# 基于零信任架构实现的物联网终端接入安全研究

## Research on Access Security of IoT Terminal Based on Zero Trust Architecture

王首媛[1]，孙宁宁[1]，曹　盛[2]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 成都蜀诚通信技术有限公司，四川 成都 646000）
Wang Shouyuan[1], Sun Ningning[1], Cao Sheng[2] (1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. Chengdu Shucheng Communication Technology Co., Ltd., Chengdu 646000, China)

**摘　要：**
提出了一种基于零信任安全架构实现的物联网终端认证平台，可提供设备授权、身份鉴权、密钥管理、加密传输、会话管理、数据签名等多种功能，保护物联网设备及数据免受重放攻击、伪造攻击、数据篡改、会话劫持等网络攻击，满足碎片化不同的物联网终端类型的接入安全需求，实现了基于无证书标识密码强安全的快速认证接入能力，并通过国密无证书TLS[1]安全通道实现了与企业后端业务平台无缝集成，保障整个通信链路的安全和数据完整性。

**关键词：**
零信任；无证书标识密码；物联网；密码算法；PKI/CLA；身份认证
doi：10.12045/j.issn.1007-3043.2021.07.004
文章编号：1007-3043(2021)07-0013-06
中图分类号：TN929.5
文献标识码：A
开放科学（资源服务）标识码（OSID）：

**Abstract:**
It proposes a trusted IoT terminal authentication platform based on zero trust security architecture, which can provide device authorization, identity authentication, key management, encrypted transmission, session management, data signature and other functions, and protect IoT devices and data from replay attack, forgery attack, data tampering, session hijacking and other network attacks. It meets the access security requirements of different types of fragmented IoT, realizes fast authentication access capability based on strong security of certificateless identification password, and realizes seamless integration with enterprise back-end business platform through nation secret certificateless TLS security channel, so as to ensure the security and data integrity of the whole communication link.

**Keywords:**
Zero trust; Certificateless identity password; IoT; Cryptographic algorithm; PKI/CLA; Identity authentication

**引用格式：**王首媛，孙宁宁，曹盛. 基于零信任架构实现的物联网终端接入安全研究[J]. 邮电设计技术，2021(7)：13-18.

## 1 概述

本文基于对物联网终端的连接管理以及终端连网的安全研究，针对终端的身份伪造、数据泄密等问题，结合零信任安全架构理念，构建物联网终端安全接入的安全保障体系，满足物联网终端安全可信接入的场景需求。

### 1.1 物联网安全现状

传统物联网终端缺少应用安全机制，更没有强安全、强身份认证机制，简单的口令验证很容易被破解或绕过，容易被直接攻入设备系统从而被控制，成为网络攻击的新方向。5G网络大连接、大带宽、低时延特性大大增加了攻击的潜在规模，海量设备一旦被非法控制，将发起前所未有的大规模网络攻击，使基础网络瘫痪。5G通信的SDN、NFV、云、MEC等新型网络架构，使网络边界模糊化，边界防护无法生效，在增加了灵活性的同时也扩大了攻击暴露面，面临DDoS攻击、侧通道攻击、开放API威胁等问题，网络切片技术

收稿日期：2021-05-17

也带来资源共享、跨域安全、认证授权等新型网络安全问题。

当前物联网面临的主要安全风险有：

a）物联网系统入侵。

b）物联网僵尸网络拒绝服务攻击。

c）物联网敏感信息泄露。

### 1.2 问题分析

在5G网络环境下，物联网终端设备面临业务场景复杂，对网络的带宽传输能力以及终端设备自身硬件、软件运算要求较高，终端面临身份伪造、数据泄密、信令重放、DDoS攻击等多种安全隐患。传统的网络安全架构大都基于查杀堵截模式，通常在网络边界部署安全设备。随着各行业数字化转型升级，云大物移智等新兴技术的应用，IT基础架构发生根本性变化，平台、业务、用户、终端呈现多样化趋势，开放协同需求增加了数据的互联互通，传统的物理网络安全边界逐渐消失，VPN、BYOD等提供了对网络的不可信访问。

### 1.3 传统终端接入模式

如图1所示，传统网络接入模式下，物联网终端及网络安全的整体方案总体是基于网络安全设备的功能叠加和AI大数据加持的网络安全态势感知技术的发展。传统的物联网系统安全方案思路，基本集中在网络边缘侧的查杀堵截和事后的补救，采用了先连接后认证的机制，在TCP/IP协议基础之上，结合VPN模式，实现端到端的通信。缺乏零信任的系统思路，从安全架构层面去解决根本性安全问题。

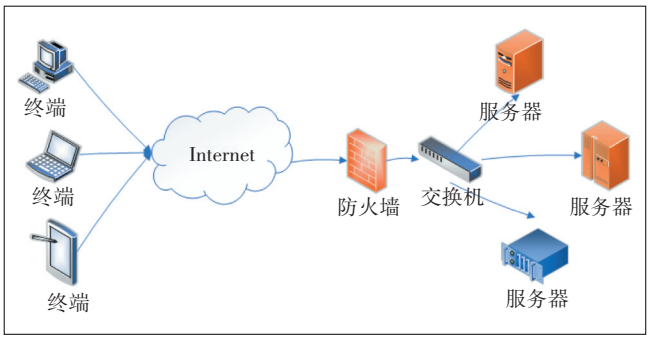


图1　传统网络接入模式

## 2 零信任架构核心思路

### 2.1 技术思路

随着5G、云计算、物联网、工业互联网技术的发展，安全防护需要一种新的信任模型——以永不信任、持续认证、最小特权为原则的零信任安全模型。基于零信任的身份管理架构以身份为基石实现业务安全访问、持续信任评估和动态访问控制，建立基于全网数字身份认证和动态访问控制策略为核心的零信任安全机制，可保障网络系统的整体安全。

基于零信任架构采用了以身份为中心，采用先认证、后连接的方式，使网络和认证形成统一，实现仅对授权用户开放连接。

### 2.2 最新进展

通过搭建零信任物联网终端认证平台，预计在2022年，面向生态系统合作伙伴开放的80%的新数字业务应用程序将通过零信任网络访问（ZTNA）进行访问，应用SDP技术实现软件定义边界，从传统的以网络为中心转变为以身份为中心进行最小权限访问控制，持续监控可疑用户活动。

## 3 零信任物联网终端认证方案设计

### 3.1 设计要点

物联网终端认证平台结合零信任[2]架构理念，基于无证书标识密码技术提供了终端安全的入网能力，包括设备授权、身份鉴权、密钥管理、加密传输、会话管理、数据签名等多种功能，保护物联网设备及数据免受重放攻击、伪造攻击、数据篡改、会话劫持等网络攻击，实现基于无证书标识密码强安全的快速认证接入能力，通过终端和安全认证网关建立的国密无证书TLS安全通道实现与企业后端业务平台无缝集成。

#### 3.1.1 动态智能防火墙技术应用

传统的网络安全是基于防火墙的物理边界防御，也就是大众熟知的“内网”。防火墙的概念起源于20世纪80年代，该防御模型前提假设是企业所有的办公设备和数据资源都在内网，并且内网是完全可信的。

然而，随着云计算、大数据、物联网等新兴技术的不断兴起，企业IT架构正在从“有边界”向“无边界”转变，传统的安全边界逐渐瓦解。随着以5G、工业互联网为代表的新基建的不断推进，还会进一步加速“无边界”的进化过程。与此同时，零信任安全逐渐进入人们的视野，成为解决新时代网络安全问题的新理念、新架构。

物联网终端安全认证平台基于零信任的架构理念，结合了动态智能防火墙技术，云端智能态势感知中心会实时动态监控物联网终端设备与后台应用的连接状态，实时更新黑白名单策略，并对端口进行实

时封堵、放行控制，基于动态安全策略实时地调控终端对应用后台的访问行为，实现实时动态安全管理。

3.1.2 PKI/CLA无证书密码技术应用

CLA无证书密码技术[3]是针对非对称密钥分配和管理的实际应用需求，用于生成、分发和管理用户实体密钥。CLA无证书密码技术采用一种新型的具有双密钥、基于SM2椭圆曲线的、无双线性对运算的无证书公钥密码体制[4]，利用现有SM2椭圆曲线密码算法，实现对用户密钥的分配和有效管理。

PKI/CLA具有以下技术优势。

a）高安全性：可实现点对点（P2P）认证和主动安全；用户对私钥具有完全自主权，外界（包括CLA）对用户的私钥不可知；用户的公钥标识中不显式的包含用户的公钥，也不包含CLA对公钥标识的签名。

b）认证效率高：公钥标识短，密钥存储成本低，创新应用国密算法，实现更快的密码计算、更高认证效率、更安全的运算，支持物联网低时延、大连接认证应用，支持海量物联网设备的接入认证和密钥管理。

c）公钥自证性：基于国密算法的创新应用，无证书密码体系具备去中心化和设备离线验证的能力，满足物联网跨域认证的实际需求；并且支持与PKI/CA对接能力。

### 3.2 架构设计

整体架构包含云端安全认证中心、接入层安全认证网关以及感知层物联网终端三大板块，是覆盖端-管-云全链路的整体安全体系。

3.2.1 基于零信任架构的物联网终端认证平台

如图2所示，平台基于零信任新型网络安全架构整体设计，主要包含平台侧、网络侧和终端侧3个部分。

a）平台侧：包含统一身份管理系统、终端权限管控系统、智能态势感知系统。

b）网络侧：安全认证网关零信任安全套件。

c）终端侧：由物联网安全终端和物联网安全边缘网关的零信任安全代理客户端组成。

3.2.2 零信任物联网安全的关键功能

3.2.2.1 数字身份构建

整个系统内所有实体单元进行全面数字身份化，包括物联网终端用户、终端设备、SIM卡、终端模组、应用服务器、服务器应用、应用服务接口API等均赋予数字化身份。

基于移动通信的物联网终端以SIM卡ICCID和

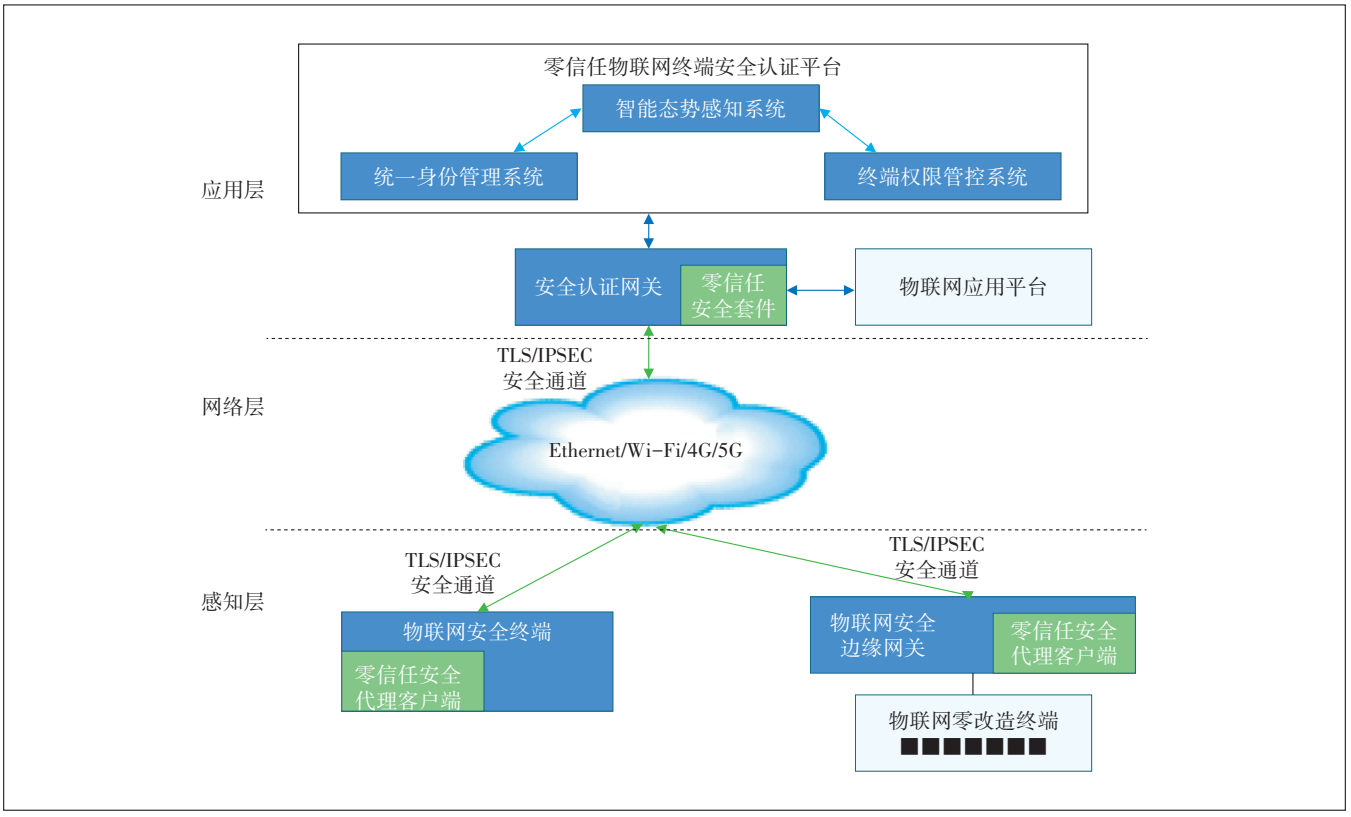


图2　物联网终端安全认证系统架构图

IMSI为基础身份，终端在接入应用过程中，采取各种身份动态组合，生成接入访问的临时身份，该临时身份包含了终端在接入时的各维度的实时状态。

3.2.2.2 安全访问链路

移动终端蜂窝模组作为终端的安全代理介质、实现与物联网应用系统之间基于PKI/CLA+TLS/IPSEC的数据安全链路，基于国密安全通道进行全流量加密数据传输。

对于终端请求，终端蜂窝模组拦截后根据终端临时身份向零信任安全认证网关请求授权，授权通过后，通过TLS/IPSEC加密通道将请求发送给应用服务器。对于应用服务器返回的特权指令，终端应用需通过基于安全SIM的密码安全运算，进行强安全的密码验签来验证服务器临时身份授权，身份认证通过后方能运行权限内的指令。

3.2.2.3 持续信任评估

零信任物联网终端安全认证平台集成了智能态势感知大数据系统，根据风险评估模型和大数据分析AI算法，结合安全认证网关和终端的验证反馈，不断优化调整动态身份条件下的策略，为零信任网络提供自适应动态的策略调控能力。

3.2.2.4 动态访问控制

终端临时身份获得安全认证网关的认证和授权后，需要基于最小权限原则分配其服务和资源访问权限。零信任物联网终端安全认证平台集成了终端权限管控系统，基于身份安全基线、行为安全基线、应用安全基线、终端安全基线、黑白名单策略、信任评估模型，实现对安全认证网关和终端的动态访问控制。

### 3.3 流程设计

物联网安全认证平台基于统一身份技术、动态防火墙技术，结合了零信任的架构理念，是覆盖端-管-云全链路安全的系统方案，能够满足物联网多业务场景和多种终端类型交叉认证，满足安全通信的实际需求。

物联网安全认证平台终端接入流程如图3所示。

安全认证网关默认关闭所有的TCP端口，实现网络隐身，只有通过认证后，才会接入应用后台。

物联网终端安全接入流程如下。

a）管控平台上线启动。

b）安全认证网关上线，与管控平台建立TLS连接。

c）终端侧模组应用程序首先向零信任客户端管控套件申请接入请求，管控套件对接入请求进行指令签名，之后向管控平台发送身份认证请求。

d）管控平台验证用户设备信息，建立TLS连接，返回授权票据和对应的应用网关信息。

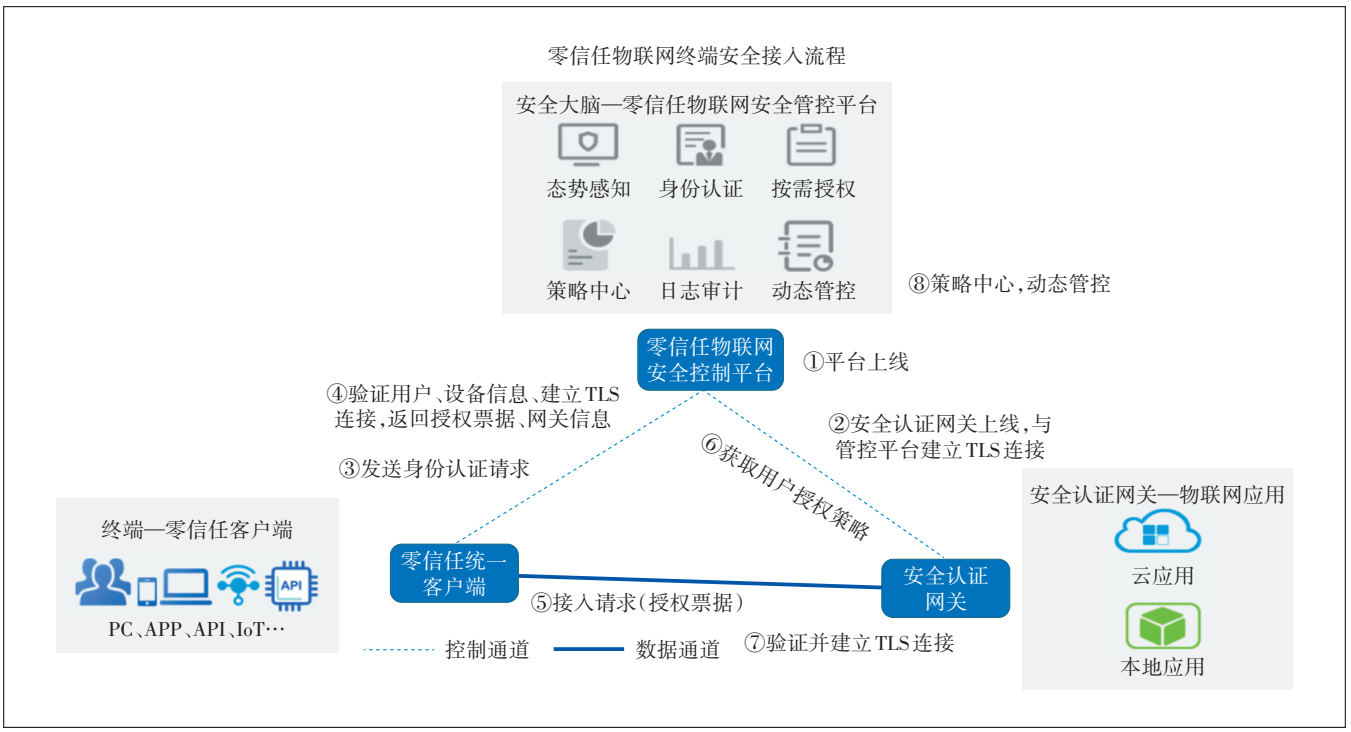


图3　零信任物联网终端安全接入流程图

e）终端应用程序携带票据信息向对应的安全认证网关发起TLS连接建立请求。

f）安全认证网关收到请求后向管控平台获取用户授权策略信息。

g）按照用户既定策略验证完成后，安全接入网关与终端之间完成基于TLS握手协议标准流程。完成了TLS握手之后，终端通过网关的认证，接入物联网应用系统后台。

h）安全大脑管控平台基于实时信息反馈，动态实时管控网关和终端的行为策略，调整策略基线。终端零信任管控套件会实时采集终端信息上报给管控平台，同时管控平台会基于安全策略对终端进行实时监控，基于业务的安全行为基线（黑名单、白名单、威胁情报、病毒库、DDOS攻击）给安全认证网关下发配置策略，网关会执行策略和处置命令，动态管控终端和应用的行为，对终端的行为实时阻断、隔离、审计等行为处置。

### 3.4 组件设计

零信任物联网终端安全管控平台业务架构的组件设计如图4所示。

#### 3.4.1 统一身份管理

负责数字化身份的维护。需要将SIM卡、用户、终端、应用和服务等信息按照身份编码规则录入系统。同时还需要维护、采集身份相关的状态和属性。

负责综合身份的认证。通过认证模型对综合身份进行分析认证，认证通过则签发身份证书，认证失败则根据认证情况拒绝其接入或要求其提供其他身份要素。

统一身份管理系统支持基于国密SM2的无证书标识密码认证技术，为用户实体提供基于国密SM2无证书标识算法的身份认证、身份查询、身份绑定等接口，受理终端用户的认证申请，完成对终端用户真实身份的认证。

#### 3.4.2 身份服务管理

负责收集接入请求场景，验证反馈和身份关联的状态、属性等信息，通过大数据分析和智能算法，不断优化身份认证模型，为身份管理系统提供持续信任评估能力。智能态势感知系统基于终端系统提供的终端用户相关的数据信息（包括身份信息、GIS分布、终端状态、异常事件、终端日志等）进行业务建模、数据清洗、挖掘分析，动态智能调整基线策略。

#### 3.4.3 安全认证网关

作为服务端的安全代理，安全认证网关将服务和资源对外接口进行隐藏，基于TLS协议的无证书标识密码认证技术提供对终端身份的安全认证能力以及对于数据包的加密解密能力，确保数据传输的安全性、完整性、可用性以及终端身份的不可抵赖性等安全能力保证；对于数据包的发送源进行身份验签，成

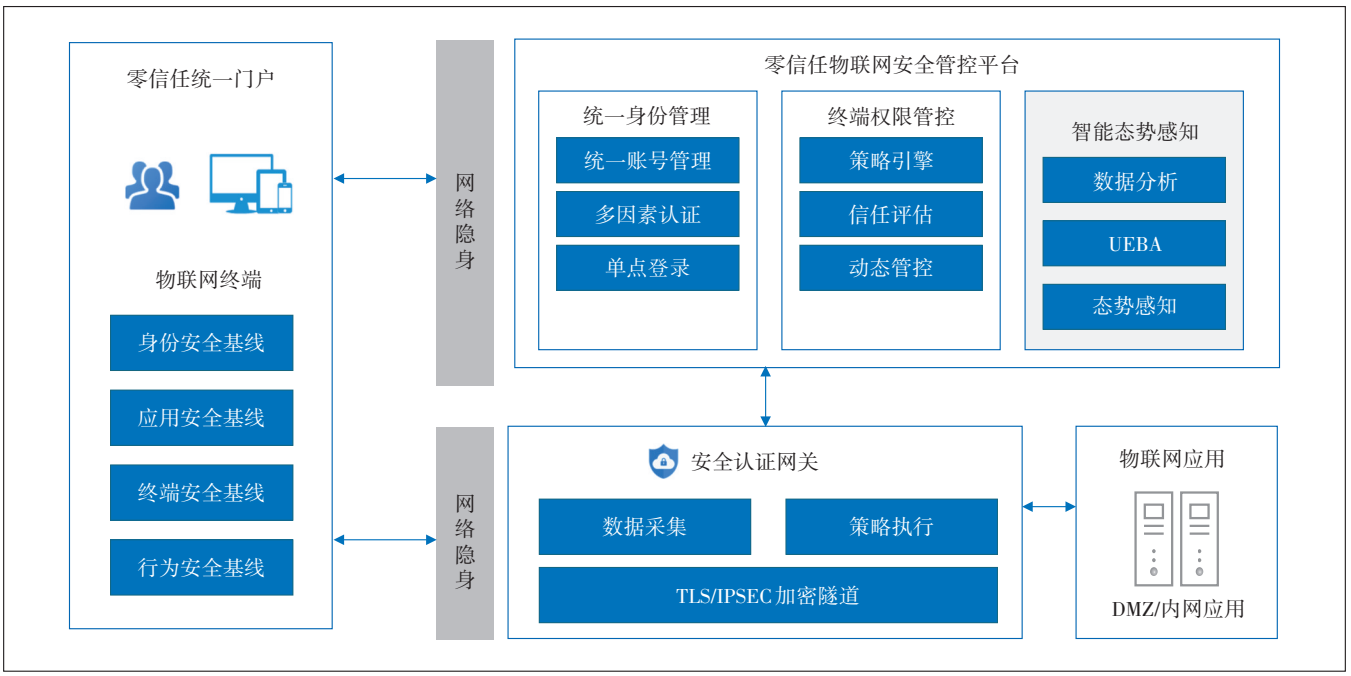


图4　零信任物联网终端安全管控平台业务架构图

功验签的终端数据包方能接入云端物联网业务系统；同时接收终端安全认证系统的处置命令，实现对终端或物联网应用平台的入口出口安全控制，及时阻断、隔离。

3.4.4 终端权限管控

负责身份权限的分配。根据身份映射到其最小权限角色，通过RBAC权限模型，获取角色权限。同时根据身份的关联属性，通过ABAC权限模型，计算动态权限。2个权限集合取交集作为最终的最小权限。终端权限管控系统基于应用策略对终端进行实时监控，基于业务的安全行为基线（黑名单、白名单、威胁情报、病毒库等，DDoS攻击），对安全认证网关下发处置命令，实时阻断、隔离终端的业务行为。

3.4.5 终端零信任安全代理

终端零信任套件主要实现如下功能。

a）基于硬件模组和SIM卡的密码能力，提供对终端上层应用的加解密和签名验签的密码服务。

b）对终端状态运行信息进行动态采集，将安全事件定时上报云端的功能。

c）实现对终端设备的管控功能，接收云端指令和策略信息，并分析策略和执行指令的功能。

d）终端套件支持基于无证书标识密码的TLS协议，实现与安全认证网关的双向认证能力，并实现数据的安全传输能力。

零信任物联网终端安全系统，以安全SIM卡为密码载体，以轻量无证书公钥标识技术为核心，保障终端敏感数据的可靠安全传输，实现终端身份的安全认证、防抵赖的核心能力。

## 4 结束语

零信任物联网终端安全认证平台具备开放化的密码技术的支持能力，支持多因子统一身份认证的能力，自动兼容PKI/CLA以及PKI/CA等多种密码体制。作为5G物联网时代基于国密算法实现的新型零信任网络架构的统一安全认证平台，其具有革命性意义，是国家提倡5G全面战略化发展的重要的安全基础，对工业互联网、智能车联网、数字经济应用等重要应用而言，是核心的网络安全基础设施。

后续计划整合运营商产业链的资源，打通终端、SIM卡、网络一体化认证。身份认证技术采用ICCID号（SIM卡号）作为密码标识。ICCID作为运营商统一可控的终端连网通信模块中的必须标识，具有全球号码参数唯一、编码规则管理有效、运营商体系安全的特点；“SIM卡号+SIM/eSIM卡”作为身份认证技术的“标识+安全计算环境”具备天然优势，对于运营商建立基于SIM卡号为标识的身标识份认证能力具有深远的战略意义。

建设零信任统一身份能力，实现国密算法产品落地。基于零信任的架构模式结合国密SM系列算法以及动态智能防火墙技术，实现移动终端设备和应用系统之间基于TLS进行双向握手认证和加密安全传输，为各种移动终端提供入网的强安全身份认证通道，保障终端身份及应用层数据安全的能力。

**参考文献：**

[1] DIERKS T. The Transport Layer Security（TLS）Protocol Version 1.2[J/OL]. [2021-03-26]. http://www.rfcreader.com/#rfc4346.
[2] 熊荣华. 一种无双线性对运算的无证书公钥密码体制的实现方法：CN104539423.3[P]. 2015-04-22.
[3] 埃文·吉尔曼，道格·巴斯. 零信任网络[M]. 北京：人民邮电出版社，2019.
[4] CLA无证书认证及密钥管理系统技术白皮书[R]. 北京：北京鼎九信息工程研究院，2016.
[5] 郭仲勇，刘扬，张宏元，等. 基于零信任架构的IoT设备身份认证机制研究[J]. 信息技术与网络安全，2020，523(11)：27-34.
[6] 刘远，孙晨，张嫣玲. 基于Overlay技术的零信任网络研究[J]. 信息网络安全，2020，238(10)：87-95.
[7] 张文迪. 零信任身份安全解决技术分析[J]. 科技经济导刊，2020，706(8)：42-42.
[8] 刘增明，崔雪璐，马靖，等. 基于零信任框架的能源互联网安全防护架构设计[J]. 电力信息与通信技术，2020，199(3)：19-24.
[9] 林蓉，胡敏，刘翔. 构建"零信任"安全体系 护航数字化转型发展[J]. 金融电子化，2020(5).
[10] 马靖，许勇刚，刘增明，等. 基于零信任框架的泛在电力物联网安全防护研究[J]. 网络安全技术与应用，2020(1).
[11] 鲁阳. 物联网终端可信认证与自动接入技术研究与实现[D]. 南京：南京邮电大学，2020.
[12] 刘锦利. 物联网终端认证技术研究[D]. 沈阳：辽宁大学，2016.
[13] 林扬武. 物联网的安全认证技术研究[J]. 无线互联科技，2012(10)：6-7.
[14] 吴卫. 边缘计算环境下物联网身份认证与隐私保护技术研究[D]. 西安：西安电子科技大学，2019.
[15] 钟晶，王颖凯. 物联网终端安全接入方法研究与设计[J]. 电子产品可靠性与环境试验，2013，31(3)：33-35.

**作者简介：**
王首媛，毕业于北京邮电大学，工程师，硕士，主要从事5G物联网密码创新技术研究与应用；孙宁宁，毕业于北京交通大学，工程师，硕士，主要从事信息技术研发，产品技术方案研究等工作；曹盛，毕业于西北工业大学，工程师，学士，主要从事信息技术研发工作。