn.1671−5152.2026.10.002

一种物联网燃气表本地管理接口集中式接入认证方案及其实现

龙祥均[1, 2]，郝　强[1, 2]

1.重庆市智能燃气计量仪表企业工程技术研究中心；2.重庆前卫表业有限公司

摘　要：红外、蓝牙、星闪等本地管理接口，在给物联网燃气表的维护带来方便的同时，也带来了一些较大的安全隐患，比如接入时认证方式简单甚至缺乏认证，操作权限没有分级控制，燃气公司对接入账号不能集中掌控等。针对这些安全隐患问题，本文基于“集中接入认证+逐次鉴权+分层审计”的3层架构思想、可信终端绑定和动态凭证机制，融合硬件安全芯片与轻量级协议，设计了1种针对物联网燃气表本地管理接口的集中式接入认证控制方案。本方案既能有效解决物联网燃气表本地管理接口的接入安全控制问题，又能显著提升燃气公司对接入燃气表账号的管控能力。

关键词：物联网；燃气表；本地管理接口；安全；认证；鉴权

A Centralized Access Authentication Scheme for Local Management Interface of Internet of Things Gas Meter and Its Implementation

LONG Xiangjun[1,2], HAO Qiang[1,2]

1. Chongqing Smart Gas Metering Instrument Enterprise Engineering Technology Research Center;
2. Qianwei Meters (Chongqing) Co., Ltd.

Abstract: Local management interfaces, such as infrared, Bluetooth, and SparkLink, bring convenience to the maintenance of Internet of Things gas meters, but they also introduce some major security hazards, such as simple or even missing authentication methods during access, no hierarchical control over operational permissions, and the inability of gas companies to centrally control access accounts. To address these security hazards, this paper designed a centralized access authentication control scheme for the local management interface of Internet of Things gas meters, based on the three-layer architecture concept of “centralized access authentication + step-by-step authorization + hierarchical audit”, trusted terminal binding, and dynamic credential mechanism, integrating hardware security chips and lightweight protocols. This scheme can not only effectively solve the access security control problem of the local management interface of Internet of Things gas meters, but also significantly improve the control ability of gas companies over the accounts accessing gas meters.

Keywords: Internet of Things; gas meter; local management interface; security; authentication; authorization

物联网燃气表的本地管理接口是实现设备现场调试、参数配置、数据读取与应急处置的关键通道，其主要类型包括红外接口、蓝牙接口与星闪无线接口。物联网燃气表上的这种本地管理接口在带来方便的同时，也带来了一些安全上的隐患。现有技术中，大多使用物联网燃气表以本地固定密码的方式来进行本地单点接入认证，其密码通常较为简单，且更新频率低、管理不便，容易出现密码扩散风险，易出现1个密码多人、多机共用的情况。燃气公司难以统一管理密码、认证策略和具体的操作

[第一作者简介] 龙祥均，副总工程师，中级工程师，从事网络架构、数据通信、物联网通信、产品架构工作。

权限，更无法监控到燃气表上的接入和操作情况。

本地接口的开放性是运维效率的保障，但若缺乏系统性的安全控制和管理机制，可能会产生物联网燃气表安全风险。

1 本地管理接口存在的安全隐患分析

对燃气表管理接口的接入、登录，燃气公司和表厂往往缺乏可操作、简单、有效的控制手段，管不了，控不住。若管控过度，燃气表的运维便陷入僵局，导致故障定位迟滞，难以得到及时解决。部分表虽提供了简单的接入密码认证，但缺乏接入终端可信性保证机制、操作鉴权、审计能力，导致攻击者可轻易实施物理层入侵。管理接口的常见安全隐患如表1所示。

实践中，静态或动态加密方案，只是保证了通信过程、用户数据的安全，但不能对接入物联网燃气表的操作者身份、账号有效性、操作权限进行控制和管理，存在局限性。

2 解决方案和思路

针对上述安全隐患，本地管理接口的安全控制需满足如下“两统”和“四可”核心要求。

统一管理：接入登录燃气表的账号创建和删除、密码设置和修改、操作权限设置、账号绑定的登录终端设备、账号激活/去激活，必须实行集中的统一管理。

统一认证：所有本地接入请求，必须到认证服务器上进行统一认证，认证服务器可以掌握所有的接入登录信息。

可认证：所有本地接入请求必须验证登录者身份，实现“人–账号–维护终端”的唯一关联，拒绝未注册终端接入。

可鉴权：不同角色（运维员、工程师、管理员）拥有差异化操作权限，支持基于角色的访问操作权限控制，禁止越权操作。

可追溯：所有本地操作行为必须生成不可篡改的审计日志，日志包含：登录接入时间戳、认证结果、离开时间戳、操作类型、操作者ID（账号）、终端设备ID，日志存储于加密存储区或安全芯片，不可被篡改、销毁。

可动态：认证凭证必须具备时效性与一次性，采用连接心跳探测和随机接入码（或临时加密会话密钥）验证机制，杜绝重放攻击。

通过构建“一次一码（密码）、一次一认证、一次一鉴权、操作留痕、权限分层、设备可信”的本地接入安全控制体系，可实现燃气表本地管理接口由“被动安全”向“主动防护”的升级。

3 本地管理接口的接入安全控制总体方案

本方案采用“集中接入认证+逐次鉴权+分层审计” 的3层架构，融合硬件安全芯片与轻量级协议，实现端到端安全闭环。系统总体架构如图1所示，核心思想是将传统的、静态的、孤立的单点认证，提升为1个动态的、中心化的、联动闭环的接入控制系统。

认证服务器：用于创建、管理和维护接入认证账号，审计接入认证情况，也可部署服务器与物联网燃气表间临时会话密钥的分配功能。1个认证账号包括以下信息：账号、账号有效性、账号对应

表1 管理接口的安全隐患

安全隐患类型	攻击方式	实证案例	影响后果
无认证机制	红外重放攻击	攻击者使用红外捕获设备截获合法维护指令（如“清零计数”），在非授权时段重放指令	导致计量数据篡改、偷气逃费
无鉴权机制	蓝牙MITM攻击	利用蓝牙协议BLUFFS漏洞，伪造运维终端与燃气表建立连接，获取设备内部参数	可远程修改阶梯气价、关闭安全阀、植入恶意固件
无审计追溯	无日志记录	所有本地操作（红外/蓝牙/星闪）均不生成操作日志，无时间戳、无操作者标识	无法追溯异常行为责任主体，事故调查依赖人工排查，效率低、证据链缺失
物理接触风险	拆机逆向	攻击者拆卸表壳，通过JTAG接口读取MCU固件，提取加密密钥与认证算法	可批量克隆设备身份，构建“伪运维终端”网络

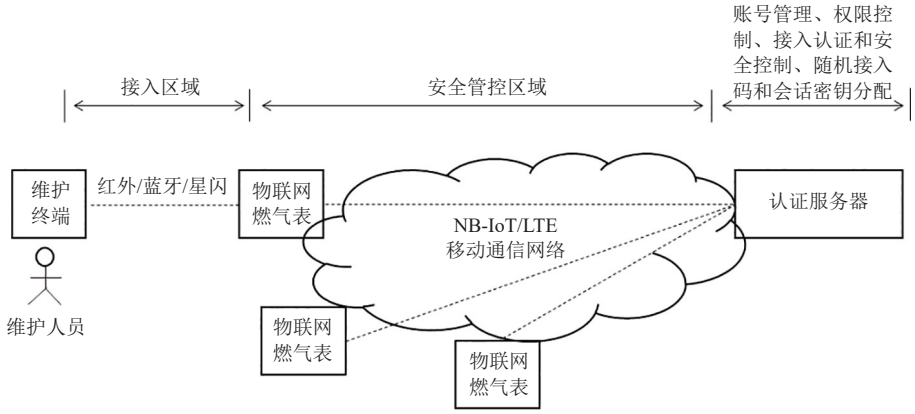

图1 燃气表接入安全控制总体方案

的操作权限、接入设备唯一ID（一般用设备MAC代替）。其可单独部署，也可与物联网燃气表设备管理系统合并部署，甚至是设备管理系统的1个软件功能模块。

物联网燃气表：须支持带硬加密总线的加密存储区或加密芯片，用于保存认证信息，包括账号、账号有效性、接入设备ID、账号对应的操作权限、随机接入码。

维护终端：须支持对本地临时的随机接入码进行加密存储。

认证服务器，不仅仅只是1个身份验证的“闸口”，更是1个实时的安全策略引擎和数据管理中心，承担着以下几方面的关键职责。

（1）策略动态生成：可根据接入环境、时间、设备类型等因素，动态生成认证策略。例如，特定时段可以提升认证复杂度。认证服务器可以直接把策略下发给燃气表，这样策略就可以随时灵活升级，但会增加通信量。也可以把各种策略进行统一编号，只需把策略编号作为账号对应的操作权限下发给燃气表，但策略变化时，燃气表软件需要跟着升级。

（2）信任域协同计算：在处理认证请求时，不仅验证账号和密码，更重要的是核实终端的“可识别ID”（如MAC地址、蓝牙地址等），进行全局唯一性校验和合法性审核。

（3）安全状态动态评估：实时分析每1台燃气表和每个运维账号的使用动态，若发现非正常认证行为（如异地登录、高并发操作等），主动采取限速/锁定等措施。

每个账号对应的操作权限，可以基于（运维员、工程师、管理员等）角色的访问控制来定义，也可以采用属性访问控制来定义，还可以将两者结合起来使用。具体的权限包括：功能级（如修改网络参数、升级固件等）、字段级（如只允许读写部分数据）、操作级别（如开/关阀等）。这种粒度确保了操作的合规性。

4 接入安全控制的产品架构

4.1 认证服务器安全接入控制软件架构

认证服务器的软件架构如图2所示。

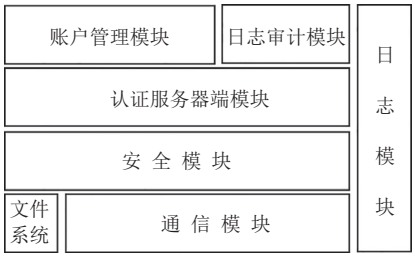

图2 认证服务器软件架构

各模块功能描述如下。

账户管理模块：实现管理接口接入账号的创建/删除、激活/去激活，认证策略、登录账号操作权限（鉴权策略）设置等基本功能。为了增强管理能力，还可以增加身份生命周期管理功能，比如：账户预配置与激活、激活状态和生命周期设定、账号非法使用惩罚措施（自动锁定及锁定时长）等。

日志审计模块：远程读取燃气表端保存的日志信息，对各物联网燃气表管理接口的接入、认证、

命令操作等日志信息进行分类统计和报表查询。

认证服务器端模块：对所有认证客户端模块发起的认证请求进行集中的账号、账号操作权限认证处理和管理，把认证结果和分配的随机接入码、会话密钥等信息返回给认证客户端模块。

安全模块：认证服务器软件的登录管理，认证服务器与燃气表间通信报文的加密和解密，关键认证信息的本地加密存取。

日志模块：认证服务器软件的登录、运行过程中的操作和认证等关键事件及信息的记录。

文件系统：认证服务器软件保存账号、权限、日志等数据和信息的载体，全部采用加密存储。

通信模块：实现认证服务器与燃气表间的信息交互。

当发现有不合规、非法或暴力破解认证请求时，认证服务器应支持将此类重要事件和关键审计日志事件主动推送到相关人员（如值班人员、运维负责人）的工作台或手机上。

4.2 物联网燃气表安全接入控制软件架构

物联网燃气表上安全接入控制的软件架构如图3所示。



图3 燃气表安全接入控制软件架构

鉴权模块：对维护终端发送的操作命令执行权限检查，只有与账号对应的操作权限相匹配的命令才允许执行。

认证客户端模块：与认证服务器交互，通过认证服务器的集中认证和鉴权后，获得分配的随机接入码、会话密钥等信息。

存储模块：燃气表上保存账号、权限、日志等数据和信息，全部采用加密存储，或保存在加密芯片中。

安全模块：管理接口的登录管理，燃气表与认证服务器间通信报文的加密和解密，关键认证信息的本地加密存取。

日志模块：燃气表端管理接口的登录、接入认证、鉴权等关键事件及信息的记录。

存储驱动模块：燃气表上一般没有文件系统，需要通过本模块才能实现数据存取。

通信模块：实现燃气表与认证服务器间的信息交互。

4.3 维护终端设计

维护终端的设计也应做到硬件层级的加固和软件的安全编程。所有敏感信息（账户、临时会话密钥、临时随机接入码等）都应该存放在终端安全的独立可信区域。与燃气表的每一次数据交换都应携带账号、临时随机接入码信息，以便燃气表进行安全检查。为了保证与燃气表间的通信连接处于可监控状态，维护终端应周期向燃气表发送心跳报文。

5 本地管理接口的接入安全控制设计和实现

5.1 接入认证过程

管理员首先在认证服务器上创建维护账号和密码，设置激活状态、操作权限等，并与维护终端的唯一ID进行绑定。

维护终端作为接入登录设备，接入认证客户端运行在物联网燃气表上，认证服务器端运行在云上的服务器中。

本方案的安全接入认证过程如图4所示。

维护终端与物联网燃气表间的物理管理接口链路连通后，维护终端向燃气表发送接入请求到最终完成操作断开连接，一共包括6个阶段。

阶段1 维护终端发起接入请求：维护终端向物联网燃气表发送接入请求消息。

阶段2 接入安全预处理：燃气表收到接入请求后，会先在其本地记录该终端最近的访问请求和尝试次数，并按照其内部防御策略完成防攻击预处理，一旦触发阈值会立刻拒绝该接入并向认证服务器报警。

阶段3 中心认证与全局检查：燃气表向认证服务器发起认证请求。认证服务器验证请求的真实性后会做全局检查，判定是否是克隆设备，比如根据此终端ID最近的在线情况判定是否存在多个设备同

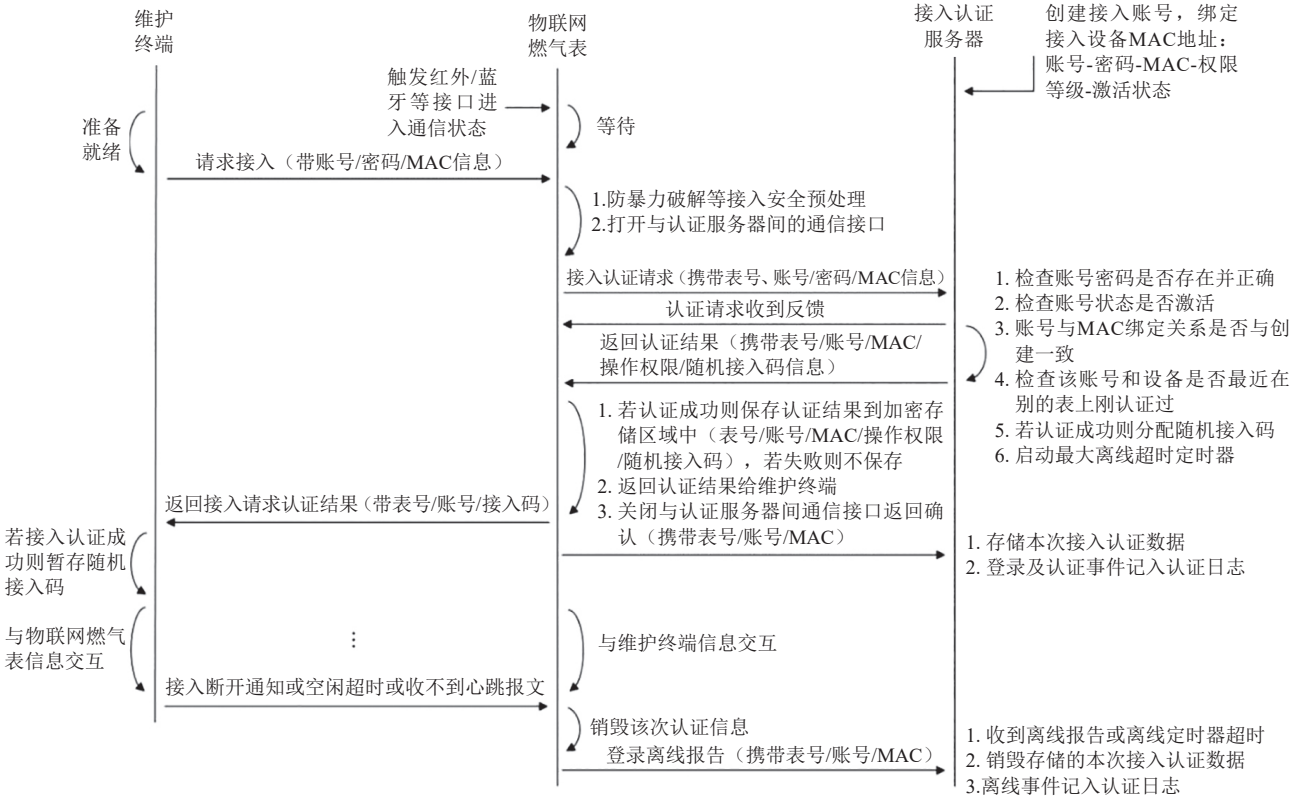

图4 燃气表安全接入控制交互过程

时在线。再进行账号信息正确性和账号状态检查。

阶段4 授权与临时凭证下发：认证服务器查找账号对应的操作权限或授权策略，生成一次性随机接入码，并下发给请求认证的燃气表。

阶段5 命令操作与鉴权：维护终端与燃气表间连接建立后，向燃气表发送命令操作，燃气表根据该终端对应账号的操作权限（或授权策略）执行鉴权，鉴权通过后执行命令，并向终端返回执行结果。维护终端周期向燃气表发送心跳报文，以保持并证明连接的安全性。

阶段6 会话终止与凭证销毁：当认证失败、操作结束或出现异常时，燃气表和维护终端应立即销毁此次会话所有认证相关的会话密钥和凭证（随机接入码）。燃气表同时通知认证服务器本次会话结束，进行同样的销毁操作。

整个接入认证的通信过程，通常需要采用报文动态加密进行，以确保认证过程的安全，这方面的论述已经比较多了，在此不做赘述。燃气表上的认证信息、安全日志信息全部保存在加密存储区域或加密芯片中，维护终端上的随机接入码、认证服务器上的认证信息、安全日志信息须加密后保存。如图5所示。

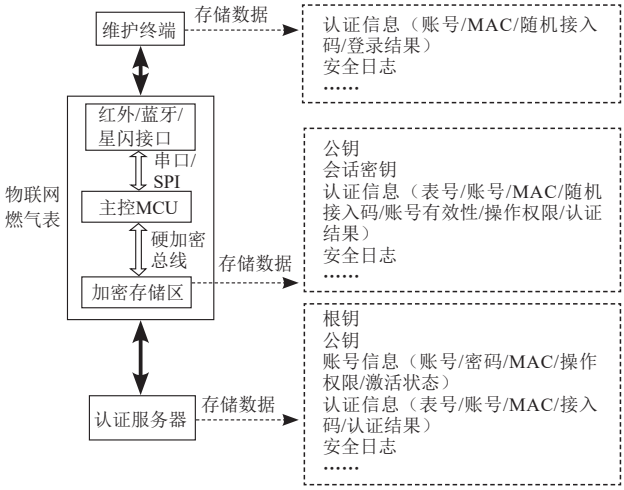

图5 燃气表安全接入控制交互过程

5.2 管理接口的工作过程

物联网燃气表管理接口有4个状态，分别是空闲态、接入态、认证态、工作态，4个状态间的转换过程如图6所示。

空闲态：管理接口已经打开但没有收到任何

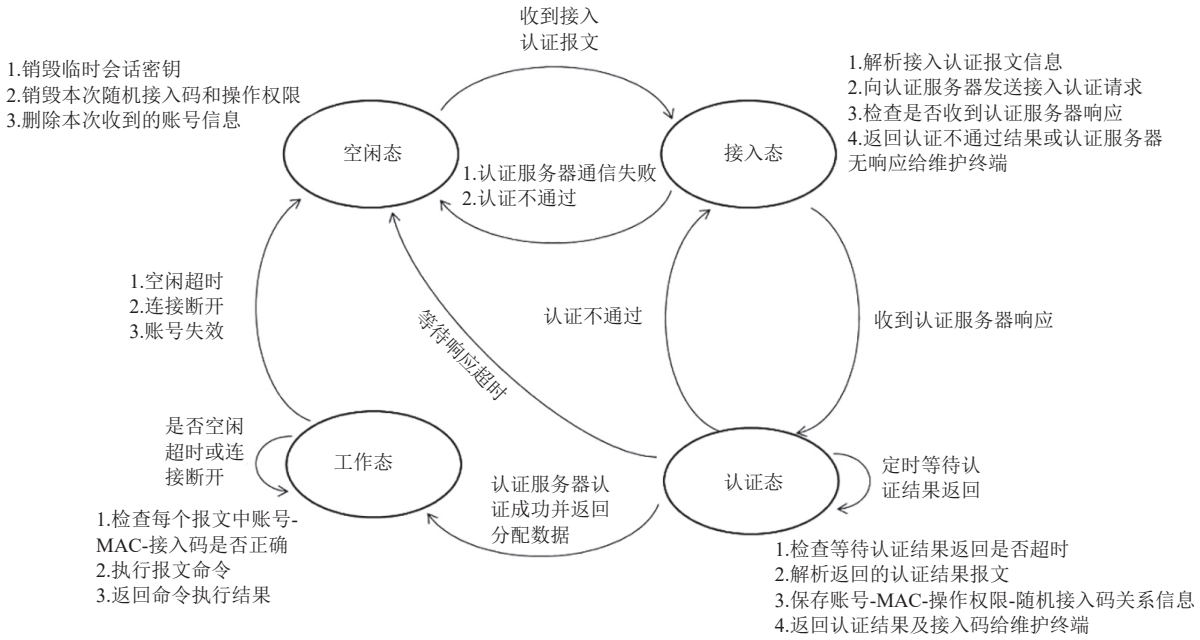

图6 燃气表管理接口工作状态机

维护终端的接入请求时所处的状态。进入空闲态有4种场景，一是刚触发打开管理接口进入通信；二是接入态下收不到认证服务器的认证请求响应；三是认证态下认证服务器反馈认证结果超时；四是工作态下与维护终端间的无交互空闲时间超时，或与维护终端间物理连接断开。从工作态进入空闲态时，需要对本次通信的接入认证数据、信息进行销毁，包括临时会话密钥、账号信息和随机接入码。

接入态：物联网燃气表收到维护终端发送的接入请求，向接入认证服务器发送了接入认证请求。进入接入态有两种场景，一是空闲态收到了维护终端的接入请求并向接入认证服务器发送出了接入认证请求；二是认证态下的认证没有通过。

认证态：物联网燃气表收到了接入认证服务器的认证请求确认反馈。进入认证态只有1种场景，即收到了接入认证服务器对接入认证请求的确认。

工作态：维护终端的接入请求已经认证通过，并收到了认证服务器返回的其他必要账户信息（如操作权限等）和分配的随机接入码，物联网燃气表向维护终端返回接入请求的确认结果和认证信息，双方就可以正常交互信息了。进入工作态只有1种场景，即收到了认证服务器的认证成功结果。

维护终端与物联网燃气表间的正常信息交互时，每个报文中均须携带自己的MAC地址、随机接入码、账号，物联网燃气表须对每个接收自维护终端的这些信息进行检查，流程如图7所示。

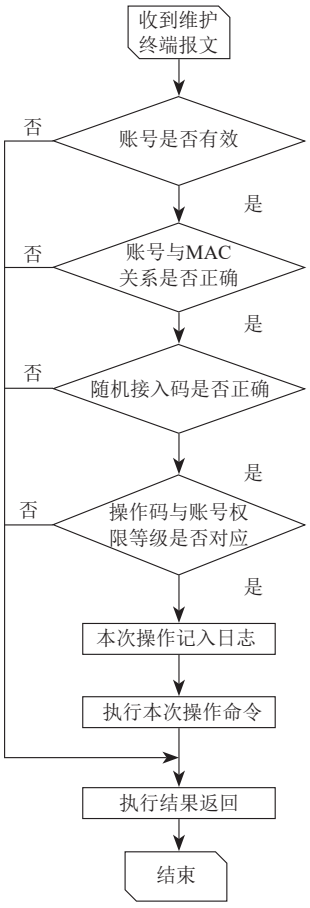

图7 燃气表管理接口接收报文的安全检查

维护终端与物联网燃气表间的通信结束，有两种方式，一种是维护终端主动结束交互，向燃气表发送请求结束通信报文，物联网燃气表收到结束请求后断开与物联网燃气表间的连接；另一种是维护终端长时间不与物联网燃气表交互信息，物联网燃气表的连接空闲定时器超时，从而主动断开与维护终端间连接通道。

不管采用哪种方式，维护终端与物联网燃气表都应当在连接断开后，主动销毁本次连接产生的随机接入码等认证信息。若通信过程使用了动态加密机制，则双方还应销毁掉此次连接产生的临时会话密钥。

6 防暴力破解和账号克隆

在上述设计方案下，为进一步增强物联网燃气表的接入安全，还可采取以下简单但非常有效的措施。

尝试频率限制：同一账户连续认证失败次数达到门限，锁定并关闭接口一段时间，阻止字典攻击。

接入设备数限制：若单位时间内接入的维护终端MAC数量超过门限，锁定并关闭接口一段时间，防止仿冒设备遍历攻击。

心跳检测：维护终端周期向燃气表发送心跳报文（携带账号-MAC-接入码），燃气表连续若干周期没有收到或收到错误的心跳报文，则断开连接，重新认证。

限定操作时间：特定类型的账号（如工程师），只能在规定时间内进行接口访问，如果尝试在非工作时间（如夜间的特定时段）操作，认证服务器将返回鉴权失败。

限制同一账号并发在线：某账号接入认证时，若发现该账号在最近某个时间段内刚认证过，则拒绝此次新的认证，防止克隆终端。

7 结论

本方案通过轻量级协议，在实现全方位、无死角安全管控的同时，确保了现场运维的效率不受影响。认证与鉴权过程的智能化和自动化设计，以及“连接超时自动销毁凭证”等机制，取得了高效运维和合规安全间的平衡。

本方案将登录账号的管理对象扩展到人员（账号）、终端（设备唯一ID）、权限（角色与操作）、过程（全量日志）4大维度。通过集中式的认证服务器实现对账号生命周期的统一管理、终端可信性的强制绑定、操作权限的粒度划分，以及所有操作行为不可篡改的全程追溯，为燃气公司建立了一个看得见、管得住、查得清的运维安全管控体系。

本方案的设计充分考虑了物联网设备的资源约束和多样化场景需求。其核心的3层架构（中心认证、设备鉴权、分层审计）与动态凭证机制具有与通信接口（红外、蓝牙、星闪、NB-IoT等）解耦的高度灵活性，可应用于其他智能仪表（如热力表）及各类工业物联网终端设备的本地调试接口。

综上所述，本方案为当前物联网燃气表本地管理接口的安全问题提供了1个实用、有效、系统化的解决方案，它的实施将推动智能燃气行业从“功能实现”走向“安全可信”的高质量发展阶段，为保障能源计量安全与用户资产安全构筑坚实的技术防线。

参考文献

[1] T/CGAS 003-2017 民用智能燃气表通用技术要求[S].

[2] T/CGAS 006-2019 基于窄带物联网(NB-IoT)技术的燃气智能抄表系统[S].

[3] GM/T 0021-2023 动态口令密码应用技术规范[S].

[4] 华为技术有限公司. 华为园区网络星闪SLE物联数采技术白皮书[EB/OL].(2025-09-27)[2026-3-30].https://e.huawei.com/cn/material/enterprise/d3033a6065a34427a7c182b3c4ce3a90

欢迎订阅《城市燃气》杂志

扫描此二维码订阅杂志

扫描此二维码关注杂志

《城市燃气》杂志社官方网站：www.gas800.com