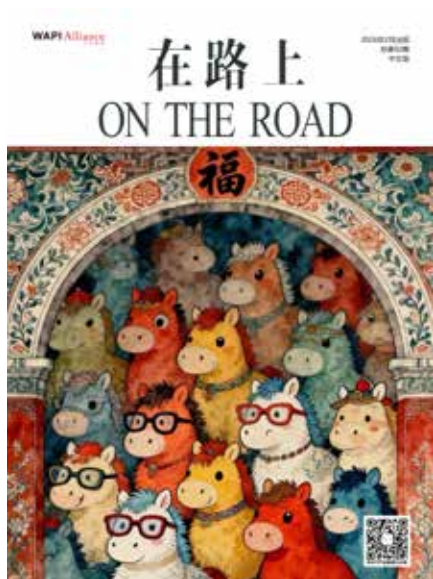


# 在路上

## ON THE ROAD





### 理事成员：

中国移动通信集团公司  
中国电信集团有限公司  
中国联合网络通信集团有限公司  
国家密码管理局商用密码检测认证中心  
国家无线电监测中心检测中心  
西电捷通公司  
北京中电华大电子设计有限责任公司  
中电科普天科技股份有限公司  
深圳市明华澳汉智能卡有限公司  
北京数字认证股份有限公司

### WAPI产业联盟

理事长：曹军  
秘书长：张璐璐

### 《在路上 On The Road》编辑部

主 编：张璐璐  
编 辑：周园 刘剑昕 刘婷  
王立华 陈博

美术编辑：周园

### WAPI产业联盟秘书处

会员服务部 标准化部 市场与产业部  
测试实验室 综合管理部

### 联络单位

ISO/IEC JTC 1/SC 6中国对口委员会  
工业和信息化部宽带无线IP标准工作组

### 联系方式

地 址：北京市海淀区知春路27号量子芯座1608室  
邮 编：100191  
电 话：010-82351181  
传 真：010-82351181 ext.1901  
邮 箱：wapi@wapia.org  
网 站：http://www.wapia.org.cn

公众号：



WAPI产业联盟公众号

## 新春致禧 Happy Chinese New Year

05 新春贺词：实干辞旧岁 奋进启新程

## 特别报道 Special Report

06 盘点：2025年WAPI亮点

## 媒体聚焦 Media Focus

- 10 新华社等：我国牵头的多项数据通信网络国际标准提案项目正按计划稳步推进
- 12 通信世界等：第四届无线网络安全标准化工作委员会第二次会议召开 共绘安全无线标准新蓝图
- 18 飞象网等：WAPI产业联盟召开2025年第四次标准工作和项目组会议（总第136次）
- 22 中国信息化周报等：规范数字证书流程管理 WAPI产业联盟发布两项团体标准
- 24 中国信息化周报等：WAPI产业联盟发布高质量安全无线局域网标准体系首项标准

## 联盟关注 Alliance Concerns

26 联盟发布洞察报告《AS在WAPI三元对等架构中的核心地位与行业合规部署》

## WAPI 问答 WAPI FAQ

31 WAPI问答（系列连载）第十七部分（PART 17）

## 产经要闻 Industrial & Economic News

- 35 习近平：突出科技创新引领 健全国家安全体系
- 35 习近平：筑牢网络安全和数据安全防线
- 36 李强：推进科技创新和产业创新深度融合 加快发展新质生产力
- 36 何立峰：加快高水平科技自立自强 引领发展新质生产力
- 37 国家发展改革委：深化智慧城市发展 筑牢数字化转型安全防线
- 37 工信部：提升园区数字化安全保障水平
- 38 北京市人民政府：推进科技成果转化落地

## 联盟工作 Alliance Work

- 39 弘扬文化自信与工匠精神 赋能新质生产力发展 WAPI产业联盟组织参观湖北省博物馆党的主题活动
- 41 党建引领聚合力科创赋能担使命 WAPI产业联盟参加海淀夜校启动暨专题党课学习
- 42 无线网络安全标准化工作委员会2025年第四次主任委员会议（总第15次）顺利召开
- 43 联盟发布新版《WAPI标准产业应用及环境监测报告》
- 43 联盟发布新版《WAPI问答合辑》
- 44 许继软件WAPI系列终端通过联盟测试
- 45 莲雾科技WAPI系列终端通过联盟测试
- 46 北京至周科技WAPI CPE终端通过联盟测试
- 47 平高运检WAPI无源无线避雷器状态监测装置通过联盟测试

## 新成员 New Member

- 48 WAPI产业联盟再添2家新成员

## 成员与市场 Member & Marketing

- 50 南方电网完成业内首个网省跨域WAPI漫游认证现网测试
- 51 广哈通信赋能电力行业安全新发展
- 52 通科公司WAPI创新成果突出 成广东电网企业矩阵核心成员
- 53 中兴与字节跳动携手推出WAPI“豆包”手机
- 53 中威电子发布支持WAPI的多功能电缆沟智能盖板
- 54 国网山东电力科学研究院等单位申请“基于零信任的WAPI电力通信安全接入方法、系统和存储介质”专利
- 54 博洛米WAPI终端安全证书系统实现方法专利获授权
- 55 数字认证牵头和参与的多项密码行标获发布

## 产业技术论坛 Industry & Technology Forum

- 56 关于WAPI低功耗卡片机的表计识别解决方案

## 新春贺词

### 实干辞旧岁，奋进启新程

岁序更替，华章日新，值此辞旧迎新之际，WAPI 产业联盟向大家致以衷心的感谢和美好的祝福！愿您和家人：健康平安，阖家幸福，事业蒸蒸日上！

过去一年，WAPI 规模建设持续推进，应用从“覆盖量增长”迈向“业务贯通+规模运维”的阶段性跃迁。面对复杂多变的外部环境与深水区挑战，联盟紧扣“高质量发展与高水平安全”主线，坚持标准引领、应用牵引、测试保障，持续深化产业市场协作创新与生态共建。

岁月流金，实干者兴，在您的参与和支持下，WAPI 标准链、产业链、供应链不断壮大，公共服务与测评能力持续完善，市场建设更加科学规范高效。依托 WAPI，越来越多业务场景实现了从“可用”到“好用”、从“单点”到“系统”的跨越。在国防、能源、政务、交通等关键领域，WAPI 安全无线局域网有力支撑了新型行业系统构建，促进了传统行业数字化转型升级。

当前，我们正站在“十五五”开局新起点，向高质量发展的纵深阶段迈进。联盟愿与您并肩携手，以实干赴新程，继续当好网络强国建设的主力军和排头兵！



WAPI 产业联盟  
秘书长

A handwritten signature in black ink, appearing to be '张琳琳' (Zhang Linlin), written in a cursive style.

乙巳年岁末

## 盘点：2025年WAPI亮点

2025年,WAPI产业迈向“工程实现如何高质量、规模网络如何可运营、生态治理如何可持续”的系统工程。

据媒体报道,国防、电力等行业WAPI规模化贯通持续深化,应用从“覆盖量增长”进一步走向“业务贯通+规模运维”的阶段性跃迁;与之并行,面向802.11be等技术演进、关键安全能力的标准制修订与发布同步推进,测试项与测评服务加速升级,逐步形成“可验证”的质量底座。与此同时,规模建设进入“深水区”后显现的质量、架构、运维、合规等复合问题,被WAPI产业联盟以《行动计划》、典型风险拆解与防范、测试能力建设与规则治理正面回应:从管理帧保护、快速切换、AE驻留位置、硬件安全模块到数字证书全生命周期管理,问题被清单化、测试化、工程化,治理路径更可落地。

围绕“高质量安全无线局域网规模建设”,联盟与无线网络安全标准化工作委员会进一步构建“标准一测评一试点示范一采购验收”的闭环机制,并在组织治理与制度供给上持续完善:以技术标准为边界、以测试评价为抓手、以示范应用为牵引、以生态协同为保障,推动WAPI从“能用、好用”走向“高质量、可运营、可持续演进”,为各行业规模建设提供长期稳定的组织能力与公共技术支撑。

### 亮点一：电力行业“全程全网贯通”迈向规模运维阶段，示范效应凸显

电力行业仍是WAPI规模应用最具代表性的领域之一,2025年的进展不止在覆盖量,更体现在业务系统贯通与运维化转换。

据媒体报道显示,南方电网公司打通变电站WAPI无线局域网与移动应用门户APP、电网管理平台等业务系统接口,实现“全程全网贯通”,并在南网超高压公司、广西电网公司相关站点实现规模化应用;同时披露已完成超千个站点的WAPI网络覆盖建设,并明确下一阶段将从“大建设”走向“大运维”和“全面应用”。

电网侧“场景化落地”呈现更细颗粒度:南网超高压围绕智能巡检、智能监测、智慧安监、移动作业、移动办公等场景推进应用;国网山东截至2025年底覆盖1093座变电站、接入17250台业务终端,并提出“十五五”期内更大规模的部署目标与统一综合网管建设方向。这意味着,WAPI在电力行业的价值正从“安全接入能力”上升为“支撑移动作业数字化、可管可控可追溯”的基础设施能力,并开始沉淀跨单位可参考的贯通路径与运维范式。

### 亮点二：产业建设进入“深水区”，联盟以行动计划回应质量与合规的复合挑战

随着规模部署扩大,难点从“顺利连接”变为“长期稳定、合规一致、可持续演进”。规模化推进中面临一系列复合挑战:高安全与高可用如何兼顾、差异化需求与规模化推进如何平衡、当下建设与未来演进如何衔接等。迎战深水区不是“召开更多会议”,而是把问题清单化、测试化、规则化,并形成可执行的整改与演进路线。

对此联盟在高质量安全无线局域网创新应用大会上发布《针对高质量安全无线局域网规模建设相关问题的行动计划》，围绕管理帧保护、AP 间快速切换、AE 驻留位置、低功耗模组“软算法”等关键问题，给出测试、整改与后续标准 / 检测能力建设方向，并发出倡议：“深水区”破局，要依赖产业链上下游的“系统思维”与“创新协同能力”，形成合力。此后，生态治理从“事后纠偏”转向“体系化预防”。通过行动计划把问题拆解、把验证手段规范化、把整改路径公开化，为用户选型与工程交付提供可执行依据。

2025 年 12 月，联盟发布高质量无线局域网标准体系首项标准《高质量无线局域网 总体要求》，从目标边界、关键指标、一致性要求三个维度作出上位牵引，为实现“可落地、可验收、可持续”的高质量无线局域网体系化建设与治理，提供了统一依据和行动指引。

### 亮点三：质量治理进一步“抓关键症结”，四类典型风险被公开拆解

2025 年 12 月，标委会会议期间，产业链上下游对“WAPI 建设深水区痛点”予以更具体的拆解。聚焦四大核心挑战给出典型案例与应对思路，包括：

- 检测不到位导致“简单测试通过但现场不好用”（如：部分 AP 未按标准执行重传机制，干扰环境下易接入失败 / 掉线，且简易工具难以检出问题）；
- 工程架构“省事化”引发安全红线风险（如：瘦 AP 架构下 AE 加解密与密钥协商拆分实现导致密钥跨设备传输风险，用户难以在常规验收中识别）；
- 低功耗终端“降本优先”造成密钥泄露隐患（如：密钥直接存储于 FLASH，缺乏硬件防护）；
- “弱化 / 绕过 AS”带来系统性风险（如：为降低切换时延屏蔽 AS 鉴别，动摇三元对等架构信任根基）。

这些“点名式”的问题拆解，把生态治理从“泛泛谈质量”推进到可复现、可检测、可约束的工程层面，也为后续行动计划、测试项升级和招采验收条款提供了落脚点。

### 亮点四：工程化指南持续迭代，面向 802.11be 等演进给出实现路径

工程化能力是规模应用的“地基”。2025 年 7 月，联盟发布团体标准《无线局域网产品工程化实现指南 第 11 部分：WAPI 与 IEEE 802.11be》。在“用户要升级、网络要演进”的实际需求下，把 WAPI 工程实现与 802.11be 等演进关系纳入标准体系。面向用户侧，强调 WAPI 体系并非“割裂存在”，而是要与新一代无线技术迭代协同考虑；面向供给侧，强调工程实现要有统一方法与可验证边界，减少不同厂商实现差异造成的互通风险与运维成本。这一团体标准的发布，为安全无线局域网产品与 IEEE 802.11be 技术融合的工程化实现提供了清晰、明确且可操作的指导，降低了用户对“割裂、替换成本、兼容风险”的顾虑，也为厂商提供更一致的实现与验收参考。

### 亮点五：关键安全能力标准“修订 + 发布”并行，夯实管理帧保护等核心内功

2025 年的一个明显趋势是：标准修订更强地服务于工程痛点与质量治理，而不止于“条款完备”。

例如：管理帧保护等机制是“既关安全也关可用”的关键抓手。对此联盟年中相继发布《无线局域网安全技术规范 第1号修改单》(WAPI 2.0)和新版《管理帧保护技术规范》两项团体标准，测试实验室同步完善WAPI 2.0测试能力，为技术落地提供支撑。

### 亮点六：测试能力持续升级，形成“可验证”的质量底座

2025年上半年联盟测试实验室两次升级测试项，紧跟技术标准演进以满足市场需求，并通过联盟官网等公开渠道发布“通过联盟测试”的产品与终端信息，供市场采购参考。

媒体对WAPI产业联盟测试能力进行了更系统的画像：联盟依标研发“WAPI功能测试项目300余项”，通过测试的产品在标准符合性、互通性、兼容性方面表现良好；通过测试的产品信息在联盟网站公开，实现“透明可查、放心选用”。

业界评价，这类升级反映出联盟测试体系不仅在“扩项”，也在“持续吞吐”新产品进入市场。其行业意义在于，把“能否符合标准、是否存在工程风险”从争论变为证据，推动产业从“口径不一”走向“可量化评估”。对用户而言，这意味着从“听厂商自己说”转为“看得见的证据”。

### 亮点七：低功耗模组与端侧生态持续推进，同时把“安全底线”前置

低功耗方向是生态扩容的重要一环。2025年WAPI产业联盟持续提示低功耗端侧的典型安全隐患（密钥存储于FLASH、缺少硬件安全模块保护），开展针对低功耗WAPI模组及集成终端的“WAPI协议基础要素测评”服务，并提示用户核验测评报告的方法。这反映出生态扩容不是“只追数量”，而是把端侧安全底线纳入测试与选型机制，避免规模化后再付出高昂整改成本。

该测评服务的核心目标是：从产品实现底层进行严格测评，重点核查产品是否采用具备国家密码主管部门批准算法能力的安全芯片，确保密钥的生成、存储、运算等全流程均在安全硬件环境中完成，从根本上防范密钥泄露等潜在安全风险，为用户选型提供权威技术依据。测评服务推出后，得到行业头部企业的积极响应。南方电网数字电网科技（广东）有限公司、北京联盛德微电子有限责任公司、西安芯语慧联信息科技有限公司等单位的多款低功耗WAPI模组及终端产品通过测评。

### 亮点八：证书管理被上升为规模运维核心议题，标准与工程化方案齐头并进

当建设规模从“试点”迈向“广域”，证书生命周期管理决定了网络是否“可运营”。

2025年3月，联盟针对WAPI大规模部署中证书管理的复杂性和多样性需求，召开证书管理解决方案专题会议。会上产业市场达成共识：当部署规模从“百点”走向“千点、万点”，证书全生命周期管理（签发、分发、更新、吊销、审计）不再是后台细节，而成为影响可用性与安全治理的核心能力。要把“可运营”作为系统工程来正面解决，推动制定高效、自动化、可扩展的解决方案。

12月，联盟发布两项“数字证书管理”团体标准，以规范数字证书流程管理，提升无线局域网数字证书

应用的安全性、规范性与高效性。结合上述标准，国网山东省电力公司等联盟成员也提出通过工程服务集标识符（SSID）与预置工程证书，实现线上化签发、到期自动更新、吊销联动下线等工程化解决方案。

### 亮点九：后量子安全议题持续升温，WAPI 2.0 与迁移路线被纳入体系化视野

2025 年，后量子（抗量子攻击）成为安全领域的高频议题，联盟及其成员相关标准化工作成果显著。

据新华社报道，中国专家在 ISO/IEC JTC1/SC6 会议上提交“如何设计抗量子攻击的通信网络安全协议”提案并获通过，将牵头推进协议设计指南，为全球通信网络向后量子密码迁移提供引导。

2025 年期间，媒体披露多项国际标准项目进展：如 ISO/IEC 9594-13《密码算法迁移》项目进入 DIS 阶段，以及包括 ISO/IEC PWI 25513《向后量子加密技术迁移背景下的通信安全协议设计指南》在内的一批 PWI 获批继续研究等，业界评价称，从产业角度看，这类进展的价值不只是“参与国际标准”，而是为 WAPI 及相关安全体系的长期演进提供“可迁移、可升级”的上层设计空间。

### 亮点十：行业洞察报告密集发布，推动用户侧“选型有依据、建设有方法”

2025 年，WAPI 产业联盟在“市场洞察与方法论”类报告上行动迅速，帮助用户把复杂问题结构化。相继发布《工业网络选择中短距离无线通信技术路线的基本原则》《瘦 AP 组网架构下的 WAPI 产品工程化实现与部署》《AS 在 WAPI 三元对等架构中的核心地位与行业合规部署》等洞察报告，《WAPI 标准产业应用及环境监测报告》以及《WAPI 问答》等。

这些报告的共同作用，是把“该怎么建、怎么测、怎么选、怎么运维”的隐性经验显性化、文档化，从而降低用户试错成本。

### 亮点十一：组织治理与行业影响力稳步提升，产业协同机制更成熟

标准化与产业推广需要强组织能力支撑。2025 年，WAPI 产业联盟凭借完善的治理体系、显著的产业服务成效及深厚的社会公信力，再次获评 5A 级社会组织，且为本次唯一获评 5A 的产业联盟。这类“组织能力”的外部评价，虽不直接等同于技术指标，但对产业协同的意义在于：提高生态组织的公信力与动员能力，便于跨行业、跨企业协同创新，推进标准落地、测试互认与示范应用。

### 结语：以系统工程思路 稳步推进高质量安全无线局域网发展

WAPI 生态正在形成一条更清晰的路径：以技术标准为边界、以测试评价为抓手、以行业规模应用为牵引、以行动计划与治理机制保障质量，并将后量子时代的安全演进纳入长期布局。

展望下一阶段，WAPI 的关键命题将从“规模铺开”进一步走向“规模运营”：包括证书颁发与更新的自动化、跨厂商互操作的常态化验证、面向典型行业的参考架构沉淀，以及与新一代无线技术演进之间更细颗粒度的工程协同等等。对产业而言，真正的高质量不在于某一次项目上线，而在于能否在复杂环境中持续稳定、持续合规、持续可演进。

# 新华社等：

## 我国牵头的多项数据通信网络国际标准提案项目 正按计划稳步推进

【编者按】2025年10月，ISO/IEC JTC 1/SC 6（系统间远程通信和信息交换）中期会议及首届SC 6技术研讨会在北京成功召开。

会议由联盟会员单位新华三公司协办。会上，我国牵头的多项数据通信网络国际标准提案项目均按计划稳步推进，涵盖光纤通道网络、抗量子网络通信、下一代网络架构等前沿领域，相关成果将通过国际标准、技术报告和研究报告等形式向全球输出。新华社、新华网、中华网、新华财经/中国金融信息网等媒体发布报道。

以下是新华社的报道：



（新华社记者 刘羽佳）记者日前从中关村无线网络安全产业联盟（WAPI产业联盟）获悉，我国牵头的多项数据通信网络国际标准提案项目正按计划稳步推进。相关项目涵盖光纤通道网络、抗量子网络通信、下一代网络架构等前沿领域，相关成果将通过国际标准、技术报告和研究报告等形式向全球输出。

相关项目包括：西电捷通公司牵头、WAPI产业联盟及会员单位参与的《向后量子加密技术迁移背景下的通信安全协议设计指南》；国网山东省电力公司牵头，新华三技术有限公司、西电捷通公司参与的《无线局域网网络切片技术》；国网山东省电力公司牵头，山东大学、山东科技大学、西电捷通公司参与的《非移动边缘设备无线有序传输规范》等。这些国际标准预备工作项目，以及多项中国专家牵头的技术报告、预备工作项目均按计划稳步推进。

**部分媒体新闻链接:**

新华社: <https://h.xinhua.com/vh512/share/12823994?docid=12823994&newstype=1001&d=13501e9&channel=weixin>

新华网: <http://www.xinhuanet.com/liangzi/20251114/52cd8888c7fd49b8bf3e3c210cb7fa70/c.html>

中华网: [https://m.life.china.com/2025-11/13/content\\_509008.html](https://m.life.china.com/2025-11/13/content_509008.html)

新华财经/中国金融信息网: <https://www.cnfin.com/hg-1b/detail/20251113/4334442-1.html>

中国财经: <http://finance.china.com.cn/news/20251113/6277982.shtml>

中国科技网: [https://www.stdaily.com/web/gdxw/2025-11/13/content\\_431591.html](https://www.stdaily.com/web/gdxw/2025-11/13/content_431591.html)

中国高新网: [http://www.chinahightech.com/chanye/2025-11/14/content\\_432194.html](http://www.chinahightech.com/chanye/2025-11/14/content_432194.html)

中国新媒体信息网: <https://www.cciatv.com/kj/kjzx/11763.html>

京报网: <https://www.bjd.com.cn/news/2025/11/13/11404819.shtml>

证券时报网: <https://www.stcn.com/article/detail/3493574.html>

澎湃新闻: [https://www.thepaper.cn/newsDetail\\_forward\\_31966333](https://www.thepaper.cn/newsDetail_forward_31966333)

新浪财经: <https://finance.sina.com.cn/jjxw/2025-11-13/doc-infxhcvy3888403.shtml>

搜狐网: [https://roll.sohu.com/a/953966541\\_267106](https://roll.sohu.com/a/953966541_267106)

# 通信世界等：

## 第四届无线网络安全标准化工作委员会第二次会议召开 共绘安全无线标准新蓝图

【编者按】2025年12月17日，第四届无线网络安全标准化工作委员会第二次会议在武汉召开，汇聚产学研用50余位代表，推进高质量安全无线局域网建设的共识。会议围绕标委会年度工作总结与下一年度重点任务，开展审议表决、经验交流与应用研讨，并对优秀委员、优秀项目编辑予以肯定，为新晋委员颁发证书和信物。同时，会议宣讲并发布标准化工作制度修订计划，听取并审议各工作组年度工作汇报及后续计划建议，形成会议决议。通信世界、飞象网、中国信息化周报等媒体对此进行了报道。

以下是通信世界的报道：



2025年12月17日，第四届无线网络安全标准化工作委员会（以下简称“标委会”）第二次会议在湖北武汉顺利落幕。作为WAPI标准体系建设与产业应用推进的关键节点会议，本次大会汇聚产学研用多方力量，围绕年度工作总结、重点任务部署、技术创新实践、制度体系完善等核心议题，通过政策宣讲、经验分享、专题研讨、激励先进等多元环节，既聚焦安全无线局域网建设“深水区”的核心痛点，又明确了2026年标准化工作的行动路径，为WAPI标准体系完善与规模化高质量应用凝聚广泛共识、注入强劲动能。

本次会议由WAPI产业联盟主办，数字认证（武汉）有限责任公司协办，标委会副主任委员、WAPI产业联盟秘书长张璐璐主持。

来自无线网络安全技术国家工程研究中心、中国电力科学研究院有限公司、国网山东省电力公司电力科学研究院、南方电网数字电网科技（广东）有限公司、北京数字认证股份有限公司、西电捷通公司、北京联盛德微电子有限责任公司、迈普通信技术股份有限公司、新华三技术有限公司、北京智芯微电子科技有限公司、北京华信傲天网络技术有限公司、广州莲雾科技有限公司、深圳市智开科技有限公司、西安芯语慧联信息科技有限公司、深圳市国电科技通信有限公司、重庆物奇微电子股份有限公司、上海久壬信息科技有限公司、南京南瑞信息通信科技有限公司、广电计量检测集团股份有限公司、江苏省电子信息产品质量监督检验研究院(江苏省信息安全测评中心)、西安邮电大学等产业链核心单位，以及ISO/IEC JTC 1/SC 6国内技术对口单位、工业和信息化部宽带无线IP标准工作组等标准组织的50余位代表参会，共同为无线网络安全标准化事业建言献策。



图：标委会副主任委员  
WAPI产业联盟秘书长 张璐璐



图：会议合影

### 锚定国家战略：以标准化筑牢体系安全能力基石

无线网络安全标准化事关国家安全与发展全局。标委会主任委员曹军在书面致辞中指出，随着工业无线、城市与园区互联、车联网与低空通信、AI与边缘计算承载等场景的快速发展，网络安全已从单点防护技术迈向体系能力建设与生态治理新阶段。标准化作为产业发展的“共同语言”，需将安全目标、责任边界、技术要求、测试方法和互操作规则固化落地，实现安全能力的可验证、可复用、可协同。

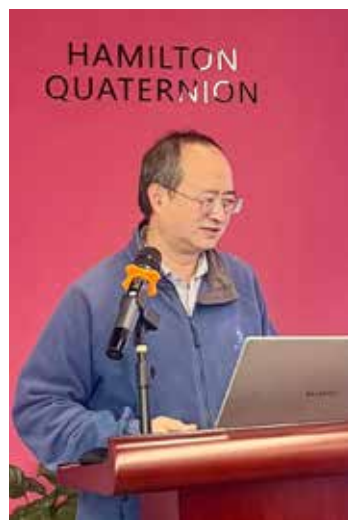
面向2026年工作，曹军提出四点核心建议：一是胸怀“国之大者”，紧扣新型工业化、数字中国、网络强国等重大战略任务，聚焦工业无线、园区、城市公共无线、车联网、低空通信等关键场景，构建分级分类、可落地的安全基线与实施指南，做到网络“可用、可管、可追溯”；二是坚持问题导向与目标导向相统一，针对量子技术、身份与信任、密钥管理、供应链安全、AI应用等带来的新型风险，从全生命周期、全链条提升网络安全性与健壮性，在标准制定中把要求写硬、把边界讲清，实现“能落地、可验证、可评估”；三是强化协同攻关，贯通团标—行标—国标转化通道，构建“标准—测评—试点示范—采购验收”闭环体系，通过标准符合性和互操作测试提升标准质量与公信力；四是坚持广泛参与和透明性，持续完善利益冲突管理、公开征求意见、专家复核与争议协调机制，并加强与主管部门、行业组织、检测机构、重点企业及用户侧协同，形成“政策—标准—测评—应用”闭环，推动标准真正转化为可执行的治理能力。



图：WAPI产业联盟测试实验室  
王立华



图：北京数字认证股份有限公司  
副总经理 侯鹏亮



图：北京华信傲天网络技术有限公司  
总监 范小伟

北京数字认证股份有限公司副总经理侯鹏亮在致辞中表示，将坚持产学研用协同创新机制，以标准化促产业高质量发展，并围绕数字信任与数据安全能力建设、联合实验室与实训基地等工作进行了介绍。

### 直击“深水区”痛点：以创新实践推动高质量落地

当前，WAPI建设已步入“深水区”，产业关注的焦点从“能否部署”转向“如何部署得更好、更稳、更安全”。在“无线安全与WAPI高质量发展创新实践分享”环节，WAPI产业联盟测试实验室王立华聚焦关键症结，剖析四大核心挑战，并详细介绍了联盟的系统化应对举措。

一是检测不到位导致“简单测试通过但现场不好用”。例如：部分AP未按标准执行重传机制，在干扰环境中易出现接入失败、掉线等问题，且简易工具难以检测。对此，联盟已开发专项测试项、升级检测系统，推动隐性缺陷前置解决。

二是工程架构“省事化”引发安全红线风险。例如：部分厂商在瘦AP架构中采用“AE加解密在AP、密钥协商在AC”的拆分实现，导致密钥跨设备传输，增加窃取、篡改风险，而用户难以从招采文本或常规验收中识别该风险，容易把“能连上”误当成“符合安全架构”。对此，联盟已启动公共预警、新增测试项及瘦AP产品重测专项，引导市场回归合规路径。

三是低功耗终端“降本优先”造成密钥泄露隐患。部分低功耗WAPI模组将密钥直接存储于闪存（FLASH），缺乏硬件防护，且隐患隐蔽性强。对此，联盟已建立协议基础要素测评能力并纳入测试项目体系，提示用户选型时重点核验联盟测评报告。

四是“弱化/绕过AS”引发系统性风险。部分工程为降低切换时延屏蔽AS鉴别功能，动摇WAPI三元对等架构的信任根基。对此，联盟已形成AS合规部署原则与策略建议，强调结合信息系统安全策略优化部署模式。

侯鹏亮针对WAPI大规模应用中的异厂商AS互通不足、端到端测试缺失、AS漫游配置复杂、故障定位与运维可视化不足等痛点，倡议构建“标准统一、测试前置、落地可靠”的闭环机制，推动漫游日志全链路记录与标准化，并纳入联盟测试。同时，他结合两项已发布的数字证书管理团体标准，提出通过工程服务集标识符（SSID）与预置工程证书实现线上化签发、到期自动更新与吊销联动下线等工程化解决方案。

在同期开展的“安全无线局域网（WAPI）应用与发展交流研讨”中，与会代表围绕市场建设痛点攻坚、场景驱动型产品创新、标准化需求落地等议题深入交流，形成多项共识。

### 夯实发展根基：标准体系与生态建设双轮驱动

会议审议并通过《无线网络安全标准化工作委员会2025年工作总结》。报告显示，标委会全年聚焦“构建高质量安全无线局域网标准体系并推动标准实施”核心目标，稳步推进了12项重点任务：标准制定方面，《高质量安全无线局域网总体要求》完成两轮征求意见进入报批阶段，《数字证书管理》两项团体标准正式发布，《高质量安全无线局域网服务能力要求》《高质量安全无线局域网服务能力评价方法》等新增项目成功立项；标准实施方面，持续完善宣贯材料、开展运维工具与场景验证、专题研讨与实践分享，联盟测试测评能力得到用户广泛采信；平台与生态方面，优化文本质量提升机制与委员履职规范，强化与主管部门沟通及国际标准推进力度。

会上，标委会对2025年表现突出的优秀委员与优秀项目编辑予以肯定和鼓励。一年来，数十位委员积极履职，在标准起草实施、国家及行业标准引用推广、成果宣传等方面成效显著，为WAPI标准服务市场需求提供了重要支撑。同时，标委会专家队伍进一步壮大，新增9位委员后总规模达93人。会议为新晋委员颁发证书与信物，迈普通信技术股份有限公司产品总监韩志强代表新晋委员发言表示，将与全体委员携手开展协同创新，推动WAPI规模部署与标准推广，为我国标准化事业贡献力量。

联盟新会员代表上海久壬信息科技有限公司总经理陈进茹介绍了面向电网核心侧的WAPI深度应用规划，并表示将依托联盟平台加强产业协作，加速规模化落地。



图：对2025年优秀委员和项目编辑予以鼓励



图：标委会新晋委员合影

### 明确行动纲领：制度完善与任务部署引领新征程

会议听取并原则通过《关于修订并发布三项标准化工作制度的提案》，计划对《中关村无线网络安全产业联盟标准化工作管理办法》等三项制度修订完善后，于2025年12月31日前提交函审报批，2026年1月正式发布。

在工作组年度工作汇报环节，总体工作组（WG1）、网络安全工作组（WG2）、无线网络工作组（WG3）、产品与解决方案工作组（WG4）、互操作测试工作组（WG5）、特别任务管理工作组（WG6）、生态环境工作组（WG7）分别汇报2025年工作总结与2026年计划建议。会议审议并原则通过《无线网络安全标准化工作委员会2026年重点任务计划》，明确四大核心方向：一是持续完善《高质量安全无线局域网》标准体系；二是健全WAPI 2.0、证书管理技术标准体系及综合网管、管控一体机产品规范；三是研究制定WAPI与人工智能、智能人形机器人等融合应用的技术与产品标准；四是推动重点领域团体标准向国家标准转化。会议要求细化完善计划并按程序提交全体委员函审。

会议期间，与会代表还对数字认证（武汉）有限责任公司进行参访调研，实地了解企业在无线网络安全领域的技术研发与实践应用成果，为后续产业协作搭建了务实桥梁。



图：上海久壬信息科技有限公司  
总经理 陈进茹



图：标委会副主任委员、WG1组长  
黄振海



图：参访调研数字认证（武汉）有限责任公司

作为我国无线网络安全标准化领域的核心平台，标委会自2006年由WAPI产业联盟发起以来，始终秉持开放、专业、务实的原则，汇聚93名委员及全产业链力量，累计开展200余项标准制修订工作，为构建最基础最共性的网络安全架构体系提供了有效支撑，其中已发布（获发布）国际标准（ISO/IEC）23项、欧洲标准3项，国家标准42项，国家军用标准4项，行业标准7项，地方标准1项、中关村标准3项、团体标准107项。此次会议的成功召开，进一步凝聚了产业共识、明确了发展路径，将推动无线网络和网络安全标准体系持续完善与规模化高质量应用，为网络强国建设筑牢无线安全基石。

部分媒体新闻链接：

通信世界：<https://www.cww.net.cn/article?id=606247>

飞象网：<http://www.cctime.com/html/2025-12-25/1726100.htm>

中国信息化周报：<https://www.cio360.net/show-598-104614-1.html>

飞象网等：

## WAPI产业联盟召开2025年第四次标准工作和项目组会议 (总第136次)

【编者按】12月18日，WAPI产业联盟召开2025年第四次标准工作和项目组会议（总第136次），围绕第四季度工作进展、上一次项目组集中会议要点落实、已发布标准宣贯、已立项项目讨论、国际化推进以及标委会平台质量提升相关议题展开。飞象网、通信世界、中国信息化周报等媒体对此进行了报道。

以下是飞象网的报道：



12月18日，WAPI产业联盟召开2025年第四次标准工作和项目组会议（总第136次），围绕第四季度工作进展、上一次项目组集中会议要点落实、已发布标准宣贯、已立项项目讨论、国际化推进以及标委会平台质量提升相关议题展开。



图：会议合影



图：会议现场

来自无线网络安全技术国家工程研究中心、南方电网数字电网科技（广东）有限公司、西电捷通公司、北京数字认证股份有限公司、北京联盛德微电子有限责任公司、北京华信傲天网络技术有限公司、重庆华联众智科技有限公司、重庆物奇微电子股份有限公司、华为技术有限公司、新华三技术有限公司、西安芯语慧联信息科技有限公司、广电计量检测集团股份有限公司、广州莲雾科技有限公司、迈普通信技术股份有限公司、南京南瑞信息通信科技有限公司、上海久壬信息科技有限公司、深圳市国电科技通信有限公司、深圳市智开科技有限公司、深圳市明华澳汉智能卡有限公司、中国电信股份有限公司研究院、中国电力科学研究院有限公司、湖北经济学院、西安邮电大学等单位代表，以及ISO/IEC JTC 1/SC 6国内技术对口单位、工业和信息化部宽带无线IP标准工作组，无线网络安全标准化工作委员会委员等参加会议。

WAPI产业联盟秘书长、标委会副主任委员张璐璐表示，2025年是WAPI产业在高质量发展道路上笃定前行的关键一年，实现了标准体系从“量的积累”向“质的飞跃”的重要跨越。她指出，一年来，WAPI标准产业共同体成果丰硕：**标准创新与成果转化深度推进**，全年推进30项重点标准项目，紧密对接市场需求，扎实服务产业落地，WAPI标准已深度融入能源电力、国防、工业控制、智能仓储等关键领域，让“度量衡”的价值真正体现在网络和数据安全的每一个环节；**技术引领与国际布局成效显著**，面对量子计算带来的安全挑战，积极贡献抗量子网络安全“中国方案”，推动中国技术、中国标准走向世界，同时聚焦AS-CIS 功能分离部署、边缘轻量化演进等前沿，为工业互联网、车联网等新兴场景提供安全支撑；**生态建设持续壮大**，标准队伍全面覆盖产学研用各环节，南网、国网等市场用户深度参与，让标准更贴合实际需求，一批优秀企业和个人快速成长，为产业发展注入强劲动力。

张璐璐强调，2026年，标委会将秉承开放、协商一致的原则，持续激发标准化平台活力，保障每一位参与者在创新实践中无顾虑、有作为。标准产业共同体将继续以场景需求为导向，加快前沿领域标准布局，深化国际交流合作，持续优化生态平台建设，携手推动WAPI标准产业再上新台阶。



图：WAPI产业联盟秘书长  
标委会副主任委员 张璐璐



图：工信部宽带无线IP标准工作组秘书长  
标委会副主任委员 黄振海

工业和信息化部宽带无线IP标准工作组秘书长、标委会副主任委员黄振海表示，在前一天召开的标委会全体会议上，我们对标委会2025年工作进行了系统回顾与总结，通过对重点任务执行情况和对整体工作过程和成果的深入梳理，不仅清晰看到了成绩与亮点，也直面了那些未达预期的环节，以及制约产业发展的堵点与难点，同时凝练出若干影响标准应用的痛点与薄弱环节。这些问题正是我们未来必须集中力量攻克的关键所在，需要依托扎实的技术研究与充分的交流，在标准制定与实施的每一个环节上持续发力、精准突破。2026年，标委会将按照既定任务目标，稳扎稳打推进标准制定工作。我们充分认识到，标准的开发不仅是技术文本的编写过程，更是产业各方达成共识的过程。只有在“共享共治”的理念下，经过充分协商与广泛参与，形成兼顾各方利益、凝聚集体智慧的标准，才能真正拥有生命力，并在实施中发挥长久而深远的作用。

会议通报了2025年第四季度标准产业市场应用阶段性进展：发布《信息安全技术 数字证书管理 第3部分：证书颁发》《信息安全技术 数字证书管理 第4部分：证书撤销》两项团体标准；召开2025年第四次标委会主任委员会议（总第15次）；多厂商多款产品通过联盟测试，其中西安芯语慧联信息科技有限公司低功耗模组通过WAPI协议基础要素测评；发布4份技术报告和服务手册，为行业应用提供有力支撑。

黄振海还报告了第四季度标准工作具体情况。**团体标准方面**，发布2项，进入报批阶段7项、送审阶段8项、征求意见阶段2项、草案稿阶段5项，新立项3项；2项解决方案进入草案稿阶段；**国际标准推进方面**，2025年10月16日至2025年12月16日，SC 6国内技术对口单位对内流通国际提案文件6份，向国际反馈投票/意见3份。组织中国专家参加ISO/IEC JTC 1/SC 6 WG 1和WG 7中期工作组会议，稳步提升我国在国际无线网络安全标准领域的话语权。

会议期间，无线网络安全标准化工作委员会委员于双双对T/WAPIA 013.3—2025《信息安全技术 数字证书管理 第3部分：证书颁发》、T/WAPIA 013.4—2025《信息安全技术 数字证书管理 第4部分：证书撤销》两项团体标准进行宣贯解读。标委会委员郑骊回顾了2025年第三次项目组集中会议决议落实情况，确认所有项目均按计划推进。

在已立项项目讨论环节，与会代表集中讨论《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第1部分：服务和协议》等7项、《应用于抽水蓄能领域的电力物模型WAPI产品规范》《无线局域网网络切片技术要求》《信息安全技术 引入可信第三方的实体鉴别及接入架构规范》《采用CAPWAP协议的无线局域网接入点集中管理通用技术规范》《基于终端预置工程证书的WAPI证书在线管理方案指南和示例》《安全无线局域网综合管理系统通用技术要求》《无线局域网安全技术规范》《采用MQTT协议的无线局域网接入点集中管理通用技术规范》《无线局域网设备技术规范 第6部分：管控一体机》《高质量安全无线局域网 服务能力要求》《高质量安全无线局域网 服务能力评价方法》18项已立项标准以及《基于WAPI的智能仓储解决方案》《基于终端预置工程证书的WAPI证书在线管理解决方案》2项解决方案项目，并协商一致。

在标准国际化专题讨论中，郑骊介绍2026年ISO/IEC JTC 1/SC 6领域国际标准化工作安排。

会议同期，联盟标准化部刘婷开展团体标准文本质量提升交流培训，进一步规范标准编制流程、提升标准质量。工业和信息化部宽带无线IP标准工作组2025年第四次项目组集中工作会议同步召开。

部分媒体新闻链接：

飞象网：<http://www.cctime.com/html/2025-12-26/1726176.htm>

通信世界：<https://www.cww.net.cn/article?id=606277>

中国信息化周报：<https://www.cio360.net/show-598-104615-1.html>

# 中国信息化周报等：

## 规范数字证书流程管理 WAPI产业联盟发布两项团体标准

【编者按】2025年12月10日，WAPI产业联盟正式发布T/WAPIA 013.3—2025《信息安全技术 数字证书管理 第3部分：证书颁发》与T/WAPIA 013.4—2025《信息安全技术 数字证书管理 第4部分：证书撤销》两项团体标准，与系列标准中证书存储与使用、证书格式等相关内容紧密衔接，进一步完善了WAPI标准体系中数字证书管理的全链条架构，显著提升无线局域网数字证书应用的安全性、规范性与高效性。中国信息化周报、通信世界、飞象网等媒体对此进行了报道。

以下是中国信息化周报的报道：



日前，中关村无线网络安全产业联盟（WAPI产业联盟）正式发布 T/WAPIA 013.3—2025《信息安全技术 数字证书管理 第3部分：证书颁发》与T/WAPIA 013.4—2025《信息安全技术 数字证书管理 第4部分：证书撤销》两项团体标准，为数字证书颁发与撤销环节建立起科学完善的技术规范，将有效推动该技术在安全无线局域网领域的规模化应用，并为我国高质量网络建设和相关产业健康发展提供关键技术支撑。上述标准已于2025年12月10日实施。

其中，T/WAPIA 013.3—2025明确了数字证书颁发与更新的核心流程，细化了终端实体证书颁发的运维管理要求和安全规范，成功破解了不同厂商设备间因协议差异引发的互操作难题，降低了系统集成复杂度，为证书颁发全流程的安全性及规范性提供了有力保障。T/WAPIA 013.4—2025则界定了数字证书撤销的适用条件与实施流程，明确了终端实体证书撤销后的状态发布与更新要求、证书撤销列表（CRL）格式标准及后续处置



图：《数字证书管理》系列2项团体标准

规范，有效解决了证书撤销后设备间的协同处置问题，确保风险证书及时失效，从源头防范了恶意使用带来的网络安全风险。

两项标准的起草工作汇聚了产业链上下游核心力量，参与单位包括北京数字认证股份有限公司、中关村无线网络安全产业联盟、南方电网数字电网科技（广东）有限公司、广州莲雾科技有限公司、深圳市智开科技有限公司、西安芯语慧联信息科技有限公司、西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程研究中心、工业和信息化部宽带无线 IP 标准工作组、北京华信傲天网络技术有限公司、中能融合智慧科技有限公司等多家设备厂商与科研机构。起草过程中，联盟广泛征求业界意见，充分凝聚产业共识，确保标准兼具实用性、前瞻性与可操作性。

此次标准的发布实施，进一步完善了 WAPI 标准体系中数字证书管理的全链条架构，两项标准与系列标准中证书存储与使用、证书格式等相关内容紧密衔接，构建起覆盖数字证书全生命周期的标准化体系，将显著提升无线局域网数字证书应用的安全性、规范性与高效性，为企业开展安全无线局域网等类网络设备的证书管理工作提供了权威技术指导，将推动数字证书技术在更广泛领域实现规范化应用，为提升我国网络安全保障能力注入新动能。

部分媒体新闻链接：

中国信息化周报：<https://www.cio360.net/show-598-104587-1.html>

通信世界：<https://www.cww.net.cn/article?id=605908>

飞象网：<http://www.cctime.com/html/2025-12-12/1725184.htm>

# 中国信息化周报等： WAPI产业联盟发布高质量安全无线局域网标准体系首项标准

【编者按】2025年12月30日，WAPI产业联盟发布“高质量安全无线局域网标准体系”首项标准《高质量安全无线局域网 总体要求》（T/WAPIA 054—2025）。业内认为，该标准的发布标志着我国无线局域网标准体系在基于WAPI的“基础连接安全”之上，迈入“高质量安全”的新阶段。中国信息化周报、飞象网等媒体对此进行了报道。

以下是中国信息化周报的报道：



当前，随着数字化进程加速，在满足基本安全连接需求的基础上，如何构建和运行更高质量的安全无线局域网，成为产业链各方共同关注的方向。此次发布的《高质量安全无线局域网 总体要求》首次明确高质量安全无线局域网的基本定义与总体架构，系统提出识别认定、网络建设、监测预警、检测评估、主动防御、应急处置等方面的基本要求，为相关单位开展高质量安全无线局域网的规划建设、运行保障与质量评价提供通用依据和技术指引。

据介绍，该标准由中关村无线网络安全产业联盟、无线网络安全技术国家工程研究中心、西安西电捷通无线网络通信股份有限公司、北京数字认证股份有限公司、国家无线电监测中心检测中心、广州蓬雾科技有限公司、北京华信傲天网络技术有限公司、国网山东省电力公司、西安芯语慧联信息科技有限公司、新华三技术有限公司、南方电网数字电网科技（广东）有限公司、海南电网有限责任公司、深圳市国电科技通信有限公司、



图：《高质量安全无线局域网 总体要求》团体标准

深圳鼎信通达股份有限公司、工业和信息化部宽带无线 IP 标准工作组等单位共同起草。

业内人士表示，“高质量安全无线局域网标准体系”以网络设备产品质量、网络建设质量、网络运营和服务质量为核心，通过标准化手段推动从技术设计到运营服务的全链条规范。该标准的发布有助于产业界进一步形成对安全无线局域网“高质量”内涵与评价方法的共识，促进相关技术、模块、产品以及建设运维与服务的质量要求和评价水平提升，培育和释放安全无线局域网领域新质生产力，为高质量网络建设和产业持续健康发展提供支撑。

部分媒体新闻链接：

信息主管网：<https://www.cio360.net/show-598-104625-1.html>

飞象网：<http://www.cctime.com/html/2026-1-5/1726728.htm>

## 联盟发布洞察报告

# 《AS在WAPI三元对等架构中的核心地位与行业合规部署》

【WAPI产业联盟】

【编者按】《WAPI 市场应用洞察报告》是 WAPI 产业联盟的系列出版物，目标是指导安全无线局域网（WAPI）产业市场高质量发展。本期《洞察报告》以能源电力行业 WAPI 试点项目和在建项目为洞察样本，聚焦鉴别服务器（AS）的功能定位、部署策略演进，形成核心结论，内容如下：

### 一、本期洞察对象与结论

随着 WAPI（无线局域网鉴别与保密基础结构）在工业、政务、国防等高安全需求领域的规模化部署，三元对等架构作为 WAPI 的核心，其工程化实现与部署合理性成为产业界关注焦点。本期《洞察报告》以能源电力行业 WAPI 试点项目和在建项目为洞察样本，聚焦鉴别服务器（AS）的功能定位、部署策略演进，结合高安全场景的实践验证，形成核心结论如下：

**（一）信任根基不可动摇：**AS 是 WAPI 三元对等安全体系的信任根基，任何削弱或绕过 AS 核心功能的实现方案，均背离 WAPI 架构的设计原则，引入系统性安全风险。

**（二）部署策略需适配安全需求：**AS 部署必须以信息系统安全策略为核心导向，高安全、高可靠场景下（如电力调度、工业控制），需优先考虑热备、灾备、本地化等保障方案，严禁将“绕过 AS”作为应急处置手段。

**（三）双线演进成为明确趋势：**未来 AS 部署将呈现两大方向：一是大型中心化网络中，结合高可靠有线骨干网和 WAPI 综合网管，向“高并发 + 虚拟化 + 云化”AS 服务平台演进；二是需要数据本地化处理和低时延的场景中（如工业互联网、车联网），AS 与 CIS 功能分离，以“轻量化 + 一体化”形态下沉，部分场景可与 AC 功能融合。

### 二、WAPI 三元对等架构的技术原理与核心机制

#### （一）架构本质：三元对等的安全逻辑

WAPI 区别于传统 Wi-Fi 安全协议的核心优势，源于终端（STA）- 接入点（AP）- 鉴别服务器（AS）构成的三元对等架构：

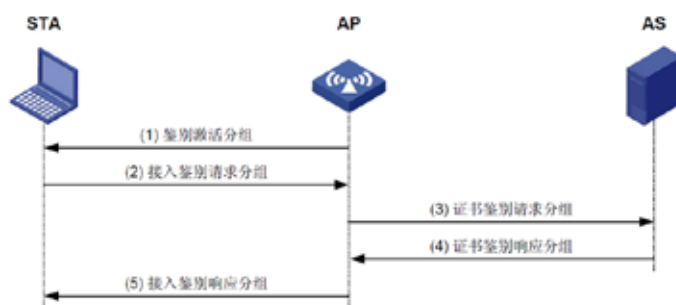
- 赋予 AP 独立身份标识，打破传统二元架构中 AP “无独立身份”的设计缺陷。
- 实现终端与 AP 的双向对等的身份鉴别，从根源上抵御“伪基站”、“钓鱼 AP”等中间人攻击。

## （二）鉴别机制：基于数字证书的可信验证

WAPI 采用基于在线可信第三方（AS）的数字证书双向鉴别机制，核心实现“网络 - 用户”双向身份验证：一方面验证接入终端（STA）的合法性，另一方面为终端验证接入点（AP）及网络的可信性，从双向维度阻断非法接入与网络伪造风险。

数字证书（也称公钥证书）是由证书签发机构（WAPI体系中即 AS）签名的标准化数据结构，核心包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息等关键要素。WAPI系统中所使用的用户证书为数字证书，通过AS对用户证书进行鉴别，可以唯一确定WAPI用户的身份及其合法性。鉴别过程采用椭圆曲线签名算法，并使用安全的消息杂凑算法实现消息的完整性，攻击者难以对进行鉴别信息进行篡改和伪造，安全强度高。

WAPI证书鉴别前STA和AP必须预先安装各自的证书，然后通过AS对双方的身份进行鉴别，根据双方产生的临时公钥和临时私钥生成基密钥，并为随后的密钥协商做好准备。证书鉴别的过程如下图所示。



图：WAPI证书鉴别过程

在 WAPI 证书鉴别的基础上，STA 和 AP 安全协商出会话密钥（避免了传输密钥带来的风险），用于后续数据通信的完整性和机密性保护。

## 三、AS 核心地位的三维解构

AS 的不可替代性源于其在信任体系、身份鉴别、网络运维三大维度的基础性作用，三者形成“信任 - 鉴别 - 管控”的闭环支撑：

### （一）维度一：信任体系的根基

AS 是整个 WAPI 安全体系的信任锚点（Trust Anchor），承担合法 STA/AP 的证书鉴别与管理职责：

- 采用“星型信任模型”，将 STA 与 AP 间的网状信任关系简化为“双方向 AS 信任”，使大规模网络（如含 10 万 + 终端的电力物联网）的信任管理复杂度大幅度降低。

- 红线原则：任何在 AS 之外建立次级信任中心的行为（如将部分鉴别功能迁移至 AC），均会破坏信任体系的唯一性，经安全测试验证，此类改造会使网络遭受攻击的风险大幅提升。

## （二）维度二：双向鉴别的核心仲裁者

WAPI 与传统 Wi-Fi 安全协议的关键差异的在于 AS 的仲裁角色：

- Wi-Fi 安全协议：AP 仅作为 RADIUS 代理，仅实现对 STA 的单向鉴别。

- WAPI 安全协议：要求 STA 和 AP 进行直接的双向对等身份鉴别。AS 作为共同信任的第三方，同时验证 STA 与 AP 的证书合法性，独立判定身份有效性并反馈结果，确保 STA 接入的是经可信鉴别的合法 AP，从理论上彻底杜绝“钓鱼 AP”攻击，其过程也确保了鉴别结果的客观性与权威性。

- 风险警示：绕过 AS 由 AC/AP 自行完成鉴别的方案，实质是赋予设备“非法信任权限”。任何试图绕过 AS 的行为都会破坏这一对等仲裁流程，给“钓鱼 AP”创造机会。

## （三）维度三：网络安全管理策略执行中心

AS 的集中化部署架构，为网络运营者提供全局性的安全可视化能力与精细化策略管控能力。作为动态信任构建流程的核心枢纽，AS 全程参与身份鉴别、密钥协商的关键环节，承担实时验证、双向协调、操作留痕的核心职能，确保每一次接入行为都处于可控、可追溯的安全框架内。

所有终端的入网身份标识、接入时间、关联 AP 物理位置（含设备 ID）、鉴别成功 / 失败、密钥协商过程等关键安全日志，均以不可篡改的形式集中沉淀于 AS。这为安全审计、攻击溯源、合规性核查提供权威、完整的一手数据源。

同时，AS 是执行最高层级安全策略的天然载体，具备策略统一下发、强制落地的核心能力：一方面支持证书注销列表（CRL）的实时生效与在线查询，确保已注销证书的终端无法接入网络；另一方面可基于终端角色（如巡检机器人、运维终端）、证书属性（如权限等级、所属区域）实现精细化访问控制与分组管理，例如限制某类终端仅能接入特定 AP 分组、访问指定业务网段，确保安全策略在全网范围内的一致性与强制性，避免“策略孤岛”问题。

综上，AS 在信任体系、身份鉴别、网络运维三大核心维度形成“信任基石-鉴别仲裁-管控中枢”的有机闭环：以“唯一信任锚点”为安全基石，通过“双向对等鉴别”实现终端与网络的可信接入，最终以“全局策略管控”完成安全能力的落地闭环，三者层层递进、不可分割，共同构成 WAPI 三元对等架构的安全核心。任何在产品工程化实现或部署过程中，对这三大维度的功能削弱、流程简化或架构扭曲（如绕过 AS 鉴别、弱化管控能力），都将直接突破 WAPI 的安全设计底线，动摇三元对等架构的根本逻辑。产业实践中的多次攻防测试与项目复盘已充分验证：坚守 AS 的核心地位、保障其功能完整性与部署合规性，是 WAPI 网络实现高安全目标的唯一必由之路，也是高安全场景规模化落地的关键前提。

#### 四、AS 工程化实现与部署的典型问题及合规方案

尽管 WAPI 标准体系对 AS 的角色有明确定义，但在实际的产业化和工程化过程中，由于对三元对等架构理解不透彻，或受传统网络建设思维惯性影响，仍存在以下问题与风险：

##### （一）问题 1：为降低切换时延，屏蔽 AS 鉴别功能

在实际应用中，有些业务如巡检机器人、无人机等需要 STA 可以在不同 AP 间快速切换，实现高清视频不卡顿。

经调研发现，个别产品实现这种快速切换能力是以牺牲安全性为代价的，具体做法是：STA 与 AP1 完成 WAPI 的鉴别及密钥协商流程，AP1 会将协商产生密钥通过 AC “分发”给附近的 AP2/AP3/……，当 STA 移动到 AP2 覆盖范围内并尝试与 AP2 进行 WAPI 连接时，就可以跳过 WAPI 身份鉴别过程直接使用密钥通信，从而达到快速切换。但是这种做法有严重的安全风险，将密钥在 AP/AC 之间的网络中传输，一旦密钥泄露，非法 STA 就可以绕过 WAPI 的身份鉴别机制，直接入侵到 WAPI 网络中。

正确的做法是：快速切换功能应在保证安全的前提下实现。STA 无论切换到哪个 AP 上，都要完整进行 WAPI 身份鉴别流程，快速切换功能可以通过诸如“双发选收”等工程化实现手段实现。

##### （二）问题 2：AS 不可用时，采用“代位鉴别”等应急方案

在 WAPI 规模部署实践中，“AP 本地部署、AS 远端集中”是当前常见架构，但在实际应用中会有一些偶发因素造成 AP 与 AS 之间的网络不通或延迟过大，一旦发生这种“AS 丢失”的应急情况，本地所有 STA 都将无法成功接入 WAPI 网络。以电力输电线应用场景为例，铁塔间通过 WAPI 无线级联组网，若 AS 在远端，一旦某个铁塔上的设备故障，可能会导致整条输电线路 STA 掉线。

经调研发现，个别产品以“私自改动 WAPI 协议”为代价来解决“AS 丢失”的应急情况，在没有 AS 参与的情况下，通过 AP “代位鉴别”或其他“变通”方式完成 WAPI 身份鉴别流程。这严重影响了安全性，甚至严格意义上已经不属于 WAPI 产品了。众所周知，WAPI 的“三元对等”安全架构中，AS 是不可或缺的一元，任何没有 AS 参与的 WAPI 身份鉴别流程都不可能完整，都无法保障安全性。

正确的做法是：通过备份部署和本地化部署提升 AS 可用性。例如在电力输电线应用场景中，可以将 AS 的发证和鉴别功能分离，将 CIS（发证）集中部署，将 AS（鉴别）下沉到本地部署，从而实现“集中管理、本地鉴别”，保障 AS 可用性。

#### 五、行业挑战与未来演进方向

##### （一）当前核心挑战

- 技术标准支撑不足：AS 技术、产品、测试已有成熟标准，但部署规范、风险防控缺乏统一指引，导致行业实践参差不齐。

- 认知偏差：部分企业受传统（如：运营商时代）网络建设思维影响，过度追求部署便利性而牺牲安全性，需通过标准宣贯与案例警示纠正。

## （二）标准化推进行动

近期立项的两项团体标准正在填补空白，为产业和市场用户提供通用的“部署说明书”和“运维指导手册”：

- 《安全无线局域网综合管理系统通用技术要求》：明确 AS 集中云化部署的安全基线与运维规范。

- 《基于终端预置工程证书的 WAPI 证书在线管理方案指南和示例》：提炼电力等重点行业最佳实践，形成可复用的部署模板。

## （三）AS 部署方式演进趋势

AS（鉴别）是一种高频、实时、在线的业务，适合本地 / 分布式部署；CIS（发证）是一种低频、非实时、在线 / 离线均可的业务，适合集中部署，根据需要二者功能可以分离。

未来 AS 部署将呈现两大方向：一是大型中心化网络中，结合高可靠有线骨干网和 WAPI 综合网管，向“高并发 + 虚拟化 + 云化”AS 服务平台演进；二是需要数据本地化处理和低时延的场景中（如工业互联网、车联网），AS 与 CIS 功能分离，以“轻量化 + 一体化”形态下沉，部分场景可与 AC 功能融合。

## WAPI问答（系列连载）

在WAPI服务各行各业及关键信息基础设施建设的过程中，联盟总结了一些市场用户的常见问题。同时，我们注意到百度百科、搜狗百科、互动百科、维基百科中文版等对WAPI技术、标准、产业及演进历程的描述存在不准确或某些错误。为帮助大家更加客观、准确地了解WAPI，推出WAPI问答（系列连载）。

WAPI问答（系列连载）覆盖WAPI技术、标准、产品、应用、检测评估、联盟与会员等方面内容，并定期更新。文件中涉及的数据与内容，均源自公开信息。

咨询请联系：staff@wapia.org

## 第十七部分（PART 17）

### ■ 1、问：WAPI AP支持WPI-SM4-OFB+CMAC-128（以下简称OFB+CMAC）和WPI-SM4-GCM-128（以下简称GCM）密码套件时，如何与STA协商确定单播密码套件和组播密码套件？

**答：**AP和STA在建立安全连接前需要先进行安全策略协商，当AP和STA的WAPI安全策略同时支持OFB+CMAC和GCM时，在工程实现上，安全策略协商应遵循以下处理逻辑：

（1）若AP同时支持OFB+CMAC和GCM密码套件，可通过配置WAPI信息元素（WAPIE）通告多个单播密码套件，但组播密码套件只能通告一个；若优先考虑兼容性，则组播密码套件建议选择OFB+CMAC。（通常AP在信标帧或探测响应帧中包含WAPIE字段，用于标识它支持的WAPI安全策略。）

（2）若STA和AP发现双方单播密码套件或组播密码套件没有相同项，则关联失败。

（3）若STA和AP发现双方单播密码套件均支持OFB+CMAC和GCM，则应优先选择GCM。

（4）若STA和AP发现AP支持OFB+CMAC和GCM，而STA仅支持OFB+CMAC，则应选择OFB+CMAC；

OFB+CMAC和GCM密码套件用于WAPI保密通信过程。2003年GB 15629.11定义了OFB+CMAC密码套件，随着WAPI技术向更高速率的演进发展，2016年发布的《WAPI与IEEE 802.11ac》团体标准中新增支持了GCM密码套件。GCM密码套件提供多分组并行加解密特性，可通过多核并行处理提升性能，提供加解密功能的同时还能提供数据完整性校验功能，无需结合额外组件，效率更高，可满足11ac、11ax、11be等高性能网络需要。

## ■ 2、问：在实现WAPI保密通信时，OFB+CMAC和GCM两种密码套件在工程实现方面有哪些区别？

**答：**OFB+CMAC和GCM在WAPI保密通信中提供了满足不同速率需求的数据保密性与完整性保护能力，为WAPI应用于多样化场景（如企业无线接入、工业控制、物联网等）提供了可灵活选用的安全方案，确保了网络通信在高效与安全之间的平衡。

OFB+CMAC和GCM两种密码套件在工程实现方面，在密钥、初始向量（IV）、完整性校验码计算三方面有显著区别：

（1）使用OFB+CMAC时，应使用2个密钥，分别为加密密钥和完整性校验密钥；使用GCM时，仅使用1个密钥即可完成加密和完整性校验。

（2）使用OFB+CMAC时，IV取值为128位（16个八位位组）的数据分组序号（PN）值；使用GCM时，IV取值为128位PN值的低96位。

（3）使用OFB+CMAC时，在计算完整性校验码时，若完整性校验数据的第一部分的长度或第二部分的长度不足16个八位位组的整数倍，则应分别在后面补零至16个八位位组对齐后，再参与完整性校验计算；使用GCM时，在计算完整性校验码时，完整性校验数据的第一部分作为算法的附加认证数据（AAD）直接参与运算，不需要补零处理。

## ■ 3、问：使用GCM密码套件时，GCM-SM4算法在计算TAG时已经包含了PDU数据的长度L，AAD数据构造是否还需包含PDU数据的长度L？

**答：**需要。

使用GCM时，完整性校验数据的第一部分作为AAD，具体字段包括帧控制（FC）、地址1、地址2、序列控制、地址3、地址4、服务质量控制、KeyId<sub>x</sub>、保留和PDU数据的长度L。完整性校验数据定义见《无线局域网安全技术规范 第1号修改单》标准的6.5.3.1。

GCM的特点是高效与安全并重，具备并行处理能力；WPI使用GCM实现了加密与完整性保护一体化，使WAPI在高速通信环境下仍能保持强大的数据完整性与抗篡改能力。

## ■ 4、问：WAPI中针对单播管理帧的保护与单播数据帧的保护，在实现处理方面有哪些异同？

**答：**相同点：使用相同的单播密码套件，即：均使用单播加密密钥、单播完整性校验密钥和IV。

不同点：单播管理帧在完整性校验码计算时，帧控制（Frame Control）字段的位4、5、6参与完整性校验；单播数据帧在完整性校验码计算时，FC字段的位4、5、6置0，不参与完整性校验。上述处理方式与无线局域网国际标准所定义的方式一致，最大程度减少了厂商的开发工作量。

2025年7月发布的最新版《管理帧保护技术规范》标准，为WAPI安全无线局域网产品提供了清晰可操作

的安全能力指引，增强了管理帧抵御仿冒、重放等攻击能力，提升了复杂环境下无线连接的安全性。

#### ■ 5、问：在实现WAPI组播管理帧保护时，完整性校验数据如何处理？

答：通过对组播管理帧的协议数据计算完整性校验码（MIC），实现WAPI组播管理帧的防篡改保护。参与完整性校验的字段包括帧控制、地址1、地址2、地址3、MAC管理协议数据单元（MMPDU）和管理MIC信息元素（MMIE）。其中，在计算前应将MMIE中的MIC字段置零，以确保校验结果的正确性。

使用WPI-SM4-CMAC-128时，若组播管理帧协议数据不足16个八位位组的整数倍，应在数据后面补零至16个八位位组对齐，补零后的数据作为完整性校验输入进行计算。

使用WPI-SM4-GMAC-128时，组播管理帧协议数据直接作为附加认证数据（AAD）参与完整性校验计算，无需进行扩展补零操作。

综上，针对组播管理帧的完整性校验机制，无论采用WPI-SM4-CMAC-128还是WPI-SM4-GMAC-128，均在《管理帧保护技术规范》标准中进行了规范。该标准最新版本已于2025年7月发布，进一步强化了信标帧的安全策略协商机制、管理帧的完整性保护能力以及组播密钥通告协议的设计，显著提升了无线局域网产品的安全防护水平，优化了密钥建立与协商的效率。

#### ■ 6、问：WAPI技术是否适用于物联网（IoT）设备？

答：适用。

WAPI技术不仅完全适配物联网设备，更在安全性、场景兼容性及合规性等核心维度，精准解决了物联网规模化应用中的关键痛点，已在多领域应用。

（1）筑牢物联网安全防线：物联网“端-边-云”链路中，智能家居传感器、工业监控终端、医疗设备等常涉及敏感数据采集与远程控制，数据泄露、篡改及非法接入风险突出。WAPI通过终端设备与接入点的双向鉴别机制及国密算法加密，有效抵御了“非法设备接入”“数据窃听”等风险。

（2）适配复杂物联网场景：物联网设备常处于海量终端并发、移动物联网终端动态连接切换等场景，WAPI技术的部署应用可直接复用现有网络架构，无需额外改造。WAPI产业群体已结合物联网应用场景需求，开发出低功耗模组、毫秒级快速切换技术和产品，适配工业实时通信、智慧城市等规模化部署需求。

（3）符合关键领域的合规性要求：政务、工业、医疗等核心领域明确要求：物联网设备应符合《网络安全法》《密码法》对网络安全与密码应用的强制性要求。WAPI物联网完全满足上述要求。

#### ■ 7、问：WAPI技术用于物联网（IoT）设备时，需要考虑哪些特殊因素？

答：物联网设备与消费电子（如手机、电脑）相比，具有低功耗、资源受限、场景碎片化、长期在线等特性，因此在集成WAPI时应重点关注以下因素：

(1) 适配低功耗：应优先采用芯片自带的硬件加密引擎（如支持SM4硬件算法的低功耗WLAN芯片），避免软件加解密占用CPU资源、增加功耗。

(2) 资源受限设备的协议栈轻量化：由于多数物联网设备的硬件资源有限（如：RAM<1MB、Flash<16MB、CPU主频低），需使用轻量化的WAPI协议栈。

(3) 证书管理的简化：物联网设备通常不具备人工操作的证书管理界面，需考虑“在线证书管理”功能。

## ■ 8、在中短距离无线通信技术路线方面，WAPI无线局域网和其它技术相比，有哪些优势？

**答：**正在演进的中短距离无线通信技术丰富多样，包括WAPI、NB-IoT、LoRA、EUHT、WIA-FA、星闪、蓝牙等，它们各具特点和优劣势，适用于不同的应用场景和需求。

在选择采用具体中短距离无线通信技术路线时，需遵循五项基本原则，即：法律合规性、标准符合性、功能/性能匹配性、产业成熟度、可持续发展性。具体详见《WAPI市场应用洞察报告——工业网络选择中短距离无线通信技术路线的基本原则》。

## ■ 9、无线局域网技术可用于民用无人驾驶航空器的相关通信么？

**答：**可以。

无线局域网（英文简称WLAN）具有带宽高、成本低、部署方便等特点，可在局部区域（室外300米）内为用户提供数十Gbps的高速率数据通信服务。历经二十余年发展，WLAN已成为全球宽带信息基础设施的重要组成部分，并作为基础模块被其它行业设备集成，为海量行业设备提供了中短距离高速通信能力。

近年来，我国民用无人驾驶航空器产业取得了巨大发展，广泛应用于个人消费、植保、测绘、应急等领域，在国民经济各个领域发挥着重要作用。目前，微型、轻型和小型民用无人驾驶航空器在飞行过程中采用无线局域网信标帧广播协议，通过无线电方式周期性主动对外广播其唯一产品识别码，实现了远程识别与动态监控，保障了实时监管与空域安全。

此外，在民用无人驾驶航空器的遥控遥测数据传输、低空自组网及协同飞行等应用场景中，无线局域网技术均为典型的技术实现方案。

**习近平：**

## **突出科技创新引领 健全国家安全体系**

2025年10月20日，中国共产党第二十届中央委员会第四次全体会议上，习近平总书记就《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》向全会作说明指出，要推动高质量发展，最重要加快高水平科技自立自强，积极发展新质生产力，在推动科技创新、加快培育新动能、促进经济结构优化升级上取得实质性、突破性进展。

习近平指出，《建议》突出科技创新的引领作用，在建设现代化产业体系、加快高水平科技自立自强等方面作出部署。提出：优化提升传统产业，培育壮大新兴产业和未来产业，巩固壮大实体经济根基；加强原始创新和关键核心技术攻关，推动科技创新和产业创新深度融合；加快建设新型能源体系。

习近平指出，《建议》围绕推进国家安全体系和能力现代化，提出健全国家安全体系，加强重点领域国家安全能力建设，提高公共安全治理水平，完善社会治理体系。

**习近平：**

## **筑牢网络安全和数据安全防线**

2025年11月28日，中共中央总书记习近平在中共中央政治局第二十三次集体学习时强调，当前人工智能、大数据等新技术新应用不断涌现，给网络生态治理带来挑战，也提供新的支持条件。要鼓励网信领域新技术发展，促进研发成果转化和应用场景落地。要完善分级分类的安全监管机制，筑牢网络安全和数据安全防线。

## 李强：

### 推进科技创新和产业创新深度融合 加快发展新质生产力

2025年10月30日，中共中央政治局常委、国务院总理李强在《人民日报》发表署名文章《“十五五”时期经济社会发展的指导方针》中指出，要推进科技创新和产业创新深度融合，加快发展新质生产力。

“十五五”时期，面对高质量发展和大国博弈新形势，必须把因地制宜发展新质生产力摆在更加突出的战略位置。科技创新和产业创新是发展新质生产力的基本路径。科技创新能够催生新产业、新模式、新动能，要统筹推进教育科技人才一体发展，完善国家创新体系，瞄准世界科技前沿，在加强原始创新和关键核心技术攻关上持续用力，加快实现高水平科技自立自强。科技成果的生命力在应用，要全面推进传统产业转型升级、积极发展新兴产业、超前布局未来产业，加快建设现代化产业体系，走出一条以科技创新引领产业创新、以产业升级促进科技迭代的新路子。需要注意的是，发展新质生产力需要有一定的禀赋条件，要坚持科学理性、因地制宜，发挥比较优势推动新质生产力发展。

## 何立峰：

### 加快高水平科技自立自强 引领发展新质生产力

2025年11月11日，中共中央政治局委员、国务院副总理何立峰在人民日报发表署名文章《因地制宜发展新质生产力》指出，必须加快高水平科技自立自强，引领发展新质生产力。一是要加强基础研究和原始创新。提高基础研究投入比重，加大长期稳定支持，强化科学研究、技术开发原始创新导向，实现更多“从0到1”颠覆性突破。二是要加强关键核心技术攻关。完善新型举国体制，采取超常规措施，全链条推动重点领域取得决定性突破。三是要推动科技创新和产业创新深度融合。加快重大科技成果高效转化应用，布局建设概念验证、中试验证平台，推动创新资源向企业集聚。

## 国家发展改革委：

### 深化智慧城市发展 筑牢数字化转型安全防线

2025年10月31日，国家发展改革委印发《深化智慧城市发展推进全域数字化转型行动计划》提出，要筑牢数字化转型安全防线。强化网络安全、数据安全防护能力。健全政务云网安全保障体系。加强城市数据基础设施安全保障，实现可信接入、安全互联、跨域管控、全栈防护等安全管理。推进数据安全治理，建立健全数据安全风险防控体系，强化城市数据分类分级保护和全生命周期安全管理，完善数据安全制度规范，加强个人信息保护，压实各类主体安全责任，提升数据安全保护水平。

## 工信部：

### 提升园区数字化安全保障水平

2025年11月18日，工信部印发《高标准数字园区建设指南》提出，要提升园区数字化安全保障水平，推动园区企业实施工业互联网安全分类分级管理，开展工业控制系统网络安全评估，加强重要数据识别备案和分级防护等工作，强化网络和数据安全风险防范能力。构建安全态势感知平台，提高园区网络和数据安全威胁发现、监测预警、溯源处置水平。

## 北京市人民政府： 推进科技成果转化落地

2025年11月18日，北京市人民政府办公厅关于印发《北京市推进科技成果转化落地行动方案（2025-2027年）》提出，要以深化科技成果转化机制改革为一条主线，坚持科技创新和制度创新双轮驱动，坚持有效市场和有为政府两个抓手协同发力，从促进科技成果转化、突出企业主体地位、提高公共服务能力、激发市场要素活力、提升落地服务品质五个关键方面发力，加速科技成果“从1到10”在京落地。

《方案》提出，到2027年，要基本形成高效协同、富有活力的科技成果转化体系，成功转化一批服务国家战略需求、满足北京经济社会发展需要的重大科技成果；要促成1000家合作平台、5000项技术开发合作项目，转化孵化3000家科技型企业、600家专精特新企业，开辟未来产业新赛道，实现关键核心技术新替代，激发转型升级新动能。

# 弘扬文化自信与工匠精神 赋能新质生产力发展

## WAPI产业联盟组织参观湖北省博物馆党的主题活动

WAPI产业联盟 周园



为深入贯彻党建引领高质量发展要求，推动党建与业务同向发力、同频共振，2025年12月19日，WAPI产业联盟组织党员代表、骨干成员在湖北省博物馆开展参观学习主题活动。活动以“**弘扬文化自信与工匠精神赋能新质生产力发展**”为主线，引导大家从荆楚文明的创造力与工艺成就中汲取奋进力量，进一步深化对“以科技创新推动新质生产力发展”的认识，把学习成效转化为服务产业升级和联盟建设的行动自觉。

湖北省博物馆以系统呈现荆楚历史文化为特色，展陈内容厚重、体系完整、亮点突出。馆内常设展通过历史脉络梳理与重点文物串联，形成从远古到近世的清晰叙事。参观过程中，大家在讲解员引导下重点了解珍贵文物背后的历史故事与工艺成

就，从青铜铸造、漆器髹饰到丝织刺绣等传统技艺中，直观感受到中华文明绵延不绝的创新能力和精益求精的品质追求。

参观中，大家围绕“文化自信”展开深入交流。一致认为，荆楚文化在传承中创新、在交流中发展，启示我们要坚定文化立场、增强发展底气，把中华优秀传统文化所蕴含的创新基因、系统思维与协同理念，转化为推进产业生态建设的精神动力与价值支撑。

活动突出“科技创新”导向，进一步深化了对新质生产力内涵的理解。大家认为，新质生产力的形成关键在于以科技创新为核心驱动力，以高标准体系、数据与技术要素高效配置、产业链协同创新为重要支撑。围绕联盟业务实际，大家结合



WAPI产业联盟在无线网络安全领域的工作展开交流研讨。大家表示，推动新质生产力发展，需要在基础能力上实现“硬核突破”，在产业生态上实现“系统跃升”。WAPI相关技术与标准创新，强调安全、自主、可控与互联互通，契合新质生产力对高质量供给和高水平安全的要求。下一步，联盟将更好发挥组织平台作用，持续推动会员单位在关键技术研发、标准研制与推广、测评验证与互操作、产业化应用与生态合作等方面形成合力，以标准化、

工程化、规模化的路径提升创新成果转化效率，服务数字经济和实体经济深度融合。

活动同时聚焦“工匠精神”传承。文物所体现的严谨工艺与极致细节，启示我们在推进产业创新时必须坚持长期主义与质量意识，把“严、细、实”的作风贯穿研发、测试、验证、交付全过程。大家表示，将在标准条款打磨、互操作测试、产品一致性与工程实施等环节进一步强化质量管控与闭环改进，用精益求精的态度夯实产业可信底座，提升联盟工作的专业性与公信力。

本次党建活动既是一堂生动的文化教育课，也是一次面向新质生产力的实践动员。WAPI产业联盟将以本次活动为契机，持续深化党建引领，推动文化自信与科技创新同频共振、工匠精神与产业发展同向发力，聚焦安全无线通信关键能力建设与应用，强化标准引领、协同创新和成果转化，努力把学习成果转化为推动产业高质量发展、培育壮大新质生产力的务实成效。



## 党建引领聚合力 科创赋能担使命

### WAPI产业联盟参加海淀夜校启动暨专题党课学习

WAPI产业联盟 周园



2025年12月2日，WAPI产业联盟应邀参加在集智未来人工智能产业园区举办的“海淀夜校·花园路夜校”启动仪式，并同步参与《青年习近平的奋斗岁月》专题党课学习。此次活动由海淀区人才工作局、花园路街道党工委联合组织，联盟代表与政府有关负责同志、高校专家及辖区企业、社区代表共同见证夜校揭牌，携手构建基层学习与科创协同融合的新载体。

在专题党课环节，北京航空航天大学马克思主义学院党委书记高宁教授以青年习近平在梁家河的奋斗实践为核心，系统阐释了其带领村民建成陕西省第一口沼气池的创新实践，深刻解读了其中蕴含的扎根基层、重视科技、服务群众的奋斗精神。课程内容与“科技是第一生产力、人才是第一资源、创新是第一动力”的重要论述深度契合，为科技领域从业者筑牢理想信念根基、明晰创新方向提供了

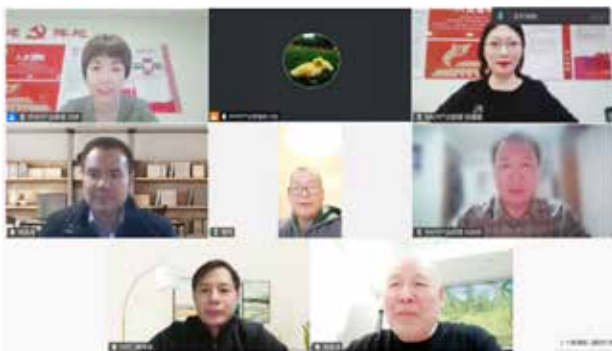
有力思想引领，WAPI产业联盟代表全程认真学习、深入领会。

活动结束后，WAPI产业联盟第一时间组织秘书处开展“奋斗精神融入科技研发”专题研讨。与会人员结合党课所学与联盟业务实际展开交流，一致认为此次学习既夯实了思想理论基础，也为无线网络安全技术创新突破与标准落地应用指明了方向。大家表示，将以青年时期习近平同志的奋斗历程为标杆，把精神伟力转化为攻坚动力，持续提升无线网络安全领域核心技术研发实力与产业协同效能。

下一步，WAPI产业联盟将深化与花园路街道及夜校平台的党建共建，通过课程共研、资源共享，实现WAPI技术知识科普与思政学习常态化。联盟将以党建引领赋能专业实践，为海淀区建设世界领先科技园区、打造高水平人才高地，以及花园路街道构建“全域学习生态”贡献科创领域的专业力量。

## 无线网络安全标准化工作委员会 2025年第四次主任委员会议（总第15次）顺利召开

WAPI产业联盟 刘婷



2025年12月2日，中关村无线网络安全产业联盟无线网络安全标准化工作委员会（下称“标委会”）2025年第四次主任委员会议顺利召开，会议由标委会主任委员曹军主持，副主任委员王立建、陶洪波、张璐璐、黄振海及联盟秘书处标准化部相关负责人出席。

会议聚焦2025年第四季度工作要点、年度重点工作落实总结、2026年标准化工作重点任务及标委会未来发展方向等核心议题，展开系统汇报与深入研讨。

联盟标准化部总监刘婷汇报第四季度工作，依据标委会《2025年重点任务计划》及相关会议决议，当前标准化工作已在多领域取得积极进展。标准制定方面，统筹推进27项团体标准，其中3项将于12月正式发布，6项进入报批阶段并计划2026年1月发布，

另有8项处于送审阶段、2项在征求意见阶段、5项为草案稿阶段，同时新立项标准达3项；标准实施层面，会员单位多款产品顺利通过联盟相关测试，针对WAPI建设中AS部署方式不规范等行业痛点，已组织编制专项应用洞察报告；标准平台建设上，2025年第三次标准工作及项目组会议已圆满召开，3名技术专家的人会申请已进入审批流程；标准生态构建领域，持续跟踪相关国际组织动态，积极参与国家及行业标准制定，推动GB 15629.11系列标准纳入规范性引用体系。

标委会总体工作组（WG 1）负责人黄振海介绍，2025年年初确定的12项重点任务已全部落地，并报告了拟提交标委会全会审议的2026年标准化重点工作任务。标委会生态环境工作组（WG 7）负责人张璐璐则报告了2025年标委会全体会议筹备进展，该系列会议定于12月17日至19日在武汉举办，将同步开展第四届标委会第二次全体会议、2025年第四次标准工作和项目组会议及标准产业交流等活动。

与会领导对2025年标委会工作成效予以充分肯定，同时就2026年标准化重点任务规划、产业协同创新和高质量发展等提出指导性意见。

## 联盟发布新版《WAPI标准产业应用及环境监测报告》

WAPI产业联盟 陈博

2025年12月30日，联盟发布新版《WAPI标准产业应用及环境监测报告》。

该《报告》是WAPI产业联盟帮助政府、厂商、市场用户深入了解安全无线局域网产业及市场全貌，服务市场建设，提升WAPI技术产业成果转化效率，加强产业链上下游企业-企业、企业-市场之间的对接合作的重要工具。主要内容包括：无线局域网及WAPI政策及配套监管、国家标准符合依据、全产业链厂商及其产品统计分析、市场应用示范案例、公共关键技术和解决方案、技术标准体系介绍等，以电子文档或印刷品形式面向政府、产业、公

众公开。《报告》中涉及的产品数据与信息，均源自公开媒体或厂商。本期《报告》所涉产业数据统计、应用情况统计、WAPI等网络安全技术标准情况统计等，均截至2025年12月30日。鉴于产业特性和技术迭代，存在一定动态变化的可能。

扫描二维码可下载完整版《报告》。



## 联盟发布新版《WAPI问答合辑》

WAPI产业联盟 陈博

2025年12月17日，联盟发布新版《WAPI技术产业市场服务手册|WAPI问答合辑》。

在服务各行各业关键信息基础设施建设过程中，WAPI产业联盟总结了业界关注的常见问题，并结合百度百科、搜狗百科、互动百科、维基百科中文版等对WAPI的解释存在一定不准确乃至错误之处进行解答，帮助业界更加客观准确地了解WAPI。

截至2025年12月，WAPI问答已发布17期，涵盖WAPI技术、标准、产品、应用、检验检测等各方面焦点问题。此次应市场和厂商要求，联盟将其

集结成册，手册包括“基本情况与业界关注”“技术标准与演进”“产品与工程化实现”“市场建设与应用”“WAPI检测与服务”“联盟与会员服务”六部分。

目前，《手册》已通过联盟网站、公众号向业界开放，后续将持续更新。

扫描二维码可下载完整版《手册》。



## 许继软件WAPI系列终端通过联盟测试

WAPI产业联盟 王立华

2025年11月13日，许昌许继软件技术有限公司（以下简称许继软件）两款WAPI终端产品通过了WAPI产业联盟无线局域网鉴别与保密基础机构（WAPI）互通性、完整性及功能测试。本次测试依据2025年4月版WAPI功能测试项开展，通过后联盟为上述设备出具了测试报告。

上述终端产品分别为物联网低功耗WAPI模组（型号iES-854-ME）与高带宽视频WAPI模组（型号iES-854-MM），两款产品均支持WAPI安全协议及2.4/5GHz双频接入，通信速率支持802.11ac协议。

据许继软件介绍，iES-854-ME 模组对私钥及证书的安全存储提供了硬件级别防护，专为电网低

功耗终端可信传输场景设计，能为压板、局放设备、温湿度传感器、烟感装置、水泵等物联网终端提供安全无线接入服务；iES-854-MM 模组则聚焦电网高速数据传输的应用场景，可应用于球机、摄像机等高带宽终端的安全无线接入。

许继软件表示，目前公司已形成包含鉴别服务器（AS）、无线接入点（AP）、接入点控制器（AC）、客户端前置设备（CPE）及终端模组的WAPI 电力无线局域网全套解决方案。未来将进一步加大WAPI技术在电力业务中的推广力度，持续完善解决方案体系，满足新型电力系统对安全无线局域网的应用需求。



图：许继软件物联网低功耗WAPI模组iES-854-ME和高带宽视频WAPI模组iES-854-MM

## 莲雾科技WAPI系列终端通过联盟测试

WAPI产业联盟 王立华



图：莲雾科技WAPI低功耗卡片机SIM218和WAPI烟雾报警器SSI18

2025年11月14日，广州莲雾科技有限公司（以下简称莲雾科技）两款WAPI终端产品通过了WAPI产业联盟无线局域网鉴别与保密基础机构（WAPI）互通性、完整性及功能测试。本次测试依据2025年4月版WAPI功能测试项开展，通过后联盟为上述设备出具了测试报告。

测试通过的两款WAPI终端产品分别为：WAPI低功耗卡片机（型号：SIM218）和WAPI烟雾报警器（型号：SSI18），均支持WAPI协议与2.4GHz接入，通信速率支持802.11n协议。

据莲雾科技介绍，两款产品具备体积小、防护等级高、检测精度高等优势。其中SIM218型低功耗卡片机可广泛应用于SF6（六氟化硫）表计抄表、机构箱、刀闸箱等状态监测场景；SSI18型烟雾报警器则适用于变电站、换流站、发电站等场景的火灾监测，为电力系统关键环节安全提供技术支撑。

莲雾科技表示，公司在WAPI领域布局深入，目

前已量产多款一体化WAPI终端，包括：STH801型WAPI温湿度传感器、SWL801型WAPI液位传感器、SWL810型WAPI水浸传感器、SW807型WAPI七要素气象传感器、SIM850型WAPI双光谱红外热成像卡片机、SIM218型低功耗卡片机、SSI18型烟雾报警器、GW410型WAPI传感器变送器、GW853/GW854型WAPI边缘计算网关、HMI101型10.1寸工控一体机、HMI070型7寸工控一体机，其中多款产品通过了联盟测试；SIM518型球机摄像头、SE153型三相电能计量装置等产品则处于样机阶段。

展望未来，莲雾科技计划进一步丰富WAPI终端产品线，重点推进现有产品鸿蒙化适配，并研发WAPI局放监测装置、变压器铁芯夹件电流监测装置、多合一气体传感器等新品。这些产品将进一步完善WAPI应用终端体系与解决方案，为推动WAPI技术在电力等行业的规模化应用注入新动能。

## 北京至周科技WAPI CPE终端通过联盟测试

WAPI产业联盟 王立华



图：至周科技WAPI CPE终端WAP6220-O

2025年12月11日，北京至周科技有限公司（以下简称至周科技）的WAPI CPE终端产品通过了WAPI产业联盟无线局域网鉴别与保密基础机构（WAPI）互通性、完整性及功能测试。本次测试依据2025年4月版WAPI功能测试项开展，通过后联盟为上述设备出具了测试报告。

测试通过的WAPI CPE终端型号为WAP6220-O，支持WAPI安全协议及2.4/5GHz双频接入，通信速率支持802.11ac协议。

据至周科技介绍，该终端产品在功能设计上匹配工业物联网需求。在安全性层面，支持WAPI协

议，保障传输数据的机密性，符合工业物联网安全合规要求。在接口和组网层面，通过RS232/RS485接口连接各类工业物联网终端，使其快速具备WAPI能力；以双千兆以太网口，实现内外网隔离与双链路备份，在提供灵活组网的同时保障网络异常时业务零中断。在上行链路层面，支持Turbo双链路漫游，可同时保持WLAN与移动通信网络两条链路的连接，当检测到跨WLAN漫游或WLAN信号异常出现丢包时，将业务数据无感切换到移动通信链路，保障连接不中断；利用两条链路的带宽与冗余能力，降低卡顿、增强连接稳定性。

# 平高运检WAPI无源无线避雷器状态监测装置 通过联盟测试

WAPI产业联盟 王立华

2025年12月31日，平高集团电力检修工程有限公司（以下简称平高运检）的无源无线避雷器状态监测装置通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及功能测试。本次测试依据2025年4月版WAPI功能测试项开展，通过后联盟为上述终端设备出具了测试报告。

此款终端产品型号为ISM-901S，专为35kV及以上电压等级交流避雷器在线监测场景设计。该产品支持WAPI安全协议及2.4GHz频段接入，通信速率支持802.11n协议，具备传输稳定、抗干扰能力强等特点，可适配变电站、开关站、换流站等复杂电磁环境下的监测需求。

据平高运检介绍，ISM-901S采用不锈钢外壳设计，防护等级达到IP67，可从容应对户外恶劣环境。装置内部集成微能量收集、高精度微电流测量、避雷器放电监测及就地显示等核心模块，其中微能量收集模块可高效捕获环境中的电能并存储于电容中，实现设备无外部电源、无电池供电的持续运行，大幅降低运维成本。该产品可与电压测量单元、监测IED（智能电子设备）及后台系统协同，构建完整的避雷器在线监测系统，实现避雷器全电流、阻性电流、阻容比、动作次数等关键参数的实时监测，为运维人员评估设备健康状态，开展预测



图：无源无线避雷器状态监测装置ISM-901S

性维护提供可靠数据支撑，对提升电网运维效率和安全运行水平具有重要意义。

平高运检表示，公司将以WAPI安全无线技术为基础，紧扣智能电网数字化发展需求，聚焦电网智能化改造升级核心任务，针对性破解传统有线在线监测装置布线复杂、施工难度大、维护成本高的行业痛点，提供定制化解决方案。目前公司正加速推进基于WAPI技术的系列监测产品落地，涵盖六氟化硫（SF<sub>6</sub>）气体监测、开关设备局部放电监测、变电站辅助环境监控等多个领域，构建覆盖输电、变电、配电全环节的安全无线监测体系，助力电力行业实现安全高效、绿色低碳的数字化转型。

## WAPI产业联盟再添2家新成员

WAPI产业联盟 周 园

随着WAPI大规模部署，越来越多的厂商积极投入WAPI产业。近期，浙江翌和智能科技有限公司、上海久壬信息科技有限公司相继加入中关村无线网络安全产业联盟（WAPI产业联盟），联盟会员增至139家。以下按加入时间对新会员进行简要介绍。



### 浙江翌和智能科技有限公司

2025年10月27日，经联盟理事会批准，浙江翌和智能科技有限公司（以下简称浙江翌和）正式加入WAPI产业联盟。

浙江翌和是一家专注于智能科技信息系统的综合性企业，多年来凭借专业的技术团队、丰富的行业经验和卓越的服务质量，在行业内树立起良好口碑。公司秉持“创新进取、客户至上、诚信共赢”的经营理念，提供高品质、定制化的智能信息系统解决方案，帮助客户高效实现业务目标。

据浙江翌和介绍，已成功创制WAPI核心设备，包括室内AP、室外AP及鉴别服务器（AS）：室内AP YH-3100D-IDP系列适配办公楼宇、数据中心等复杂室内环境；室外AP YH-3100E-ODP系列具备高防护等级与抗干扰能力，可满足电力巡检、智慧园区等户外场景的稳定接入需求；YH-WAS系列鉴别服务器拥有证书签发、漫游管理、安全审计等全功能模块，为无线网络提供端到端的安全保障。

浙江翌和表示，加入WAPI产业联盟后将积极参与联盟标准制定与技术研发，重点推动WAPI产品在智慧能源、智慧城市等场景的落地应用。同时依托联盟的资源整合优势，进一步加强与产业链上下游企业的协同创新，持续迭代产品技术，为客户提供更安全高效的无线网络解决方案。



### 上海久壬信息科技有限公司

2025年12月5日，经联盟理事会批准，上海久壬信息科技有限公司（以下简称久壬科技）正式加入联盟。

久壬科技是专注电力电子技术和能源互联网融合研发及应用的高新技术企业。近年来在电力物联网、电能质量治理、新能源系统等领域形成具有自主知识产权的产品和解决方案，拥有发明、实用新型及软件著作权等知识产权百余项，通过ISO、ITSS、CMMI-3、CS2等多项资质认证，具备能源管理体系、信息系统集成及服务三级，以及承装（修、试）电力设施许可五级等资质。

据久壬科技介绍，公司以智能传感、边缘计算为核心，构建全域互联的电力生态体系，推动输变配电系统向数字化、自动化、无人化转型。同时以多能融合、云端协同为基础，打造“源—网—荷—储”一体化能源互联网平台，加快能源体系向清洁、高效、弹性方向升级。目前公司已完成WAPI核心模块研发，推出了系列WAPI合规网络设备和终端解决方案。其中，具备WAPI功能的AP产品支持2.4GHz/5GHz双频，整机最大传输速率不低于1200Mbps；STA终端支持WAPI，可在12V至48V宽电压供电，终端配备不少于1个以太网接口和1个RS485接口，模块配备不少于1个USB接口，并支持无缝漫游，不同AP间的漫游切换时间小于30毫秒，可满足电力、工业现场对安全接入、稳定覆盖和工程化部署等需求。

久壬科技表示，加入后将积极参与联盟技术交流与协同创新，推动WAPI技术与5G-A、物联网、工业互联网等新一代信息技术的深度融合与性能优化，进一步丰富产品矩阵，开发轻量化、低成本解决方案，并携手产业链上下游伙伴共同推动WAPI测试认证体系完善与应用生态繁荣，助力我国无线网络安全产业高质量发展。

## 南方电网完成业内首个网省跨域WAPI漫游认证现网测试

【南方电网报】

南方电网报12月5日讯，近日，南方总调组织广西电网公司、海南电网公司成功开展业内首个网省跨域WAPI漫游认证现网测试，南方电网公司总部基地及广西、海南各省区WAPI网络终端实现在全网各省域内漫游接入异地WAPI网络。

本次测试以南方总调WAPI网络证书及鉴别系统（AS系统）为网级中心节点，广西电网和海南电网电力调度控制中心WAPI网络AS系统为省级枢纽节点，通过综合数据网连通各省内地调AS系统，构成漫游认证树型架构。公司总部、省级电网公司和各地供电局WAPI网络可通过漫游认证接入多个异地归属地终端，终端业务通信正常，AS认证日志清晰记录漫游鉴别全过程，满足各类业务安全、泛在、灵活、宽带的“最后一公里”无线接入需求。

据悉，截至2025年底，全网覆盖WAPI无线网络的变电站超800座，220千伏及以上厂站覆盖率超60%，全网已有17类超2000台套业务终端接入了WAPI网络，WAPI无线网络在全网区域各类厂站覆盖愈加广泛，为WAPI网络全网域漫游应用推广打下了坚实的“地基”。

实现WAPI漫游认证是建设南方电网WAPI电力无线专网、打造坚强数字生产通信底座的重要技术举措。本次试验成功，为南方电网WAPI电力无线专网实现网省跨域跨区全网全方位贯通打下坚实的基础，为能源行业安全可靠无线通信网络大规模漫游应用提供了经济、安全、可靠的“南网方案”。

## 广哈通信赋能电力行业安全新发展

【广哈通信】

2025年11月27日至29日，广哈通信在电力安全与应急技术大会上集中展示了电力安全通信与应急指挥领域的最新技术成果和解决方案，并与行业专家探讨AI时代电力安全发展新路径。



在大会核心展区，广哈通信展示了覆盖“WAPI无线网络覆盖解决方案、灵犀5G数字化管控平台解决方案、新一代调度MIS系统方案”三大完整解决方案及配套硬件，为构建新型电力系统安全体系提供了清晰的技术路径和扎实的设备支撑。

本次展出的WAPI无线网络覆盖解决方案，涉及AS、AC、AP、CPE等产品，具有自主可控、高安全、数字证书认证、管理灵活的特点。适逢“十四五”末期及“十五五”规划开局之初，也是论证调度通信技术体制发展的关键时期，广哈通信结合电力用户的实际需求、技术发展趋势以及业务发展方向，提出一整套强调提升系统安全性和深化业务拓展性的建设方案，为技术体制的可持续发展提供了坚实保障，确保电力调度通信系统能灵活应对不断变化的电力调度环境，提供更加高效、可靠的服务。

## 通科公司WAPI 创新成果突出 成广东电网企业矩阵核心成员

【潮州日报】

2025年11月，潮州日报发表《广东电网体系企业矩阵发力 绘就能源发展新图景》文章，广东电力通信科技公司（以下简称通科公司）因近年来在WAPI创新方面成果突出，成为矩阵核心成员。

通科公司是广东电网有限责任公司的全资子公司，隶属于中国南方电网有限责任公司的三级单位。公司围绕“服务电力企业发展运营、支撑数字电网安全运行”的核心功能定位，全面形成了“基础业务、科技创新、资产运营”三大业务板块布局——基础业务板块聚焦通信建设与运维服务，科技创新板块聚力关键核心技术攻关与成果转化，资产运营板块着力推动电力资源盘活与价值创造，三者协同推动了一批具有行业影响力的核心产品持续涌现。其中RIS+WAPI通信终端产品，针对公网信号盲区与机动通信需求，特别是在偏远山区等接入困难区域，使用通过与微波或WLAN设备协同工作，实现远距离、高通量的可靠无线传输。



## 中兴与字节跳动携手推出WAPI“豆包”手机

【新派网】

近期，中兴通讯与字节跳动豆包团队合作，推出了搭载豆包手机助手技术预览版的WAPI手机努比亚M153，让用户在手机上就能获得智能体AI带来的各种创新体验。

2025年以来，从DeepSeek、Manus到千问、豆包等大模型，各类生成式AI不断给人们带来惊喜，同时也让人们对未来人工智能的发展充满了期待。据豆包方面发布信息显示，基于豆包大模型的能力和手机厂商的授权，豆包手机助手能够为用户带来更方便的交互和更丰富的体验。例如在购物、旅游等应用场景中，用户只需要对着此次发布的智能手机提出需求，AI助手就能调动多个应用程序完成较为复杂的任务，让用户享受到更舒畅、智能的应用体验。

## 中威电子发布支持WAPI的多功能电缆沟智能盖板

【中国财富网】

2025年11月，中威电子发布自主研发的电缆沟智能盖板新品。据介绍，这是一款集智能运维与消防应急于一体的创新产品，具备WAPI功能，凭借无源无线设计、多技术深度融合的优势，打破传统盖板单一防护局限，为电缆安全运行提供全流程智能保障。

在核心功能实现上，该产品具有无线传输模块支持输变电物联网与WAPI无线信息通讯，适配不同场景应用需求，可实时监测功能可精准捕捉电缆沟内温度、湿度、有害气体等环境数据，并通过无线网络实时传输；自动报警机制在检测到过热、水浸等异常情况时，立即启动报警并通知维护人员；自动灭火功能内置智能感温元件，温度达到设定值即自动启动，快速释放灭火剂实现精准高效扑救；视频巡检采用低功耗定时设计，即便在完全无光环境下也能清晰成像，具备自动休眠、定时启动、智能巡视、远程控制、光学变倍等功能。

## 国网山东电力科学研究院等单位申请“基于零信任的WAPI电力通信安全接入方法、系统和存储介质”专利

【国家知识产权局】

据国家知识产权局信息显示，国网山东省电力公司电力科学研究院、国家电网有限公司、北京理工大学申请一项名为“基于零信任的WAPI电力通信安全接入方法、系统和存储介质”的专利，申请公布号CN121310135A，申请日为2025年9月3日。

专利摘要显示，本发明公开了一种基于零信任的WAPI电力通信安全接入方法、系统和存储介质，该方法包括：对终端设备进行身份认证，身份认证包括证书认证和生物特征认证，生物特征认证包括指纹认证；如果身份认证通过，则基于信任等级对网络启动动态访问策略；实时监控身份认证过程和动态访问过程，持续进行风险评估，得到风险评估结果；基于评估结果授予动态访问权限或直接终止访问。本发明通过进行动态指纹认证和动态授予访问权限，在确保安全性的同时，对资源的细粒度访问控制，可提高系统的可靠性和业务连续性，能够有效防止未经授权的访问和潜在的网络攻击。

## 博洛米WAPI终端安全证书系统实现方法专利获授权

【国家知识产权局】

据国家知识产权局信息显示，南京博洛米通信技术有限公司取得一项名为“一种WAPI终端安全证书系统实现方法”的专利，授权公告号CN116347446B。授权公告日为2025年12月5日。

专利摘要显示，该专利一种WAPI终端安全证书系统实现方法，由终端STA、接入端AP、鉴别服务器AS组成，其中AP为标准设备，终端STA上加装安全芯片，安全芯片上运行片内操作系统COS程序并与终端主芯片交互，在终端上运行相应的WAPI证书管理程序WAPI连接程序，通过程序和鉴别服务器的交互，实现WAPI证书的管理、鉴别和建立WAPI连接，最终实现WAPI通信；通过安全芯片与终端主芯片的交互，实现WAPI证书的颁发和证书鉴别，使用该方法能利用安全芯片数据难以盗取的特点，保证WAPI证书的安全性。

## 数字认证牵头和参与的多项密码行标获发布

【北京数据集团】

日前，国家密码管理局发布第54号公告，GM/T 0031-2025《安全电子签章密码技术规范》等20项密码行业标准，自2026年7月1日起实施。其中北京数字认证股份有限公司牵头编撰了GM/T 0031-2025《安全电子签章密码技术规范》标准，同时还参与了6项行业标准。

GM/T 0031-2025《安全电子签章密码技术规范》规定了电子签章的密码应用安全机制和密码应用协议，主要包括：电子印章数据格式、电子印章生成流程、电子印章验证流程，以及电子签章数据格式、电子签章流程和电子签章验证流程等，适用于电子印章系统的研制开发，也可用于指导电子印章系统使用和检测。标准所规定的密码应用安全机制健全严谨，密码应用协议清晰明确，有效提升了电子印章系统使用密码技术的安全性和规范性，有利于推动不同厂商产品之间的兼容性与协同效率，促进了电子印章的互联互通与互信互认，为行业健康有序发展奠定了技术基础。

此外，数字认证还参与了GM/T 0053-2025《密码设备管理 远程监控与合规性检验接口数据规范》、GM/T 0148-2025《证书注册子系统证书服务接口规范》、GM/T 0149-2025《工业智能机器人系统密码应用指南》、GM/T 0144-2025《基于SM2密码算法的协同签名技术规范》、GM/T 0150-2025《数字凭证安全格式规范》、GM/T 0151-2025《智能锁及系统密码应用指南》六项行标的编撰。

# 关于WAPI低功耗卡片机的表计识别解决方案

本文由广州莲雾科技有限公司供稿

在能源互联网与智能电网加速建设的行业背景下，变电站智能化升级与无人化值守已成为电力系统发展的必然趋势。但在全国范围内的存量变电站中，尤其是早期投运站点及中小型站所，大量核心设备仍依赖传统机械式表计开展状态监测，例如SF6气体密度继电器、避雷器放电计数器、变压器油位计、温度计等关键装置。此类机械表计是变电站运行状态感知的核心“传感终端”，其数据读取的精准度与时效性，直接决定着电网系统安全稳定运行的底线。传统运维模式在应对这类“哑设备”时，正面临运维成本高企、作业效率低下、安全风险突出的多重行业痛点。广州莲雾科技有限公司推出的“基于WAPI低功耗卡片机的表计识别解决方案”，精准锚定上述行业难题，以创新技术路径为变电站智能化改造提供了高效、安全且具备经济性的落地方案。

## 一、行业背景与核心挑战：传统表计巡检的固有困境

要研判本方案的应用价值，需先深度剖析当前变电站机械表计管理的现实瓶颈，具体体现在三方面：

### 1、数据采集与管理的孤岛化困境：

变电站内仪表品类繁杂、规格各异且布设分散，从SF6表计到避雷器计数器，从油位计到各类开关状态指示器，它们分散在站内的各个角落。传统模式下依赖人工现场抄录数据，不仅导致数据采集的实时性、一致性缺失，还形成“数据孤岛”，难以实现与上层生产管理系统、统一物联网平台的有效对接，阻碍数据价值的深度挖掘。



图：一个高压开关室内通常有数十个表计

## 2、数字化改造成本高昂：

若将传统机械表计替换为内置传感器的智能表计，单台带远传功能的数字化表计采购价超1万元，加之设备采购、停电施工、系统集成等工程成本，对数量庞大、预算有限的中小型变电站而言，存在显著的经济负担，形成“不改造则效率低下，欲改造则成本高昂”的两难局面。



图：数字化表计采购成本高昂

## 3、人工巡检的安全与质量隐患：

人工巡检是当前主流运维手段，但存在突出弊端：一是巡检人员需频繁进入高压高危区域，人身安全风险长期存在；二是大型变电站全面巡检耗时数小时，人力成本高且效率低；三是人工读数易受光线、视角、疲劳等因素干扰，漏检、错检频发，极端天气与夜间场景下问题更为凸显，巡检质量难以保障和追溯。



图：人工巡检成本高且效率低

综上，行业亟需一种无需大规模更换现有设备、不显著增加改造成本，且能实现机械表计数据自动、精准、安全采集的解决方案。

## 二、解决思路：非侵入式机器视觉赋能的智能化路径

莲雾科技摒弃“硬替换”的传统逻辑，采用机器视觉技术构建“非侵入式”智能化改造路径。其核心思路为：依托先进机器视觉识别技术，为传统机械表计加装“数字眼睛”，破解数据采集瓶颈。具体而言，通过在现有表计表盘前端部署专用低功耗单片机，模拟人工“视觉感知”动作，相机定时采集高清表盘图像，再经国产自主可控的WAPI无线网络将图像传输至边缘计算单元，由内置视觉识别算法完成图像智能分析，自动识别指针位置、刻度值、数字显示等信息，并转化为结构化数字读数。

该方案具备四大核心优势：

**1、低成本：**无需更换昂贵智能表计，仅需加装轻量化采集终端，大幅降低改造成本。



图：低功耗单片机安装套件

**2、非侵入：**不改动原有表计的结构与接线，不影响设备正常运行，施工便捷且安全性高。



图：低功耗单片机实际安装效果

3、**高质量**：AI算法可排除主观因素干扰，提供持续、稳定、准确的数据源。



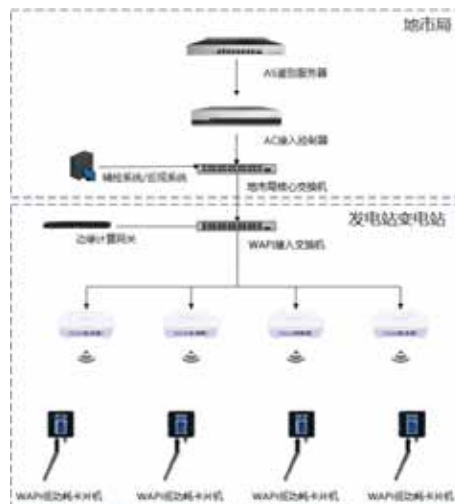
图：机械表记实现数字化读数

4、**易扩展**：单套算法模型可适配同类多型表计，新增监测点操作便捷，为后续智能化扩展奠定基础。



图：单套算法模型可适配多种表计

### 三、方案架构与技术实现：端到端的自主可控与高安全防护



图：方案架构示意

本方案最终为用户提供从数据采集、传输、识别到可视化分析的一站式服务，构建起高质量、可持续的工业级数据供应链。

本方案通过“感知-传输-边缘处理”的分层协作与“WAPI+电鸿”技术，搭建集数据采集、传输、处理与分析于一体的自动化系统，实现全链路国产化自主可控，其核心架构与技术实现如下：

### 1、感知层：WAPI低功耗卡片机

作为前端“视觉感知终端”，该设备充分适配变电站严苛工况：一是采用轻量化结构，优化内部电路布局，可适应复杂狭小安装空间，避免遮挡表盘影响读数；二是内置大容量锂电池并搭载深度功耗控制策略，典型工况下（每日采集1次图像）续航可达5年，解决频繁换电池的运维难题；三是配备300万像素高清工业摄像头，支持自动补光，保障夜间及弱光环境下的清晰图像采集；四是采用IP67工业级防护设计，可适配室内外各类复杂场景的长期稳定运行。



图：方案实际部署场景

### 2、传输层：WAPI安全无线通信技术

传输层是数据安全传输的核心，方案采用我国自主可控的WAPI（无线局域网鉴别与保密基础结构）技术，其安全性远超Wi-Fi，从根源上解决电力场景无线通信面临的身份假冒与数据泄露风险，实现无线技术在电力场站智能化改造中的安全可靠应用。其核心优势为：

- 高安全性：WAPI独创“三元对等”架构，提供双向身份鉴别机制，可杜绝“伪基站”攻击与数据窃听风险，满足电力系统对网络安全的严苛要求。
- 稳定可靠性：具备高可靠无线接入能力，保障图像数据从卡片机到接入网关的流畅传输。

### 3、边缘层：WAPI数据接入网关

作为现场“边缘计算大脑”，网关承担承上启下的关键职能：一是支持定时任务配置，可远程触发前端卡片机图像采集，并汇聚WAPI网络回传的图像数据；二是内置高性能视觉识别算法，可实时分析表盘图像并精准读取数据，同时支持监控任务与告警阈值配置，数据异常时可即时生成告警；三是提供标准接口，可将结构化数据及告警信息上传至站端物联网平台或上级云平台，实现数据集中管理与应用。



图：算法识别读数

#### 4、操作系统层：电鸿操作系统

方案底层适配电力行业首款自主可控物联网操作系统——电鸿操作系统，从底层构筑“本质安全”防线，保障终端系统稳定性与数据安全性，实现从芯片、网络、操作系统到应用的全链路国产化自主可控，满足国家关键信息基础设施的供应链安全诉求。

#### 四、方案优势与价值总结

本方案基于“WAPI+电鸿”的智能物联网终端，集成轻量化硬件、机器视觉、安全无线通信与国产操作系统，构建起全栈式、自主可控、高安全且深度适配电力物联网需求的解决方案，为电力运维等关键信息基础设施提供安全稳定的连接能力。其综合优势如下：

- 1、经济性：**以极低改造成本实现传统机械表计智能化升级，投资回报率高，适配预算敏感的中小型变电站规模化推广。
- 2、高安全性：**通过WAPI无线通信与电鸿操作系统，构建端到端高安全防护体系，化解无线技术在电力工控场景的应用顾虑。
- 3、高可靠性：**工业级硬件设计、超长续航能力与稳定识别算法，保障系统全周期稳定运行。
- 4、便捷高效：**实施过程即插即用，无需停电或大规模施工；运维阶段实现无人化自动巡检，大幅提升工作效率并降低安全风险。
- 5、数据驱动：**将人工抄录的模拟信息转化为可追溯、可分析的数字信息，为变电站的状态检修、预测性维护与智能化决策提供坚实数据支撑。

#### 五、应用案例与未来展望

某220KV变电站改造案例是本方案成功落地的典型范例。该站改造前依赖人工每日现场巡查、手动记录数据，存在前述所有行业痛点。部署本方案后，系统可自动完成表计图像采集、识别与数据上传，巡检人员无需每日进入高危区域，既彻底消除人身安全风险，又将工作人员从重复低效劳动中解放，转而聚焦设备状态分

析、故障处理等高价值工作；同时，智能读数的准确性与一致性大幅提升，为电网精细化管理筑牢数据根基。

展望未来，伴随人工智能与物联网技术的持续演进，此类机器视觉解决方案的应用场景将持续拓展，可从变电站延伸至发电厂、石油化工、水利枢纽等所有涉及机械表计监控的工业领域。莲雾科技的该方案为传统工业设施数字化转型升级提供了可复制、可推广的实践范本，标志着行业正迈入以“智慧之眼”守护工业安全的全新阶段。

### 关于莲雾科技

广州莲雾科技有限公司成立于2016年，是一家专注于物联网领域的高新技术企业，是WAPI产业联盟会员单位。作为行业领先的解决方案提供商之一，莲雾科技的产品和服务涵盖了物联网云平台、智能通信网关、各类专用传感器和执行器、行业应用解决方案等方面。公司于2018年和2021年连续两次被认定为高新技术企业。

莲雾科技坚持以客户需求为导向，提供针对不同行业特点的定制化服务。公司拥有一支技术实力强大的研发团队和专业的售后服务团队，产品已广泛应用于数字电力、数字工业、数字农业、资产管理等领域，在市场上赢得了广泛的认可和信任。

**WAPI Alliance**  
产业联盟



WAPI产业联盟公众号

地 址：北京市海淀区知春路27号量子芯座1608室

邮 编：100191

电 话：010-82351181

传 真：010-82351181 ext. 1901

邮 箱：wapi@wapia.org

网 址：<http://www.wapia.org.cn>