

在路上

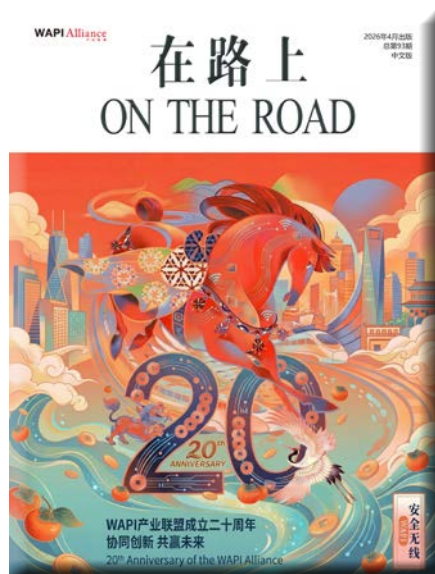
ON THE ROAD



WAPI产业联盟成立二十周年
协同创新 共赢未来

20th Anniversary of the WAPI Alliance

安全无线
WAPI



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：staff@wapia.org

网 站：http://www.wapia.org.cn

公众号：



WAPI产业联盟公众号

主编寄语 Opening Congratulations

05 同心聚力 再启新程——庆WAPI产业联盟成立二十周年

媒体聚焦 Media Focus

- 06 新华社、学习强国等：我国一项物联网安全协议测试技术成为国际标准
- 10 中国信息化周报等：WAPI产业联盟发布新版功能测试项目 强化IPv6协议能力测试
- 12 中国信息化周报等：抽水蓄能领域WAPI终端电力物模型团体标准正式发布
- 14 通信世界等：WAPI产业联盟召开2026年第一次标准工作和项目组会议（总第137次）
- 17 中国标准化等：WAPI产业联盟发布5项《无线局域网产品工程化实现指南》团体标准
- 19 飞象网等：WAPI产业联盟发布新版无线局域网设备测试方法标准

联盟关注 Alliance Concerns

21 联盟发布《WAPI市场应用洞察报告——分层筑防：点到点与端到端安全共筑》

WAPI 问答 WAPI FAQ

27 WAPI问答（系列连载）第十八部分（PART 18）

产经要闻 Industrial & Economic News

- 30 李强：统筹发展和安全 全面推进人工智能高质量发展
- 30 丁薛祥：加快建设科技强国 实现高水平科技自立自强
- 31 国务院：提升产业链供应链韧性和安全水平
- 31 阴和俊：统筹发展和安全 加快高水平科技自立自强
- 32 “十五五”规划纲要：提升网络安全保障能力
- 32 全国网信办：锚定网络强国战略目标 全面做好网络安全和信息化工作
- 32 工信部等九部门：加快多网融合进程 推动物联网产业创新发展
- 33 工信部等五部门：强化网络和数据安全保障 支撑低空基础设施发展
- 33 国家发展改革委、国家能源局：强化网络与数据安全防护 促进电网高质量发展
- 33 国家金融监管局：强化网络安全防护 加快数字金融高质量发展
- 34 科技部等四部门：加快推动网络安全保险创新应用
- 34 工信部：健全互联网交换中心监管制度 提升安全防护能力

联盟工作 Alliance Work

- 35 党建引领强根基 守护文脉促创新——WAPI产业联盟组织参观响堂山石窟研究院
- 36 WAPI产业联盟举办成立20周年公益植树暨访石经山悟初心主题党日活动
- 38 中关村论坛发布WAPI产业联盟标准化创新成果案例
- 39 以视频化解读助力标准应用：WAPI产业联盟持续完善团体标准宣贯载体
- 40 无线网络安全标准化工作委员会2026年第一次主任委员会议（总第16次）顺利召开
- 41 华为三款WAPI无线接入点通过联盟测试
- 42 东和阳光三款WAPI产品通过联盟测试
- 43 久壬科技WAPI系列产品通过联盟测试

新成员 New Member

- 44 四川东和阳光科技有限责任公司加入WAPI产业联盟

成员与市场 Member & Marketing

- 45 国网新疆信通公司率先完成国网系统内首套隔离WAPI装置测试
- 46 一芯未来WAPI鉴别服务器AS：为部队仓储无线认证筑牢安全高效基石
- 47 鼎信通达申请基于WAPI安全接入的SIP快速重注册方法及系统专利
- 47 广东信通通信申请基于WAPI通信的空调负荷调控方法专利
- 48 联盛德：旗下盛德创信正式投产
- 48 数字认证：构建密码保障体系 筑牢电力信创安全防线
- 49 数字认证入选“2026年网络安全国家标准应用实践案例”
- 50 博洛米第三代高性能WAPI通信模块量产
- 51 国安部提醒：注意词元（Token）使用带来的安全风险
- 53 伊朗中部遇袭期间该国美制通信设备集体“失灵”

产业技术论坛 Industry & Technology Forum

- 54 指标实测 场景适配——WAPI 2.0-1DN示范网取得阶段成果

同心聚力 再启新程

庆WAPI产业联盟成立二十周年

2026年3月7日，WAPI产业联盟迎来成立二十周年。在此谨向长期关心支持联盟发展的各级主管部门，向各会员单位、合作伙伴以及每一位为标准与产业发展倾注心力的同仁，致以诚挚的感谢与崇高的敬意！

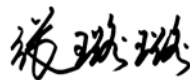
二十年来，联盟与产业链上下游同向同行，聚焦无线网络与网络安全领域协同创新，持续推进标准创制、技术研发、测试验证、成果转化与生态培育，逐步形成面向产业、面向应用、面向安全的体系化能力与实践积累。一路走来，既有携手探索的艰辛，也有合作突破的欣喜。我们始终相信：以安全筑牢底线，以标准凝聚共识，以协同创新与产业共建实现共赢，方能行稳致远。

当前，国家发展进入统筹发展和安全并重的新阶段。面对数字化、智能化、融合化加速演进的新形势，以及新一轮科技革命和产业变革带来的挑战与机遇，联盟将继续与各方一道，紧扣科技创新、产业创新与安全保障等战略部署，坚定走自主创新之路。

联盟将以“共建高质量安全无线局域网”为目标，坚持体系观念与问题导向相统一，持续完善标准体系和协同机制，推动关键技术与标准协同演进，加快将创新成果转化为现实生产力，提升安全保障能力和产业综合竞争力。同时，我们将更加关注应用落地与用户体验，让安全不仅“可用”，更“好用、易用、放心用”，让每一次连接都更可靠、更值得信任。

联盟建设从来不易，既需胸怀大局、甘于奉献，也需以专业立身、守正创新，更需久久为功的耐心与韧性。二十载再出发，我们愿继续与各方携手并肩、同心聚力、再谱华章，为网络强国、科技强国建设贡献更加坚实的产业力量！

WAPI 产业联盟 秘书长



2026年3月6日

新华社、学习强国等：

我国一项物联网安全协议测试技术成为国际标准

【编者按】2026年3月9日，我国提出的物联网安全协议测试技术（TRAIS-P TEST）提案获批成为国际标准。这是我国在物联网安全技术领域取得的又一项拥有自主知识产权的国际标准，也是深入实施网络强国战略、加强关键领域自主创新、发展新质生产力的重要成果。西电捷通公司、无线网络安全技术国家工程研究中心作为上述8项国际标准的主要技术贡献者，联合WAPI产业联盟、商用密码检测认证中心、国家无线电监测中心检测中心、国网山东省电力公司、北京市标准化研究院等十余家联盟成员及相关单位共同参与标准研制。相关成果引发国内外广泛关注，新华社、学习强国、人民网、新华网、光明网、环球网、中国网新闻中心、中国科技网、中国高新闻网、澎湃新闻、海外网等媒体相继报道。之后，通信世界、飞象网、中国信息化周报等行业媒体也对此事进行了深度报道。

以下是新华社的报道：



（新华社记者 刘羽佳）记者日前从WAPI产业联盟获悉，一项由中国提出的物联网安全协议测试技术（TRAIS-P TEST）提案，已被国际标准化组织（ISO）和国际电工委员会（IEC）联合发布成为国际标准。这是我国在物联网安全技术领域又一项拥有自主知识产权的国际标准。

当前，射频识别（RFID）技术已广泛应用于智能制造、物流仓储、医疗、电子支付等领域。TRAIS-P国际标准规范了有源RFID系统的空中接口安全防护方法，能够提供实体鉴别、安全通信等高等级安全服务，有效防范身份伪造、数据窃听与篡改等风险。本次发布的TRAIS-P TEST作为配套测试规范，明确了空中接口安全协议实现的一致性测试方法，便于对产品安全能力进行客观验证。

“至此，从技术规范到产品测试两个层面形成了完整的国际标准体系。”WAPI产业联盟秘书长张璐璐表示，此前我国在RFID、NFC等短距离通信安全领域已累计有7项包含自主技术的国际标准。加上此次发布的测试规范，共同构成物联网安全关键技术标准体系，有助于推动全球物联网的互联互通与共享共治。

据了解，西电捷通公司、无线网络安全技术国家工程研究中心是上述8项国际标准的主要技术贡献者。WAPI产业联盟、商用密码检测认证中心、国家无线电监测中心检测中心等10余家联盟成员参与了标准研制工作。

“20多年来，我们持续投入技术研发与标准制定，坚持以可信赖的安全技术应对全球网络安全挑战。”西电捷通公司董事长曹军说，“我们将继续深耕核心技术，与全球伙伴共享创新成果，助力构建安全可信的数字世界。”

以下是通信世界的报道：

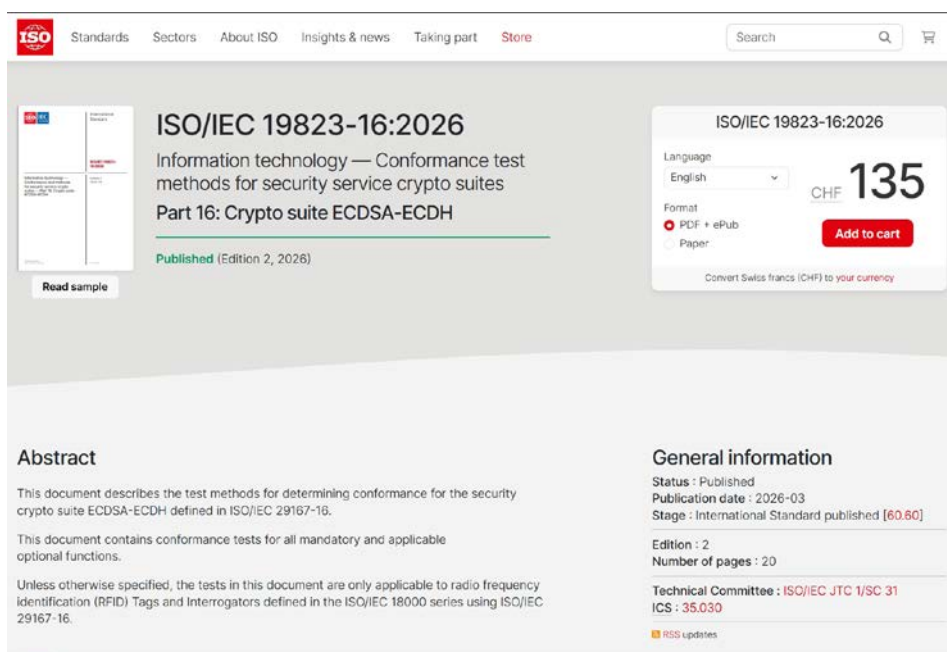


日前从WAPI产业联盟获悉，一项由中国研发的物联网安全协议测试技术（TRAIS-P TEST）提案，已被国际标准化组织（ISO）和国际电工委员会（IEC）联合发布成为国际标准。这是我国在物联网安全技术领域又一项拥有自主知识产权的国际标准，也是深入实施网络强国战略，加强关键领域自主创新、发展新质生产力的重要成果。该标准的起草单位包括：西电捷通公司、WAPI产业联盟、国家无线电监测中心检测中心、国网山东省电力公司、北京市标准化研究院。

射频识别（RFID）是一种非接触式信息传递技术，通过无线电波实现对目标物体的自动识别和数据采集，已广泛应用于智能制造、物流仓储、医疗、航空及电子支付等领域。随着万物互联规模扩大，RFID系统安全风险也日益凸显，建立统一的安全防护规范，已成为确保产业健康发展的重要前提。

据介绍，TRAIS-P国际标准规范了有源RFID系统的空中接口安全防护方法，能够提供实体鉴别、安全通信等高等级安全服务，有效防范身份伪造、数据窃听及篡改等风险。本次发布的TRAIS-P TEST作为配套测试规范，明确了空中接口安全协议实现的一致性测试方法，便于对产品安全能力进行客观验证。至此，从技术

规范到产品测试两个层面形成了完整的国际标准体系，为全球物联网安全治理提供了中国方案。本次发布的 TRAIS P TEST 国际标准为该标准 2020 年首次发布后的第二版，两个版本均采纳中国自主技术，充分体现了中国自主技术的先进性与稳定性。



图：ISO网站截图—ISO/IEC 19823-16:2026发布

WAPI产业联盟秘书长张璐璐表示，全球RFID应用正由单一的供应链追踪工具加快向全链路数字化基础设施演进，其对工业现场、智慧医疗等场景深度应用的支撑作用日益凸显。随着具身智能和AI在上述场景加速落地， TRAIS-P等标准正成为不可或缺的组成部分，它虽不负责AI的“思考”，却作为底层防线确保了系统“感知的是真相”，为AI时代的物理世界交互奠定信任基石。她说，此前我国在RFID、NFC等短距离通信安全领域，已累计有7项包含自主技术的国际标准。加上此次发布的测试规范，共同构成物联网安全关键技术标准体系，有助于推动全球物联网的互联互通与共享共治。

据了解，西电捷通公司、无线网络安全技术国家工程研究中心是上述8项国际标准的主要技术贡献者，已按照国际规则就持有的标准必要专利向全球作出“公平、合理和非歧视”（FRAND）许可声明。

西电捷通公司董事长曹军说：“20多年来，我们持续投入技术研发与标准制定，坚持以可信赖的安全技术应对全球网络安全挑战。此次国际标准的发布是新的起点，下一步，我们将继续深耕核心技术，与全球伙伴共享创新成果，助力构建安全可信的数字世界。”

部分媒体新闻链接:

新华社: <https://h.xinhuanet.com/vh512/share/13006194?docid=13006194&newstype=1001&d=13525da&channel=weixin>

学习强国: <https://www.xuexi.cn/lgpage/detail/index.html?id=8021601941242931185&item-id=8021601941242931185>

新华网: <https://www.xinhuanet.com/20260314/ac8a4e87f46549b6a1d745647e937684/c.html>

人民网: <http://finance.people.com.cn/n1/2026/0315/c1004-40682151.html>

光明网: https://m.gmw.cn/2026-03/15/content_38647945.htm

环球网: <https://baijiahao.baidu.com/s?id=1859637022890439718&wfr=spider&for=pc>

中国网: http://news.china.com.cn/2026-03/15/content_118382992.shtml

中国科技网: http://news.china.com.cn/2026-03/15/content_118382992.shtml

中国高新网: http://www.chinahightech.com/chuangye/2026-03/15/content_485840.html

澎湃新闻: https://www.thepaper.cn/newsDetail_forward_32773313

海外网: https://m.haiwainet.cn/middle/3544276/2026/0315/content_32938129_1.html

通信世界: <https://www.cww.net.cn/article?id=608145>

飞象网: <http://www.cctime.com/html/2026-3-16/1730520.htm>

中国信息化周报: <https://www.cio360.net/show-608-104704-1.html>

新浪财经: <https://finance.sina.com.cn/jjxw/2026-03-15/doc-inhramvn6532217.shtml>

中国妇女网: <https://www.cnwomen.com.cn/2026/03/14/99927254.html>

千龙网: <https://world.qianlong.com/2026/0315/8640341.shtml>

新京报: <https://www.bjnews.com.cn/detail/1773510019189590.html>

IT之家: <https://www.ithome.com/0/929/138.htm>

泉州网: https://www.qzwb.com/gb/content/2026-03/15/content_9220226.htm

湛江新闻网: <https://www.gdzjdaily.com.cn/p/2954962.html>

西安新闻网: https://www.xiancn.com/content/2026-03/15/content_7366269.htm

第一财经: <https://www.yicai.com/news/103086326.html>

财联社: <https://www.cls.cn/detail/2313020>

东南网: https://news.fjsen.com/wap/2026-03/15/content_32150190.htm

中华网: https://m.life.china.com/2026-03/14/content_552122.html

中国信息化周报等：

WAPI产业联盟发布新版功能测试项目 强化IPv6协议能力测试

【编者按】2026年3月12日，WAPI产业联盟发布《WAPI测试项2603》（2026年3月版）。自发布之日起，WAPI产品测试工作按新版要求执行。本次更新重点包括：强化STA与AP的IPv6协议能力测试；同步适配2026年1月发布的T/WAPIA 037.2—2026《设备测试方法》标准，进一步细化完善相关测试项，提升测试一致性与可落地性，更好支撑各行业规模化建设与部署安全无线局域网。通信世界、飞象网、中国信息化周报等媒体对此进行了报道。

以下是中国信息化周报的报道：



WAPI产业联盟日前发布《无线局域网鉴别与保密基础结构（WAPI）功能测试项目（2026年3月版）》（以下简称《WAPI测试项2603》）。自发布之日起，联盟将依据《WAPI测试项2603》开展WAPI产品测试，进一步满足各行业规模化部署安全无线局域网的建设需求。

据介绍，本次更新聚焦行业关注的关键能力：一是强化终端（STA）与无线接入点（AP）的IPv6协议能力测试；二是同步适配2026年1月发布的T/WAPIA 037.2—2026《无线局域网测试 第2部分：设备测试方法》，对相关测试项进行细化完善，进一步提升测试的一致性与可落地性。

近年来，安全无线局域网应用加速普及，设备数量持续增长。随着物联网终端快速增长，IPv4地址资源趋紧等问题在网络建设中日益凸显，对网络规划部署和业务场景落地带来影响。在此背景下，推动终端产品全面支持IPv6成为我国推进IPv6规模部署的重要方向。2017年，中办、国办印发的《推进互联网

协议第六版（IPv6）规模部署行动计划》提出“到2025年末，网络、应用、终端全面支持IPv6”。为落实相关要求、支撑市场应用，联盟决定全面启动IPv6协议能力测试。

考虑到无线局域网设备数量庞大、覆盖企业范围广，为稳妥推进相关工作，联盟前期已开展多项准备：一是组织走访调研无线局域网设备对IPv6协议的支持情况；二是依据《工业和信息化部关于在无线电发射设备型号核准中开展对无线局域网设备支持IPv6协议能力测试有关事宜的通知》，围绕典型网络架构与业务链路，完善IPv6协议能力测试环境建设；三是按照《通知》规定的测试方法，对部分产品进行摸底测试。联盟表示，综合前述工作，目前联盟测试实验室已具备开展无线局域网设备IPv6协议能力测试的条件，可为后续产品适配与网络建设验证提供检测支撑。

在标准体系方面，T/WAPIA 037.2—2026《无线局域网测试 第2部分：设备测试方法》已于今年1月正式发布。相较T/WAPIA 037.2—2021，新版新增面向STA、AP、AS的WAPI 2.0协议测试方法和性能测试方法，并补充WAPI多应用场景测试方法，涵盖AP间快速切换、管理帧保护、CMEE、瘦AP模式下AE驻留位置等内容，进一步提升测试方法的可操作性、可复现性与结果可比性，为无线局域网设备型式检验、行业入网检测、互联互通测试及项目验收提供统一基准。

联盟表示，基于新版标准要求，《WAPI测试项2603》同步调整相关章节编号及测试项名称，并进一步细化完善测试内容。后续将严格按照T/WAPIA 037.2—2026组织实施，确保测试结论一致、过程可追溯、结果可对比。

十余年来，WAPI产业联盟持续发挥第三方公共技术支撑平台作用，为产业发展提供技术、标准与检测等公共服务。联盟表示，将对标相关标准要求，紧跟技术演进和行业应用需求，持续完善测试内容与方法，不断提升测试项目的先进性、适用性和一致性，为产品研发适配和网络建设验证提供支撑。

部分媒体新闻链接：

中国信息化周报：<https://www.cio360.net/show-598-104694-1.html>

通信世界：<https://www.cww.net.cn/article?id=6080000>

飞象网：<http://www.cctime.com/html/2026-3-12/1730244.htm>

图：无线局域网鉴别与保密基础结构（WAPI）功能测试项目（2026年3月版）

中国信息化周报等：

抽水蓄能领域WAPI终端电力物模型团体标准正式发布

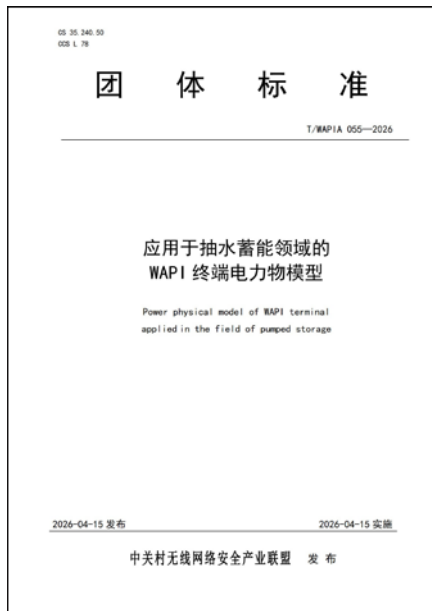
【编者按】2026年4月15日，WAPI产业联盟发布《应用于抽水蓄能领域的WAPI终端电力物模型》团体标准。标准面向抽水蓄能场景下WAPI终端设备统一建模需求，提出WAPI终端电力物模型架构、功能及参数要求，有助于提升终端设备信息的一致性、规范性和可共享性，增强终端数据采集、边缘解析、平台管理与中心应用的协同能力，为抽水蓄能电站精益化运行、智能化运维和安全稳定运行提供技术支撑。中国信息化周报、飞象网、通信世界等媒体对此进行了报道。

以下是中国信息化周报的报道：



记者从WAPI产业联盟获悉，WAPI产业联盟4月15日正式发布团体标准T/WAPIA 055—2026《应用于抽水蓄能领域的WAPI终端电力物模型》。标准面向抽水蓄能场景下WAPI终端设备统一建模需求，提出抽水蓄能WAPI终端电力物模型架构与功能，明确基本信息、技术参数、量测参数等内容要求，适用于全域物联网体系中抽水蓄能WAPI终端电力物模型建模，为相关设备信息参数的数字化描述、平台化管理和协同应用提供统一依据。

当前，我国能源结构加快向绿色低碳转型。抽水蓄能作为大规模、长周期储能的重要技术，在电力系统调峰、调频、备用以及新能源消纳等方面发挥着重要作用。近年来，抽水蓄能电站智能化、数字化建设持续推进，但设备物模型不统一、信息表达不一致、系统协同不足等问题在一定程度上影响了设备互联互通与数据高



图：《应用于抽水蓄能领域的WAPI终端电力物模型》团体标准

效利用。为此，WAPI产业联盟组织相关单位开展标准研制，形成面向抽水蓄能领域的WAPI终端电力物模型统一规范。

据联盟介绍，标准明确抽水蓄能领域WAPI终端电力物模型设计应符合相关信息模型规范要求。标准同时提出统一的信息建模方法，从基本信息、技术参数、量测参数三个维度规范终端信息建模。标准发布实施后，将有助于提升抽水蓄能场景下终端设备信息的一致性、规范性和可共享性，增强终端数据采集、边缘解析、平台管理与中心应用的协同能力，为抽水蓄能电站精益化运行、智能化运维和安全稳定运行提供技术支撑。

该标准由南方电网数字电网科技（广东）有限公司、西安西电捷通无线网络通信股份有限公司、中关村无线网络安全产业联盟（WAPI产业联盟）、无线网络安全技术国家工程研究中心、工信部宽带无线IP标准工作组、广州莲雾科技有限公司、深圳市智开科技有限公司、北京数字认证股份有限公司、南方电网储能股份有限公司信息通信分公司、海南电力产业发展有限责任公司、中国南方电网电力调度控制中心、中国南方电网有限责任公司超高压输电公司等单位共同起草。

据悉，联盟下一步将联合产业链上下游和行业用户，加强标准宣贯推广和应用实施，持续完善WAPI标准体系，为能源电力等重点行业高质量发展和新型电力系统建设提供标准与技术支撑。

中国信息化周报：<https://www.cio360.net/show-598-104753-1.html>

飞象网：<http://www.cctime.com/html/2026-4-15/1732585.htm>

通信世界：<https://www.cww.net.cn/article?id=608792>

通信世界等：

WAPI产业联盟召开2026年第一次标准工作和项目组会议 (总第137次)

【编者按】2026年3月26日，WAPI产业联盟召开2026年第一次标准工作和项目组会议（总第137次），会议围绕第一季度工作进展、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、标准国际化推进、标准工作培训等议题展开。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：



3月26日，WAPI产业联盟召开2026年第一次标准工作和项目组会议（总第137次）。会议围绕第一季度工作进展、上一次项目组集中会议要点落实情况、已立项项目进展、新项目立项建议及标准国际化推进等事项进行报告和讨论；同时对第一季度已发布标准开展宣贯，并组织标准工作培训。工信部宽带无线IP标准工作组2026年第一次项目组集中工作会议同期召开。

来自无线网络安全技术国家工程研究中心、西电捷通公司、北京数字认证股份有限公司、新华三技术有限公司、西安芯语慧联信息科技有限公司、深圳市智开科技有限公司、国网山东省电力公司、国网山东省电力公司电力科学研究院、北京市标准化研究院等单位代表，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标准工作组相关同志参加会议。

WAPI产业联盟秘书长、无线网络安全标准化工作委员会副主任委员张璐璐表示，站在“十五五”开局之年，网络安全任务正从三方面加快转变：从“单点防护”向“体系能力”转变，从“事后响应”向“主动免



图：会议合影

疫”转变，从“合规达标”向“可验证、可量化的安全效果”转变。全国两会也强调要更好统筹发展和安全，推进高水平安全保障高质量发展。她指出，当前无线网络安全领域愈发清晰地呈现出以下趋势：关键基础设施与重点行业安全要求更加具体，更可检验；新技术、新业态带来的复合风险加速显性化；标准日益成为产业协同、生态互认的“共同语言”。她强调，2026年标准产业共同体要紧扣“十五五”开局部署与两会精神的新要求，以应用场景为牵引、以标准为抓手、以测试验证为闭环，持续提升标准“可用、管用、好用”水平，推动取得“能落地、能推广、生态持续壮大”的工作成效。

工业和信息化部宽带无线IP标准工作组秘书长、无线网络安全标准化工作委员会副主任委员黄振海介绍，2026年第一季度，联盟标准化部和WG 1总体工作组围绕标委会年度重点任务形成落实计划，后续将按照既定任务目标，稳步推进标准制定和标准实施。他表示，联盟标准化的核心价值在于实施，联盟团体标准不是闭门造车的一纸文本，而是产业各方在协商中凝聚共识、在实践中检验完善的共同成果，它因协商而生，因共识而活。标委会将坚持共建共享共治，推动形成经得起应用检验的创新标准体系。

会议通报了2026年第一季度标准产业市场应用进展：联盟组织成员单位共同制定的一项物联网安全协议测试技术成为国际标准；国网山东电力获日内瓦发明展金奖；联盟发布高质量安全无线局域网标准体系首项标准、新版无线局域网设备测试方法以及5项新版无线局域网产品工程化实现指南团体标准；组织召开2026年第一次标委会主任委员会议；联盟测试实验室发布新版WAPI功能测试项目，多厂商多款产品通过测试。

会议报告了第一季度技术标准进展：团体标准方面，发布7项，报批阶段8项、送审阶段2项、草案稿阶段8项，立项审批阶段1项；国际标准推进方面，2025年12月20日至2026年3月25日，SC 6国内技术对口单位对国内群体通报国际提案文件131份，向国际反馈投票/意见36份；组织中国专家参加2026年4月ISO/IEC JTC 1/SC 6首尔会议行前会，围绕参会准备、在研项目进展、新提案提交及国际联络工作等事项进行集中交流与部署。



图：WAPI产业联盟秘书长、无线网络安全标准化工作委员会副主任委员 张璐璐



图：工信部宽带无线IP标准工作组秘书长、无线网络安全标准化工作委员会副主任委员 黄振海

在已立项项目报告环节，与会代表围绕《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》《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》等7项标准，《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，逐项讨论并形成决议。

项目承担单位对T/WAPIA 054—2025《高质量安全无线局域网 总体要求》等7项新发布团体标准进行宣贯，WAPI产业联盟测试实验室王立华对团体标准项目起草阶段的组织协调与过程管理进行培训。

会议还专题研讨了标准国际化工作，报告并总结国际标准ISO/IEC 19823-16:2026创新成果，通报2026年4月SC 6全会和工作组会议组团情况。经会议研究，决定在标委会下成立“安全无线局域网与人工智能”专项研究组。

部分媒体新闻链接：

通信世界：<https://www.cww.net.cn/article?id=608387>

飞象网：<http://www.cctime.com/html/2026-3-27/1731368.htm>

中国信息化周报：<https://www.cio360.net/show-598-104743-1.html>

中国标准化等：

WAPI产业联盟发布5项《无线局域网产品工程化实现指南》团体标准

【编者按】2026年1月30日，WAPI产业联盟发布5项新版《无线局域网产品工程化实现指南》团体标准。此次标准修订在完善技术细节的同时，显著提升了标准易用性，确保安全无线局域网产品具有更高通信性能，实现更广泛的互联互通。中国标准化、通信世界、飞象网、中国信息化周报等媒体对此进行了报道。

以下是中国标准化的报道：



记者从WAPI产业联盟获悉，WAPI产业联盟于1月30日正式发布5项新版《无线局域网产品工程化实现指南》团体标准。此次标准修订在完善技术细节的同时，显著提升了标准易用性，确保安全无线局域网产品具有更高通信性能，实现更广泛的互联互通。

随着WAPI安全技术体系持续迭代升级，以及IEEE 802.11系列标准在通信速率和传输性能方面的不断演进，通过建立标准化协同兼容机制，我国自主研发的WAPI技术已实现与新一代高速IEEE 802.11无线局域网技术体系的深度融合，为无线局域网在高速演进过程中的网络和信息安全提供了稳定可靠的保障。

据悉，WAPI产业联盟自2010年起便系统性开展《无线局域网产品工程化实现指南》系列标准的制修订工作，形成了覆盖多技术场景的T/WAPIA 007标准体系。期间，联盟始终立足产业一线，基于产业链上下游厂商的实际应用反馈，通过修改单即时发布、标准动态迭代等机制，快速响应产业市场需求与技术变革。

本次修订的5项团体标准，全面覆盖基础安全与主流高速率通信融合技术领域，具体包括：T/WAPIA 007.1—2026《无线局域网产品工程化实现指南 第1部分：WAPI与IEEE 802.11n》、T/WAPIA 007.2—2026《无线局域网产品工程化实现指南 第2部分：WAPI与IEEE 802.11e》、T/WAPIA 007.8—2026《无线局域网产品



图：五项新版《无线局域网产品工程化实现指南》团体标准

工程化实现指南 第 8 部分：WAPI 与 IEEE 802.11ac》、T/WAPIA 007.9—2026《无线局域网产品工程化实现指南 第 9 部分：WAPI 与 IEEE 802.11ad》、T/WAPIA 007.10—2026《无线局域网产品工程化实现指南 第 10 部分：WAPI 与 IEEE 802.11ax》。

本次修订在整合上一版标准以及相关修改单核心内容的基础上，重点更新了 WPI 完整性校验数据组成等关键技术内容，适配无线局域网技术向更高速率、更强安全、更广覆盖的发展趋势，并确保与《无线局域网安全技术规范》及 GB 15629.11 系列国家标准等有效衔接、协调一致，全面满足行业合规应用需求。

5 项新版团体标准的主要起草单位包括：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、中关村无线网络产业联盟（WAPI 产业联盟）、西安芯语慧联信息科技有限公司、中电科普天科技股份有限公司、中国电子技术标准化研究院、国家无线电监测中心检测中心、商用密码检测认证中心、国家信息技术安全研究中心、北大方正集团有限公司、西安邮电大学、北京傲天动联技术有限公司、创锐讯通信技术（上海）有限公司、重庆邮电大学、西安电子科技大学等。

业内专家指出，5 项新版团体标准的发布，标志着《无线局域网产品工程化实现指南》体系的进一步成熟与完善，既严格契合 GB 15629.11 系列国家标准要求，又实现了与 IEEE 802.11 系列标准的深度兼容，对规范产业发展、提升产品质量具有重要意义。标准的落地实施将为产业链厂商提供清晰明确的技术指引，加速安全无线局域网产品研发与产业化进程，为广大用户提供更安全、高效、便捷的无线网络服务，有力推动我国无线局域网产业向更高质量发展迈进。

部分媒体新闻链接：

中国标准化：<https://mp.weixin.qq.com/s/3JUPxlxeoVOZYC1t13abJw>

通信世界：<https://www.cww.net.cn/article?id=99DC82359DEA4406BA58A7D9B692B960>

飞象网：<http://www.cctime.com/html/2026-2-4/1728383.htm>

中国信息化周报：<https://www.cio360.net/show-598-104657-1.html>

飞象网等：

WAPI产业联盟发布新版无线局域网设备测试方法标准

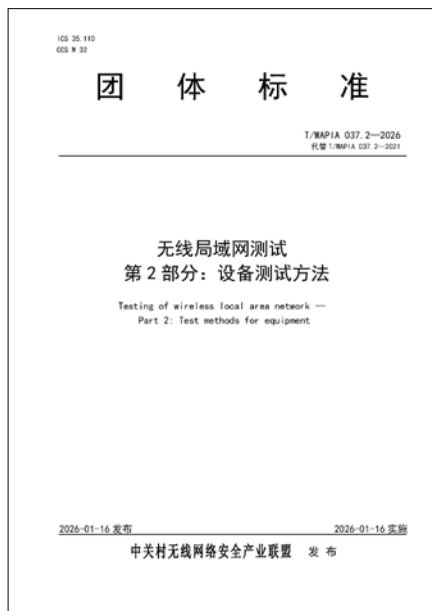
【编者按】2026年1月16日，WAPI产业联盟发布团体标准T/WAPIA 037.2—2026《无线局域网测试 第2部分：设备测试方法》。该标准在T/WAPIA 037.2—2021的基础上修订形成，主要更新内容包括：新增面向STA、AP和AS的WAPI 2.0协议测试方法，为相关能力提供可测、可判依据；新增面向STA、AP和AS的性能测试方法；新增WAPI多应用场景测试方法，涵盖AP间快速切换、管理帧保护、CMEE、瘦AP模式下AE驻留位置等内容。飞象网、通信世界、中国信息化周报等媒体对此进行了报道。

以下是飞象网的报道：



记者从WAPI产业联盟获悉，WAPI产业联盟近日发布团体标准T/WAPIA 037.2—2026《无线局域网测试 第2部分：设备测试方法》。该标准在T/WAPIA 037.2—2021的基础上修订形成，面向检测机构测试实施与设备厂商研发验证等共性需求，对被测设备测试要求与测试范围进行了工程化梳理，补充关键协议与性能测试方法，进一步提升测试方法的可操作性、可复现性与结果可比性，为无线局域网设备型式检验、行业入网检测、互联互通测试及项目验收提供统一基准。

据介绍，自2015年国家标准《无线局域网测试规范》发布以来，随着应用推进和技术迭代加快，仅依据国家标准开展测试已难以满足行业建设和应用需求，为此，WAPI产业联盟于2019年组织制定并发布团体标准T/WAPIA 037.2，与国家标准共同成为无线局域网设备型式检验、行业入网检测的重要依据，服务安全无线局域网部署建设与应用。



图：《无线局域网测试 第2部分：设备测试方法》团体标准

联盟表示，2021年该标准完成首次修订，以适应行业市场精细化、定制化、多样化需求。近年来，联盟还陆续发布《无线局域网安全技术规范》《传感器类设备专用WLAN通信模块技术规范》《工业串口类设备专用WLAN通信模块技术规范》《无线局域网产品工程化实现指南 第11部分：WAPI与IEEE 802.11be》等多项团体标准。与之配套，T/WAPIA 037.2同步启动新一轮修订，以满足当前WAPI应用行业对“高安全+高性能”并重的实际需求。

与2021年版本相比，新版T/WAPIA 037.2主要更新内容包括：新增面向STA、AP和AS的WAPI 2.0协议测试方法，为相关能力提供可测、可判依据；新增面向STA、AP和AS的性能测试方法；新增WAPI多应用场景测试方法，涵盖AP间快速切换、管理帧保护、CMEE、瘦AP模式下AE驻留位置等内容。

该标准由中关村无线网络安全产业联盟(WAPI产业联盟)、西安西电捷通无线网络通信股份有限公司、国家无线电监测中心检测中心、无线网络安全技术国家工程研究中心、北京华信傲天网络技术有限公司、新华三技术有限公司、西安芯语慧联信息科技有限公司、南京云程半导体有限公司等单位共同起草。

据悉，该标准在制定过程中，联盟测试实验室已同步开展相关能力建设。下一步，联盟将联合产业链上下游与检测机构，加强标准宣贯推广与测试能力建设，鼓励相关厂商依据新版标准开展产品研发与测试验证，提升WAPI 2.0及高性能等关键能力的可测性、可比性与可落地性，助力安全无线局域网产业高质量发展。

部分媒体新闻链接：

飞象网：<http://www.cctime.com/html/2026-1-23/1727683.htm>

通信世界：<https://www.cww.net.cn/article?id=606927>

中国信息化周报：<https://www.cio360.net/show-598-104648-1.html>

联盟发布WAPI市场应用洞察报告

分层筑防：点到点与端到端安全共筑

【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》围绕点到点通信与端到端通信的基本关系展开系统剖析，重点比较点到点安全与端到端安全的差异及其内在联系，并就产业界高度关注、持续讨论的关键议题进行深入辨析，形成核心结论。内容如下：

一、本期洞察对象与结论

在 WAPI 规模化部署过程中，不时会出现关于点到点、端到端之间的概念混淆或两者是否可以互相代替的争议。本期《洞察报告》集中剖析了点到点通信、端到端通信的基本关系，重点研究了点到点安全、端到端安全的区别与联系，对若干产业界高度关注和讨论的问题进行了深度辨析，形成结论如下：

1、点到点安全的核心目标是以身份鉴别为前提，确保数据在每一个通信链路段上的保密性、完整性和可用性，实现数据的真实性和不可否认性，防范物理窃听、链路伪造和未授权接入等威胁。端到端安全则是一种跨越中间节点、保障通信两端实体间完整通信路径的安全设计原则。两者既不存在替代关系，也不具有优劣之分，通过分层协作构建完整的网络安全纵深防御体系，共同应对多层次安全威胁。

2、无线局域网系统的安全基础是点到点的无线链路安全。IP 层 IPSec 技术、物理层安全技术，均无法取代 WAPI 对开放链路的安全防护能力。

3、在采用无线局域网的信息系统中，应合理部署点到点安全和端到端安全机制，在启用 WAPI 服务的基础上，可根据需要叠加 IP 层安全技术和与应用层业务相关的个性化安全机制，形成纵深防御体系。

二、点到点通信 vs 端到端通信

在网络通信体系中，点到点通信（Point-to-Point Communication）与端到端通信（End-to-End Communication）构成了网络连接的两个基本维度。点到点通信强调网络中两个直接相连节点之间的数据传递，是网络的“局部连接”，解决“如何在相邻节点间可靠传输数据”的问题。端到端通信强调从源到目的的跨越整个网络的逻辑连接，是网络的“全局连接”，解决“如何在网络两端之间建立逻辑连接并确保数据正确交付”的问题。端到端通信建立在多个点到点通信的基础之上，点到点通信为端到端传输提供物理与逻辑支撑。

点到点通信是网络中相邻节点间的直接数据传输机制，工作于物理介质和数据链路层（OSI 第 1-2 层），

负责在单一通信链路上可靠地传递比特流或数据帧，关注的是相邻设备间的直接连接与数据交换，是构建网络连通性的基本单元，如以太网交换、PPP 链路、无线接入点与终端间的连接等。

端到端通信是指网络中源节点与目标节点间的完整通信过程，跨越多个中间节点和链路，通常实现于网络层至应用层（OSI 第 3-7 层），如 TCP 连接、HTTP 会话、应用间的消息交换等，关注的是通信两端实体间的逻辑连接和数据交付，不依赖于具体的物理路径。

两者共同构成了现代网络通信的层次化架构，互为依托、相辅相成。

三、点到点安全 vs 端到端安全

点到点安全（Point-to-Point Security）指在网络通信中，保护物理或逻辑上相邻两个节点之间链路传输的安全机制，它通常工作在链路层，目标是以身份鉴别为前提，确保数据在每一个通信链路段上的保密性、完整性和可用性，并实现数据的真实性和不可否认性。

端到端安全（End-to-End Security）指在网络通信中，保护源节点到目标节点整个通信路径的安全机制，主要工作在网络层、传输层和应用层，目标是确保数据从发送方到接收方整个过程中的保密性、完整性和真实性。

两者构成网络安全的纵深防御体系——点到点安全保护局部链路传输，抵御物理与链路层威胁；端到端安全则保护全程通信内容，应对中间节点与应用层威胁。两者在不同层次协同工作，形成完整保护链，缺一不可。

下表展示了点到点安全与端到端安全的关系。

对比维度	点到点安全	端到端安全	关系
基本定义	保护网络中两个直接相连节点之间链路传输的安全机制。	保护从源节点到目标节点整个通信路径的安全机制。	两种安全模式共同构成网络安全的纵深防御体系，层层递进、相互补充。
防护范围	针对单一通信链路段提供保护，确保每个链路段的安全。	针对整个通信路径提供端到端的内容保护。	端到端安全覆盖整个路径，包含多个点到点安全段。
工作层次	主要工作在物理层和链路层（OSI 第 1-2 层）。	主要工作在网络层、传输层和应用层（OSI 第 3-7 层）。	两者结合形成从底层到上层的完整安全防护链，覆盖网络协议栈各层。
典型协议 / 技术	TLSec、MACSec、WAPI、WPA 系列协议等。	TIISec、IPSec、TLS/SSL、DTLS、HTTPS、S/MIME、PGP 协议等。	上层安全协议通过下层安全通道传输，形成多层次保护。
防御目标	物理层窃听、链路层伪造、未授权接入等安全威胁。	数据泄露、会话劫持、内容篡改、身份冒充等安全威胁。	点到点安全解决物理和链路威胁，端到端安全解决逻辑和应用威胁。
信任模型	基于相邻节点间的信任关系，假设威胁主要来自通信链路。	基于通信两端的直接信任关系，假设中间节点可能不可信。	点到点安全依赖节点间信任，端到端安全构建跨节点信任，两者共同形成完整信任链。

对比维度	点到点安全	端到端安全	关系
性能特点	通常由硬件加速实现，性能开销较小，透明度高。	通常在软件层实现，可能带来一定性能开销，需应用感知。	点到点安全提供高效基础保护，端到端安全提供灵活深度保护。
管理特点	集中管理，通常由网络管理员控制，便于统一策略执行。	分散管理，通常由应用开发者或终端用户控制，策略难以统一。	点到点安全便于基础设施管控，端到端安全增强用户数据自主权。
典型应用场景	数据中心内部网络安全、运营商骨干网安全、无线接入安全等。	电子商务、在线银行、即时通讯、远程办公、云服务访问等。	关键应用通常同时采用两种安全机制，形成多层次保护。
失效影响	单一链路安全受损，但不一定影响端到端的内容安全。	通信内容安全受损，但不一定影响底层网络传输安全。	一种安全机制的失效可部分由另一种机制弥补，提供故障冗余。
部署控制方	通常由网络基础设施提供商或运营商控制部署。	通常由应用服务提供商或终端用户控制部署。	不同控制方需协同合作，确保安全策略一致性和有效性。
安全演进趋势	向更高速率、更低延迟、量子安全方向发展，如 PQC 链路加密等。	向更强数据隐私、更高灵活性方向发展，如端到端量子加密等。	两种安全机制正向更紧集成方向演进，共同应对新型威胁。

四、关联问题辨析

问题 1: 在无线局域网系统中，在两个终端（STA）上启用 IPSec，是否就不需要启用链路层的 WAPI 安全机制了？

结论： 这个理解是错误的，存在根本性的安全风险。端到端安全与点到点安全，二者不存在替代关系。

认为端到端安全（IPSec）可以完全替代点到点安全（WAPI）的观点是一种危险的简化。在实际网络环境中，两种安全机制解决的是不同层面的安全问题，共同构成了完整的安全防护体系。放弃点到点安全将导致网络基础设施暴露于各种威胁之下，即使通信内容本身是加密的，网络的可用性、稳定性和某些隐私属性仍会受到严重影响。具体分析如下：

1、WAPI 提供了点到点的链路层连接安全，而 IPSec 提供的是链路层之上、端到端、穿越不同 IP 域的 IP 层安全。

IPSec 是一套工作在 IP 层的安全协议族，提供数据源鉴别、完整性和机密性保护，其工作前提是 IP 连接已建立，而这种连接的建立依赖于底层链路层（如 WAPI 保护的无线链路）的安全性。IPSec 工作在 ISO/OSI 模型第 3 层（网络层），主要提供数据包级别的加密和鉴别。而 WAPI 工作在第 2 层（链路层），负责无线接入安全和链路保护。两者在防护目标、安全边界和技术实现上存在本质差异。IPSec 可增强 IP 业务安全，但无法解决或者增强 WLAN 本身的安全。

2、即使 WLAN 系统的两个终端（STA）上启用了 IPSec，如果缺乏链路层 WAPI 安全机制，攻击者可直接嗅探无线通信、获取原始数据帧，系统无法防范来自链路层面的点到点安全威胁，具体包括：

- 链路层安全隐患。包括：未授权网络接入，端到端安全不提供接入控制功能；ARP 欺骗 /MAC 欺骗，此类链路层攻击将可能导致通信中断或被重定向，将用户的流量劫持到攻击者的设备，进行中间人攻击。

- 元数据泄露问题。端到端虽然对通信内容做了加密保护，但通信元数据（如谁与谁通信、何时通信、通信频率等）仍然可见。这些元数据在没有点到点保护的情况下可被轻易收集，被用于分析用户的流量模式、数据包大小和时间，造成隐私泄露。即使不能对数据解密，也可以发起流量分析攻击，通过分析加密流量的模式、大小和时间特征推断用户通信行为。

- 在未被保护的物理链路上发起攻击。包括：发送伪造的路由协议报文（如 OSPF、BGP），扰乱网络路由；发起生成树协议攻击，破坏交换机网络拓扑；进行 MAC 地址泛洪，导致交换机失效。

因此，无论是否启用 IPSec，均需要在链路层启用 WAPI 安全服务，保障点到点的链路层连接安全。

问题 2: 在无线局域网系统中，在已经启用链路层 WAPI 安全机制的情况下，如果在两个终端（STA）上启用 IPSec，是否对 WLAN 的连接安全有显著增强？

结论：没有显著增强。分析如下：

WAPI 通过 WAI（无线局域网鉴别基础结构）提供了基于密码学的强身份鉴别和密钥管理机制，通过 WPI（无线局域网保密基础结构）提供了数据加密和完整性保护。其三元对等安全架构从设计上解决了传统 WLAN 安全中的根本缺陷。WAPI 完全提供了机密性、完整性和真实性保障，确保了 WLAN 网络连接安全，满足了无线安全接入需求。无线局域网（WLAN）是有线网络的延伸，启用了 WAPI 安全机制的无线局域网其安全性至少达到了等同有线网络的水平。考虑到很多有线网络没有身份鉴别和通信保密机制，启用了 WAPI 安全机制的无线局域网其安全性要超过绝大部分有线网络。

针对链路层的安全风险，采用 IP 层及以上的端到端安全技术，比如 IPSec，对 WLAN 的连接安全不会有显性增强。因为 IPSec 是在有线或者无线形式的链路层安全基础上，在 IP 层的一种安全增强机制。IPSec 在链路层已受 WAPI 保护的基础上，对 WLAN 连接安全的边际增强效应接近于零。

问题 3: 在一个采用了 WLAN 无线接入方式的通信系统中，要实现系统的连接安全，可行的技术路线是什么？

结论：最佳实践是根据具体系统的威胁模型和安全需求，合理部署点到点安全和端到端安全机制，形成纵深防御体系，共同应对复杂多变的网络威胁。分析如下：

在链路层启用 WAPI 安全服务的基础上，可根据需要叠加端到端 IP 层安全技术（如 IPSec，或者采用中国自主提出并发布为国家标准的 TISec 技术）。

一个完整的 WLAN 安全技术路线应包括：

- 链路接入层安全：部署 WAPI 提供的 WAI/WPI 安全服务
- 网络传输层安全：根据需求选择 IPSec 或 TISec 技术

- 应用业务层安全：针对特定业务部署专用安全机制（如 HTTPS 等）

WAPI 提供了 WLAN 的连接安全，有些网络建设方可在基本网络连接安全的基础上，采取进一步的安全措施，比如在启用链路层安全（如有线局域网的 TLSec/802.1x/1ae，无线局域网的 WAPI）的基础上，进一步采用 IPSec/TISec 机制应对 IP 层的安全威胁，以及针对应用层业务采用该业务个性化的安全机制（如 HTTPS）等，进一步有针对性地增强业务安全性。

问题 4: 针对点到点安全，WLAN 物理层安全技术是否可以替代链路层安全技术？

结论：不可以。两者解决不同层次的安全问题，应当协同配合形成完整的点到点安全防护体系。分析如下：

1、物理层与链路层安全技术的侧重点不同。

物理层安全技术主要关注：信号传输的保护（如扩频技术、物理层加扰）、物理介质访问控制（如射频干扰检测与规避）、信号特性安全（如距离边界检测、功率控制）、物理层鉴别（如射频指纹识别）；而链路层安全技术主要关注：数据帧加密与完整性保护（如 WAPI 的 WPI 功能）、身份鉴别与接入控制（如 WAPI 的 WAI 功能）、密钥管理与分发（会话密钥协商）、防重放与序列保护（帧计数器机制）等。

2、物理层安全技术有局限性。

- 无法提供完整的身份鉴别：物理层技术难以实现复杂的身份鉴别协议、无法支持证书或密钥基础设施所需的复杂逻辑。

- 难以实现精细的访问控制：物理层主要依靠信号特性进行粗粒度控制、无法基于身份或权限实现细粒度访问策略。

- 密钥管理能力有限：物理层难以实现安全的密钥协商与分发、缺乏处理密钥生命周期的完整机制。

- 协议攻击防护不足：物理层无法防御帧格式、协议逻辑等高层攻击，对于协议漏洞利用缺乏防护能力。

3、某些 WLAN 物理层安全技术能有效解决 / 缓解无线链路面临的一个核心安全问题——被动窃听与报文侦听，但它属于物理层的增强技术，不能替代 WAPI 这样的协议层面的链路层安全技术。例如，某 WLAN 物理层安全技术的核心原理是通过接入点感知合法用户的精准位置，在发送数据报文时同步发射经过特殊算法调制的随机噪声信号，在物理空间上让非目标区域的信号成为无法解调的噪声。它可以防御来自网络覆盖区域内的被动窃听者，但它不能替代网络接入身份鉴别、密钥管理、防中间人攻击等由链路层安全协议（WAPI）负责的安全机制。

即使考虑最新的物理层安全技术（如量子密钥分发、物理层安全编码），它们仍无法提供 WAPI 等链路层安全协议的完整功能集，特别是在身份鉴别、访问控制和安全关联管理方面。这些新技术可以作为增强手段，但不能替代链路层安全机制。

因此，物理层安全技术与链路层安全技术各有所长，解决不同层面的安全问题，无法相互替代。在 WLAN 等无线网络环境中，WAPI 等链路层安全技术的核心价值（如身份鉴别、密钥管理、加密保护）无法被物理层安全技术所替代。同时，某些物理层安全特性也是链路层技术难以提供的。应当根据安全需求和威胁模型，合理部署物理层和链路层安全技术，形成多层次的点到点安全防护体系。

问题 5: 某招标采购公告中要求 WAPI CPE 产品支持应用层数据加密模块 (COB 卡), 是否合理?

结论: 不合理。分析如下:

在 WAPI 基础上叠加使用应用层数据加密模块的要求是合理的, 但是该要求应针对端到端的信源设备 (如 AGV 小车、手持业务终端等), 而不应针对 WAPI CPE/ 通信模块这样的点到点传输设备。

在网络系统中, 基本的数据安全理念是谁产生的数据, 谁就应为其提供最初级和最终级的保护。加密的责任应归属于数据的“产生者”, 而非传输管道。

要求 CPE/ 通信模块进行应用层加密, 会导致:

- 违背网络分层原则: CPE 是链路层设备, 其主要职责是高效、透明地转发 IP 包。强制要求其处理应用层数据 (如解析 JSON 后加密某个字段), 会破坏网络设备的透明性, 使其变得复杂、低效且昂贵。

- 形成单点故障与瓶颈: CPE 成为所有流量的加密解密集中点。一旦其算力不足或被攻破, 所有通过它的业务都会瘫痪或泄露。

- 密钥管理灾难: CPE 需要为所有接入的设备管理和存储应用层加密密钥。这使 CPE 成为极具吸引力的攻击目标, 并带来复杂的密钥分发、存储和轮换难题。

- 无法覆盖端到端全过程: 如上所述, 这种方式留下了“信源到 CPE”这段的安全空白, 无法实现真正的端到端保护。

五、总体结论与建议

1、安全分层防护是网络设计的必然选择, 应避免“张冠李戴”。点到点、端到端的辨析, 实则是对网络通信及安全防护理念和需求的再认识, WAPI、IPSec (或 TISec) 不是替代关系, 而是分层协作。要求点到点通信设备具有端到端加密功能, 则完全违背了网络分层原则。

2、WLAN 安全建设应遵循“内外兼修”原则。网络建设方应在网络规划阶段即考虑分层安全需求, 合理配置安全资源, 确保链路层安全与端到端安全的均衡投入, 避免安全短板。将链路安全作为基础设施安全刚性需求的同时, 根据业务需求部署端到端安全。对于政务、金融、能源等关键信息基础设施, 应采用“WAPI+IPSec/TISec+ 应用层安全”的三层防护架构, 实现从接入层到应用层的全方位防护。

3、应构建完整的 WLAN 安全评估体系。应建立涵盖物理层、链路层和网络层的完整安全评估体系, 定期对 WLAN 网络进行安全评估和渗透测试, 确保各层安全机制有效配合, 形成真正的纵深防御能力。特别关注安全机制之间的衔接点和协同效应, 避免出现安全“真空区”。

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

第十八部分（PART 18）

1、问：据市场用户反映，在招标采购WAPI设备时出现了“供货产品与送联盟测试产品不一致”等情况，能否通过查询联盟测试报告辨识此类情况？

答：可以。

在招标采购中，WAPI产业联盟出具的测试报告是证明投标产品符合技术规格、质量标准及合规性要求的权威凭证，也是防范供应链“货不对板”风险的核心依据。建议重点关注测试报告的测试时间、测试项版本、样品照片一致性以及是否包含“扩展功能”测试。防范供应链风险应关注以下细节：

（1）进行实物一致性核验：联盟测试报告中包含送测样品的实物照片（包括铭牌、接口、外观）。验收时，应严格比对报告中的照片与到货设备的型号、硬件版本、软件版本是否完全一致。

（2）核对测试规范版本：WAPI测试项目会随着技术演进，予以动态更新。一般情况下，每年会更新1-2个版本。如设备厂商持有的是时间较早的测试报告，可能无法覆盖当前的安全要求（如重传机制或管理帧保护等）。建议采购方要求设备厂商提供依据最新版测试规范/标准出具的测试报告。

（3）官方名录在线比对：登录WAPI产业联盟官网(wapia.org.cn)，查询该型号产品是否在《WAPI产业联盟产品名录》之中，且产品信息是否与报告一致。

（4）到货抽检：产品到货后，建议用户使用专业WAPI测试工具复测，验证其是否与送测样品相符。

2、如果WPI数据保密安全机制支持兼容模式，应如何进行测试？

答：WPI数据保密安全机制支持兼容模式是指：用于WPI数据保密的单播密码套件、组播密码套件、组管理密码套件，均分别同时支持WPI-SM4-OFB+CMAC-128和WPI-SM4-GCM-128。

以单播密码套件为例：测试时，配置基准设备的单播密码套件分别为“支持WPI-SM4-OFB+CMAC-128”、“支持WPI-SM4-GCM-128”以及“同时支持WPI-SM4-OFB+CMAC-128和WPI-SM4-GCM-128”三种场景，分别验证被测设备在三种场景下的单播密码套件协商结果是否正确，以及能否正确完成单播通信。

■ 3、问：是否可以将AS的功能全部或部分迁移至AC？

答：不可以。

AS是WAPI三元对等安全体系的信任根基，承担着STA和AP的身份鉴别与证书管理职责。任何削弱、替代或绕过AS核心功能的实现方案，均背离了WAPI安全架构的设计原则，引入系统性安全风险。

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，此类改造会严重削弱网络安全性，使其极易遭受攻击。

同时需要说明的是：虽然功能不可迁移，但支持“逻辑解耦、物理融合”的部署方案。即：在物理形态上，可以将AS功能模块与AC部署在一起，甚至融合为“管控一体机”（逻辑上仍是两个设备）。具体见：《WAPI市场应用洞察报告——AS在WAPI三元对等架构中的核心地位与行业合规部署》。扫码可获取《报告》。



■ 4、问：对于不支持快速切换的STA，为降低其在AP间切换时延，是否可以临时屏蔽AS鉴别功能？

答：不可以。

屏蔽AS鉴别功能，意味着密钥需在AP/AC之间的网络中传输，带来严重安全风险，一旦密钥泄露，非法STA即可绕过WAPI身份鉴别机制，直接入侵到WAPI网络中。

正确的做法是：快速切换功能的实现，必须以保证安全性为前提。STA无论切换到哪个AP，均需完整执行WAPI身份鉴别流程。对于切换时延的优化，可以通过“双发选收”等工程化手段予以解决，而不应通过牺牲安全机制来实现。

■ 5、问：AS不可用时，是否可以采用“代位鉴别”等应急方案？

答：不可以。

这类“代位鉴别”或其他“变通”方式均严重影响了安全性，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。

■ **6、问：在无线局域网系统中，如果在两个终端（STA）上启用了IPSec，是否就不再需要启用链路层的WAPI安全机制了？**

答：这种观点是错误的，存在根本性的安全风险。

认为“端到端安全（IPSec）”可以完全替代“点到点安全（WAPI）”的观点是一种危险的简化。在实际网络环境中，两种安全机制解决的是不同层级的安全问题，共同构成了完整的安全防护体系。若放弃点到点安全，将导致网络基础设施直接暴露，即使通信内容本身是加密的，网络的可用性、稳定性和隐私属性仍会受到严重威胁。

WAPI提供了点到点的链路层连接安全，而IPSec提供的是链路层之上的端到端、穿越不同IP域的IP层安全。即使WLAN系统的两个终端（STA）上启用了IPSec，如果缺乏链路层WAPI安全机制，攻击者仍可直接嗅探无线通信并获取原始数据帧，此时系统无法防范来自链路层面的点到点安全威胁，包括：非法终端接入、空口元数据泄露、在未被保护的物理链路上发起攻击等。具体见：《WAPI市场应用洞察报告——分层筑防：点到点与端到端安全共筑》。扫码可获取《报告》。



■ **7、问：在无线局域网系统中，在已经启用链路层WAPI安全机制的情况下，如果在两个终端（STA）上启用IPSec，是否会对WLAN的连接安全产生显著增强？**

答：不会。

WAPI安全机制以身份鉴别为前提，确保了数据在每一段通信链路上的保密性、完整性和可用性，实现了数据的真实性和不可否认性，满足了无线安全接入需求。

针对链路层特有的安全风险，采用IP层及以上的端到端安全技术，比如IPSec，对WLAN的连接安全并无显性增强。因为IPSec是在链路层安全基础上，在IP层的一种安全增强机制；在链路层已受WAPI充分保护的前提下，IPSec对WLAN连接安全的边际增强效应趋近于零。

具体见《WAPI市场应用洞察报告——分层筑防：点到点与端到端安全共筑》。

■ **8、问：针对点到点安全，WLAN物理层安全技术是否可以替代链路层安全技术？**

答：无法相互替代。

物理层安全技术和链路层安全技术，分别解决不同层面的安全挑战，无法相互替代。在WLAN环境中，链路层WAPI安全技术的核心价值（如：身份鉴别、密钥管理、加密保护等）无法被物理层安全技术所替代。同时，某些物理层安全特性也是链路层技术难以提供的。应当根据安全需求和威胁模型，合理部署物理层和链路层安全技术，形成多层次的纵深防御体系。

具体见《WAPI市场应用洞察报告——分层筑防：点到点与端到端安全共筑》。

李强：

统筹发展和安全 全面推进人工智能高质量发展

2026年2月11日，国务院总理李强在主持国务院第十八次专题学习时强调，要全面推进人工智能科技创新、产业发展和赋能应用，培育壮大新质生产力，推动高质量发展。要坚持统筹发展和安全，加强人工智能治理，完善相关法律法规、政策制度、应用规范、伦理准则，为人工智能应用筑牢安全保障。

丁薛祥：

加快建设科技强国 实现高水平科技自立自强

2026年1月26日，中共中央政治局常委、中央科技委员会主任丁薛祥在全国科技工作会议上指出，要加快建设科技强国，实现高水平科技自立自强。要夯实科技基础支撑，加快培育高质量发展新动能。要努力抢占国际竞争制高点，牢牢掌握科技竞争主动权。要坚持“四个面向”的战略导向，系统谋划部署科技工作，坚持规划引领和项目带动，加强基础研究，提高科研基础条件自主保障能力。要建强用好国家战略科技力量，优化各类科技力量功能定位，深化国际科技合作，提升国家创新体系整体效能。要推动科技创新和产业创新深度融合，强化企业创新主体地位，加快构建科技金融体制，更好引领新质生产力发展。要加强国际科技创新中心建设，发挥区域科技创新中心辐射带动作用，实现因地制宜、优势互补、共同发展。

国务院：

提升产业链供应链韧性和安全水平

2026年4月7日，国务院发布《国务院关于产业链供应链安全的规定》，旨在防范产业链供应链安全风险，提升产业链供应链韧性和安全水平，维护经济社会稳定和国家安全。《规定》共18条，主要规定了以下内容。

一是明确产业链供应链安全工作原则。规定产业链供应链安全工作贯彻总体国家安全观，统筹发展和安全，统筹国内国际，推进高水平对外开放，促进全球产业链供应链稳定畅通。明确国家引导产业链供应链合理有序布局，加强产业链供应链领域国际合作，支持关键领域核心技术攻关，促进产业链供应链高质量发展。

二是建立健全产业链供应链安全制度措施。建立健全产业链供应链安全工作机制。规定国务院有关部门和省、自治区、直辖市人民政府产业链供应链安全工作有关职责。加强关键领域产业链供应链安全保障，建立健全信息共享、风险监测预警、风险防范、应急管理制度，维护关键领域的原材料、技术、设备、产品等的生产与流通稳定、持续运行。

三是规定反制措施和域外适用。针对外国国家、地区和国际组织以及外国组织、个人损害我国产业链供应链安全的，建立产业链供应链安全调查制度，国务院有关部门可据此开展产业链供应链安全调查，采取反制措施。我国境内的组织、个人应当执行有关反制措施。任何组织、个人违法开展与产业链供应链有关的信息收集活动的，有关部门依法采取相应处理措施。

阴和俊：

统筹发展和安全 加快高水平科技自立自强

2026年1月26日，科技部党组书记、部长阴和俊在全国科技工作会议上做工作报告时强调，“十五五”时期是基本实现社会主义现代化夯实基础、全面发力的关键时期，是实现高水平科技自立自强、建成科技强国的关键攻坚期，要以支撑高质量发展为主题，以加快高水平科技自立自强、引领发展新质生产力为主线，以原创性引领性科技攻关为主攻方向，统筹发展和安全，加强科技创新全领域布局、全链条部署，持续锻造长板，强化补齐短板，确保科技强国各项任务落实落地。要加强基础研究战略性、前瞻性、体系化布局，强化原始创新和关键核心技术攻关，加快组织实施重大科技项目，强化国家战略科技力量体系化攻关能力。要加快推动科技创新和产业创新深度融合，强化创新链产业链无缝对接，进一步强化企业科技创新主体地位，加快培育壮大科技领军企业，加快重大科技成果高效转化应用，创新科技金融服务。要高水平推进三大国际科技创新中心建设，加快建设区域科技创新中心，打造辐射带动区域高质量发展的创新增长极，因地制宜发展新质生产力。要加强高水平深层次科技开放合作，深入推进“一带一路”科技创新合作，营造具有全球竞争力的开放创新生态。

“十五五”规划纲要： 提升网络安全保障能力

2026年3月13日，《中华人民共和国国民经济和社会发展第十五个五年规划纲要》正式发布。《纲要》强调，要提升网络安全保障能力。要深化网络空间安全综合治理，加快国家网络安全防御体系建设。要健全关键信息基础设施安全防护、网络安全审查、云计算服务安全评估等基础制度，完善互联网内容管理、网络平台治理等法规。要支持网络安全技术创新和产业发展，鼓励发展安全可靠的信息产品和服务。要深度参与网络空间全球治理和国际规则制定，积极拓展国际网络安全合作。

全国网信办： 锚定网络强国战略目标 全面做好网络安全和信息化工作

2026年1月5日，全国网信办主任会议在京召开，会议重点强调，要锚定网络强国战略目标，推动网信事业发展迈向更高水平，全面做好网络安全和信息化工作。要筑牢安全屏障，强化网络安全防护、网络数据安全管理和人工智能安全治理，全面推进国家网络安全体系和能力现代化。要注重赋能增效，着力推进网信领域科技创新、网信产业生态建设、信息基础设施建设、信息化应用等工作，以信息化助力高质量发展。要夯实法治根基，统筹推进网络领域立法执法普法，深入推进网络空间法治建设。

工信部等九部门： 加快多网融合进程 推动物联网产业创新发展

2026年3月31日，工信部、中央网信办、国家发展改革委、教育部、生态环境部、住房城乡建设部、国家卫生健康委、市场监管总局、国家数据局九部门联合印发《推动物联网产业创新发展行动方案（2026—2028年）》提出，要加快多网融合进程。推动移动物联网、无线局域网、有线网络等多网协同部署，加快物联网固移融合、宽窄结合等进程，提升物联网传输服务能力和网络资源连接汇聚能力；突破异构网络融合关键技术，推动物联网与工业、交通、环保等行业专网融合，提升全场景物联网融合服务能力。

工信部等五部门：

强化网络和数据安全保障 支撑低空基础设施发展

2026年2月10日，工业和信息化部办公厅、中央网络安全和信息化委员会办公室秘书局、中央空中交通管理委员会办公室综合局、国家发展和改革委员会办公厅、中国民用航空局综合司五部门联合印发《关于加强信息通信业能力建设，支撑低空基础设施发展的实施意见》指出，要加强信息通信业和低空装备制造业等协同发展，持续提升信息通信业技术基础能力、产业供给能力、网络支撑能力和安全保障能力。要强化网络和数据安全保障，探索构建信息类基础设施网络和数据安全保障体系，落实网络安全等级保护、关键信息基础设施安全保护等制度要求，深化信息通信业网络安全防护管理，加强数据分类分级保护，推进网络和数据安全标准研制，开展监测预警、检测评估、应急处置等能力建设，推动相关企业落实安全主体责任。

国家发展改革委、国家能源局：

强化网络与数据安全防护 促进电网高质量发展

2025年12月26日，国家发展改革委、国家能源局联合印发《关于促进电网高质量发展的指导意见》指出，要推进配电网柔性化、智能化、数字化转型；要强化电网安全风险辨识与管控能力，强化电力网络安全防御；要建立健全电网数据安全管理制度，持续提高电网数据安全保护水平；要完善电力系统安全稳定、电网智能化调度技术标准。

国家金融监管局：

强化网络安全防护 加快数字金融高质量发展

2025年12月22日，国家金融监督管理总局办公厅关于印发《银行业保险业数字金融高质量发展实施方案》，鼓励和引导银行业保险业加快发展数字金融，充分发挥数字技术和数据要素的双轮驱动作用，赋能金融服务提质增效。《方案》指出，要加强科技研发能力建设，提升科技自主可控能力。要提高网络安全韧性，加强数字金融生态下的网络安全边界延展控制，提高纵深防御水平。要加快推动安全运营体系和平台建设，常态化开展网络攻防对抗演习，提升威胁态势感知、风险监测预警和协同处置能力，有效应对网络攻击和重要数据资产安全威胁。要防范数字生态外部合作风险，加强对数字金融业务合作机构的管理，明确网络安全、数据安全等方面责任。

科技部等四部门： 加快推动网络安全保险创新应用

2026年3月2日，科技部、金融监管总局、工业和信息化部、国家知识产权局联合印发《关于加快推动科技保险高质量发展 有力支撑高水平科技自立自强的若干意见》提出，要推动网络安全保险创新应用。要持续开展网络安全保险服务试点，发布网络安全保险服务典型方案目录，扩大保险应用范围。要围绕电信和互联网、工业领域、金融领域及能源、教育、医疗卫生等重点行业差异化风险管理需求，鼓励保险机构开发多元化网络安全保险产品。要支持网络安全企业、专业网络安全测评机构等网络安全保险服务机构，开展网络安全风险评估、监测预警、应急处置等安全技术服务。

工信部： 健全互联网交换中心监管制度 提升安全防护能力

2025年12月30日，工信部印发《关于加快推进国家新型互联网交换中心创新发展的指导意见》提出，要健全交换中心监管制度，提升安全防护能力。要认真履行国家和行业网络与数据安全监管要求，建立健全网络安全、数据安全、信息安全管理制度，参照行业关键信息基础设施防护标准，定期开展安全评测和风险排查，做好通信网络和数据安全防护工作；要加强技术手段建设，提高网络安全、数据安全、信息安全风险监测和事件处置能力，实现重大安全威胁、风险和事件的实时感知与及时上报，保障服务安全可控。

党建领航强根基 守护文脉促创新

WAPI产业联盟组织参观响堂山石窟研究院

WAPI产业联盟 陈博

为推动党建与业务深度融合、互促共进，2026年3月27日，WAPI产业联盟组织十余家会员单位党员代表与技术骨干在河北邯郸响堂山石窟研究院开展主题党日活动。本次活动以“弘扬文化自信、守护历史文脉、赋能创新发展”为主线，引导党员同志在历史文化与数字技术交融的场景中深化认知、凝聚共识，把学习成果转化为推动标准化与产业协同的实践动力。

选择在邯郸开展活动，既是一次文化寻根，也是一堂“秩序与规则”的现场课。邯郸建城逾三千年，曾以“天下名都”闻名史册。从邯郸到邺城、大名、广府的历史变迁启示我们：繁华从来不是偶然，通达带来机遇，治理塑造秩序，而秩序最终沉淀为可持续的能力与规则。放到今天的数字世界，网络越互联、系统越复杂、产业越繁盛，越需要共同规则与体系能力作支撑。标准不是文件与口号，而是可验证、可复用、可推广的共同成果，是产业共同体长期主义的沉淀。

活动期间，在研究院专业人员的讲解下，大家系统学习了响堂山石窟的历史沿革与艺术特色，并通过高清影像、三维复原等展陈方式，深入了解文物数字化采集、资料建档、保护修复与展示传播的技术路径及管理流程，直观感受数字技术对文化遗产“保护第一、合理利用”的关键支撑作用。党员同志一致认为，石窟艺术所承载的审美创造与工艺智慧，是中华文明绵延不绝的重要见证。要从中



中华优秀传统文化中汲取精神力量，坚定文化立场、增强发展底气，将对历史文脉的理解转化为立足岗位、履职尽责的责任感与使命感。

参观交流中，大家对响堂山石窟研究院在文物数字化保护方面的成效印象深刻：相关工作流程规范、口径统一、管理可追溯、质量闭环完善。这种把分散经验沉淀为可复用方法体系的实践，与标准化工作的要义高度契合——通过一条款一条款推敲、一轮评审一轮评审打磨，使成果经得起工程检验、经得起产业放大、经得起时间考验。大家表示，将把研究院在规范化管理与质量控制方面的经验，转化为联盟标准研制与推广、测评验证与互操作、关键技术协同攻关与生态合作的具体举措，持续严把标准化工作全流程质量关，以更高水平的创新与协作，助力无线网络安全产业高质量发展。

WAPI产业联盟举办成立20周年公益植树暨访石经山悟初心主题党日活动

WAPI产业联盟 周园



2026年4月18日，WAPI产业联盟成立20周年公益植树暨访石经山悟初心主题党日活动在北京举行。联盟秘书处工作人员、会员单位党员、入党积极分子及业务骨干等40余人参加活动，以植绿添彩的实际行动践行绿色发展理念，在历史文脉中涵养初心使命、凝聚奋进力量。

燕东公园栽连翘：一锹土一桶水，共绘绿色底色

今年是联盟组织公益植树活动的第18年。自2009年以来，联盟持续以公益植树为纽带，把“为首都添绿、为社会尽责”融入联盟文化，累计栽植树苗逾万株。

活动现场既有多年参与的“老搭档”，也有光荣在党五十年的老党员，还有朝气蓬勃的青少年

儿童。“老带新”“一老一小”结对协作，挖坑扶苗、培土围堰、提水浇灌一气呵成，一株株连翘迎风挺立，为公园增添了一抹亮丽的新绿。

大家在劳动中深刻体会到，绿色发展不是口号，而是靠一代接着一代干出来的实事。此次在燕东公园栽植连翘，也让大家更加直观地感受到“增绿惠民”的意义：让身边的公园更美、让城市的春色更浓、让群众的绿色获得感更实。

走进房山石经山：在“刻经不辍”中体悟接续奋斗

植树活动后，全体人员前往房山石经山开展主题党日活动。从“前人栽树后人乘凉”的生态接力，到“藏之名山、传之万世”的文化接力，一堂跨



越时空的党性教育与文化教育课在山水间展开。

据现场讲解介绍：隋代僧人静琬为防典籍散佚、存世不全，立志将典籍刻于石板、藏入石洞。这项工程延续千余年，历经多个朝代接力完成，留下数量可观的石经与珍贵的历史见证。大家在了解史实后进一步体会到，石经山所体现的“刻经不辍”，其要义在于信念之坚、恒心之韧、接力之久；放到今天，就是“咬定青山不放松”的坚守，也是“功成不必在我、功成必定有我”的担当。

不少党员代表结合所见所感表示：当年刻经人未必知道谁会读到这些文字，却仍以毕生投入守护传承；这种面向长远、甘于奉献、接续传承的精神品格，与共产党人久久为功、接续奋斗的追求高度契合。孩子们也在山路与石刻间听得入神，更直观

地理解到，无论是种树、刻经还是国家建设，都离不开脚踏实地、持之以恒的“钉钉子精神”。

大家表示，面向今后工作，无论是生态建设还是科技创新，都要保持战略定力、坚持长期主义：把基础工作做扎实，把难题攻关做深入，把成果沉淀做持久，在接续奋斗中积小胜为大胜。

以实干致初心，以接力向未来

此次活动既是生态文明建设的生动实践，也是一次凝心聚力的思想动员。作为我国自主创新技术产业组织，WAPI产业联盟在推动无线网络安全技术标准化与产业协同发展的道路上，始终坚持守正创新、攻坚克难。大家表示，将把“种好一棵树”的务实担当与“守护一份传承”的责任意识，转化为“干好一项事业”的持久动力，在科技自立自强的新征程上接续奋斗，持续推动产业高质量发展，为全面建设社会主义现代化国家贡献产业力量！



中关村论坛发布WAPI产业联盟标准化创新成果案例

WAPI产业联盟 刘剑昕

日前，WAPI产业联盟标准化成果案例入选《标准引领高精尖产业高质量发展经验汇编》，并在3月26日召开的中关村论坛——标准化与科技创新发展论坛现场正式发布。此次案例入选，既是对联盟标准化工作成效的充分肯定，也凸显了相关成果在产业实践中的示范引领价值和广泛行业影响力。

本次论坛以“标准赋能科技创新与产业创新发展”为主题，集中发布“十四五”时期首都标准化工作成果，系统呈现科技前沿领域标准化应用的实践成效，为推动标准与科技创新、产业创新深度融合搭建交流平台。

WAPI产业联盟此次入选的案例题为《实现国际化突破，筑牢无线网络安全》，全面系统展现了联盟在标准与产业协同创新过程中，坚持问题导向、结果导向相统一，构建起“需求驱动—标准制定—检验检测—规模应用”的闭环体系，培育形成了协同高效、良性循环的产业生态。依托该体系，联盟



有效推动了我国无线网络安全标准落地应用，为国防、能源、政务、交通等关键行业高质量安全无线局域网规模化建设提供有力支撑，显著提升了相关行业网络安全防护能力，走出了从技术研发到产业应用的标准化创新发展之路。

作为推动标准与产业协同创新的重要载体，WAPI产业联盟长期致力于标准研制与推广应用一体化工作，在国家标准、行业标准、团体标准的研制、优化、推广等方面持续深耕，不断完善标准体系、强化应用落地，同时在国际标准研制与合作交流方面持续发力，积累了丰硕成果。

面向未来，联盟将坚持开放合作、协同创新理念，进一步推动标准化与科技创新、产业创新深度融合，积极参与国际标准研制与交流合作，加快标准成果推广应用和产业生态建设，持续提升数字基础设施安全保障能力，为我国数字经济高质量发展注入强劲动力、贡献更大力量。



以视频化解读助力标准应用

WAPI产业联盟持续完善团体标准宣贯载体

WAPI产业联盟 刘 婷

为进一步提升团体标准宣贯的针对性和实效性，WAPI产业联盟近日启动重点领域团体标准宣贯视频录制工作，探索以“标准文本+可视化解读”相结合的推广方式，持续完善标准宣贯载体，更好服务产业应用需求。

根据标委会重点任务计划，自去年以来，联盟标准化部围绕产学研用各单位在标准理解、工程落地等方面的实际需求，开展宣贯需求调研与路径论证，明确宣贯视频的制作方向、内容框架与发布安排，为系列化推进奠定基础。

2026年4月10日，联盟完成了团体标准T/WAPIA 010.11—2025《无线局域网产品工程化实现指南 第11部分：WAPI与IEEE 802.11be》宣贯视频录制。这是联盟在标准文本发布、会议宣讲等工作基础上形成的又一项宣贯成果，推动标准信息产品从“单一发布”向“多元供给”延伸。

宣贯视频以更直观、易理解的方式对标准要点进行梳理与呈现，突出工程化实施的关键关注点，便于相关单位和专业人员把握重点内容、技术要点与实施价值。相较于会议宣讲，视频产品更便于在线传播与反复学习，有助于扩大标准宣贯覆盖面，提升传播力与影响力。

下一步，WAPI产业联盟将围绕已发布团体标准持续推进宣贯视频录制与发布工作，并通过联盟网站、公众号等渠道陆续上线，推动形成一批可传播、可复用、可积累的标准信息产品，为标准化工作深入推进和产业高质量发展提供支撑。

扫描二维码观看视频：



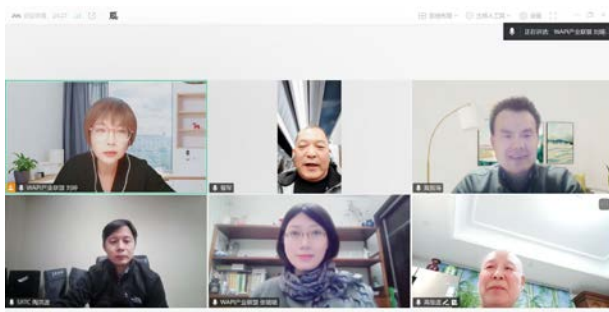
无线网络安全标准化工作委员会 2026年第一次主任委员会议（总第16次）顺利召开

WAPI产业联盟 刘婷

2026年3月18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”）2026年第一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总监刘婷出席。

会议围绕第一季度工作要点、标委会年度重点任务落实计划、2026年第一次标准工作和项目组会议筹备情况以及联盟未来重点工作和方向等议题进行报告与讨论。

刘婷报告第一季度工作，依据标委会2026年重点任务计划及相关会议决议，各项工作有序推进。标准制定方面，统筹推进25项团体标准，其中7项已发布，8项进入报批处理阶段，2项进入送审意见处理阶段、8项处于草案稿阶段；联盟及其成员参与的1项物联网安全技术提案获发布为国际标准。标准实施方面，联盟依标更新发布了新版WAPI功能测试项目，会员单位多款产品顺利通过联盟测试；针对WAPI建设中AS部署方式不规范等行业痛点，发布专



项应用洞察报告。标准平台及生态建设方面，圆满召开第四届标委会第二次会议、2025年第四次标准工作和项目组会议；持续跟踪相关国际组织动态，积极建立与其他标准开发组织的联络关系，促进WAPI相关标准纳入规范性引用体系；推进标准宣传形式多元化。会上还报告了2026年第一次标准工作和项目组会议筹备情况。

总体工作组（WG 1）负责人黄振海报告标委会23项年度重点任务的落实计划。

与会主任委员、副主任委员对上述工作给予充分肯定，并就2026年标委会重点任务、标准产业高质量发展、未来机遇与挑战等提出指导意见。

华为三款WAPI无线接入点通过联盟测试

WAPI产业联盟 王立华



图：华为WAPI无线接入点AirEngine 5770、AirEngine 5776I-X6EH、AirEngine 8770

2026年3月23日，华为技术有限公司（以下简称华为）的三款无线接入点（AP）产品通过了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，包含AE（鉴别器实体）驻留位置测试项，通过后联盟为上述设备出具了测试报告。

此次通过测试的AP产品型号为：AirEngine 5770、AirEngine 5776I-X6EH、AirEngine 8770，三款产品均支持支持WAPI协议及2.4/5GHz双频接入，通信速率符合802.11ac标准，采用瘦架构组网，支持本地转发和集中转发模式，并实现了AE完全驻留在AP中。

据华为介绍，上述是三款高性能AP产品，最高通信速率可符合802.11be标准，并提供2.5GE、10GE等多种接口类型，可满足室内外、高低密等不同场景需求，适用于电力、能源、政府等行业。产品基于华为云杉平台开发，具备敏捷架构、智能运维、开放兼容和高可靠性等特点。

为满足产业与市场发展需求，WAPI产业联盟在提供专业全面的WAPI测试服务同时，还为产业链上下游提供阶段性产品开发验证与技术支持。本次测试与阶段性成果聚焦于802.11ac模式：目前三款产品已完成802.11ac模式下的全部功能测试。后续将在此基础上，继续推进在802.11ax及802.11be模式下的功能开发与演进。

东和阳光三款WAPI产品通过联盟测试

WAPI产业联盟 王立华



图：东和阳光鉴别服务器DH-AS5002，无线接入点DH-WA5430和DH-WA5530

2026年3月17日，四川东和阳光科技有限责任公司（简称东和阳光）三款WAPI产品通过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。测试依据《无线局域网鉴别与保密基础结构（WAPI）功能测试项（2026年3月版）》（简称《WAPI测试项2603》）开展，联盟已为相关产品出具测试报告。

这三款WAPI产品分别为：型号DH-AS5002的鉴别服务器（AS）产品、型号DH-WA5430与DH-WA5530的无线接入点（AP）产品，能够满足目前行业高并发、移动性、大连接的应用需求。其中，AS支持漫游功能，鉴别性能达到1846次/秒；两款AP产品支持IPv6和2.4GHz/5GHz双频接入，通信速率符合802.11ac标准，采用瘦架构组网，支持本地转发和集中转发模式。

本次测试严格依据最新版《WAPI测试项2603》实施，确保测试指标与行业最新应用场景和技术要求保持一致，提升测试结果的权威性、可比性与一

致性，降低了产品研发适配与组网验证风险，为产品选型部署及规模化应用提供可靠支撑。

联盟测试实验室的WAPI测试服务紧跟技术标准演进以满足市场需求，近年来多次迭代更新《WAPI测试项》，持续完善测试内容与方法、提升测试能力与服务水平。实验室采用以需求牵引的“咨询型”服务模式，既提供WAPI互通性、完整性、性能等测试，承担标准符合性与互通能力的“合规把关”职责，又同步提供贯穿测试全流程的分析定位、整改建议、技术指导与复测验证服务。与此同时，实验室还提供WAPI协议基础要素测评服务，检验密钥安全存储与密码运算能力。另外可按需搭建仿真环境开展方案可行性、互联互通与业务压力等系统测试。配套检测能力建设、测试基准设备短期借用及远程调试等服务，为产业链上下游提供阶段性开发验证与技术支持。通过联盟测试的产品纳入相关产品信息名录，供市场用户采信与择优选型。

久壬科技WAPI系列产品通过联盟测试

WAPI产业联盟 王立华



图：久壬科技JR-WAPI-CPE和JR-WAPI-AP

2026年2月10日，上海久壬信息科技有限公司（以下简称久壬科技）WAPI系列产品通过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。测试依据2025年4月版WAPI功能测试项开展，联盟已为相关产品出具测试报告。

此次测试通过的产品共两款：分别为型号JR-WAPI-CPE的终端（STA）产品和型号JR-WAPI-AP的无线接入点（AP）产品。两款产品均支持WAPI协议和2.4GHz/5GHz双频，通信速率符合802.11ac标准。

据久壬科技介绍，JR-WAPI-CPE为小型客户端前置设备（CPE），支持12V至48V宽电压供

电，配备一个以太网接口和一个RS485接口，具备安全接入、稳定传输、良好适配性等特点，可满足工业无线网络终端快速接入WAPI网络的应用需求。JR-WAPI-AP为工业级室外AP，工作温度范围为-40℃~+85℃，浪涌与冲击抗扰度达到4级B类，防护等级为IP67，平均故障间隔时间（MTBF）大于50,000小时，适用于对环境适应性要求较高的应用场景。

久壬科技表示，公司正积极推进WAPI相关技术与产品研发，已形成涵盖STA与AP的产品布局。下一步将持续加大研发投入，进一步丰富产品系列、完善技术方案，增强与行业应用场景的融合能力，推动WAPI技术在更多领域落地应用。

四川东和阳光科技有限责任公司加入WAPI产业联盟

WAPI产业联盟 周 园

2026年3月12日，经联盟理事会批准，四川东和阳光科技有限责任公司（以下简称“东和阳光”）正式加入联盟。至此，联盟会员单位累计达到140家。



东和阳光成立于2017年，总部位于成都高新西区，是一家专注软件开发与信息技术服务的高新技术企业。公司业务覆盖人工智能应用开发、大数据服务、物联网、云计算、5G通信与工业互联网等领域，并延伸至智慧能源方向，提供储能技术、太阳能与风力发电等绿色能源解决方案。

东和阳光将WAPI业务作为未来重要的战略增长方向之一，依托在电力、能源、党政、应急等重点行业的项目经验，加快推进基于WAPI的终端产品研发与市场推广。目前，公司在成都、西安、北京设立三大研发中心，通过自研与共研协同推进，持续拓展WAPI在相关行业的落地应用。同时加快完善研发与交付体系，推动多款WAPI AP、WAPI AS产品落地和演进。

目前，东和阳光已与国家电网、中国移动、中国电信、中国通信服务、成都市兴蓉集团，以及四川大学、西南交通大学等企业及高校建立合作关系，后续将依托完善的系统集成与运维能力，持续为政府、电力、通信、科研及大型企业客户提供贯穿规划建设、实施交付、运营维护的全生命周期数字化、智能化转型服务。

国网新疆信通公司率先完成 国网系统内首套隔离WAPI装置测试

【中国日报网】

2026年2月，国网新疆信通公司与南京南瑞信息通信科技有限公司联合研发的隔离型WAPI（无线局域网鉴别与保密基础结构）装置测试成功，标志着公司成为系统内首家完成该测试的单位。此次测试是公司在电力无线通信领域内的积极探索，为未来新疆智能电网跨越式发展筑牢技术基础。

近年来，随着新疆电网数字化转型加速，无线通信技术在配网巡检、设备监控、远程运维等场景的应用日益广泛。传统无线专网通信手段若要满足生产和生活同时使用，需进行分别建网。隔离型WAPI终端作为传统WAPI技术的升级版，具备高强度的身份鉴别和数据加密能力，可满足生产控制大区和互联网大区终端同时接入需要，为沙戈荒地区偏远厂站内外网安全通信需求提供低成本、高可靠的解决方案。为验证方案的可行性，公司组织技术骨干在新型通信技术实验室开展隔离型WAPI技术测试。

此次隔离型WAPI装置测试涉及功能、安全、系统管理、稳定性等四个方面19个子项。经过技术人员历时2天的测试，隔离型WAPI装置各项性能指标均满足电力信息安全传输要求，其中AP到CPE的单向时延仅为50ms，数据丢包率低于1%。此次，隔离型WAPI装置的测试成功，不仅填补了新疆电网隔离场景无线安全防护测试的空白，更为后续WAPI技术在全疆电网规模化应用奠定了坚实基础。未来随着隔离型WAPI在变电站的落地应用，可满足海量无线智能采集终端的接入需求，进一步提升电网的智能化水平。

下一步，国网新疆信通公司将以此测试为契机，持续深化网络安全技术创新与应用，推动无线通信安全防护体系的迭代升级，为新疆新型电力系统建设和能源保供安全提供更坚实的技术保障。

一芯未来WAPI鉴别服务器AS： 为部队仓储无线认证筑牢安全高效基石

【科技资讯】

随着部队仓储信息化深入推进，无线网络广泛应用于物资盘点、手持终端作业、环境监控等场景。与此同时，接入设备数量快速增长、应用场景日趋复杂，传统无线认证在体系建设、证书管理、跨域漫游和审计追溯等方面短板凸显，给信息安全与管理带来挑战。

针对需求，一芯未来推出WAPI鉴别服务器AS，面向部队仓储构建高性能、自主可控、集中管理、支持跨域漫游的无线认证基础设施，从源头提升接入可信度。

据介绍，该产品基于国产硬件平台，面向高强度认证业务提供算力支撑，并通过集中化平台实现证书全生命周期管理，支持证书颁发、吊销、更新、查询等，满足大规模终端并发接入需求。管理端可集中配置认证策略、监控运行状态、审计接入日志，并提供多种接口，便于与仓储网络系统对接。

在安全能力方面，服务器基于WAPI双向认证机制，对接入终端开展证书校验，结合吊销与黑名单机制降低非法入网风险；同时可按角色与设备类型实施差异化授权，强化精细化权限管控，减少越权访问与数据泄露隐患。

此外，跨管理域漫游认证支持人员在不同库区移动作业时保持连接、减少重复认证，保障巡查、盘点、调拨等任务连续性；完善的审计日志记录认证与证书操作，为合规检查与事件追溯提供依据。

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。

鼎信通达申请 基于WAPI安全接入的SIP快速重注册方法及系统专利

【知识产权局】

据国家知识产权局信息显示，深圳鼎信通达股份有限公司申请一项名为“一种基于WAPI安全接入的SIP快速重注册方法及系统”的专利，公开号CN121486823A，申请日期为2025年11月。

专利摘要显示，本申请涉及一种基于WAPI安全接入的SIP快速重注册方法及系统，该方法包括采集终端设备的接入标识信息和当前网络状态参数，基于WAPI认证机制完成对终端设备的身份认证操作，并由认证结果生成认证状态对象；将认证状态对象与终端设备的接入标识信息进行加密绑定，并将加密绑定结果写入认证状态缓存结构中以形成认证状态缓存；向SIP服务器发送SIP_REGISTER请求，在接收到SIP_REGISTER响应报文后，从SIP注册响应报文中提取注册参数数据，并生成注册状态快照对象；将注册状态快照对象与终端设备的接入标识信息进行关联绑定，以形成注册快照映射结构。本申请具有增强终端接入的连续性的效果。

广东信通通信申请 基于WAPI通信的空调负荷调控方法专利

【知识产权局】

据知识产权局信息显示，广东信通通信有限公司申请一项名为“基于WAPI通信的空调负荷调控方法、装置及电子设备”的专利，公开号CN121677113A，申请日期为2025年12月。

专利摘要显示，本发明公开了一种基于WAPI通信的空调负荷调控方法、装置及电子设备，包括：通过多参数采集模块获取与待控制空调对应的目标参数，目标参数包括环境参数、运行状态参数和用户密度参数；基于WAPI通信模块将目标参数传输至核心控制单元和上位机调控平台，上位机调控平台基于目标参数生成上位机指令，并将上位机指令下发至核心控制单元；核心控制单元基于目标参数和上位机指令，通过预设负荷调控算法生成调控信号，并将调控信号下发至执行模块；执行模块根据调控信号对待控制空调的运行参数进行调节，以对待控制空调的负荷实现柔性调控；实现了空调运行参数的实时采集、安全传输与动态调控，同时联动电网负荷平台，达成空调负荷的柔性管理与能源优化。

联盛德：旗下盛德创信正式投产

【联盛德微电子】

2025年12月26日，盛德创信科技（瑞安）有限公司（以下简称“盛德创信”）正式投产。

北京联盛德微电子有限责任公司CEO李庆在投产暨开业庆典上介绍了盛德创信的发展愿景与产业布局。本次一期投产的生产线，全线采用全自动化生产、AI视觉检测、全系统追溯等先进技术，产品将直接服务于WAPI信创、5G通信、工业控制等国家战略性新兴产业，全面满足党政、能源、电力、交通等关键基础设施的国产化替代需求。

“本次产线投产，要感谢龙芯创投和海越创投的鼎力支持。这不仅是对联盛德技术实力和商业前景的充分肯定，更是一次深度的战略协同。今天的投产，不是终点，而是信创安全无线通信规模化的起点。我们将以此次为新动能，持续加大研发投入，与生态伙伴一道，打造更多自主可控、安全可信、全球领先的无线通信产品，为数字中国、智慧城市建设做出自己的贡献！”李庆表示。

数字认证：构建密码保障体系 筑牢电力信创安全防线

【数字认证】

在近日召开的“第三届电力企业信创国产化技术研讨会”上，数字认证公司企业金融事业部副总监冯媛媛就如何构建应需而动的密码保障体系，筑牢电力安全防线，同与会嘉宾进行了深入探讨与交流。

冯媛媛表示，我国正处于新型电力系统深度变革期，高比例新能源、储能和可控负荷的大规模并网，形成了“源-网-荷-储”频繁跨区交互、业务交织融合、网络边界模糊的新格局。这意味着，仅靠现有的网络边界隔离技术与传统的密码供给模式，已无法满足新型电力系统对于高弹性密码服务、体系化密码支撑、高质量密码保障的新需求。

在坚持“安全分区、网络专用、横向隔离、纵向认证”十六字建设方针前提下，新型电力系统可通过构建以密码算力基础设施体系、密码应用与能力体系、密码运行保障体系、密码评估体系、密码监管体系为核心的密码保障体系，打造全面适配信创环境的分布式密码架构，从而实现密码资源的统一、动态与实时保障，助力电力企业落实密评密改合规要求，保障关键业务高效稳定运行，推动重构电网弹性边界，提升数据安全交互效率，最终形成新型电力系统网络安全主动防御与自主可控。截至目前，数字认证已成为国家电网、南方电网、长江电力、大唐集团、华能集团等电力企业的信任之选。

数字认证入选“2026年网络安全国家标准应用实践案例”

【数字认证】

近日在全国网络安全标准化技术委员会2026年第一次“标准周”活动上，北京数字认证股份有限公司与四川省市场监督管理局数据应用中心联合申报的“GB/T 45577-2025《数据安全技术 数据安全风险评估方法》等标准在市场监督管理局‘多证合一’场景下的应用”成功入选网络安全国家标准应用实践案例。



该入选案例是数字认证依托GB/T 45577-2025《数据安全技术 数据安全风险评估方法》、GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》两项国家标准，针对四川省市场监督管理局数据应用中心“多证合一”场景千万级高敏感政务数据，全面开展数据安全风险识别、数据安全能力成熟度评估与全生命周期防护建设的实践。

入选案例保障了政务服务数据在采集、存储、传输、共享、使用等环节的安全合规，为政务领域数据安全治理提供了可复制、可推广的标准化实施路径，实践成效显著。



博洛米第三代高性能WAPI通信模块量产

【博洛米通信】

日前，南京博洛米通信技术有限公司（以下简称博洛米）的第三代高性能WAPI通信模块已完成相关测试、试验和认证，开始批量生产。

据介绍，上述WAPI模块分为单通道和双通道两种款式，和上一代产品相比，大幅提升了性能并降低了尺寸和功耗。

模块支持IEEE 802.11 a/b/g/n/ac/ax网络协议标准和2.4/5GHz工作频率，单通道款空口速率最高可达600Mbps，尺寸约为32×32×3.2mm，单天线，系统连接器为FFC/FPC，因其超小超薄的显著特点，适用于对尺寸、功耗敏感且相对固定使用的宿主设备，如扫码贴签终端、手持机、平板电脑、固定读写设备、高性能传感器等。

双通道款空口速率最高可达1,200Mbps，尺寸约为51×30×3.1mm，使用标准的mini-PCIE管脚定义，双天线，支持极速漫游功能，适用于对性能要求更高，或需在快速移动环境中联网使用的宿主设备，如叉车平板、穿梭车、AGV、无人机、机器人、移动读写设备等。

模块内嵌WAPI安全协议，符合GB 15629.11国家标准和SJ/T 11940、SJ/T 11942、SJ/T 11943、SJ/T 11944等信创标准；内置安全芯片，用以存储证书和私钥，防泄露或盗用；支持SM2、SM3、SM4全国密算法；工作温度：-41℃~+70℃，贮存温度：-55℃~+85℃；可靠性高，鲁棒性强。

据博洛米介绍，模块硬件国产化，软件自主可控，可选支持COB卡密码模块；支持Intel、AMD以及飞腾、龙芯、兆芯、海光、鲲鹏等国产CPU，已适配Windows、Linux以及统信、麒麟、鸿蒙等国产操作系统。



第三代高性能WAPI通信模块单通道款



第三代高性能WAPI通信模块双通道款

国安部提醒：注意词元（Token）使用带来的安全风险

【中国信息安全】

近期，国家数据局正式定名的AI领域核心术语词元(Token)成为网络热词。据统计，截至今年3月，我国日均词元调用量已超过140万亿，较2024年初增长1000多倍。"词元"这个新词实际上早已融入生活的方方面面。面对新技术新应用，我们既要主动拥抱，善加运用，又要防范风险，确保安全。

什么是词元(Token)?

简单来说，词元是AI大模型处理信息的最小单元，兼具可计量，可定价，可交易三大特征。它不仅是智能时代的价值锚点，更是连接技术供给与商业需求的"结算单位"。词元应用场景远超AI领域，与日常生活紧密相关。

身份凭证类，相当于数字世界的"临时身份证"，用于便捷登录各类平台，完成转账授权等，如微信登录第三方小程序，手机银行动态口令等，有明确有效期，兼顾便捷性与安全性。

AI场景类，即官方定名的"词元"核心应用，是使用如AI写作，修图，剪辑等AI服务的消耗性资源。

权益凭证类，可以理解成区块链场景下的"通证"，相当于数字化权益证明，如电子票，游戏皮肤，会员积分等，具有不易伪造，便于流转的特点。

词元(Token)热潮下的信息安全隐患

随着词元的爆火，一些不法分子开始打起了词元的主意，伺机布设各种陷阱。同时，词元本身在使用过程中也存在一定的安全风险，需要我们加以防范。

泄露劫持风险。不法分子可通过跨站脚本攻击(XSS)，公共Wi-Fi嗅探等方式，窃取，截获未加密的词元。一旦词元泄露，攻击者可直接盗用用户身份，获取隐私信息，登录账号，篡改数据，甚至实施诈骗，转账等操作，直接威胁个人财产安全。如果海量词元被汇总分析，则可能引发系统性风险，危害数据安全与国家安全。

伪造篡改风险。若词元缺乏加密或签名防护，不法分子可直接修改词元的权限字段，伪造管理员身份绕过系统验证，非法获取用户敏感隐私数据，实施越权操作。同时，不法分子还有可能制造"虚假词元"，诱导用户泄露身份证号，手机号等隐私信息。

诈骗陷阱风险。当前，各类"词元骗局"层出不穷：用低价AI词元套餐，词元投资等噱头，诱骗用户资金；冒充官方平台，以官方升级，验证为由，骗取个人隐私信息。尤其是宣称"囤词元能暴富""场外交易赚差价"等行为，不仅涉嫌非法金融活动，还可能被境外间谍情报机关用以开展数据窃取，资金渗透，危害国家经济安全与数据安全。

词元(Token)这么火，应该注意点啥?

面对词元热潮，我们既要理性看待其价值，又要注意信息安全，隐私安全，提高安全防范意识，做到了解

词元，善用词元。

认清词元属性。词元可作为数字身份凭证，并非投资品，防范以“词元投资”“高收益回报”“词元理财”“词元挖矿”等为噱头的各类骗局，切勿盲目购买未经官方认证的小众，虚拟词元，不随意注册来路不明的词元服务，从源头上避免因贪利，跟风导致的个人隐私信息泄露和财产损失。

强化使用规范。使用词元相关服务时，优先选择正规平台与加密传输通道，不在公共网络，不安全环境下进行登录，转账，填写隐私信息等敏感操作；不点击陌生链接，不下载非官方APP，不扫描可疑二维码，及时更新设备系统与安全软件；严格保管词元口令，授权码及绑定的手机号，身份证号等信息，开启双因素认证，不共用账号，不设置通用密码，发现账号异常立即采取改密，解绑，报备等止损措施。

遵守法律法规。面对词元等AI领域的新兴应用与概念，应保持理性认知，既不盲目追捧，也不跟风炒作，自觉遵守法律法规与监管要求，主动学习官方发布的词元安全知识与风险提示，提高辨别能力；科学区分身份凭证类，AI场景词元与区块链通证，加密货币，不参与非法加密货币交易，如遭遇诈骗，信息泄露或发现非法活动，应及时向有关部门反映。

伊朗中部遇袭期间该国美制通信设备集体“失灵”

【新华社】

新华社德黑兰4月15日电 据伊朗法尔斯通讯社14日报道，在伊朗中部伊斯法罕省遇袭期间，伊朗境内大量美国制造的通信设备突然失灵，操作系统崩溃。

报道说，出故障的通信设备全部来自美国的思科、飞塔和朱尼珀等品牌。

报道援引伊朗网络安全专家分析认为，该国的通信网络此次可能遭受四种恶意攻击。一是隐藏访问：相关产品中包含即使没有互联网连接也能激活的“后门”，能够破坏设备；二是恶意数据包：从网络内部发送特殊数据，致使系统瞬间瘫痪；三是潜伏式“僵尸网络”：潜伏多年的恶意软件，在特定事件发生时被激活；四是生产链污染：硬件和软件在进入该国前已被篡改，即使更换操作系统也无法解决问题。

报道说，此次事件表明，一个国家网络安全的支柱不能依赖外国设备。真正的安全始于自主拥有和生产本土技术。发展国产设备不再是一句口号，而是在网络战中生存的必要条件。

熟悉网络安全的消息人士告诉法尔斯通讯社，伊朗的网络实验室将在近期公布更多证据和信息，表明相关设备制造企业与美国和以色列政府之间存在技术合作。

指标实测 场景适配

WAPI 2.0-1DN示范网取得阶段成果

本文由无线网络安全技术国家工程研究中心、WAPI产业联盟联合撰写

一、摘要

WAPI 2.0是面向后量子时代长期安全需求的新一代无线局域网安全技术标准体系。它通过安全协议与密码机制的代际演进，提升了无线接入的身份可信、数据保密与抗攻击能力；同时，该体系支持与既有WAPI 1.0网络的无感共存与平滑迁移，为后续与后量子密码体系协同演进预留了敏捷扩展空间。

在无线承载关键数据与核心业务不断增加、密码体系面临新型威胁、合规要求持续升级的背景下，行业用户正处于在保证现网连续运行的基础上，评估未来风险、布局长期安全的关键窗口期。WAPI 2.0目前已进入标准持续完善与产业化提速的双轨道阶段，适合通过示范试点实现需求牵引与实效验证，即将“标准先进性”转化为“可验证、可复制、可演进”的工程样本，将“技术先进性”转化为“可采购、可部署、可运维、可证明价值”的产品与生态能力。为此，在WAPI产业联盟组织下，无线网络安全技术国家工程研究中心开展了WAPI 2.0-1DN示范网建设工作。该示范网摒弃了生产网“一次性替换”的高风险模式，通过小范围概念验证先行、受控范围实测、渐进式扩展的策略，已完成第一阶段验证任务。

本阶段成果聚焦关键能力的穿透性验证，重点验证互通、性能体验与深度安全能力（包括管理帧保护、快速切换、身份信息保护等），沉淀出一套可复用的网络架构、标准化部署与测试方案及问题闭环清单，并为行业提供了极具参考价值的WAPI 1.0/2.0 双模并存及分阶段迁移路线建议。

二、建设背景

（一）WAPI 1.0技术标准体系

WAPI 1.0技术标准体系于2000年启动，2003年起陆续发布GB 15629.11系列标准，采用三元对等安全架构与国密算法体系，提升了无线接入的身份鉴别与数据保护能力，降低“假基站”“蹭网”等典型风险。相关核心技术亦形成国际标准ISO/IEC 9798-3，以及百余项国家、行业和团体标准，并在电信、能源、国防、政务等领域持续应用，产业生态与配套标准体系不断完善。

（二）WAPI 2.0技术标准体系

WAPI 2.0技术标准体系于2015年启动，面向量子计算发展对传统密码算法与安全协议可能带来的风险提出应对方案，首个标准T/WAPIA 046于2021年发布，重构面向未来的安全基础结构，新增原子密钥建立与实体鉴别协议、快速切换机制，增强面向量子威胁的缓解与演进能力；同时适配通用商密算法，强化身份保护和

抗离线字典攻击能力。目前，WAPI 2.0体系正分阶段演进，并与后量子密码算法标准化进程协同推进，逐步构建面向量子时代的长期安全保障体系，服务工业互联网、物联网、车联网等场景，为关键信息基础设施的连接与互联安全提供支撑。

截至2026年第一季度，WAPI 2.0技术标准体系已构建起初步完备的矩阵。以核心标准 T/WAPIA 046—2021《无线局域网安全技术规范》为基石，辅以T/WAPIA 046—2021/XG1—2025（第1号修改单）的持续迭代，以及T/WAPIA 054—2025《高质量安全无线局域网 总体要求》和 T/WAPIA 037.2—2026《无线局域网测试 第2部分：设备测试方法》等关键规范的发布，标志着 WAPI 2.0已完成从技术定义到落地指引的多维度覆盖。

通过在加密算法、身份鉴别机制及密钥管理策略等维度的深度重构与持续进化，WAPI 2.0 展现出显著的代际跨越：相较于WAPI 1.0，它不仅实现了抵御量子计算攻击能力的增强，更引入身份信息保护机制，显著提升了系统安全防护能力与数据隐私保障水平，为关键信息基础设施夯实了“底座级”安全保障。

WAPI 2.0带来的核心能力：

- **长期安全与可升级：**引入原子密钥建立与实体鉴别（AKEA）等新机制，采取混合设计策略缓解量子威胁，敏捷算法架构支持标准化升级接口，为后续与后量子密码体系协同演进预留空间。
- **更强抗攻击能力：**强化对等鉴别与密钥建立，增强抵御接力攻击、离线字典攻击等能力。
- **身份信息保护：**接入过程中对证书等身份信息进行保护传输，降低身份暴露与轨迹被追踪风险。
- **更好的移动体验：**支持快速切换机制，降低漫游时延与业务中断概率，适配音视频等实时业务。
- **平滑演进与兼容互通：**支持与WAPI 1.0网络/终端并存运行，便于分阶段升级与渐进式替换。

三、建设目标

WAPI 2.0-1DN示范网的建设，旨在锻造一个完全符合T/WAPIA 046标准要求、面向量子时代长期安全需求的高质量安全无线局域网样板环境。通过在复杂真实的业务实境下，对WAPI 2.0关键能力及产品规模化应用成熟度进行“全量实测”，将沉淀出一套低风险跨越、分阶段演进、高效率运维的工程化落地方案，从而为WAPI 2.0的规模市场化应用输出可复刻、可推广的标准化范式。

具体目标包括：

- 1) **核心技术指标实测：**为WAPI 2.0产品面向规模部署的成熟度验证提供环境，验证技术与产品从实验室到现网应用的可行性；
- 2) **多场景适配：**完成典型应用场景下的部署，支撑实际业务运行；
- 3) **成本可控性验证：**测算能耗、运维人力等全生命周期成本，为规模化部署提供降本方向；

- 4) **跨行业合作标杆**：落地办公、教育、远程会议等典型行业应用案例，验证跨场景价值；
- 5) **现网平滑演进**：通过WAPI 1.0与WAPI 2.0双模并存实测，验证迁移与切换能力，优化现网升级路径；
- 6) **人才储备**：培养网络建设、运维服务等专业能力；
- 7) **行业交流**：开展成果发布与行业交流，促进产业认知与应用转化。

四、建设原则

(一) **合规性**：严格遵循WAPI核心标准（T/WAPIA 046、T/WAPIA 007、T/WAPIA 010.3、GB 15629.11）及相关配套规范，并按测试方法开展验证。

(二) **成熟性**：优先选用经过联盟实验室/第三方测试验证或已有工程验证记录的设备与版本，降低部署与运维风险。

(三) **经济性**：控制硬件采购与施工成本，适配中小规模场景预算需求。

(四) **兼容性**：支持与现有WAPI 1.0网络兼容互通，满足渐进式演进需求。

五、建设方案

WAPI 2.0-1DN示范网采取“三步走”方式有序推进：

第一阶段：基础验证期（当前已圆满收官）。聚焦标准体系核心能力，重点完成了WAPI 2.0关键能力的穿透性验证与初步的异构互联互通。

第二阶段：能力迭代期。依托规模化试点，旨在实现性能体验的极速化、运维管理的智能化以及安全保障的全方位升维。

第三阶段：示范推广期。面向全场景规模示范应用，旨在沉淀出可直接复刻、具备多行业普适性的全栈解决方案与实践范式。

目前，第一阶段基础验证工作已高效完成，为后续的大规模应用奠定了坚实的实证基础。

（一）网络架构设计

WAPI 2.0-1DN示范网整体架构上采用部署复杂度低的“核心-接入”两级简化架构：

1) **核心层**：在中心部署支持WAPI 2.0和WAPI 1.0的证书签发与鉴别服务器（CIS&AS），负责整个网络的管理和鉴别。

2) **接入层**：在中心及分中心部署支持WAPI 2.0+WAPI 1.0双模的AP设备，覆盖目标区域。

网络拓扑架构见图1。证书签发与鉴别服务器通过局域网或互联网与接入层AP连接，终端通过WAPI 2.0或WAPI 1.0协议接入网络。

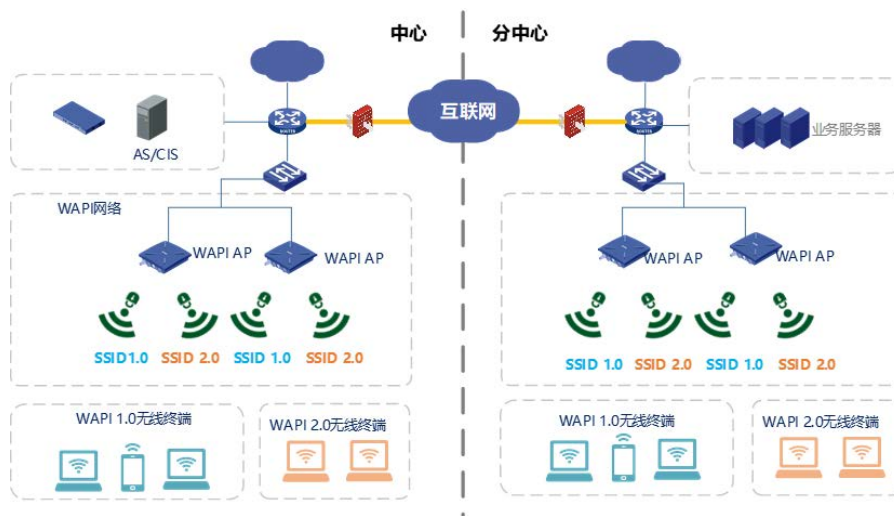


图1：WAPI 2.0-1DN第一阶段示范网拓扑架构

(二) 设备选型

1) 终端 (STA)

- a) 支持2.4GHz/5GHz频段；
- b) 支持WAPI2-CERT、WAPI-Cert、WAPI2-PSK和WAPI-PSK安全模式；
- c) 支持WPI-SM4-OFB+CMAC和WPI-SM4-GCM加密模式；
- d) 支持WAPI快速切换 (WAPIFT) ；
- e) 支持WAPI管理帧保护功能；
- f) 符合GB 15629.11和T/WAPIA 046等WAPI相关标准。

2) 无线接入点 (AP)

- a) 采用双频设计，支持2.4G/5G频段工作模式；
- b) 支持WAPI2-CERT、WAPI-Cert、WAPI2-PSK和WAPI-PSK安全模式；
- c) 支持WPI-SM4-OFB+CMAC和WPI-SM4-GCM加密模式；
- d) 支持WAPI快速切换 (WAPIFT) ；
- e) 单AP支持 ≥ 64 个终端接入，支持PoE网线远程供电；
- f) 支持WAPI管理帧保护功能；
- g) 符合GB 15629.11和T/WAPIA 046等WAPI相关标准。

3) 证书签发与鉴别服务器 (CIS&AS)

- a) 支持WAPI 1.0证书与WAPI 2.0证书的签发、撤销和查询等证书管理功能;
- b) 支持WAPI 1.0证书鉴别与WAPI 2.0证书鉴别;
- c) 支持多用户并发鉴别能力, 鉴别性能≥500次/秒;
- d) 支持WAPI漫游证书鉴别;
- e) 符合GB 15629.11和T/WAPIA 046等WAPI相关标准。

(三) 部署方案

第一阶段部署方案(见图2)深度契合前期需求调研与示范场景属性, 实现了从网络架构细化设计到现场组网开通的全流程工程化闭环。在示范网稳定运行期间, 项目组开展了全维度、高强度的功能与性能实测: 涵盖了WAPI 1.0与WAPI 2.0的协议深度兼容性验证、极限带宽压力下的流量传输测试、高密度并发连接性能评估, 以及管理帧保护机制的安全强度校验等核心项。通过对网络稳定性的持续打磨与可运维性的深度优化, 示范网成功构建了“实测、优化、再验证”的演进机制, 为后续示范范围的扩大与规模化应用奠定了坚实的技术底座与工程范式。

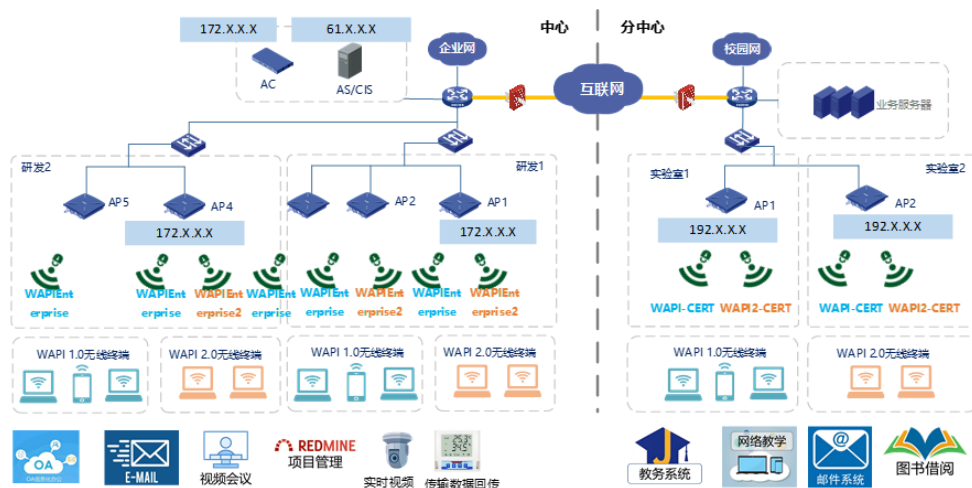


图2: WAPI 2.0-1DN第一阶段示范网部署方案

1) 设备清单

序号	设备名称型号	数量
1	WAPI 无线接入点	7
2	WAPI 无线客户端	100
3	WAPI 证书签发与鉴别服务器	1
4	WAPI 接入点控制器	1
5	WAPI 无线 CPE	10

2) 业务场景设计

a) 科研与办公应用场景：支持科研数据访问、办公系统使用及信息共享等业务，验证网络在日常生产环境中的稳定性与安全性。

b) 视频会议与网络教学场景：支持高清实时视频会议和在线教学应用，验证网络对实时业务的带宽保障与低时延能力。

c) 数据采集与物联网接入场景：支持终端设备数据采集与实时上传，验证网络在多终端接入场景下的可靠接入能力。

d) 移动视频传输与漫游场景：移动终端在不同接入点间移动并进行实时视频回传，验证快速漫游切换与业务连续性。

e) 无线安全能力验证场景：通过管理帧保护、主动身份保护及增强密码算法等机制，验证网络整体安全防护能力。

f) 协议兼容与演进场景：WAPI 1.0与WAPI 2.0 终端同时接入网络，验证协议兼容性与网络平滑升级能力。

(四) 实境验证

1) 协议兼容与演进场景

在示范网中开展协议兼容与演进场景验证测试。通过部署同时支持WAPI 1.0和WAPI 2.0的无线接入点，并接入不同版本协议的终端，验证两种协议在同一网络环境下的兼容互通能力。测试过程中，WAPI 1.0终端与WAPI 2.0终端能够正常完成接入鉴别并开展业务通信，网络运行稳定，未对现有业务产生影响。同时，支持WAPI 2.0的终端接入时可启用相应安全机制，实现更高等级的安全保护。测试结果表明，示范网能够在保持现有WAPI 1.0终端正常运行的基础上，支持向WAPI 2.0安全方案演进，为无线网络的升级部署与规模化推广提供兼容性支撑。

2) 移动视频传输与漫游场景

在示范网中开展了视频回传业务场景下的无线快速切换测试（见图3、图4）。测试过程中，终端在不同接入点间移动并持续进行实时视频数据回传。测试结果表明，在启用WAPI 2.0快速切换机制下，单射频终端在不同接入点间的平均切换时延小于50ms，切换过程平滑稳定。与未启用快速切换机制的传统无线网络相比，WAPI 2.0可减少漫游过程中的业务中断时间，提升视频监控等对时延与连续性要求较高业务的支撑能力。

3) 无线安全能力验证场景

在示范网中开展管理帧保护能力的对比测试（见图5），通过模拟无线管理帧攻击场景，对启用与未启用管理帧保护机制的网络运行情况进行验证。测试结果表明，在启用WAPI管理帧保护机制后，无线网络能够对

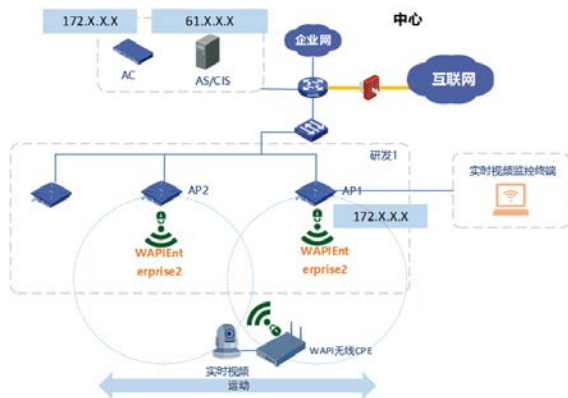


图3: WAPI 2.0-1DN第一阶段示范网
视频回传快速切换验证场景拓扑

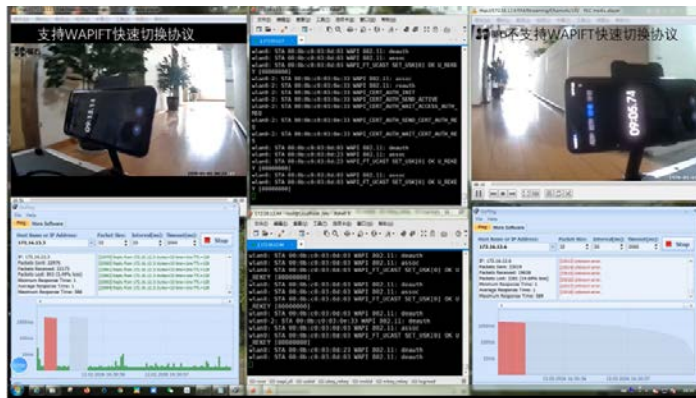


图4: WAPI 2.0-1DN第一阶段示范网
视频回传对比测试

伪造或恶意管理帧进行有效识别与防护，提升对管理帧攻击的抵御能力；在未启用相关保护机制的情况下，网络在攻击场景下更易受到干扰，可能影响终端接入与业务通信。测试表明，WAPI管理帧保护机制有助于增强无线网络的安全性与稳定性。

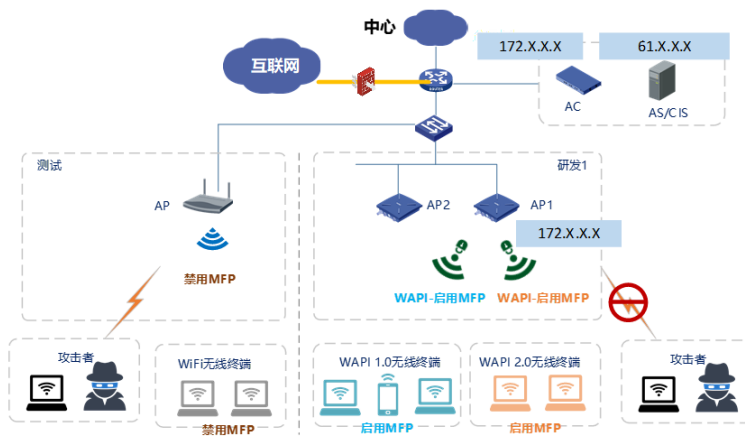


图5: WAPI 2.0-1DN第一阶段示范网WAPI管理帧保护验证场景拓扑

六、示范效果

WAPI 2.0-1DN示范网第一阶段已完成从顶层规划、实境部署到权威验证的全链条任务。通过在真实业务流量环境下深度部署WAPI 2.0安全机制，成功构建起集高安全性、稳健可靠性与敏捷兼容性于一体的无线局域网实战化样板。

项目组围绕身份鉴别、数据保密、快速切换及管理帧保护等关键维度的核心能力进行了系统性穿透验证。验证数据表明，示范网整体运行稳健，各项功能响应与性能指标均达到预期目标，其核心实证价值体现在以下维度：

（一）经济性

在满足终端/接入设备软硬件能力与产品实现条件的前提下，WAPI 2.0部分能力可通过软件版本升级与配置优化实现增强，从而降低改造成本与迁移风险。对于不具备升级条件的存量设备，可结合双模并存、分区替换等方式分阶段演进，避免对现网业务造成冲击。

（二）高安全性

WAPI 2.0通过引入先进的身份鉴别机制与更高强度的密码算法体系，提高无线接入的整体安全等级。在示范网运行过程中，在防范字典攻击、保护用户身份信息以及提升数据通信安全性等方面体现出明显优势。同时，通过增强管理帧保护机制增强对拒绝服务攻击等安全威胁的抵御能力，提升网络安全性与稳定性。

（三）高可靠性

WAPI 2.0支持更加高效的快速切换机制，在终端移动接入过程中实现更加平滑的网络漫游与切换，降低业务中断概率，提高无线网络连接的连续性与稳定性，从而保障关键业务应用的稳定运行。

（四）良好兼容性

示范网采用同时支持WAPI 1.0与WAPI 2.0的设备，实现对现有网络环境的兼容，并为向WAPI 2.0安全方案升级提供平滑过渡路径，满足产业对兼容互通与渐进式升级的实际需求。

总体而言，WAPI 2.0-1DN示范网第一阶段的成功建设，不仅有效验证了WAPI 2.0技术在防御升维、链路稳健及体验优化维度的显著工程化实效，更打通了从“标准先进性”向“现实生产力”转化的关键路径。这一阶段性成果不仅确立了新一代安全无线局域网的实战基准，更为后续规模化部署与技术跨行业应用提供了具有参考价值的工程蓝本与决策依据。

七、下一步工作

随着无线网络应用场景不断拓展及网络安全威胁形态持续演进，无线局域网对安全机制、可靠性与可管理性的要求将不断提高。WAPI 2.0作为新一代无线局域网安全技术，在身份鉴别机制、密码算法体系、用户隐私保护以及管理帧安全等方面具备技术基础与发展潜力。

未来，将在WAPI 2.0-1DN示范网既有成果基础上，进一步扩大WAPI 2.0应用范围，在更多典型场景（如企业园区网络、行业专网及公共无线网络等）持续开展验证与实践，不断完善技术方案与部署经验。同时，结合产业发展需求，持续优化快速切换、安全鉴别与网络管理能力，提升无线网络整体安全水平和运行效率。

此外，随着量子计算技术的发展，网络安全体系抵御量子计算攻击的需求将逐步增强。WAPI 2.0在量子安全方面的技术探索，可为构建面向未来的无线网络安全体系提供支撑。通过持续推进技术研究、产品优化与标准化工作，有望推动WAPI安全技术体系在更广泛领域的应用，进一步提升无线局域网整体安全防护能

力，为无线网络的安全、稳定和可持续发展提供支撑。

八、欢迎产业链各环节单位参与示范网建设

联盟诚挚欢迎产业链各环节单位以联合测试、联合试点、联合示范等方式积极参与，共同促进标准技术演进、互通成熟与应用落地。

为降低用户尝试成本、减少对现网影响并加快产业互通成熟，本示范网提供分层参与路径。各参与方可根据自身资源与业务敏感度，灵活选择选择从“验证”到“示范”的不同梯度，逐步推进。

我们期待与各方携手合作，共同探索创新应用场景，促进WAPI 2.0技术成果转化与规模化推广。

联盟联系方式：

电话：010-82351181

邮箱：staff@wapia.org

网站：www.wapia.org.cn

关于无线网络安全技术国家工程研究中心

无线网络安全技术国家工程研究中心（以下简称“工程中心”）是国家发展改革委在基础性网络连接和互联安全领域布局的唯一产业技术创新基础设施，成立于2011年12月，设有技术集成研发、密码工程验证、协议测试技术、电子政务应用、智能电网研发应用、产业协作等六个中心。

自2011年12月成立以来，工程中心聚焦网络空间安全基础共性技术，聚合国内外优质创新资源，开展区域性跨学科、大协同的基础研究和应用基础研究，持续攻关网络信息领域原创性关键技术和“卡脖子”技术，推动科技成果转化与产业化，在“新基建”中发挥好产业技术创新基础设施的国家队作用。

工程中心为全球用户提供不断创新的网络安全协议技术与解决方案、安全网络装备与解决方案，致力于保障网络连接的安全与可信。对密码算法、密码机制的长期深入研究，保障了安全协议安全高效执行和法规遵从。

在我国三元对等（虎符TePA）网络安全技术架构及体系诞生和发展成熟的历程中，工程中心一直承担着“从0到1”的国家使命——首个技术提案；首个国际标准；首个国家标准；首行标准代码；首个安全协议栈；首套样机/装备；首个通用示范网络；首个技术转移案例。

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：staff@wapia.org

网 址：<http://www.wapia.org.cn>