

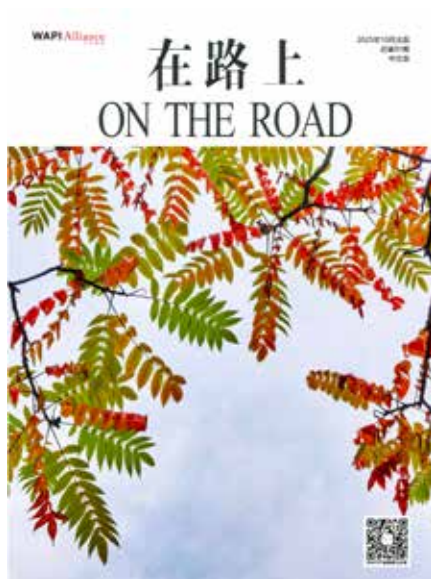
WAPI Alliance
产业联盟

2025年10月出版
总第91期
中文版

在路上

ON THE ROAD





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：



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

喜报 Congrats

05 第五届北京社会组织推介活动成功举办 WAPI产业联盟蝉联5A级社会组织

媒体聚焦 Media Focus

07 通信世界等：WAPI产业联盟召开2025年第三次标准工作和项目组会议（总第135次）

11 飞象网等：筑牢工业无线安全屏障 WAPI产业联盟持续开展瘦AP重测

13 中国信息化周报等：芯语慧联TH6180低功耗模组通过WAPI协议基础要素测评

联盟关注 Alliance Concerns

15 联盟重磅发布《工业网络选择中短距离无线通信技术路线的基本原则》洞察报告

WAPI 问答 WAPI FAQ

19 WAPI问答（系列连载）第十六部分

产经要闻 Industrial & Economic News

23 李强：强化标准引领保障作用 以标准升级促进经济高质量发展

23 李乐成：全面贯彻总体国家安全观 加强对“黑天鹅”“灰犀牛”事件的跟踪研判

24 网络安全法修正草案：强化网络安全法律责任

24 二十届四中全会：提出“十五五”时期经济社会发展的主要目标

25 国务院办公厅：加强电子印章规范管理 服务政务活动和经济社会数字化发展

25 工信部、国家市场监管总局：促进电子信息制造业稳定增长 提升产业链供应链韧性和安全水平

26 国家市场监管总局等15部门：强化网络和数据安全保护 加快推进质量认证数字化发展

26 住房城乡建设部等9部门：强化网络安全防护 推进新型城市基础设施建设

27 国家能源局：《能源行业数据安全管理办法（试行）（征求意见稿）》强化网络安全要求

联盟工作 Alliance Work

- 28 党建引领科创路 精神传承启新程——WAPI产业联盟组织参观周恩来邓颖超纪念馆
- 30 WAPI产业联盟组织观看抗战胜利80周年阅兵直播 凝聚科技报国力量筑牢网络安全防线
- 31 海淀区举办“世界标准日”主题活动 WAPI产业联盟携核心成果助力标准创新示范区建设
- 32 无线网络安全标准化工作委员会2025年第三次主任委员会议（总第14次）顺利召开
- 34 联盟标委会队伍持续壮大,为标准创新发展注入新动能
- 35 博洛米WAPI系列终端通过联盟测试
- 36 北京数字认证WUAS-A4000鉴别服务器通过联盟测试

成员与市场 Member & Marketing

- 37 南方电网推进贵州WAPI建设
- 38 智芯公司荣获第二十五届中国专利金奖
- 38 鼎信通达无线语音通信系统专利获授权
- 39 天宽科技打造电力行业智能巡检新标杆
- 40 WAPI技术赋能遨游三防手机：“危急特”场景信息安全升级
- 41 中科鸿略发布开源鸿蒙WAPI解决方案
- 42 高通发布第五代骁龙8至尊版移动平台 支持WAPI
- 42 联发科发布天玑9500移动芯片 支持WAPI
- 43 神州数码入围中国企业500强与战略性新兴产业领军企业
- 43 数字认证获CNVD“2024年度原创漏洞发现贡献单位”荣誉称号

产业技术论坛 Industry & Technology Forum

- 44 浅析WAPI 2.0中的身份信息保护机制

第五届北京社会组织推介活动成功举办 WAPI产业联盟蝉联5A级社会组织

2025年10月28日，第五届北京社会组织推介活动成功举办，活动现场公布2025年度市级社会组织评估结果，中关村无线网络安全产业联盟（WAPI产业联盟）再度荣获5A级社会组织，成为本次唯一获评5A级的产业联盟，同时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成为重点推介对象。民政部社会组织管理局副局长张琳，中共北京市委社会工作部副部长卢建，北京市社会组织管理中心党委书记温育梁、主任郭卫亮出席活动。



图：WAPI产业联盟荣获北京市5A级社会组织

本次评估严格遵循民政部《社会组织评估管理办法》规定，从社会组织党的建设、内部治理、发挥作用、遵章守规、诚信建设等维度开展等级评估，今年共有 374 家社会组织参与，经评估委员会审议，最终确定 WAPI 产业联盟等 44 家社会组织为 5A 级。

WAPI 产业联盟秘书长张璐璐介绍，联盟长期聚焦国家战略与首都“四个中心”建设任务，历经近 20 年发展，已构建起科学有效的协同创新和内部治理体系，在技术产业创新服务领域形成显著优势，且在自律诚信建设与管理创新中持续主动探索。



图：WAPI 产业联盟秘书长张璐璐
参加授牌仪式



图：高德发布WAPI产业联盟等
5A社会组织公益地图

活动对 WAPI 产业联盟产业贡献进行重点推介：作为我国无线网络安全领域的重要行业组织，联盟牵头建设无线网络安全技术国家工程研究中心；通过标准化、产业化与国际化协同推动，已完成近 200 项标准制修订，包括 23 项国际标准与 100 余项团体标准，相关成果多次荣获中国标准创新贡献奖；通过搭建测试实验室等公共平台，为产业提供五大类服务，其测试报告获得市场广泛认可。同时，联盟持续组织产业链协同攻关，推动技术示范应用并完成多项国际标准超前布局，显著提升了我国在该领域的全球话语权，为北京国际科创中心建设贡献了关键力量。

"蝉联 5A 级社会组织是荣誉更是责任。"张璐璐表示，未来联盟将继续深耕无线网络和网络安全领域，推动技术创新与标准升级，深化国际标准化合作，助力 WAPI 技术融入全球数字安全体系，为首都“五子联动”新发展格局及国家网络安全战略实施提供坚实支撑。

活动期间，高德地图发布北京 5A 级社会组织公益地图，市民可通过该地图精准查询服务资源，让包括 WAPI 产业联盟在内的社会组织服务更可达、更便捷。

数据显示，截至目前北京市登记注册市级社会组织达 4454 家，涵盖社会团体 2105 家、社会服务机构 1507 家、基金会 842 家，其中 3A 级（含）以上社会组织 1580 家。“十四五”以来，全市社会组织积极发挥桥梁纽带作用，在科技创新、社区服务、乡村振兴、京津冀协同发展等领域开展专业化服务，为中国式现代化建设与首都高质量发展赋能增效。

通信世界等：

WAPI产业联盟召开2025年第三次标准工作和项目组会议 (总第135次)

【编者按】日前，WAPI产业联盟召开2025年第三次标准工作和项目组会议（总第135次），围绕第三季度工作进展、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、新项目立项建议、国际化推进、标准培训等议题展开。通过会议，进一步汇聚政产学研用各方力量，推进标准产业协同创新，为无线网络安全产业的高质量发展夯实基础。通信世界、中国信息化周报、飞象网等媒体对此进行了报道。

以下是通信世界的报道：



日前，WAPI产业联盟召开2025年第三次标准工作和项目组会议（总第135次），围绕第三季度工作进展、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、新项目立项建议、国际化推进、标准培训等议题展开。



图：会议合影

来自无线网络安全技术国家工程研究中心、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、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、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、广州莲雾科技有限公司、深圳市智开科技有限公司、南京南瑞信息通信科技有限公司、天津光电通电子科技有限公司、深圳市明华澳汉智能卡有限公司等单位代表,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、天津民盟河东区委会相关负责人,无线网络安全标准化工作委员会委员等参加会议。



图：会议现场

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表示,2025 年世界标准日的主题是“美好世界的共同愿景:增强伙伴关系,共促可持续发展”——这和我们 WAPI 标准产业共同体的理念高度契合。在 10 月 15 日李强总理主持的国务院第十六次专题学习中明确提出,支持产业联盟等市场力量在标准研制上发挥更大作用,促进团体标准健康发展;强化标准实施,坚持严格监督和优化服务并举,用好检验检测、认证认可等手段推动标准实施。今年 7 月联盟召开的“无线网络安全产业创新应用大会”使市场和产业进一步达成了“直面深水区,共建高质量安全无线局域网”的目标共识,第四季度标委会将继续加强平台建设,持续推动标准体系的演进和发展,推动标准高质量实施,圆满完成标委会 2025 年各项重点工作。

WAPI 产业联盟秘书长、标委会副主任委员张璐璐表示,今年以来,联盟标委会严格依照《2025 年重点任务计划》,聚焦标准制定、实施、平台、生态四大核心领域,系统推进 12 项重点工作,第三季度各项任务均取得扎实进展。当前,全球技术竞争日趋激烈,产业界对“高质量安全无线局域网”的需求日益迫切,下一步需集中力量攻坚三大重点:一是持续完善标准体系,二是推动与国军标、行业标准的有效衔接,三是促进团体标准的采信与引用。要进一步凝聚标准产业共同体合力,广泛联合天津民盟等政产学研用各方力量,将标准优势转化为产业市场竞争力,协同推动产业高质量发展。



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



图：WAPI产业联盟秘书长、标委会副主任委员张璐璐



图：天津民盟河东区委会金融科技支部主委周茜茜

会议通报了 2025 年第三季度工作进展：

在标准制定层面，24 项团体标准正在梯次推进，2 项发布、9 项即将报批、7 项正式立项。从 WAPI 与 IEEE 802.11be 的工程化指南，到产业急需的设备测试方法，再到 WAPI 2.0 核心标准修订，每一项都紧扣“安全、务实、高效”，直击产业痛点；国际标准推进取得新进展，SC 6 国内技术对口单位期间流通国际提案文件 6 份，反馈国际投票意见 3 份。

在标准实施层面，依标升级联盟 WAPI 2.0 测试能力，开展瘦 AP 重新测试专项，6 家会员 18 款产品通过测试，让标准更高效服务市场建设；积极参与国家标准、行业标准制定，推动 GB 15629.11 系列标准纳入规范性引用；发布《WAPI 市场应用洞察报告》，提出工业网络选择短距离无线通信技术的五项核心原则，经专业分析研判，明确 WAPI 是当前契合需求的最佳技术路线。

在标准平台建设层面，新增黄琪、郑崇剑、董治江 3 位委员，标委会队伍壮大至 90 人。

在生态环境建设层面，WAPI 产业联盟获评北京市 5A 级社会组织，连续 15 年获 ISO 9001 质量管理体系“优秀”评价；成功举办高质量无线局域网创新应用大会，聚焦“WAPI 建设深水区”挑战，明确行动方向。

会上，张璐璐为新任委员代表颁发了证书和信物。



图：张璐璐副主任委员为新任委员颁发证书、信物

标委会委员郑骊回顾了第二次项目组集中会议决议和落实情况。标委会委员、项目编辑张变玲就 T/WAPIA 007.11—2025《无线局域网产品工程化实现指南 第 11 部分：WAPI 与 IEEE 802.11be》标准进行宣贯。

在已立项项目讨论环节，对 12 项已立项标准《高质量安全无线局域网总体要求》、《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》、《无线局域网测试 第 2 部分：设备测试方法》、《无线局域网产品工程化实现指南》、《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》、《应用于抽水蓄能领域的电力物模型 WAPI 产品规范》、《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》、《基于 MQTT 协议的无线局域网接入点集中管理通用技术规范》和 2 项解决方案项目《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》，以及拟立项项目进行了逐项讨论，形成一致决议。

此外，会议还专题研讨标准国际化工作，通报 2025 年 10 月 WG 1 和 WG 7 工作组中期会议情况，并开展标准化知识交流培训。

工信部宽带无线 IP 标准工作组 2025 年第三次项目组集中工作会议同期召开。

部分媒体新闻链接：

通信世界：<https://www.cww.net.cn/article?id=604645>

中国信息化周报：<https://www.cio360.net/show-598-104478-1.html>

飞象网：<http://www.cctime.com/html/2025-10-20/1721067.htm>

飞象网等：

筑牢工业无线安全屏障 WAPI产业联盟持续开展瘦AP重测

【编者按】为规范工业领域WAPI网络建设，筑牢无线通信安全屏障，联盟发布《关于针对AE驻留位置开展WAPI瘦AP产品重新测试的通知》，并启动专项重新测试工作，目前福建星网锐捷、许继电气、上海诺基亚贝尔等多家企业的多款产品已通过测试。飞象网、通信世界网、信息主管网等媒体对此进行了报道。

以下是飞象网的报道：



为规范工业领域 WAPI 网络建设应用，筑牢无线通信安全屏障，2025 年 5 月 21 日，WAPI 产业联盟正式发布《关于针对 AE 驻留位置开展 WAPI 瘦 AP 产品重新测试的通知》，启动专项重新测试工作。截至目前，已有福建星网锐捷、许继电气、上海诺基亚贝尔等多家企业的多款产品通过测试，获得新版测试报告。

WAPI 瘦 AP 在架构中采用“接入控制器（AC）集中控制、无线接入点（AP）协同接入”的模式，实现终端设备（STA）的安全管理。其中，鉴别器实体（AE）的鉴别与保密功能不可拆分——若拆分将导致加解密密钥在 AC 与 AP 间传输，引入重大安全风险。从技术原理看，AE 可完全驻留于 AP 或 AC 中，但结合产品工程化实践，AE 完全驻留于 AC 的方案目前无法实现。因此，AE 必须完全驻留于 AP，才能确保 WAPI 安全服务与应用体验达到最佳水平。

为提前防范风险、规范产业发展，WAPI 产业联盟于 2024 年 4 月发布《对 WAPI 标准体系中鉴别器实体驻留设备的澄清和说明》，就 AE 驻留位置问题进行行业预警；2025 年 4 月进一步发布《WAPI 市场应用洞察报告——瘦 AP 组网架构下的 WAPI 产品工程化实现与部署》，同步修订《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》（2025 年 4 月版），新增 AE 驻留位置测试项。



图：联盟为通过重新测试的厂商出具测试报告

考虑到部分已通过旧版测试的产品需进行技术整改，且整改可能影响设备功能性能，联盟从严谨性出发，明确所有相关产品须重新测试。为减轻企业负担、支撑产业高质量发展，联盟同步推出鼓励政策：厂商在规定期限内可免费申请重新测试，通过后发放新版测试报告，助力企业满足市场采购需求、提升核心竞争力。

本专项测试工作的推进，不仅进一步明确了 WAPI 瘦 AP 产品的技术规范，更从源头保障了工业等关键领域无线局域网的安全可控。下一步，联盟将持续强化 AE 驻留位置等核心技术要求的行业宣贯，把相关测试标准纳入产品常态化检测体系，对新申请测试的 WAPI 瘦 AP 产品实行“全覆盖、严把关”。同时，联盟将动态跟踪已通过重新测试产品的市场应用情况，结合工业场景需求变化迭代优化测试项目，为各行各业高质量安全无线局域网建设和稳定运行保驾护航。

部分媒体新闻链接：

飞象网：<http://www.cctime.com/html/2025-10-28/1721707.htm>

通信世界：<https://www.cww.net.cn/article?id=604920>

信息主管网：<https://www.cio360.net/show-598-104486-1.html>

中国信息化周报等：

芯语智联TH6180低功耗模组 通过WAPI协议基础要素测评

【编者按】西安芯语智联信息科技有限公司自主研发的低功耗WAPI模组（型号：TH6180）成功通过WAPI产业联盟“WAPI协议基础要素测评”。该模组集成了通过商用密码产品认证的安全芯片，可支持ECDSA、ECDH、SHA-256等多种算法，实现了对密钥从生成、存储到运算的全过程硬件级安全防护。这一成果标志着该企业在低功耗、高安全无线通信模组领域的技术实力与产品可靠性获得行业权威认可，也为我国物联网终端设备的无线网络安全接入再添优质解决方案。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：



西安芯语智联信息科技有限公司（以下简称“芯语智联”）自主研发的低功耗 WAPI 模组（型号：TH6180）成功通过中关村无线网络安全产业联盟（以下简称“WAPI 产业联盟”）“WAPI 协议基础要素测评”。这一成果标志着该企业在低功耗、高安全无线通信模组领域的技术实力与产品可靠性获得行业权威认可，也为我国物联网终端设备的无线网络安全接入再添优质解决方案。

作为我国自主可控的无线网络安全技术标准，WAPI（无线局域网鉴别与保密基础结构）已深度融入各行各业，成为保障国家网络和信息安全的重要技术支撑。当前，传感器、手持终端、智能穿戴等物联网业务终端，普遍通过集成低功耗 WAPI 模组快速具备安全接入能力。然而，市场调研发现，部分低功耗 WAPI 模组及集成终端在工程实现方面存在安全隐患——未能采用符合国家密码主管部门批准算法能力的安全芯片，对密钥的存储与密码运算缺乏硬件级防护，存在密钥泄露风险，影响整个无线通信系统的安全稳定运行。



图：芯语慧联TH6180低功耗WAPI模组

为从源头化解这一行业共性问题，WAPI产业联盟主动布局测评能力建设，于2024年8月正式启动针对低功耗WAPI模组及集成终端的“WAPI协议基础要素测评”服务。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，为市场用户选型提供权威技术依据。

测评服务推出后，迅速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等企业的多款低功耗WAPI模组及终端产品率先通过测评，充分展现了他们在无线通信安全领域的前瞻布局与技术积淀。此次芯语慧联TH6180模组的顺利通过，进一步壮大了合规产品阵营。

据了解，芯语慧联在TH6180低功耗WAPI模组的设计阶段，即把安全防护作为核心技术指标，严格遵循WAPI标准及国家密码相关要求。该模组集成了通过商用密码产品认证的安全芯片，可支持ECDSA、ECDH、SHA-256等多种算法，实现了对密钥从生成、存储到运算的全过程硬件级安全防护。

芯语慧联相关负责人表示，将持续深化WAPI技术与低功耗物联网终端的融合创新，进一步优化模组性能和兼容性，为智慧能源、工业物联网、智能安防等领域提供更安全、更可靠、更具性价比的无线通信解决方案。

WAPI产业联盟表示，将继续完善测评体系，扩大合规产品覆盖面，推动我国自主无线网络安全标准在物联网领域的高质量应用。

部分媒体新闻链接：

中国信息化周报：<https://www.cio360.net/show-598-104475-1.html>

通信世界：<http://www.cww.net.cn/article?id=604619>

飞象网：<http://www.cctime.com/html/2025-10-17/1720944.htm>

联盟重磅发布《工业网络选择中短距离 无线通信技术路线的基本原则》洞察报告

【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》给出了工业网络选择中短距离无线通信技术路线的五大基本原则，并依据上述原则形成结论。同时对 WAPI 技术路线演进所遵循的原则进行了声明。

《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》全文如下：

本期洞察对象与结论

在工业互联网络中，数米至 300 米以内的中、短距离无线网络是现场接入网络与工业核心网络之间的关键连接桥梁，其覆盖了工业场景超 90% 的设备互联需求，像产线工位间通信（小于 50 m）、车间级设备组网（50 m ~ 200 m）以及厂区覆盖（100 m ~ 300 m）等场景，性能直接关乎工业生产系统的可靠性与响应时效。因此，在工业网络建设进程中，挑选适宜的中短距离无线通信技术路线尤为重要。

本报告给出工业网络在选择该技术路线时需遵循的五项基本原则，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。基于这些原则深入剖析可知，安全无线局域网（WAPI）是当前工业网络选择中短距离无线通信的最佳技术路线。

一、高质量工业网络急需中短距离无线通信作支撑

伴随着新一轮科技革命和产业变革深入发展，推进数字化转型是顺应技术发展趋势、加快产业转型升级的必然。在数字化转型浪潮中，数字技术与实体经济深度融合，传统产业借助网络化、智能化实现升级，运用人工智能、大数据、云计算、区块链等技术提升业务效率，达成高质量发展目标。

网络化通过网络技术实现工业内部各系统以及系统间的互联互通，打破信息孤岛，促进数据的流通与共享。工业网络作为推动工业数字化转型的核心基础设施，构建起大带宽、低时延、高安全的通信底座，能直接支撑在线监测、智能制造、远程运维等新型业务场景的实现，提升工业链条协同效率，成为工业互联网、能源互联网等新型产业生态的基础保障，对工业智能化升级的深度与广度有着直接影响。

工业场景对通信有多重核心要求：需精准覆盖各类设备，实时控制场景需要确定的低延迟，同时还要与现有工业协议深度适配。在此背景下，中短距离无线通信技术成为工业网络“最后一百米”的最佳解决方案。

传统工业网络的接入方式存在明显短板：若采用 4G/5G 等公网通信，易出现信号盲区且资费较高；若依赖有线连接，则建设运维成本高、施工周期长。因此，高质量工业网络的建设，迫切需要一种具备充足带宽、

确定低时延、安全可控、部署灵活且易于扩展的中短距离无线通信方式。

二、中短距离无线通信技术：类型多样，各有优劣

近年来，全球中短距离无线通信技术呈现多维度协同演进态势，通信速率、时延和安全性指标有了突破性提升，异构网络互联互通、云网边协同、人工智能（AI）驱动等技术架构正深度融合。同时，高密度自动导引车（AGV）调度、可穿戴设备、移动机器人控制、智慧园区传感网络等典型应用场景不断扩展，标准化与产业生态得到协同发展。

目前已有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。

三、中短距离无线通信技术路线选择的基本原则

1. **法律合规性**：需严格符合国家无线电管理法规、网络安全、密码等方面的相关法律法规要求。
2. **标准符合性**：需有成熟的、已发布的国家或行业标准作为建设依据。
3. **功能/性能匹配性**：需满足工业网络中短距离无线通信应用场景的功能和性能要求（如信号覆盖范围、数据传输速率、功耗、时延、连接密度、移动性、可靠性、可扩展性、可运维性、集中管理等）。
4. **产业成熟度**：非处于实验验证阶段或试点应用阶段，要在相关行业有长期成熟应用；具备健康稳定的产业生态，有多厂商可提供产品，产品价格经过充分的市场竞争趋于合理，具备完整的检测认证体系。
5. **可持续发展性**：围绕该技术路线，需具备持续演进的标准体系和标准化创新平台。

四、为什么 WAPI 是当前工业网络中短距离无线通信的最佳技术路线

依据上述五项基本原则对 WAPI 技术进行深入分析评估，形成 WAPI 技术路线的模型对照表（见表）。结果显示，WAPI 在各方面表现优异，高度契合工业网络需求，是当前工业网络中短距离无线通信的最佳技术路线。

序号	模型元素	模型评估结论	WAPI 模型对照说明
1	法律合规性	满足	遵守网络安全法、密码法、标准化法、国家安全法、数据安全法、个人信息保护法。 遵守无线电管理条例、商用密码管理条例、计算机信息系统安全保护条例、关键信息基础设施安全保护条例、网络安全等级保护条例、网络安全审查办法、商用密码应用安全性评估管理办法。
2	标准符合性	满足	符合无线局域网技术规范 GB 15629.11 (所有部分)、无线局域网测试规范 GB/T 32420、等级保护基本要求 GB/T 22239、密码应用基本要求 GB/T 39786 等国家标准; YDC 079、GM/T 0042 等行业标准; T/WAPIA 007 (所有部分)、T/WAPIA 040 (所有部分)、T/WAPIA 047 (所有部分) 等团体标准。共百余项标准。
3	功能 / 性能匹配性	高	基于 WAPI 技术标准, 已构建了完善的产品生态体系, 能满足当前几乎所有工业场景下通信功能与性能需求, 如高清视频流传输、高速数据交互等关键应用, 并在持续进行技术迭代与性能优化。 实测单站点速率已达 1.6Gbps, 通信时延小于 10ms, 另有高安全等关键特性: 管理帧保护、快速切换、多 SSID 支持、AP 集中管理、综合网管、网络切片、跨域漫游、AS 分级管理、QoS 支持、信道优化等, 确保了高安全、高效和易于管理。
4	产业成熟度	高	WAPI 产业发展成熟, 在多个行业拥有规模化长期应用。具备覆盖芯片、模组、终端到系统的全链条检测认证体系, 市场参与主体多元且竞争有序, 产业生态健康稳定。 截至 2025 年 6 月, 支持 WAPI 的安全无线局域网芯片已超过 500 款型号、全球累计出货量超过 300 亿颗, 移动终端和网络侧设备等已超过 23000 款。WAPI 已在全国海关 20 余个关区, 国防领域数百座后勤保障仓库以及野战医院等联勤保障, 南方电网 / 国家电网数千座变电站 / 换流站, 公安、政务、金融、医疗、教育等行业广泛应用, 并服务北京大兴国际机场、新疆地铁、城市地下综合管廊等国家地方重大项目, 以及北京奥运会、北京冬奥会、国庆 70 周年阅兵等重大活动。
5	可持续发展性	高	WAPI 已构建起持续演进的标准体系与标准化创新平台。 经过近 30 年技术积累, WAPI 数据通信与管理控制协议已迭代至第七代, 安全协议则进入面向量子时代的 WAPI 2.0 标准体系阶段。与此同时, 基于 WAPI 技术的高质量安全无线局域网标准体系已初步建成, 目前正处于持续优化与完善阶段。 WAPI 产业联盟是国家发展改革委、科技部、工信部指导成立的、专注于网络安全且具国际影响力的产业组织, 目前会员 137 家, 包括三大电信运营商和有代表性的 ICT 领域企业, 覆盖从芯片设计到整机、系统集成、测试等产业链各环节的骨干企业。和工业和信息化部宽带无线 IP 标准工作组、国际标准组织 ISO/IEC JTC 1/SC 6 国内技术对口单位、无线网络安全技术国家工程研究中心 (我国在基础性网络安全领域设立唯一的产业技术创新基础设施)、无线网络安全标准化工作委员会, 以及有推动 WAPI 技术、标准和产业创新发展的共同目标和愿景的组织和个人形成了 WAPI 标准产业共同体, 协同推动安全无线局域网高质量发展。

注: 更详细情况, 请参考《WAPI 标准产业应用及环境监测报告》最新版。

五、WAPI 技术路线演进声明

全球无线局域网（WLAN）技术已经发展了近 30 年，在最基础的数据传输和管理控制协议层面，形成了一套相对统一的技术框架。WAPI 技术使 WLAN 实现了高安全性和自主可控。这种成熟的技术模式，既是全球和中国产业链长期创新的成果，也得益于充分的市场竞争，目前技术和产业相当成熟。

作为支持工业数字化转型的重要基础设施，WAPI 技术及相关标准的发展，始终遵循开放、兼容、逐步推进的理念。它基于三元对等安全架构（TePA）并符合国际标准的体系，力求在技术可行性、商业可持续性和满足用户需求之间找到动态平衡。

在具体的技术发展和演进上，遵循以下行动指南：

- 1. 在保障网络安全基础上提升效能。**网络安全是网络演进的基石。WAPI 在保障在网络安全的前提下，持续优化网络性能，力求实现安全可靠与高效传输的统一，为工业网络提供坚实可靠的通信保障。
- 2. 渐进式创新路径。**采用“评估 - 融合 - 验证”的迭代模式，在现实约束下寻求最大化的实用和发展价值，确保新技术引入时的互操作性和稳定性，稳步推动技术的发展与进步。
- 3. 技术和商业平衡。**技术上严格评估 MAC/PHY 层技术融合的工程实现成本；商业上确保技术和标准更新与产业链升级节奏相匹配；工业应用体验上维持向后兼容性，控制终端设备更新成本。
- 4. 产业驱动共识。**借助 WAPI 产业联盟等平台，建立多方参与评估的协同机制，涵盖技术方（技术研究者）对技术先进性与可行性的评估、模块方（芯片 / 模组厂商）对协议实现一致性的把控、产品方（设备 / 系统集成商）对功能可扩展性的考量、应用方（工业用户）对场景适配性的需求等，达成多方利益共同体共识、共同推进 WAPI 技术的发展与应用。

技术演进是通过综合考虑解决实际问题，而不是单纯追求某一项指标上的最优。未来，随着芯片工艺进步和频谱政策优化，更先进技术将在以上行动指南下，逐步融入安全无线局域网技术和标准体系，更好地服务工业数字化转型。

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

第十六部分（PART 16）

■ 1、问：WAPI STA“双发选收”是如何实现STA在AP间快速切换的，对网络侧设备有没有特殊要求（例如：是否需要STA和AP是同品牌/厂商的）？

答：通过“双发选收”实现快速切换的STA，对网络侧设备没有特殊要求。

实现“双发选收”的STA有射频A和射频B两组射频，在AP间切换类似于两只脚走路，但总有一只脚不离地面——当STA在AP1与AP2之间切换时，射频A保持与AP1稳定连接，同时射频B开始连接AP2，连接稳定后，射频A与AP1断开，以此类推——始终保持有一组射频处于稳定连接状态，从而实现“无感”切换。早在2021年就有相关（两组射频）CPE产品通过了WAPI产业联盟测试，实现了移动高清视频等业务无间断、不卡顿、实时传输，实测切换时间小于20ms。

■ 2、问：行业用户使用WAPI与使用Wi-Fi相比有哪些优势？

答：WAPI是无线局域网技术路线中，唯一符合我国法律法规和国家标准体系的。WAPI较之Wi-Fi，有4个方面的核心优势：

- （1）更加安全。
- （2）具有法律合规性——符合网络安全、密码、无线电管理等法律法规。
- （3）具有标准符合性——符合GB 15629.11等百余项中国标准。
- （4）中国自主安全协议，符合国家自主可控发展战略。

■ 3、问：WAPI使用数字证书有哪些安全性优势？

答：安全性优势包括：

- (1) 强身份鉴别。
- (2) 防止中间人攻击。
- (3) 不可否认性。
- (4) 易于集中管理。
- (5) 易于网络规模的扩展。

通俗地说，数字证书就像一个电子身份证，帮助确认连网设备身份，确保“只有合法终端才能接入合法网络”，提高了无线网络的安全性。

■ 4、问：有些家用/餐厅/酒店的无线局域网采用的是口令方式，适用于工业场景吗？

答：不适用。

- (1) 口令方式是所有网络用户共用一个密钥。口令极易外泄，并且无法追查。
- (2) 即使网络用户实施了一些违法违规行，但因为使用的是同一口令，行为无法追溯到该用户。

口令方式面临的安管理风险大、仅适用于满足短时间临时组网的需求，是绝不能用于能源电力等工业场景的。

■ 5、问：证书绑定MAC地址，目前被用于防止非法持有者的初级冒用、误用，但MAC地址可以被伪造，那么证书绑定MAC地址还有价值和意义吗？

答：有价值和意义。原因如下：

(1) 数字证书的安全性是靠设备的私钥保障的，私钥的存储和相关运算是不出合法设备的，即便非法持有者伪造了合法设备的MAC地址，但因为没有相应的私钥而无法合法使用该证书。

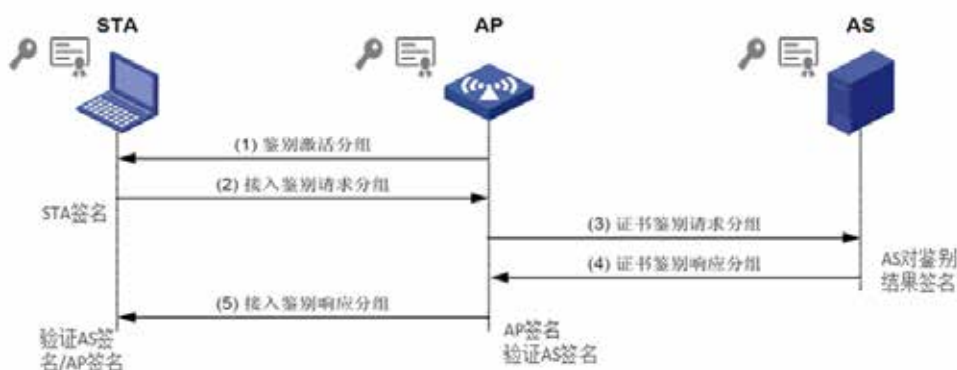
(2) 当实践中当出现证书冒用、误用的情况时，证书绑定MAC地址可以初步识别非法设备，有效地节约AS端的鉴别算力资源。此外，数字证书绑定MAC地址，还有助于网络运维人员快速定位终端和接入点设备，便于排查和管理设备。

(3) 通俗地说，身份证上印上照片，并非是为了防伪，而是有助于初步识别持有身份证的是不是本人，有效防止初级冒用。

6、问：WAPI协议“五次传递”具体传递的是什么信息，会传递密钥吗？

答：（1）“五次传递”具体指的是WAPI的身份鉴别过程，传递的信息是证书鉴别协议分组，关键数据包括STA身份证书、AP身份证书、STA和AP密钥协商参数、STA和AP对消息的签名数据、AS生成的鉴别结果及对鉴别结果的签名等。“五次传递”确保了“合法终端接入合法网络”，期间不会传递终端或者AP的私钥。

（2）五次传递后，将进行会话密钥协商、得到数据加密密钥，用于后续业务数据的保密传输。在保密传输中，即使网络窃听者能通过无线方式得到传输数据，但无法破解、无法获得通信的内容。



7、问：WAPI鉴别过程需要传输私钥么？会传输公钥吗？

答：WAPI鉴别过程不会传输私钥——私钥由STA、AP、AS本地存储使用，鉴别过程中不传输。

STA和AP的公钥在鉴别过程中，以数字证书形式传输——因为公钥本来就是让其他设备知晓的（用于验证签名），所以不会带来安全问题。

8、问：WAPI数据加解密传输过程中需要使用公钥/私钥吗？

答：不需要。

WAPI数据加解密使用的是对称密码算法SM4，使用的密钥为协商产生的会话密钥（单播密钥、组播密钥等）。

9、问：为什么要协商加解密密钥？直接用公钥/私钥加解密数据可以吗？

答：不可以。原因是：

（1）公钥/私钥采用的密码算法是非对称密码算法。数据保密通信需要对大数据量进行加密和解密，采用非对称密码算法将导致通信效率极低，因此必须采用对称密码算法（SM4）——双方有相同的加解密密钥。

（2）加解密密钥是在身份鉴别之后的密码协商过程中协商出来的，WAPI协议已对其作了规范。

■ 10、问：加解密密钥多久会更新一次？密钥更新过程中还需要再次鉴别吗？

答：（1）WAPI协议中，提供了加解密密钥按照需求更新的机制。通常按照使用时间（例如24小时）或者通信流量，启动密钥更新。

（2）密钥更新需要重新进行身份鉴别。密钥更新过程不会引起通信中断。

■ 11、问：在“支持WAPI 1.0与2.0功能兼容模式”的实际测试中，针对STA、AP、AS分别需开展哪些测试？

答：（1）对于STA，需要测试其能否根据网络提供服务情况，灵活选用WAPI 1.0或WAPI 2.0模式接入对应网络（不同的SSID）。

（2）对于AP，需要测试其能否支持两种模式的STA同时接入。

（3）对于AS，需要测试其能否同时鉴别两种模式的证书。

李强：

强化标准引领保障作用 以标准升级促进经济高质量发展

2025年10月15日，国务院总理李强主持国务院第十六次专题学习时强调，要加快推进标准化工作改革创新，促进实体经济提质升级，持续增强高质量发展内生动力。

李强指出，标准是重要基础性制度，对构建现代化产业体系、建设全国统一大市场等具有重要作用。要把标准升级摆在更加突出位置，加快构建适应高质量发展要求的标准体系，更好发挥标准引领保障作用。

李强强调，要优化标准供给，紧贴经济社会发展实际，坚持急用先行、有序提升，逐行逐业梳理标准需求，强化人工智能等数字技术赋能，系统推进标准制定修订。要强化标准实施，坚持严格监督和优化服务并举，用好检验检测、认证认可等手段推动标准实施，建立强制性标准实施责任清单，注重在产业政策、政府采购、招投标中引用推荐性标准，引导企业执行高水平标准。要提升标准国际化水平，深化标准国际合作交流，稳步扩大标准制度型开放。

李强指出，要坚持以改革创新为动力，持续完善标准化工作体制机制，全面提升标准总体水平和标准化管理效能。要处理好政府和市场的关系，发挥政府部门顶层设计和规范引导作用，支持企业、产业联盟等市场力量在标准研制上发挥更大作用，促进企业标准、团体标准健康发展。要处理好国家层面标准和地方标准的关系，进一步厘清各级标准定位，精简标准层级，加快破除制约全国统一大市场建设的标准障碍，切实形成国家统一规则和地方特色补充的良好格局。要处理好标准管理和行业治理的关系，完善统筹组织、分工负责、协调配合的工作机制，推动形成标准化工作改革合力。

李乐成：

全面贯彻总体国家安全观

加强对“黑天鹅”“灰犀牛”事件的跟踪研判

2025年10月22日，工业和信息化部党组书记、部长李乐成在《新型工业化》发表署名文章提出，我国工业发展正处在由大变强的重要关口，结构性、体制性、周期性问题相互交织，面临的矛盾和风险挑战明显增多，必须把防风险放在突出位置，全面贯彻总体国家安全观，树牢发展是硬道理、安全也是硬道理的理念，强化底线思维、极限思维，加强对可能出现的各种“黑天鹅”“灰犀牛”事件的跟踪研判，及时完善应对预案，做到心中有数、手中有策、行动有力。防范和化解风险是未来一个时期的重大课题，要深入研究、抓实抓牢。

网络安全法修正草案： 强化网络安全法律责任

2025年9月8日，网络安全法修正草案首次提请全国人大常委会会议审议。此次修改重点强化网络安全法律责任，加大对违法行为处罚力度，加强与数据安全法、个人信息保护法、行政处罚法等相关法律有机衔接，科学设置网络运行安全、网络信息安全等不同类型违法行为的法律责任。在完善不依法履行网络运行安全保护义务行为的法律责任方面，修正草案区分造成大量数据泄露、关键信息基础设施丧失局部功能等严重情形，以及造成关键信息基础设施丧失主要功能等特别严重情形，参照数据安全法有关规定，提高罚款幅度。

二十届四中全会： 提出“十五五”时期经济社会发展的主要目标

2025年10月20日至23日，中国共产党第二十届中央委员会第四次全体会议提出了“十五五”时期经济社会发展的主要目标：

高质量发展取得显著成效，科技自立自强水平大幅提高，进一步全面深化改革取得新突破，社会文明程度明显提升，人民生活品质不断提高，美丽中国建设取得新的重大进展，国家安全屏障更加巩固。

在此基础上再奋斗五年，到2035年实现我国经济实力、科技实力、国防实力、综合国力和国际影响力大幅跃升，人均国内生产总值达到中等发达国家水平，人民生活更加幸福美好，基本实现社会主义现代化。

国务院办公厅：

加强电子印章规范管理 服务政务活动和经济社会数字化发展

2025年10月9日，国务院办公厅发布《电子印章管理办法》要求加强电子印章规范管理，服务政务活动和经济社会数字化发展。《办法》要求，电子印章管理全过程应当建立完善的信息保护制度，采取必要措施确保电子印章相关信息的安全，并对收集的单位（组织）和个人的信息严格保密，防止未经授权的访问以及信息泄露、篡改或者毁损、丢失。电子印章相关信息系统的建设、使用和运行维护应当符合国家密码管理、网络安全、数据安全等相关法律法规和标准规范。涉及国家秘密信息的电子印章相关信息系统的建设、使用和运行维护，应当按照国家保密管理有关规定执行。

工信部、国家市场监督管理总局：

促进电子信息制造业稳定增长 提升产业链供应链韧性和安全水平

2025年9月4日，工信部、国家市场监督管理总局联合印发《电子信息制造业2025 - 2026年稳增长行动方案》，聚焦优供给、扩需求、强创新3方面部署了16项任务。

一是促进产业转型升级，深化构建高质量供给体系。推动电子整机高端化，提升产品供给水平；优化产业布局，改善产业结构；加强上下游对接，提升产业链协同水平；健全标准化工作机制，引领质量建设；强化知识产权保护，促进可持续创新。

二是促进国内外市场畅通经济循环，深挖需求潜力。扩大新场景，挖掘大众消费潜力；培育新业态，强化行业应用赋能；引导企业稳步走出去，深度嵌入国际体系；促进国际资源引进来，深化产业国际合作；促进国内国际双循环，稳妥应对国际贸易壁垒。

三是推动科技创新与产业创新融合，建设现代化产业体系。加快重大项目建设，强化撬动作用；强化集成攻关，保障产业链供应链安全稳定；加强基础技术研究，抢占前沿领域高地；强化企业主体地位，加快科技成果产业化；深入推动数字化转型，增强企业竞争力；强化人才资本支撑，夯实要素基础。

《方案》重点提出，要坚定不移推动“国货国用”，持续推动短板产业补链、优势产业延链、传统产业升链、新兴产业建链，加大对产业链关键企业的政策支持，提高企业根植性，强化关键核心技术攻关，提升重点产业链供应链韧性和安全水平。

国家市场监督管理总局等15部门：

强化网络和数据安全保护 加快推进质量认证数字化发展

2025年9月12日，国家市场监督管理总局、中央网信办、国家发展改革委、教育部、工信部、公安部、民政部、生态环境部、水利部、农业农村部、商务部、国家卫生健康委、中国人民银行、国家数据局、国家密码管理局15部门联合印发《关于加快推进质量认证数字化发展的指导意见》提出，要强化网络和数据安全保护。要推进网络关键设备和网络安全专用产品认证、网络安全服务认证，筑牢网络安全防护屏障。要推行信息安全管理等认证，提升企业信用和市场竞争能力。要积极开展数据安全管理和个人信息保护认证，探索实施个人信息保护合规审计、数据安全风险评估等服务认证，深化数据安全治理。要创新评价技术，推进商用密码认证体系建设，探索零信任、区块链和隐私计算等可信数字化认证。

住房城乡建设部等9部门：

强化网络安全防护 推进新型城市基础设施建设

2025年10月17日，住房城乡建设部、国家发展改革委、工信部、公安部、财政部、商务部、金融监管总局、国家数据局、国家消防救援局9部门联合印发《贯彻落实〈中共中央办公厅、国务院办公厅关于推进新型城市基础设施建设打造韧性城市的意见〉行动方案（2025—2027年）》，推进数字化、网络化、智能化新型城市基础设施建设。

《行动方案》提出，要推进数字家庭产品平台互联互通，推进与政务服务、社会化专业服务等相关平台对接，加强数据安全和个人隐私保护，推动编制通用技术要求及测试评估方法标准。要加强平台数据共享和安全保障，严格落实网络和数据安全法律法规和政策标准，加强设施设备、智慧应用和重要数据资源的安全管控，推动安全可控技术和产品应用。

国家能源局：

《能源行业数据安全管理办法（试行）（征求意见稿）》

强化网络安全要求

2025年9月10日，国家能源局向社会公开征求《能源行业数据安全管理办法（试行）（征求意见稿）》意见。《办法》规定，利用互联网等信息网络开展能源行业数据处理活动的，应落实网络安全等级保护、关键信息基础设施安全保护、密码保护和保密等制度要求。存储处理能源行业重要数据的信息网络应落实三级及以上网络安全等级保护要求；存储处理能源行业核心数据的信息网络，如涉及关键信息基础设施，应在网络安全等级保护制度的基础上，落实关键信息基础设施安全保护要求；不涉及关键信息基础设施的，应落实四级网络安全等级保护要求。法律法规和国家有关规定要求使用商用密码进行保护的，还应遵守商用密码保护有关规定。

党建引领科创路 精神传承启新程

WAPI产业联盟组织参观周恩来邓颖超纪念馆

WAPI产业联盟 周 园



为深化党建与科技创新深度融合，以红色精神赋能产业高质量发展，2025年10月17日，WAPI产业联盟组织20余家单位党员代表与核心技术骨干，赴周恩来邓颖超纪念馆开展“传承先辈精神 筑牢科创初心”主题党建活动，在沉浸式学习中汲取奋进力量。

作为我国无线网络安全领域的“创新排头兵”，WAPI产业联盟始终以“党建链激活创新链”为核心思路，将党建优势转化为产业创新的“硬实力”。

坐落于天津的周恩来邓颖超纪念馆，是全国爱国主义教育示范基地、全国廉政教育基地，更是传承红色基因、弘扬革命精神的重要阵地。馆内“人

民总理周恩来”“邓颖超——20世纪中国妇女运动的先驱”两大核心展区，以5000余件珍贵文物、3万余张历史图片及大量影像史料为依托，生动还原了两位伟人从天津爱国青年成长为坚定马克思主义者的光辉足迹：从五四运动中奔走呼号，到长征路上的风雨同舟；从建国后为国家建设殚精竭虑，到晚年仍心系人民的赤子情怀，全方位展现了他们为中国革命、建设和改革事业奉献终身的崇高精神，以及携手相伴、共赴使命的革命情谊。

活动中，同志们循着历史脉络，深入参观纪念馆核心展区。在“为中华之崛起而读书”主题展板前，大家驻足良久，结合联盟推动我国自主无线



网络标准从“跟跑”到“领跑”的历程，感怀先辈“实业救国、科技强国”的初心；在西花厅复原场景内，周恩来总理办公桌上的旧电话、邓颖超同志记录工作的笔记本等实物，让在场技术骨干深受触动——“总理深夜伏案工作的身影，和我们团队攻坚国际标准时连续熬夜调试代码的场景高度契合，这种‘功成不必在我’的坚守，正是我们需要传承的精神内核”，一位参与TRAIS协议研发的党员工程师感慨道。此外，在纪念馆“科技强国”专题展区，周恩来同志推动“两弹一星”等国家重大科技项目的史料，更让大家明确了“自主创新、保障国家信息安全”的使命担当。



在庄严肃穆的瞻仰厅，面对周恩来、邓颖超同志汉白玉雕像，全体党员举起右拳，齐声重温入党誓词，铮铮誓言回荡展厅，进一步坚定了“为共产主义事业奋斗终身”的理想信念，强化了作为科技工作者的责任与担当。

“此次活动不是简单的参观学习，而是联盟党建与科创工作的‘思想对标会’。”WAPI产业联盟秘书长表示。参与活动的会员代表也纷纷表示，将以此次党建活动为契机，把先辈的奋斗精神融入技术研发与产业服务中，让“红色基因”成为推动无线网络安全产业技术创新的“动力源”。



WAPI产业联盟组织观看抗战胜利80周年阅兵直播

凝聚科技报国力量筑牢网络安全防线

WAPI产业联盟 周园



2025年9月3日，是中国人民抗日战争暨世界反法西斯战争胜利80周年纪念日。WAPI产业联盟组织秘书处全员集中观看阅兵直播，在缅怀先烈中凝聚科技报国力量。

联盟会议室庄严肃穆，全员齐聚屏幕前。国歌奏响时，众人起身肃立高唱，充满对祖国的热爱与对历史的缅怀。受阅部队严整军容与先进装备依次亮相，展现出新时代军队实力与护和平决心，全员专注聆听解说。

当首次亮相的网络空间部队方队迈着坚定步伐受阅时，全员倍感振奋。作为解放军力量结构新布局的重要展示，这支部队的“赛博灰”军旗彰显“奋战无声、制胜无形”特质，让众人深切体会

到网络空间作为“第五作战域”的战略意义。在数字化浪潮席卷全球的今天，网络空间已成为继陆、海、空、天之后的“第五作战域”，其战略地位日益凸显，从关键信息基础设施防护到个人信息安全保障，从网络攻击防御到数字技术自主可控，网络安全已从单纯技术保障层面，上升为关乎国家主权、安全和发展利益的战略组成部分。

观礼后，联盟秘书长张璐璐组织研讨。秘书处同志们提出，要以阅兵为契机，深耕网络安全技术研发与标准推广，守护“数字边疆”。张璐璐表示，联盟将进一步深化党建与产业融合，汇聚力量突破核心技术，推动WAPI等标准在关键领域应用，以自主技术筑牢网络安全防线。

海淀区举办“世界标准日”主题活动

WAPI产业联盟携核心成果助力标准创新示范区建设

WAPI产业联盟 刘剑昕



图：WAPI联盟标准化成果展示

10月14日，北京市海淀区第56届“世界标准日”主题活动暨第四届标准创新大会举行，活动以“为建设世界领先科技园区贡献标准创新力量”为主题。WAPI产业联盟携无线网络安全标准化领域多项核心成果参展，通过实物陈列、互动交流等形式，全面展示标准成果转化与产业赋能实践成效，为海淀打造“标准创新示范区”注入强劲动能。

活动现场，WAPI产业联盟重点展出近期通过联盟实验室检测的代表性产品，覆盖网络核心设备、终端模组、行业传感器等全产业链环节，直观体现标准化对产品质量的刚性保障作用。其中，WAPI 2.0系列网络核心设备，展现了技术在高速率、高安全场景下的最新突破；丰富的WAPI终端模组，可充分满足数字化、信息化领域对安全无线局域网的应

用需求；多款通过标准符合性测试的行业传感器，构建起面向工业互联网的安全感知终端集群，为关键行业信息传输安全提供保障。据介绍，2025年上半年，联盟测试实验室依据T/WAPIA 046《无线局域网安全技术规范》等标准，紧跟技术标准演进步伐完成两轮测试项优化升级，进一步提升测试精度与颗粒度，精准匹配市场对产品安全性能的高标准要求。

交流中，联盟向与会嘉宾系统介绍了从标准研制到产业落地的全流程支撑能力。联盟始终以构建自主可控的无线网络安全标准体系为核心目标，经多年实践形成“标准制定→技术研发→检验检测→产业推广”创新闭环；截至2025年三季度，累计发布（获发布）国际标准23项、国家标准46项、欧洲标准3项、行业标准7项、团体标准100余项，构建起多层次、广覆盖的标准体系；已为超过150家企业提供专业测试测评服务，推动数百款产品标准化落地，加速安全无线局域网技术在各行业规模化应用。”

作为扎根海淀、服务全国的社会组织，WAPI产业联盟此次参展，是响应海淀区“科技创新-标准转化-产业应用”全链条建设号召的具体行动。下一步，联盟将持续依托“海淀标准化公益赋能团”平台，为辖区企业提供标准创制、测试测评等服务，助力更多创新成果通过标准化实现产业化落地，为海淀建设世界领先科技园区贡献力量。

无线网络安全标准化工作委员会2025年第三次主任委员会议（总第14次）顺利召开

WAPI产业联盟 刘婷



图：会议现场

2025年10月12日，无线网络安全标准化工作委员会2025年第三次主任委员会议在北京召开。标委会主任委员曹军主持会议，副主任委员王立建、王宏、陶洪波、张璐璐、黄振海，联盟秘书处标准化部负责同志出席会议。

会上，与会人员围绕2025年第三季度工作要点、2025年标委会重点工作落实阶段总结、联盟未来重点工作和方向等议题进行报告与讨论。

联盟标准化部总监刘婷报告了2025年第三季度工作要点。依据标委会《2025年重点任务计划》及2025年第二次标准工作和项目组会议决议，各项工作稳步推进，在标准制定、标准实施、标准平台和生态等方面均取得积极进展。

在标准制定层面，联盟共组织推进24项团体标准，其中新立项5项，9项即将进入报批阶段。新发布T/WAPIA 010.3—2025《信息技术 系统间远程通

信和信息交换 局域网和城域网 特定要求 第11部分：
无线局域网媒体访问控制和物理层规范 第3号修改
单：管理帧保护技术规范》和T/WAPIA 007.11—
2025《无线局域网产品工程化实现指南 第11部分：
WAPI与IEEE 802.11be》2项团体标准。

在标准实施层面，联盟于9月发布《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》，为工业场景技术选型提供
专业指引；开展“针对AE驻留位置启动WAPI瘦AP
产品重新测试专项”并推出鼓励政策，助力厂商提
升产品质量，多家企业已申请免费复测。

在标准平台建设层面，2025年第二次标准工作及
项目组会议顺利召开；9月增补3名委员后，标委会
委员总数达90名。

在标准生态环境层面，联盟再度获评北京市5A

级社会组织，连续第15年通过GB/T 19001-2016 idt
ISO 9001:2015质量管理体系认证评审。7月举办的高
质量无线局域网创新应用大会，通过成果展示与技
术交流破解产业发展难题，目前WAPI技术已在电力
输电场景实现突破并于南网展开试点示范。积极参
加国家标准、行业标准制定，推动GB 15629.11系列
标准纳入规范性引用。

标委会总体工作组（WG 1）黄振海汇报2025年
重点工作落实情况时表示，年初确定的12项重点任务
均按计划推进，后续将持续优化标准化管理制度，完
善WAPI标准体系被引用的信息汇总与处理流程。

与会主任委员、副主任委员对上述工作给予高
度评价，强调要持续聚焦网络安全国家战略需求，
发挥标委会平台作用，为我国网络空间安全保障提
供坚实支撑。

联盟标委会队伍持续壮大 为标准创新发展注入新动能

WAPI产业联盟 陈博

2025年前三季度，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（以下简称“标委会”）专业队伍持续壮大，邱勇、刘婷、江涛、黄琪、郑崇剑、董治江6位同志通过审查正式履职，标委会委员总数增至90人，为我国无线网络安全领域标准创新发展注入新动能。

作为无线网络与网络安全领域的专业技术标准组织，该标委会主要承担WAPI产业联盟团体标准起草、技术审查、推广实施等工作。自成立以来，标委会已组织制定、发布107项团体标准，其中近20项成功转化为国家标准，多项入选工信部百项团体标准应用示范项目。这些标准既有效补充了国家标准

与行业标准体系，又因快速响应市场需求、解决产品开发与应用中的实际问题，被市场建设方与用户广泛采信，成为构建高质量安全无线局域网的重要支撑。

此次新增的6名委员均来自行业核心单位，覆盖运营商及行业用户、芯片研发、设备制造、终端等关键环节。进一步完善了标委会的专业结构与产业代表性。专家的持续加入，不仅夯实了标准化工作的人才根基，更彰显了标委会开放共赢的合作理念。

未来，标委会将继续秉承公平、公正、开放的原则，凝聚产学研用创新力量，为无线网络和网络安全标准创新与发展提供有力支撑。



图：新加入标委会的专家委员

博洛米WAPI系列终端通过联盟测试

WAPI产业联盟 王立华



图：博洛米WAPI模块A0203-M4GX和WAPI无线网卡B0821A

2025年9月12日，南京博洛米通信技术有限公司（以下简称博洛米）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。

本次测试通过的两款WAPI终端产品分别为：WAPI模块（型号：A0203-M4GX）和WAPI无线网卡（型号：B0821A），支持WAPI协议、支持2.4/5GHz双频接入，通信速率支持802.11ac协议。

据博洛米介绍，WAPI模块A0203-M4GX已实现100%国产化，通过了工信部五所电子元器件清单评估，采用标准mini-PCIE结构，可扩展支持千兆网口、USB、UART等接口，能通过任一接口与其他设

备/机具连接，使其快速具备WAPI功能。同时支持“双发选收”，可实现快速切换功能。WAPI无线网卡B0821A符合SJ/T 11940-2024、SJ/T 11942-2024、SJ/T 11943-2024、SJ/T 11944-2024等行业标准，已适配飞腾、龙芯、兆芯、海光等国产CPU和统信、麒麟、鸿蒙等国产操作系统，可广泛应用于信创电脑市场。

博洛米表示，目前公司已有多款终端/模组通过联盟测试，包括：WAPI CPE终端A0203-C、B0801A-PH；WAPI模块A0203-M、M0804C、M0804C-PH。未来将进一步丰富WAPI终端产品种类，完善解决方案体系，满足数字化和信息化领域对安全无线局域网的应用需求。

北京数字认证WUAS-A4000鉴别服务器通过联盟测试

WAPI产业联盟 王立华



图：北京数字认证全国产鉴别服务器WUAS-A4000

2025年10月14日，北京数字认证股份有限公司（以下简称数字认证）的鉴别服务器通过了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、功能及性能测试。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。

通过测试的鉴别服务器型号为WUAS-A4000，配置上采用角色管理设计，支持漫游功能，鉴别性能达到500次/秒以上。能够满足目前行业高并发、移动性、大连接的应用需求。

据数字认证介绍，WUAS-A4000实现了全国产，采用角色管理设计，可清晰划分证书签发、系统管理及审计等权限，同时支持无线接入点（AP）与终端（STA）数字证书的分组管理，仅允许同组内终端接入对应网络，为行业用户提供灵活的分域安全管控能力。

数字认证表示，公司深耕网络安全领域20余年，始终以密码技术为核心推进国产化产品研发，未来将持续优化产品性能，为数字化领域构建自主可控的安全无线局域网提供技术支撑。

南方电网推进贵州WAPI建设

【根据网上公开信息整理】

南方电网继广西南宁500千伏民歌变电站建成首个WAPI示范站之后，正将贵州作为后续试点，逐步复制“综合数据网+WAPI延伸”的通信模式。尽管具体项目投运信息尚未完全公开，但结合行业趋势和历史试点经验，预计2025年底前将有更多变电站完成WAPI网络部署，为数字电网建设提供安全、高效的通信支撑。

据2025年7月至10月的公开信息显示，南方电网在贵州地区的WAPI应用主要聚焦于设备采购、技术研发及试点项目推进。

在WAPI设备采购与招标落地方面：2025年7月4日，贵州电网有限责任公司发布《物资类（WAPI网络设备、主站端二次安防其他装置等）公开招标公告》，明确采购WAPI网络设备、通信网管安全防护设备等。该项目涉及18个标的、28个标包，重点覆盖变电站无线通信安全需求。招标范围：包括AS鉴别服务器、AC接入点控制器、AP无线接入点等核心设备。2025年8月7日，项目中标候选人公示发布，标志着WAPI设备采购进入实施阶段。这次招标是贵州电网继2021年在贵阳席官变、万松变试点WAPI后，进一步扩大技术应用的重要举措。通过构建高安全无线网络，贵州电网将解决变电站“最后一公里”设备接入问题，支持巡检机器人、无人机等智能终端的可靠运行。

在技术研发与创新项目推进方面：开展基于WAPI的智能压板采集系统研制，2025年7月7日，超高压输电公司贵阳局启动职工创新项目，研发“基于WAPI无线局域网的智能压板采集系统”，计划于10月30日前交付，该系统旨在实现变电站保护压板状态的自动采集与远程监控，结合WAPI的双向认证机制，提升二次设备运维的安全性和效率。促进技术融合，项目重点研究WAPI协议与压板采集技术的适配性，解决复杂电磁环境下的通信稳定性问题，为后续规模化应用提供技术储备。

智芯公司荣获第二十五届中国专利金奖

【智芯公司】



2025年10月13日，第二十五届中国专利奖颁奖大会在大连举行。北京智芯微电子科技有限公司发明专利“用于制备高压LDMOS器件的方法及器件”获第二十五届中国专利金奖。

该专利打破了电力高耐压电源和隔离芯片中关键LDMOS器件的技术壁垒，攻克了LDMOS器件的高耐压、长寿命和高良率核心技术，关键性能指标国际领先，保障了电力芯片在强电磁环境下可靠运行。基于专利研制的芯片产品已获得广泛应用，为助力我国新型电力系统建设作出积极贡献。

中国专利奖是我国授予发明创造的最高科技奖励，由世界知识产权组织与国家知识产权局共同授奖。

鼎信通达无线语音通信系统专利获授权

【电通信技术专利快讯】

2025年10月21日，深圳鼎信通达股份有限公司的“无线语音通信系统、方法、设备及存储介质”专利正式进入专利权的授权阶段，该专利涉及无线语音通信中的跨接入点漫游认证场景，通过状态同步控制器缓存WAPI认证信息并同步至分布式状态缓存集群，实现跨AP的认证状态快速加载。

天宽科技打造电力行业智能巡检新标杆

【天宽科技】

2025年9月19日，天宽科技携手昇腾与云深处，面向全球首次发布以WAPI为通讯基础的“基于昇腾软件栈打造的全国产化AI智能巡检解决方案及行业算力库”。

基于昇腾软件栈的全国产化AI智能巡检解决方案，依托天宽科技AI智能算法，搭载华为昇腾提供的算力平台及CANN异构计算框架，并对云深处新一代具身智能四足机器人进行各类传感硬件加装改造。其中异构计算框架 CANN更是大幅加速智能分析速度，显著提升硬件工作效率，最终实现对电力设备的全流程智能化管理。该方案采用国产化华为无线WAPI进行高密度组网，构建低延时、高可靠的无线网络，支持机器人智能漫游与抗干扰通信。巡检数据经边缘节点预处理后，通过安全通道高效汇聚至后台，保障数据稳定回传与集中管理。

据介绍，该方案已落地某大型换流站，成效显著：人工巡检工作量大幅减少，巡检效率较此前提升约3倍；AI算法精准定位故障，助力客户每年停电事故率下降30%；智能平台实现巡检数据集中管理，推动应急响应与维修效率提升20%，为电力行业智能化巡检树立标杆。除巡检方案外，天宽科技还拥有包括智能消缺工具、无源外骨骼机器人、移动作业终端在内的辅助装备体系，为电力作业人员提供更安全、更高效的保障，形成了“巡检+作业+平台”的全链条能力闭环。



WAPI技术赋能遨游三防手机 “危急特”场景信息安全升级

【遨游通讯】

在无线通信技术飞速发展的今天，网络安全已成为不可忽视的核心议题。遨游通讯作为“危、急、特”场景智能设备及解决方案服务商，将其工业三防手机与中国自主研发的无线局域网安全标准WAPI深度融合，为高安全性需求的领域提供了可靠的技术保障。WAPI是中国在网络安全领域自主创新的安全接入技术标准，其采用双向认证加密机制，有效防范了非法接入、数据窃取和网络监听等安全威胁。

遨游三防手机本身具备卓越的物理防护能力，通过IP68/IP69K防尘防水认证及MIL-STD-810G军工标准测试，能够在极端环境下稳定运行。在集成WAPI技术标准后，其安全性能得到了进一步升级。WAPI的安全机制包含无线局域网鉴别（WAI）和保密基础结构（WPI）两部分：WAI采用公钥证书体系，实现对终端和设备端的双向身份鉴别；WPI则采用国家密码管理局批准的SM4分组密码算法，对传输数据加密保障完整性和保密性。这种架构从根本上解决了传统Wi-Fi协议中单向认证机制的安全缺陷，显著提升了通信过程的安全性。

在实际应用中，遨游三防手机WAPI功能可广泛应用于能源行业、应急救援、电力等对网络安全要求极高的场景，通过WAPI网络进行安全认证和高速数据传输，无论是上传现场采集的敏感数据，还是接收指挥中心的加密指令，整个通信过程都得益于WAPI的强加密特性，避免了信息泄露或被篡改的风险。例如在石化行业，利用WAPI的可鉴别机制和保密传输，能够有效保护生产控制指令和数据采集信息的安全。

此外，WAPI的快速漫游能力也优化了遨游三防手机在不同接入点间的切换体验，为移动办公和工业巡检提供了连续稳定的安全连接。遨游三防手机已构建起一套适应复杂环境的综合解决方案，为构建自主可控、安全可靠的网络基础设施提供了重要支撑。



中科鸿略发布开源鸿蒙WAPI解决方案

【中科鸿略】

在数字化转型持续深入的今天，网络安全已成为行业系统稳定运行的前提。面对政府、国企、金融、军工等关键领域对无线通信安全日益严格的要求，北京中科鸿略科技有限公司（以下简称“中科鸿略”）推出开源鸿蒙支持WAPI的行业解决方案，以自主可控的技术路线，为行业用户构建高安全、可信赖的无线网络通信环境。

中科鸿略基于开源鸿蒙系统进行深度集成与适配，实现WAPI协议在鸿蒙平台上的完整落地。目前WAPI正逐步被政务系统、国有企业、金融行业以及军工单位所采用，成为中国网络空间安全的重要支撑。中科鸿略始终坚持“安全优先、生态共建”的技术路线，通过与开源鸿蒙、WAPI等国产技术的深度融合，打造真正自主、安全、可用的网络解决方案。



高通发布第五代骁龙8至尊版移动平台 支持WAPI

【高通】

2025年9月24日，高通技术公司发布第五代骁龙8至尊版移动平台，支持WAPI（无线局域网鉴别与保密基础结构）。

第五代骁龙8至尊版移动平台旨在提升用户对移动终端的核心期待体验，包括：极速的多任务处理和流畅的应用切换，持久的游戏时长，兼具卓越性能和能效表现。骁龙8系移动平台赋能个性化智能体AI助手，可以跨应用为用户提供定制化操作。通过持续的终端侧学习和实时感知，多模态AI模型能够深度理解用户，实现主动推荐和基于情境的提示优化——同时确保用户数据始终存放在终端设备上。

据悉，中兴、Xiaomi、vivo、索尼、三星、ROG、红魔、REDMI、realme、POCO、OPPO、一加、努比亚、iQOO和荣耀等全球OEM厂商和智能手机品牌将在其旗舰产品中采用第五代骁龙8至尊版，全新终端即将陆续面市。

联发科发布天玑9500移动芯片 支持WAPI

【联发科】

2025年9月22日，MediaTek（联发科）发布天玑9500旗舰级移动芯片，支持WAPI（无线局域网鉴别与保密基础结构）。

天玑9500作为迄今为止天玑最强大的移动芯片，采用了业界先进的第三代3纳米制程，集成了强力焕新的全大核CPU、GPU、NPU、ISP图像处理器等高算力单元，在端侧AI、专业影像、主机级游戏体验以及网络通信等方面开启领航未来的全面跃升。

据悉，首批采用MediaTek天玑9500芯片的智能手机将于2025年第四季度上市。

神州数码入围中国企业500强与战略性新兴产业领军企业

【神州数码】

近期，中国企业联合会、中国企业家协会发布“2025中国企业500强”及“2025中国战略性新兴产业领军企业100强”榜单，神州数码位列中国企业500强第211位，并在战略性新兴产业领军企业100强榜单中排名第37位。

据悉，今年的榜单以2024年企业营业收入为依据。数据显示，“500强”企业全年实现营业收入110.15万亿元，入围门槛提升至479.6亿元，营收超过千亿元的企业数量增至267家，占比已超过一半。同时，入围企业平均研发强度连续八年提升，2024年达到1.95%的新高。

数字认证获CNVD

“2024年度原创漏洞发现贡献单位”荣誉称号

【数字认证】

2025年9月16日，数字认证旗下子公司北京安信天行科技有限公司荣获2024年度国家信息安全漏洞共享平台（CNVD）“2024年度原创漏洞发现贡献单位”称号。

2024年，数字认证以攻防实验室为核心技术枢纽，深度聚焦安全漏洞挖掘、威胁情报研判、应急响应处置以及攻防技术前沿探索，时刻关注网络安全态势变化，积极承担CNVD技术支撑工作，通过自主创新的漏洞挖掘技术以及科学严谨的分析方法，及时发现并报送高质量原创安全漏洞。这些漏洞的精准捕获与及时上报，不仅有效阻断了相关产品及系统的安全风险传导路径，更切实筑牢了用户网络运行安全与数据安全的防护屏障，为维护国家网络空间安全提供了有力支撑。



浅析WAPI 2.0中的身份信息保护机制

本文由无线网络安全技术国家工程研究中心供稿

作为新一代无线局域网安全协议，WAPI 2.0在适配SM2/SM3并持续沿用SM4国密算法基础上，新增WAI增强协议、快速切换机制及身份信息保护等关键技术，大幅提升了抗离线字典攻击与抗量子计算攻击的能力。其中，身份信息保护机制通过密码技术，确保用户身份仅在WAPI鉴别过程中参与实体间受控传递，从根源上杜绝攻击者窃听报文获取身份、追踪用户行为的可能。

一、背景：身份信息保护成为网络安全核心需求

传统信息安全聚焦数据的机密性（不被非授权访问）、完整性（不被篡改）、可用性（能持续服务）等基础维度，以系统和流程保护为核心，致力于防止非授权访问和数据篡改。随着数字经济与社会生活深度融合，身份信息保护已从后台支撑性需求升级为战略性核心需求——身份证号、生物特征等关联法律主体的信息，成为数字空间最具价值的资产，也是攻击者窃取交易的主要目标。

这一转变下，安全防护从“保护系统中的数据”扩展至“保护作为数据主体的人”。身份信息保护也超越了传统机密性范畴，成为独立的保护维度。例如国家推广的基于芯片信息的“网证”（如CTID），通过生成仅包含必要属性的二维码，让验证方仅获“鉴别是否成功”的结果，实现身份信息“可用不可见”；公众对身份保护意识也显著提升，电商平台“防窥证件卡套”的流行，正是防范公共场所身份信息被窥视的体现。

身份信息泄露的危害已十分明确：深圳某银行曾发生客服偷拍客户信息，同伙用假证、手机号猜测网银密码，盗取30余万元存款的案件，凸显身份信息全程防护的紧迫性。

二、身份信息保护的核心作用

1、升级用户隐私保护

(1) 防范身份信息滥用：传统鉴别需提供完整身份信息（用户名、密码或证书等），一旦泄露易引发：

- 金融盗窃：攻击者直接盗取账户资金。
- 社会工程攻击：利用身份信息实施精准诈骗。
- 隐私曝光：敏感个人信息被非法出售。

身份信息保护机制应遵循“最小化信息披露”原则，在鉴别过程中仅传递权限等级等必要属性，从源头降低风险。

(2) 抵御追踪与行为分析：通过匿名鉴别技术隐藏真实身份，实现“不可链接性”，阻断互联网环境中

通过身份关联建立用户画像的隐形追踪。

2、强化网络系统安全

(1) 防御主动攻击：通过加密技术隐藏身份信息，让攻击者难以发起中间人攻击（无法冒充服务端窃密）、重放攻击（难以伪造鉴别数据）。

(2) 降低被动窃听威胁：身份信息保护机制对鉴别过程中所有敏感数据加密，即使通信流量被窃听，也无法获取有效身份信息。该特性在金融、政务等高安全需求场景中尤为关键。

三、WAPI 2.0如何实现身份信息保护

身份鉴别与密钥协商作为网络安全的核心，需同时保障“身份真实”与“会话安全”。WAPI 2.0通过系统化的身份信息保护机制，实现身份信息“防泄露、防滥用、防追踪”。

1、核心保护目标

- (1) 隐私性：通信双方身份信息不被第三方窃取。
- (2) 不可链接性：避免不同会话中的身份信息被关联追踪。
- (3) 抗流量分析：隐藏通信特征，降低身份推测风险。
- (4) 延迟披露：在符合条件的情况下尽可能推迟披露身份信息，防止身份过早暴露。

2、关键技术实现

(1) 延迟身份信息暴露：将身份信息传输推迟至鉴别协议后期。例如WAPI 2.0中，身份信息仅在密钥加密方案协商完成后才传递，IKEv1主模式在最后阶段通过加密方式传输身份信息。这些均确保了协议初期数据安全，避免攻击者通过早期数据推测真实身份。

(2) 加密传输身份信息：通过两种加密技术保障身份信息传输安全：一是用协商的会话密钥做对称加密，二是通过接收方公钥做非对称加密。在WAPI 2.0中，证书及身份信息均采用公钥加密技术传输，彻底阻断未授权解密风险。

四、总结与展望

随着数字化加速，身份信息保护已成为网络安全的“必选项”。既要确保身份验证有效，又要防止敏感信息泄露，在隐私保护、安全升级、合规满足中发挥关键作用。

在无线局域网领域，WAPI 2.0从设计阶段就集成身份信息保护机制，通过密码技术实现身份“受控传递+延迟披露”。这一设计不仅满足当前无线局域网的安全需求，更能适配未来进阶场景，为构建可信数字环境筑牢技术基础。

关于WAPI 2.0技术演进

2000年，为弥补无线局域网（WLAN）国际标准ISO/IEC 8802-11存在的严重安全缺陷，中国业界在多年技术积累基础上，自主研发提出了全新的安全架构和WLAN安全协议——WAPI（无线局域网鉴别与保密基础结构），2003年被采纳入国家标准GB 15629.11/1102。WAPI所基于的三元对等安全架构，较之ISO/IEC 8802-11所基于的二转三元过渡架构具有显著技术优势，解除了接入点缺乏独立鉴别身份、依赖于与网络服务器额外建立安全传递通道，无法直接实现与终端的直接双向鉴别等安全隐患。GB 15629.11/1102标准的发布，标志着WAPI 1.0技术标准体系的形成。后续八十余项国家、行业、团体标准陆续得到发布，WAPI 1.0技术标准体系不断完善，联盟测试实验室的产品和系统测试项目，演进四个版本，持续支撑着产业创新发展。

随着量子技术的快速发展以及商业化进程的加快，采用传统密码算法的网络安全协议体系正面临重大挑战，因此亟需构建并完善WAPI 2.0技术标准体系，为无线局域网提供抗量子攻击能力。同时，SM2、SM3国密算法的发布，也使无线局域网在身份信息保护、抗离线字典攻击等方面产生了新的安全需求，这些需求亟待WAPI 2.0技术标准体系中得到响应与规范。

基于上述，WAPI产业联盟于2021年12月发布了T/WAPIA 046《无线局域网安全技术规范》。该团体标准在适配SM2和SM3并持续沿用SM4的基础上，新增了WAI增强协议、身份信息保护、快速切换机制等适配选项，进一步强化了密码算法强度、抗离线字典攻击及抗量子计算攻击等安全性能，可满足当前及未来对无线局域网安全技术与应用的新需求。

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>