

在路上 ON THE ROAD

WAPI产业联盟

17岁了



WAPI产业联盟公众号



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中心
国家无线电监测中心检测中心
西电捷通公司
北大方正集团有限公司
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 简 练 米 东
王立华 刘剑昕

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 zhouy@wapia.org
网 站： <http://www.wapia.org.cn>
公众号：



主编寄语 17 Years

05 17载时光洗练 而今迈步从头越

媒体聚焦 Media Focus

06 中国电子报/电子信息产业网等：

虎符TePA系列标准及实施入选“工业和信息化领域商用密码典型应用方案名单”

14 通信世界等：WAPI产业联盟召开2023年第一次标准工作及项目组会议（总第125次）

WAPI 问答 WAPI FAQ

22 WAPI 问答（系列连载）第三部分

特别报道 Special Report

18 密码讲堂：什么是密码？

联盟关注 Alliance Concerns

20 国务院机构改革方案

23 加快建设质量强国 着力推动高质量发展

26 两会声音——全国政协委员、国家无线电监测中心主任程建军：

构建现代化频谱治理体系 维护安全有序电波秩序 推动无线电事业高质量发展

产经要闻 Industrial & Economic News

28 习近平：要加快科技自立自强步伐 解决外国“卡脖子”问题

29 习近平：要打好科技仪器设备、操作系统和基础软件国产化攻坚战

29 王志刚：科技政策要聚焦自立自强

30 工信部：三方面发力 加快工业互联网规模化发展

31 证监会：聚焦网络和信息安全领域 网络和信息安全管理

32 国家能源局：多措并举 推进电力行业网络与信息安全

32 市场监管总局标准技术司：加强国家标准制修订周期管理

33 北京市政府：发挥中关村新一轮先行先试改革和创新示范引领作用 打造世界领先科技园区

33 湖北省市场监管局等十四部门：促进团体标准高质量发展

联盟工作 Alliance Work

- 34 WAPI产业联盟2项WLAN通信模块团体标准正式立项
- 35 WAPI产业联盟组织专家参加 ISO/IEC JTC 1/SC 6/WG 7中期会议
- 36 深国电无线局域网系列产品通过联盟测试
- 37 2023年无线网络安全标准化委员会 第一季度主任委员会议（总第4次）顺利召开
- 38 WAPI产业联盟发布最新版《WAPI标准产业应用及环境监测报告》

新成员 New Member

- 39 WAPI产业联盟再添4家新成员 联盟会员达118家

成员与市场 Member & Marketing

- 41 国网烟台供电公司投运国网首座“SPN+可信WLAN”通信新技术应用示范变电站
- 42 电力行业四大厂商联合创新 无线组网标准数字化变电站方案落地德阳
- 44 WAPI助力电力行业数字化 打造广东茂名首个智慧物资区域仓立体库
- 45 智芯公司获评国务院国资委世界一流专精特新示范企业
- 46 数字认证多项应用方案入选 “工业和信息化领域商用密码典型应用方案名单”
- 47 锐捷网络与佰才邦达成战略合作 助推全球行业数字化进程
- 48 迈普连续十五年蝉联服务满意度第一
- 49 使用神经网络 NIST抗量子算法第四次被破解
- 51 多家科技巨头提醒员工 不要向ChatGPT泄露敏感信息

产业技术论坛 Industry & Technology Forum

- 52 物联网安全国际标准体系中的中国贡献

17载时光洗练 而今迈步从头越

2023年3月7日，WAPI产业联盟17岁了！

17岁，恰风华正茂。我们有历练、有积累、更有干劲儿。

随着WAPI服务能源、国防、政务、交通等命脉行业的步伐不断加快，用户能更放心地享受无线网络带来的便利。在市场的千锤百炼中，WAPI产业链、创新链、供应链、标准链持续壮大。联盟公共服务平台，在关键基础技术、产品、测评、网络系统建设等方面取得丰硕成果，161项国际国家团体标准，发挥扎实的基础性指导性作用，系统完备的测试工具，让WAPI建设更加高质量科学有效。

离离春风，万物生长。而我们更深知：凡是过去，皆为序章。

新征程路上，我们要继续和您一起并肩奋斗，为国家网络安全作出积极贡献。我们要继续和您一起坚持创新，实现科技自立自强。我们更要继续和您一起，敢于斗争、善于斗争，不畏强权、勇于胜利。

世界随时都在重新开始，一切又从今天开始了。

主编：张珞珞

2023年3月7日

中国电子报/电子信息产业网等： 虎符TePA系列标准及实施入选 “工业和信息化领域商用密码典型应用方案名单”

【编者按】日前，由工业和信息化部、国家密码管理局主办的“工业和信息化领域商用密码典型应用方案”征集活动经过主办方严格审查并组织专家综合评审，最终确定了100项工业和信息化领域商用密码典型应用方案名单。WAPI产业联盟（中关村无线网络安全产业联盟）与西电捷通公司联合申报的“应用商用密码的虎符TePA系列标准及实施建设方案”入选该名单。本方案通过在网络通信协议技术体系创新中应用商用密码，和形成标准体系和研制标准符合性参考设计，促进应用商用密码的设备部署后提供安全通信网络服务。中国电子报/电子信息产业网、通信世界、飞象网等媒体对此进行了报道。

以下是中国电子报/电子信息产业网的报道：



日前，由工业和信息化部、国家密码管理局主办的“工业和信息化领域商用密码典型应用方案”征集活动经过主办方严格审查并组织专家综合评审，最终确定了100项工业和信息化领域商用密码典型应用方案名单。WAPI产业联盟（中关村无线网络安全产业联盟）与西电捷通公司联合申报的“应用商用密码的虎符TePA系列标准及实施建设方案”入选该名单。

典型应用方案			
55.	工业互联网安全监测分析与管理典型应用方案	重庆信息通信研究院	重庆微天信志有限公司 中国移动通信集团重庆有限公司
56.	5G核心网设备接入管理平台典型应用方案	中国移动通信集团河南有限公司	无
57.	基于商用密码的机械制造业工业互联网安全建设方案	湖南安泰信息技术有限公司	无
58.	基于高性能商用密码标准管理行业个人信息和重要业务数据保护建设方案	浙江睿源大数据中心	北京梳石网络科技有限公司
59.	基于商用密码的数字孪生应用典型应用方案	中国航天科工集团研究院有限公司	格尔软件股份有限公司
60.	应用商用密码的虎符TePA系列标准及实施	西安西电通信无线网通信股份有限公司	中关村网信网络安全产业联盟

国家安全三大支撑技术（密码、核、航天）中，密码技术涉及到复杂且多样化的通信网络空间，居于特殊重要的位置。但长期以来，在战略性前沿技术——计算机TCP/IP四层网络通信协议/密码安全协议技术规则和产业领域，我国总体仍处于国外密码大行其道、我国商用密码应用有限的被动局面，亟需掌握网络发展的主动权。

“应用商用密码的虎符TePA系列标准及实施建设方案”的工作包括：在我国自主虎符TePA网络安全协议技术创新中应用商用密码，形成标准体系，研制标准符合性参考设计，形成应用商用密码的设备，推动形成规模部署，提供安全通信网络服务。经过前期多年工作，在有线以太网（LAN）、无线近距离通信（射频识别RFID、近场通信NFC）、IP层安全可信通信等领域，已经形成了虎符TePA系列创新技术和国际/国家/行业/团体标准体系（22项），并完成参考设计的开发，为业界规模化使用商用密码提供了技术支撑，前期成果已经在多个关键领域和重大活动中应用。

本次商用密码典型应用方案征集活动，是根据《工业和信息化部 国家密码管理局关于征集工业和信息化领域商用密码典型应用方案的通知》（工信部联办函〔2022〕216号）部署安排，由工业和信息化部会同国家密码管理局、各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市密码管理局、通信管理局，及有关中央企业组织开展，旨在深入推进工业和信息化领域商用密码应用，推动商用密码产业高质量发展。

媒体新闻链接：

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20230314/119382.html>

通信世界：<http://www.cww.net.cn/article?id=575576>

飞象网：<http://www.cctime.com/html/2023-3-14/1645775.htm>

通信世界等：

WAPI产业联盟召开2023年第一次标准工作及项目组会议（总第125次）

【编者按】3月16日，WAPI产业联盟组织召开2023年第一次标准工作及项目组会议（总第125次）。会议包括：2023年第一季度标委会主任工作会议情况通报、2023年第一季度技术标准产业工作报告、无线网络安全技术标准最新动态分享、联盟新团体标准宣贯、在研标准项目讨论和审议、复审修订标准计划和拟立项项目建议、标准国际化专题研讨、标准化知识交流与培训等。通信世界、飞象网等媒体对此进行了报道。

以下是通信世界的报道：



3月16日，WAPI产业联盟组织召开2023年第一次标准工作及项目组会议（总第125次）。

会议包括：2023年第一季度标委会主任工作会议情况通报、2023年第一季度技术标准产业工作报告、无线网络安全技术标准最新动态分享、联盟新团体标准宣贯、在研标准项目讨论和审议、复审修订标准计划和拟立项项目建议、标准国际化专题研讨、标准化知识交流与培训等。来自无线网络安全技术国家工程研究中心、国家无线电监测中心检测中心、北京信息安全测评中心、陕西省网络与信息安全测评中心、江苏省电子信息产品质量监督检验研究院、广州广电计量检测股份有限公司、中国电信股份有限公司研究院、中国电子技术标准化研究院、中国科学院重庆绿色智能技术研究院、香港未来网络标准化研究院、华为技术有限公司、西电捷通公司、国家电网山东省电力公司、中国南方电网电力调度控制中心、深圳市国电科技通信有限公司、北京数字认证股份有限公司、高通无线通信技术（中国）有限公司、紫光展锐科技有限公司、北京联盛德微电子有限责任



图： 会议合影（部分）

公司、新华三技术有限公司、北京智芯微电子科技有限公司、北京北斗弘鹏科技有限公司、北京华信傲天网络技术有限公司、迈普通信技术股份有限公司、广州莲雾科技有限公司、山东思极科技有限公司、瑞斯康达科技发展股份有限公司、深圳市智开科技有限公司、深圳市信锐网科技术有限公司、南京博丰通信科技有限公司、瑞晟微电子（苏州）有限公司、西安芯语慧联信息科技有限公司、西安西电开关电气有限公司、南京博洛米通信技术有限公司、重庆华联众智科技有限公司、重庆源盾科技集团有限公司、四川岁月文明科技有限公司、江苏图码信息科技有限公司、安徽皖通邮电股份有限公司、北京邮电大学、北京工业大学重庆研究院、南京航空航天大学、金陵科技学院网络与通信工程学院、重庆邮电大学、长安大学、桂林电子科技大学等单位代表，无线网络安全标准化委员会专家委员，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代表共70余人参加会议。

WAPI产业联盟秘书长、无线网络安全标准化委员会副主任委员张璐璐在会议致辞中表示，随着WAPI服务能源、国防、政务、交通等命脉行业的步伐不断加快，用户能更放心地享受无线网络带来的便利。在市场

的千锤百炼中，WAPI产业链、创新链、供应链、标准链持续壮大。联盟公共服务平台，在关键基础技术、产品、测评、网络系统建设等方面发挥了支撑保障作用。161项国际/国家/行业/地方/团体标准，系统完备的测试工具，让WAPI建设更加高质量科学有效。

新年新气象，WAPI标准产业共同体迎来更多发展和机遇。

一是从用户方面反馈，WAPI已成为关基行业无线局域网建设的首选，具备“满足国家战略需求、符合国家法律/行政法规/行业部门规章要求、能防范已有安全漏洞、技术先进、产业成熟度高配套全、扩展性强、技术潜力大”等特征。今年初国家能源局印发布的《2023年电力安全监管重点任务》和证监会发布的《证券期货业网络和信息安全管理暂行办法》，均明确了推进本行业网络与信息安全工作的相关举措。

二是在WAPI市场大规模建设与服务中，标准产业共同体进一步壮大。2023年第一季度，佰才邦、瑞斯康达、莲雾科技、皖通邮电等单位相继加入联盟，联盟成员增至118家。这些企业既关注WAPI存量市场，也提出希望发挥自身优势，去拓展和带动WAPI增量市场。

三是在联盟的组织协同下，成员之间的WAPI产品研发与合作愈发紧密，形成了更多WAPI整体解决方案。“应用商用密码的虎符TePA系列标准及实施建设方案”，入选了工信部、国家密码管理局百项工业和信息化领域商用密码典型应用方案名单。

四是WAPI团体标准作为市场自主制定标准的重要组成部分，得到长足发展，市场认可度不断提高。近日中共中央、国务院印发的《质量强国建设纲要》中，有84处提到标准，多处和WAPI标准、产业紧密相关。相信在《纲要》指导下，WAPI团体标准实施将迎来新的机遇，也将为产业提供新的发展动力。

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委员会副主任委员黄振海在致辞中表示，《质量强国建设纲要》从发挥联盟平台作用、提升团体标准供给、打通标准应用渠道、国内国际标准协同发展等4个方面提出了明确要求。多年来，WAPI标准产业共同体在上述方面已持续开展了大量工作。作为新型产业标准开发平台，WAPI标准产业共同体将继续在新的技术和产业演进中，充当好行业管理、企业、科研机构、用户的桥梁作用，发挥好无线网络安全标准的联通和支撑作用。在过去的一年，WAPI产业在重要行业应用的步伐不断加快，关键基础技术、产品、测评技术、网络系统建设、密评等新的标准需求不断涌现，关键信息基础设施落地取得新的进展；技术标准和法律、行政法规、部门规章、政策文件等构成的产业合规性体系，其基础性指导性作用也越来越明显。希望大家共同努力，做好技术标准工作，通过所有利益相关方和贡献方的技术洞察和经验反馈，实现共同发展。

会上报告了无线网络安全标准化委员会2023年第一季度主任委员会议情况：

一是确定了标委会2023年重点工作，讨论了具体行动计划要点。包括：第一、深入推进制度和组织建设，巩固高水平的标准化可持续发展平台；第二、按流程推进标准化项目，严格进度管理，确保标准质量水平；第三、做好新项目立项工作，加强标准化与产业发展的相互支撑；第四、推进标准实施，提升已发布标准

的易用性，充分发挥标准的联通与支撑作用；第五、密切与委员和外部组织的联络关系，构建可持续发展的标准化生态网络；第六、深入落实国家战略，合规、创新、合作保障网络安全。

二是邀请WG3张国强组长做《WAPI应用于工业场景等需求分析》汇报，分析了当前工业互联网对通信网络提出的新要求，并按使用范围厘清了通信网络在工厂内和工厂外的网络承载业务，总结了与此相关的国内外技术及标准情况。大家一致认为，WAPI无线局域网技术产业，可提供大容量、高带宽、高速率、高安全的无线通信网络，网络时延毫秒级别，可广泛适用于工业应用场景，能满足工业自动化大部分场景的通信要求，包括高可靠、强实时、高安全、高密度、低抖动、低功耗和低成本等。

会议报告了第一季度团体标准和国际标准工作情况：

一是在团体标准方面，组织开展编制草案稿9项，形成征求意见稿1项，形成送审稿1项，形成研究报告1项。

二是在标准国际化方面，SC6国内技术对口工作稳步推进，第一季度共对内流通国际提案文件58份，向国际上反馈投票/意见24份；我国主导/参与的2项“无线局域网接入控制”完成国际标准草案（DIS）投票，正在进行意见处理及文本更新工作；2项“未来网络—基于代理模型的服务质量”正式发布为国际标准。

三是在国际标准推进方面，SC6国内技术对口单位将组织包括联盟专家在内的25人中国代表团，参加2023年3月20日至24日在奥地利召开的ISO/IEC JTC1/SC6全会和工作组会议。

WAPI产业联盟市场总监简练报告了2023年第一季度标准产业市场应用阶段性进展，重点包括：深国电、锐捷网络、佰才邦等公司的WAPI系列产品通过了联盟测试，联盟已为上述产品出具了测试报告；电力行业WAPI应用向深度、广度方向发展，国家电网烟台供电公司110千伏建昌变电站将SPN（切片分组网）传输和WAPI接入两种新一代自主可控通信技术融合应用，南方电网广东茂名区域仓检储配集成基地项目率先融合运用WAPI通讯、自动化技术、物联网技术、虚拟数字孪生等技术；在WAPI服务各行各业关键信息基础设施建设过程中，联盟及时梳理市场用户和厂商关注的问题，开展了系列WAPI问答科普活动，让大家通俗客观地了解WAPI标准、技术、产业。

中国南方电网电力调度控制中心陈宝仁专家介绍了未来3年南网WAPI应用规划，计划到2026年实现110千伏及以上电压级别的变电站WAPI全覆盖，将尽可能多的业务接入WAPI网络。同时也介绍了应用过程中一些新需求新挑战，例如在低功耗传感器、摄像头等方面，存在旺盛的产品需求，希望借助联盟的组织作用和公共技术保障作用，实现产业与应用的协同发展。

在技术产业新动态分享环节，3家联盟新会员分别介绍了本单位WAPI推进情况。北京智芯微电子科技有限公司产品经理范海明表示，作为国家电网二级单位，智芯微电子的产品已广泛应用于电网企业，希望能与联盟和行业伙伴们一起合作推动WAPI基础产品解决方案在电力行业的广泛应用。瑞斯康达科技发展股份有限公司行业市场部总经理曹凌表示，作为通信设备和信息化解决方案提供商，瑞斯康达正积极布局WAPI系列产品，年内将实现在港口物流、智能交通、工业制造等领域的应用。广州莲雾科技有限公司创始人吴泽雄介绍了

公司服务工业和电力无线传感平台、物联网生态的情况，以及传感器、智能网关、在线监测系统、智能工具柜等产品。

会上，与会专家对已立项标准《信息系统无线局域网密码应用基本要求》《无线网络安全术语》《无线局域网证书鉴别漫游应用扩展技术规范》《无线局域网设备技术要求与测试方法》《信息安全技术 证书管理 第2部分：证书私钥存储和使用技术》《信息安全技术证书管理 第5部分：证书格式》《信息安全技术 三元鉴别可扩展协议消息封装扩展要求》《信息技术 无线局域网媒体访问控制和物理层规范信息元素扩展要求》《传感器类设备专用WLAN通信模块技术要求与测试方法》《工业串口类设备专用WLAN通信模块技术要求与测试方法》等进行了集中讨论和协商一致，形成了相关决议。无线网络安全技术国家工程研究中心张变玲报告了《高速WLAN与WAPI团体标准体系融合研究项目》的进展情况，与会专家在讨论基础上形成决议，将继续推进该研究项目。

期间，联盟还开展了标准国际化专题研讨和标准化知识交流与培训活动，发布了2023年3月版《WAPI标准产业应用及环境监测报告》。

张璐璐表示，2023年联盟秘书处将进一步发挥好桥梁纽带作用，组织和服务好无线网络安全领域的标准技术产业协同创新，支持企业去赢得市场、获得发展。也希望继续和大家携手，为我国科技自立自强和质量强国建设，发挥更多方面的重要作用。

媒体新闻链接：

通信世界：<http://www.cww.net.cn/article?id=575776>

飞象网：<http://www.cctime.com/html/2023-3-17/1646142.htm>

WAPI 问答（系列连载）

在WAPI服务各行各业关键信息基础设施建设过程中，联盟总结了一些市场用户的常见问题，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，开辟WAPI问答（系列连载）栏目，帮助大家更加客观准确地了解WAPI。

欢迎您随时和我们交流探讨。

联系方式：010-82351181, staff@wapia.org

第三部分（PART3）

■ 1. 问：国家发布《质量强国建设纲要》，WAPI产业有新的机会么？

答：WAPI标准产业共同体将在质量强国建设中发挥多方面的重要作用。

近日中共中央、国务院印发了《质量强国建设纲要》，要求各地区各部门结合实际认真贯彻落实。《纲要》有84处提到标准，多处和WAPI标准、产业紧密相关。

尤其是，《纲要》要求深入推进标准化运行机制创新，优化政府颁布标准与市场自主制定标准二元结构，不断提升标准供给质量和效率，推动国内国际标准化协同发展；同时还要求发挥行业协会商会、学会及消费者组织等的桥梁纽带作用，开展标准制定、品牌建设、质量管理等技术服务，推进行业质量诚信自律。截止目前和WAPI产业相关的国家、行业、团体，以及国际、欧洲地区标准已有超160项得到发布，尤其是WAPI产业联盟承担首批国标委团体标准试点工作以来，WAPI团体标准作为市场自主制定标准的重要组成部分，得到长足发展，市场认可度不断提高，在《纲要》指导下，WAPI团体标准实施将迎来新的机遇，也将为产业提供新的发展动力。

■ 2. 问：目前等保标准中没有明确要求使用WAPI，那是不是意味着等保信息系统建设和产品选型时不需要考虑WAPI？

答：这种理解是错误的。

等保作为一种网络安全保障体系，通常不会限定使用特定技术（例如WAPI），但是可以要求不使用已知

有安全缺陷的技术（例如WEP）。从目前无线局域网领域可选择的安全协议来看，只有WAPI才完全符合等保要求。具体分析如下：

（1）网络信息系统是否符合等级保护要求，判断的准则是系统是否达到了某种层级安全防护的效果。对照等保标准中移动互联安全扩展要求和安全通用要求，只有采用符合WAPI标准产品建设的系统，才能满足等保标准和体系要求。

（2）与等保1.0相比，在2019年发布的等保2.0标准体系中，除安全通用要求外，另外增加了对移动互联场景下的安全扩展要求，其中，对密码管理、边界防护、访问控制、入侵防范等方面，对于各级的安全防护指标都做出了明确要求。符合上述全部要求的技术只有WAPI，且最低符合等保三级要求，经扩展可达到四级。

（3）有人说使用Wi-Fi的证书模式，也能满足移动互联安全扩展要求三级中“采用鉴别服务器实现身份鉴别”的要求，因此Wi-Fi网络可以满足等保三级要求，这种理解是错误的。因为等保标准中，和WLAN相关的规范要求，除了移动互联安全扩展要求，还包括安全通用要求，在安全通用要求的“密码管理”部分，明确要求二级以上均应遵循密码相关的国家标准和行业标准。所以，采用Wi-Fi技术和产品建设WLAN，不管是PSK模式，还是证书模式，都是不符合等保标准要求的。

■ 3. 问：启用WAPI的预共享密钥模式，对保障网络安全是否已经足够了？

答：不是。预共享密钥模式仅适用于临时组网。

（1）设置简单的8位数字作为口令，业内实践大概三分钟可以破解。数字设置长一点后较难估计，因为如果采用的数字组合比较常见，那么字典攻击就可能很快见效（比如以分钟计）。如果数字组合设置很复杂，24位较难破解，但对用户来说，记住24位复杂组合的字符也很困难。

（2）增加共享口令长度只是增加了暴力破解的难度，但不能解决身份识别的问题，属于类似“加长木桶的一块木板”的做法。在大规模部署后，很难保障这个共享口令不外泄，管理难度很大。

（3）预共享密钥的方式，只适用于临时组网。较长期的专业网络应用，须使用证书方式安全才有保障（和实体关联，抗抵赖）和方便管理（方便追溯行为）。

■ 4. 问：用户使用WAPI网络服务是否涉及版权、专利授权等问题，最终用户产品制造商的设备具备WAPI功能是否涉及版权、专利授权等问题？

答：WAPI技术和标准涉及的专利权和版权等，和其他技术标准相同，均应符合国家《专利法》和《著作权法》，具体而言：

(1) 标准版权：应用标准（包括但不限于设备厂商和最终用户）不涉及标准版权，对标准进行复制、销售、修改等才会涉及标准版权。

(2) 软件版权：软件嵌入式设备（如AP、AC等）的软件默认包含在设备的价格内，有些软件需要设备厂商授权使用范围（例如AS支持的最大数字证书管理数量）。

(3) 专利授权：最终用户产品制造商需要取得专利许可，最终用户不涉及。

■ 5. 问：为什么有些地方部署了WAPI网络，但用手机搜不到WAPI信号？

答：WAPI网络的部署，会广播WAPI网络的SSID（服务集标识，通俗理解为该网络的名字），手机或其他终端通过扫描到WAPI网络的SSID来进行连接认证操作。

能否搜到WAPI网络，是由网络拥有者的安全策略决定的，如果采用了隐藏SSID的部署策略，手机就无法搜索到WAPI信号了。

在安全性要求较高的场所，网络所广播的SSID一般会被要求隐藏，用户手机无法主动扫描到SSID，只有预先授权的用户才掌握SSID信息，才可手动添加SSID，进行下一步连接认证操作。

■ 6. 问：随着移动通信技术（5G/6G）的发展和演进，无线局域网（WLAN）会不会被逐渐取代？WAPI的生命力又如何？

答：从目前技术发展看，WLAN技术在未来10-20年内不会被取代。而随着发展演进，WAPI将具有长期生命力和竞争力。

无线局域网（WLAN）是无线高速数据通信两大主流技术之一（另一个是4G/5G/6G），具有带宽高、成本低、部署方便、工作于开放频段等特点，可在局部区域（约100米）内为用户提供高达数十Gbps的高速率数据通信服务。经过二十余年的发展，WLAN已经成为全球宽带信息基础设施的重要组成部分，是目前各国网络用户最主要的宽带接入方式之一。

WLAN技术和标准体系的不断演进——速率的不断演进，应用方式的不断翻新，模块化技术的不断发展，包括安全技术的发展，推动了WLAN成为“生命力顽强”的短距离无线通信体系。其中，基本速率的不断演进，是一个显性的主线。100-300m局部区域通信手段上，没有可直接匹敌的竞争者；100m之内短距离通信，和蓝牙、RFID、NFC、Lora等技术比有明显优势。

由于WAPI有效地解决了WLAN国际标准存在的安全问题，进一步推动了全球WLAN技术标准产业的发展。在WAPI产业联盟的组织和业界逾百家机构的持续研发下，围绕安全基础技术、安全应用技术、安全测试

技术三个技术集，形成了网状网重鉴别、自组网鉴别、预鉴别、漫游鉴别、实体证书管理、多信任证书、分离MAC模式会聚无线控制安全、本地MAC模式会聚无线控制安全、多无线网络协同安全、用户分级控制、机载网络安全、快速配置安全、终端零干预计费、负面测试、安全评估等数十项创新技术，推动WAPI技术体系不断发展，已形成了包括国家标准、行业标准、团体标准、运营商企业标准和国际标准在内的百余项WAPI标准体系。

WAPI新一代可运营可管理高安全无线局域网技术和标准体系正在持续演进。面对开放融合环境下的新技术、新应用的演进和挑战，新的网络安全技术体系正在研究和完善，具有机密性、完整性、可用性、抗量子攻击、可运营可管理等特性，并有效支持人工智能、区块链、物联网、大数据、万物互联等应用。

■ 7. 问：如何参与WAPI产业联盟团体标准的制修订？

答：WAPI产业联盟欢迎任何感兴趣的单位和个人加入到标准产业协同创新中来。团体标准的制修订过程是公开透明的。首先，大家可以报名参加团体标准创制，做出技术贡献或参与标准实践。其次，在标准征求意见阶段，产业链上下游主流厂商均会被纳入征集范围，确保最终发布的标准符合各方意见一致。

联盟认为，标准化工作的成功，很大程度上取决于现实中不同供应商的技术洞察和实现经验能反馈到标准制定过程中，我们也一直不遗余力地去创造公平、公正、公开的技术贡献和评议机会。

■ 8. 问：如何获取WAPI产业联盟团体标准的文本？

答：首先，WAPI产业联盟团体标准发布后，联盟秘书处将把团体标准主动分享给会员单位、标准项目参编单位以及参与征求意见的厂商。其次，没有参与标准工作但需要实施标准的单位，可以联系联盟秘书处获得标准文本。第三，已发布的联盟团体标准会上传全国团体标准信息平台（<http://www.ttbz.org.cn/>），提供在线阅读服务。

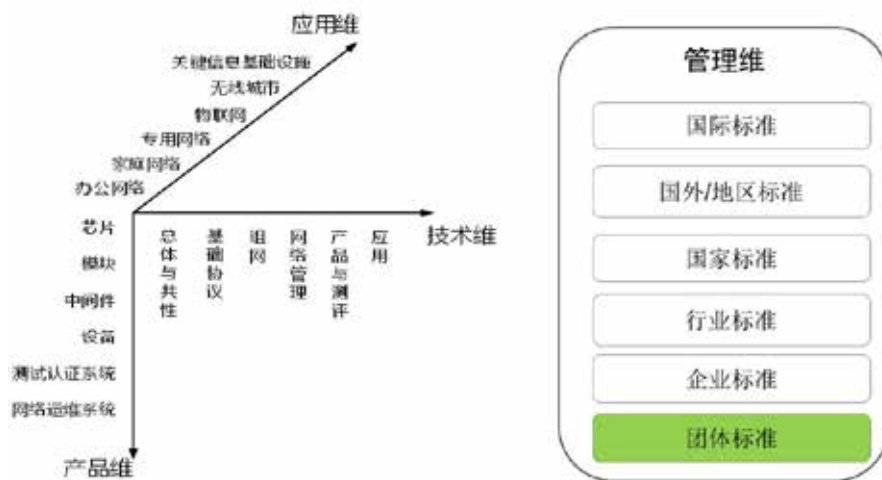
目前，WAPI产业联盟许多团体标准已被广泛实施，如：《无线局域网产品工程化实现指南 第1部分：WAPI与IEEE 802.11n》、《无线局域网产品工程化实现指南 第8部分：WAPI与IEEE 802.11ac》、《无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax》、《WAPI应用接口规范 第1部分：移动终端》、《WAPI证书管理 第5部分：证书格式范例》、《管理帧保护技术规范》、《无线局域网测试 第2部分：设备测试规范》、《关键信息基础设施无线局域网技术要求 第1部分：通用要求》等。

9. 目前WAPI标准体系情况是怎样的？

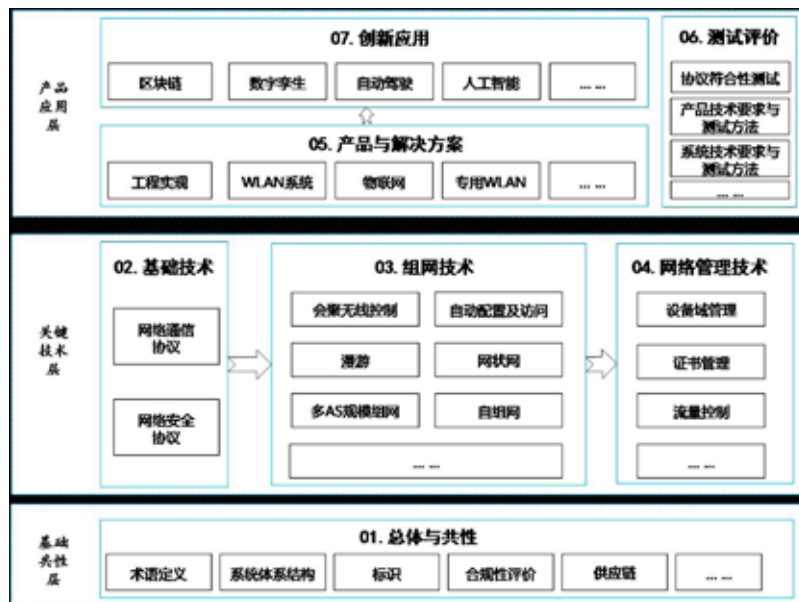
答：十几年来，为持续推动安全无线局域网的深度应用和发展，WAPI产业联盟联合成员单位和其他标准化组织，以GB 15629.11系列国家标准为基础，从总体与共性、基础、组网、网络管理、产品与解决方案、测试评价、创新应用等七个方面规划布局，已构建了完整的基于WAPI的无线局域网标准体系。围绕该体系制定并获发布的国家标准、行业标准、团体标准、企业标准等共70余项。

WAPI标准体系由无线网络安全标准化委员会总体工作组（WNSSC/WG1）规划和更新维护，现行有效的标准体系文件已在2022年第3次标准工作会议上发布。

WAPI标准体系价值链图示如下：



WAPI标准体系架构图如下：



密码讲堂：什么是密码？

零信任安全研究院

“什么是密码”，因为日常生活中的“密码”并不是我所说的这个“密码”。日常生活中所说的“密码”，实际上是口令，英文是password，是登录账户所需的认证凭证。而密码讲堂中所说的密码的英文是cryptography。建议广大读者以后不要再把口令说成是密码了。

那什么是密码？2020年1月1日正式施行的《中华人民共和国密码法》的第二条给出了准确和权威的答案：本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。根据这个定义，我们就能准确地理解什么是密码。

首先就是明确定义了密码的形态。密码是一项技术，称为密码技术；也可以是一种产品，称为密码产品；也可以是一种服务，称为密码服务。密码以三种形态存在，可以是技术、产品和服务，这为密码从业者指明了发展方向，可以从事密码技术研究，可以从事密码产品研发、生产和销售，也可以提供密码服务，以服务形式来提供密码产品，通常指云密码服务或称密码云服务。

第二就是明确定义了密码的用途。密码可用于加密保护和安全认证，准确理解这个用途非常重要，给密码从业者指明了密码到底该用在什么地方。请大家注意：第一个用途是加密保护，这是用途最广泛的应用，如HTTPS加密、邮件加密和数字签名、文档加密和数字签名、软件代码数字签名等。CA机构所签发的SSL证书、电子邮件证书、电子文档证书、代码签名证书等就是用于上述加密保护用途的。第二个用途是安全认证，用数字签名技术来实现安全可靠的用户身份认证。这就是国内CA机构签发的USB Key证书所实现的用途，而国际CA机构所做的业务则是提供市场更广泛的加密保护用途的各种数字证书。相信各个国内CA机构应该能从这里看到差距和改革的方向，第一个用途更有前途，这也是为何密码的定义是加密保护在前、安全认证在后的根本原因。本密码讲堂将重点讲密码在加密保护方面的技术、产品、服务及其应用。

第三就是明确了技术路线，那就是通过特定变换的方法来实现。这里所指的特定变换的方法就是密码算法，用密码算法来实现特定变换。《密码法》中所指的密码算法是特指国产密码算法，如：SM2、SM3、SM4和SM9等商用密码算法，不包括国外的密码算法，这一点非常重要，一定不能搞错，虽然整个密码法全文都没有明确指出。

第四就是明确了密码的保护对象：信息等，信息需要用密码来实现加密保护，信息同时需要密码来实现安全认证后才能获取。这里还有一个“等”字非常重要，“信息”这个词范围非常广，包含了人类社会传播的一切内容，如音讯、消息、通讯系统传输和处理的各种对象；但如果还有未包含的，则用“等”字来包含，所有等等都可以用密码来实现加密保护和安全认证，这就不难理解为何其他相关法律如《数据安全法》、《个人信息保护法》等都要求采用密码来保护数据安全和个人信息安全。

大家从上面的解读《密码法》第二条就可以看到，《密码法》虽然不到5000字，但内容博大精深，仅仅一条只有42个字的第二条就包含了四层含义，每一层又有多个含义。所以，密码从业者或对密码感兴趣的读者一定要仔细解读《密码法》，网上有不少的解读，笔者仅仅是从技术上解读了其中最关键的一条。

密码讲堂所讲的所有内容均属于商用密码范畴，不涉及到核心密码和普通密码范畴。按照《密码法》第八条“商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全”，密码讲堂所讲的所有内容都属于使用商用密码保护网络与信息安全的技術、产品和服务。

《密码法》第二十一条则特别明确了“国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展”，这为密码从业者指明了发展方向，鼓励大家从事商用密码技术的研究和开发，鼓励大家从事商用密码技术的学术交流，鼓励大家把商用密码研究成果进行产业化转化和推广应用 to 各行各业，并且是要建立一个既开放又要有序竞争的市场体系，从而促进商用密码产业的健康发展。

《密码法》是一个博大精深的国家大法，有了《密码法》，就可以让密码技术、密码产品和密码服务在法律的保護下健康蓬勃发展，让《密码法》能真正为保障我国万物互联安全提供法律保障。

最后需要特别说明的是，密码讲堂中提到的很多名词名称如：国密算法、国密SSL证书、国密证书透明、国密证书自动化管理等等，可以同时对应地理解为：商用密码算法(商密算法)、商用密码SSL证书(商密SSL证书)、商用密码证书透明(商密证书透明)、商用密码证书自动化管理(商密证书自动化管理)等等，笔者喜欢用前一组名称，因为这组名称有一种自豪感，一种用我国自己的密码技术来保障我国万物互联安全的自豪感和责任感。

国务院机构改革方案

新华社

党的二十届二中全会通过了《党和国家机构改革方案》，深化国务院机构改革是其中的一项重要任务。必须以习近平新时代中国特色社会主义思想为指导，以加强党中央集中统一领导为统领，以推进国家治理体系和治理能力现代化为导向，坚持稳中求进工作总基调，适应统筹推进“五位一体”总体布局、协调推进“四个全面”战略布局的要求，适应构建新发展格局、推动高质量发展的需要，加强科学技术、金融监管、数据管理、乡村振兴、知识产权、老龄工作等重点领域的机构职责优化和调整，转变政府职能，加快建设法治政府，为全面建设社会主义现代化国家、全面推进中华民族伟大复兴提供有力保障。

一、重新组建科学技术部。加强科学技术部推动健全新型举国体制、优化科技创新全链条管理、促进科技成果转化、促进科技和经济社会发展相结合等职能，强化战略规划、体制改革、资源统筹、综合协调、政策法规、督促检查等宏观管理职责，保留国家基础研究和应用基础研究、国家实验室建设、国家科技重大专项、国家技术转移体系建设、科技成果转移转化和产学研结合、区域科技创新体系建设、科技监督评价体系建设、科研诚信建设、国际科技合作、科技人才队伍建设、国家科技评奖等相关职责，仍作为国务院组成部门。

将科学技术部的组织拟订科技促进农业农村发展规划和政策、指导农村科技进步职责划入农业农村部。将科学技术部的组织拟订科技促进社会发展规划和政策职责分别划入国家发展和改革委员会、生态环境部、国家卫生健康委员会等部门。将科学技术部的组织拟订高新技术发展及产业化规划和政策，指导国家自主创新示范区、国家高新技术产业开发区等科技园区建设，指导科技服务业、技术市场、科技中介组织发展等职责划入工业和信息化部。将科学技术部的负责引进国外智力工作职责划入人力资源和社会保障部，在人力资源和社会保障部加挂国家外国专家局牌子。

深化财政科技经费分配使用机制改革，完善中央财政科技计划执行和专业机构管理体制，调整科学技术部的中央财政科技计划（专项、基金等）协调管理、科研项目资金协调评估等职责，将科学技术部所属中国农村技术开发中心划入农业农村部，中国生物技术发展中心划入国家卫生健康委员会，中国21世纪议程管理中心、科学技术部高技术研究发展中心划入国家自然科学基金委员会。

国家自然科学基金委员会仍由科学技术部管理。

科学技术部不再保留国家外国专家局牌子。

二、组建国家金融监督管理总局。统一负责除证券业之外的金融业监管，强化机构监管、行为监管、功能监管、穿透式监管、持续监管，统筹负责金融消费者权益保护，加强风险管理和防范处置，依法查处违法违规行为，作为国务院直属机构。

国家金融监督管理总局在中国银行保险监督管理委员会基础上组建，将中国人民银行对金融控股公司等金融集团的日常监管职责、有关金融消费者保护职责，中国证券监督管理委员会的投资者保护职责划入国家金融监督管理总局。

不再保留中国银行保险监督管理委员会。

三、深化地方金融监管体制改革。建立以中央金融管理部门地方派出机构为主的地方金融监管体制，统筹优化中央金融管理部门地方派出机构设置和力量配备。地方政府设立的金融监管机构专司监管职责，不再加挂金融工作局、金融办公室等牌子。

四、中国证券监督管理委员会调整为国务院直属机构。中国证券监督管理委员会由国务院直属事业单位调整为国务院直属机构。强化资本市场监管职责，划入国家发展和改革委员会的企业债券发行审核职责，由中国证券监督管理委员会统一负责公司（企业）债券发行审核工作。

五、统筹推进中国人民银行分支机构改革。撤销中国人民银行大区分行及分行营业管理部、总行直属营业管理部和省会城市中心支行，在31个省（自治区、直辖市）设立省级分行，在深圳、大连、宁波、青岛、厦门设立计划单列市分行。中国人民银行北京分行保留中国人民银行营业管理部牌子，中国人民银行上海分行与中国人民银行上海总部合署办公。

不再保留中国人民银行县（市）支行，相关职能上收至中国人民银行地（市）中心支行。对边境或外贸结售汇业务量大的地区，可根据工作需要，采取中国人民银行地（市）中心支行派出机构方式履行相关管理服务职能。

六、完善国有金融资本管理体制。按照国有金融资本出资人相关管理规定，将中央金融管理部门管理的市场经营类机构剥离，相关国有金融资产划入国有金融资本受托管理机构，由其根据国务院授权统一履行出资人职责。

七、加强金融管理部门工作人员统一规范管理。中国人民银行、国家金融监督管理总局、中国证券监督管理委员会、国家外汇管理局及其分支机构、派出机构均使用行政编制，工作人员纳入国家公务员统一规范管理，执行国家公务员工资待遇标准。

八、组建国家数据局。负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，由国家发展和改革委员会管理。

将中央网络安全和信息化委员会办公室承担的研究拟订数字中国建设方案、协调推动公共服务和社会治理信息化、协调促进智慧城市建设和、协调国家重要信息资源开发利用与共享、推动信息资源跨行业跨部门互联互通等职责，国家发展和改革委员会承担的统筹推进数字经济发展、组织实施国家大数据战略、推进数据要素基础制度建设、推进数字基础设施布局建设等职责划入国家数据局。

九、优化农业农村部职责。为统筹抓好以乡村振兴为重心的“三农”各项工作，加快建设农业强国，将国家乡村振兴局的牵头开展防止返贫监测和帮扶，组织拟订乡村振兴重点帮扶县和重点地区帮扶政策，组织开展东西部协作、对口支援、社会帮扶，研究提出中央财政衔接推进乡村振兴相关资金分配建议方案并指导、监督资金使用，推动乡村帮扶产业发展，推动农村社会事业和公共服务发展等职责划入农业农村部，在农业农村部加挂国家乡村振兴局牌子。

全国脱贫攻坚目标任务完成后的过渡期内，有关帮扶政策、财政支持、项目安排保持总体稳定，资金项目相对独立运行管理。

不再保留单设的国家乡村振兴局。

十、完善老龄工作体制。实施积极应对人口老龄化国家战略，推动实现全体老年人享有基本养老服务，将国家卫生健康委员会的组织拟订并协调落实应对人口老龄化政策措施、承担全国老龄工作委员会的具体工作等职责划入民政部。全国老龄工作委员会办公室改设在民政部，强化其综合协调、督促指导、组织推进老龄事业发展职责。

中国老龄协会改由民政部代管。

十一、完善知识产权管理体制。加快推进知识产权强国建设，全面提升知识产权创造、运用、保护、管理和服务水平，将国家知识产权局由国家市场监督管理总局管理的国家局调整为国务院直属机构。商标、专利等领域执法职责继续由市场监管综合执法队伍承担，相关执法工作接受国家知识产权局专业指导。

十二、国家信访局调整为国务院直属机构。贯彻落实新时代党的群众路线，加强和改进人民信访工作，更好维护人民根本利益，将国家信访局由国务院办公厅管理的国家局调整为国务院直属机构。

十三、精减中央国家机关人员编制。中央国家机关各部门人员编制统一按照5%的比例进行精减，收回的编制主要用于加强重点领域和重要工作。

改革后，除国务院办公厅外，国务院设置组成部门仍为26个。根据国务院组织法规定，科学技术部、农业农村部等国务院组成部门的调整和设置，由全国人民代表大会审议批准。

国家市场监督管理总局、国家金融监督管理总局、中国证券监督管理委员会、国家信访局、国家知识产权局、国家数据局、国家乡村振兴局等国务院组成部门以外的国务院所属机构的调整和设置，将由新组成的国务院审查批准。

加快建设质量强国 着力推动高质量发展

中共市场监管总局党组

人民日报

近日，中共中央、国务院印发了《质量强国建设纲要》（以下简称《纲要》），这是以习近平同志为核心的党中央立足全面建设社会主义现代化国家、着眼统筹“两个大局”、着力推动经济社会高质量发展作出的重大决策部署，是贯彻落实党的二十大精神、推进中国式现代化的重大举措，是新时代建设质量强国的宏伟蓝图，在我国质量事业发展史上具有重大里程碑意义。

建设质量强国具有重大而深远的意义

党的十八大以来，以习近平同志为核心的党中央统揽全局，把推动发展的立足点转到提高质量和效益上来，大力促进质量发展，狠抓质量提升，推动我国质量事业实现跨越式发展，取得历史性成效。

建设质量强国是全面建设社会主义现代化国家的必由之路。国家强必须质量强，质量不仅是国家现代化的基础支撑，也是国家竞争力的重要标志。经济发展规律表明，一个国家或地区在经历高速增长后，必须推动实现从量的扩张转向质的提高的根本性转变，才能真正走上强盛之路。我国已经成为世界第二大经济体，但发展的质量效益仍有待提升，必须把质量上升为国家战略，树立质量第一的强烈意识，推动质量变革、效率变革、动力变革，努力走以质取胜发展之路，为中国式现代化提供坚实的质量支撑。

建设质量强国是推动经济高质量发展的重大举措。推动高质量发展需要树立提高发展质量效益的鲜明导向，以提高供给质量作为主攻方向，将全面提高产品和服务质量作为提升供给体系的中心任务，振兴实体经济。要下最大气力抓全面提高质量，强化质量技术、管理和制度创新，增强企业质量和品牌发展能力，提高产业链质量竞争力，促进区域质量协调发展，以质量提升助力打造自主可控、安全可靠、竞争力强的现代化产业体系。

建设质量强国是推动构建新发展格局的重要保障。质量一头连着供给，一头连着需求，贯通了整个产业链条，融入了经济发展全域，全面提升产品和服务质量有助于促进生产、流通、消费等环节循环畅通，推动国民经济良性循环。质量是深度参与全球产业分工与合作的关键要素，要深化质量基础设施互联互通，深入开展双多边质量合作交流，发展更有质量的开放型经济，推动国内国际双循环相互促进、更有活力。

建设质量强国是满足人民对美好生活需要的关键要求。质量体现着人们对美好生活的向往，产品和服务质量水平直接影响着群众生命健康、财产安全和生活品质。要把更好满足人民群众的需要，作为质量强国建设

的出发点和落脚点，提高供给质量，不断释放和扩大内需潜力，让人民群众买得放心、吃得安心、用得舒心，增强人民群众的质量获得感、满足感、幸福感。

准确把握质量强国建设的总体要求

《纲要》对我国质量强国建设作出整体部署，明确了全方位建设质量强国的指导思想和发展目标。

全方位建设质量强国，必须坚持以习近平新时代中国特色社会主义思想为指导。习近平总书记强调，“要树立质量第一的强烈意识，下最大气力抓全面提高质量”“中国致力于质量提升行动，提高质量标准，加强全面质量管理，推动质量变革、效率变革、动力变革，推动高质量发展”。党的二十大报告提出，“加快建设制造强国、质量强国、航天强国、交通强国、网络强国、数字中国。”这是质量强国建设的根本遵循，必须长期坚持。要立足新发展阶段，完整、准确、全面贯彻新发展理念，构建新发展格局，深入实施质量强国战略，牢固树立质量第一意识，健全质量政策，加强全面质量管理，促进质量变革创新，着力提升产品、工程、服务质量，着力推动品牌建设，着力增强产业质量竞争力，着力提高经济发展质量效益，着力提高全民质量素养，积极对接国际先进技术、规则、标准，全方位建设质量强国，为全面建设社会主义现代化国家、实现中华民族伟大复兴的中国梦提供质量支撑。

全方位建设质量强国，必须明确总体发展目标。《纲要》提出，到2025年，质量整体水平进一步全面提高，中国品牌影响力稳步提升，人民群众质量获得感、满意度明显增强，质量推动经济社会发展的作用更加突出，质量强国建设取得阶段性成效。经济发展质量效益明显提升，产业质量竞争力持续增强，产品、工程、服务质量水平显著提升，品牌建设取得更大进展，质量基础设施更加现代高效，质量治理体系更加完善。到2035年，质量强国建设基础更加牢固，先进质量文化蔚然成风，质量和品牌综合实力达到更高水平。

切实抓好质量强国建设重点任务落实

《纲要》明确了八个方面重点任务，这些都是质量强国建设的重点领域和主攻方向，需要全面准确把握，统筹推进落实。

一是推动经济质量效益型发展。协同开展质量领域技术、管理、制度创新，突破一批重大标志性质量技术和装备，增强质量发展创新动能。开展重点行业 and 重点产品资源效率对标提升行动，树立质量发展绿色导向。开展质量惠民行动和放心消费创建活动。

二是增强产业质量竞争力。分行业实施产业基础质量提升工程，强化产业基础质量支撑。加强产业链全面质量管理，打造技术、质量、管理创新策源地，实施区域质量发展示范工程，推动区域质量协同发展。

三是加快产品质量提档升级。实行全主体、全品种、全链条监管，提高农产品食品药品质量安全水平，确保人民群众“舌尖上的安全”。实施消费品质量提升行动，建立首台（套）重大技术装备检测评定制度，推进实施重点产品质量阶梯攀登工程。

四是提升建设工程品质。全面落实各方主体的工程质量责任，强化质量责任追溯追究，强化工程质量保障。促进从生产到施工全链条的建材行业质量提升，提高建筑材料质量水平，实施建设工程质量管理升级工程，打造中国建造升级版。

五是增加优质服务供给。推动产业链与创新链、价值链精准对接、深度融合，提高生产服务专业化水平。加强生活服务质量监管，加强便民服务设施建设，推进实施服务品质提升工程。

六是增强企业质量和品牌发展能力。引导企业加大质量技术创新投入。创新质量管理理念、方法、工具，推动全员、全要素、全过程、全数据的新型质量管理体系应用。开展中国品牌创建行动，实施中国品牌建设工程，争创国内国际知名品牌。

七是构建高水平质量基础设施。建立高效权威的国家质量基础设施管理体制，建设系统完备、结构优化、高效实用的质量基础设施，加快建设国家级质量标准实验室，加强质量基础设施能力建设。实施质量基础设施拓展伙伴计划，推进实施质量基础设施升级增效工程。

八是推进质量治理现代化。健全质量法律法规，严厉打击制售假冒伪劣商品、侵犯知识产权、工程质量违法违规等行为。完善多元化、多层级的质量激励机制，创新质量监管方式，健全产品召回管理体制机制，实施质量安全监管筑堤工程，深入开展全民质量行动。开展质量监管执法和消费维权双多边合作，定期举办中国质量大会，积极参加和承办国际性质量会议，加强质量国际合作。

建设质量强国，必须坚持党对质量工作的全面领导，把党的领导贯彻到质量工作的各领域各方面各环节，确保党中央决策部署落到实处。建立质量强国建设统筹协调工作机制，强化部门协同、上下联动。促进产业、财政、金融、科技、贸易、环境、人才等方面政策与质量政策协同，确保任务落地见效。开展督察评估，加强中央质量督察工作，建立纲要实施评估机制，形成有效的督促检查和整改落实机制。

《人民日报》（2023年02月28日 10版）

两会声音：

全国政协委员、国家无线电监测中心主任程建军： 构建现代化频谱治理体系 维护安全有序电波秩序 推动无线电事业高质量发展

人民邮电报

无线电频谱资源是国家战略性稀缺资源，以无线电频谱为资源引导、以无线技术为核心驱动的新一代信息技术，与各产业结合形成数字化生产力和数字经济，成为现代化经济体系发展的重要方向。与此同时，卫星互联网、无人机等新业态的密集应用，给传统无线电监管手段带来极大挑战。

“党的二十大报告指出，要推进新型工业化，加快建设制造强国、网络强国、数字中国等，加快发展数字经济。因此，在实现高质量发展的过程中，无线电事业前景广阔、大有可为。”全国政协委员、国家无线电监测中心主任、国际电信联盟无线电规则委员会委员程建军对无线电事业的未来充满信心。

推动无线电管理能力大幅提升

程建军表示，近年来，全国无线电管理机构在党的领导下，以习近平新时代中国特色社会主义思想为指导，不断推进治理体系和治理能力现代化，科学管理、高效利用无线电频谱资源，维护国家电磁空间安全，全面支撑经济社会发展和国防建设。

一是无线电法治体系化。逐步形成了以《中华人民共和国无线电管理条例》《中华人民共和国无线电管制规定》两部行政法规为主体，以《无线电频率使用许可管理办法》等10项部门规章及全国30余项地方性法规和地方规章为基础的无线电管理法治体系，为促进无线电频谱资源有效利用，推动无线电管理各项工作规范化、制度化提供了法律保障。

二是频谱资源管理精细化。随着数字经济和新一代信息技术的快速发展，无线电技术与应用在各个领域的渗透也更为深入，频谱资源供需矛盾更加突显。国家无线电管理机构统筹规划5G、车联网、物联网、能源互联网等相关频谱资源，积极开展卫星频率轨道资源国际申报和协调，有力保障了信息通信、交通运输、航空航天、公共安全等重点行业、部门以及国家重大工程的频率使用需求。

三是安全保障能力系统化。初步建成国家短波监测网、卫星监测网、超短波监测网，以及覆盖到全国地市一级的无线电管理信息网络及业务系统等技术设施。圆满完成党的二十大、建党百年、国庆70周年、北京冬奥会等国家级重大活动无线电安全保障任务。与相关部门建立长效机制，确保航空、铁路、水上交通等关系人民生命财产安全的无线电专用频率使用安全，持续高压打击“黑广播”“伪基站”“GoIP诈骗”等新型电信网络诈骗活动，全力防范和打击利用无线电发射设备在国家重大考试中进行作弊行为。

四是国际交流多元化。圆满完成2019年世界无线电通信大会各项任务，推荐我国21位专家当选国际电信联盟无线电通信部门顾问组、研究组等管理层领导职务，组织我国专家团队在频谱管理、技术创新、产业发展等方面深度参与国际事务，不断深入参与无线电频率和卫星轨道资源国际治理。积极推动双（多）边合作，深入开展无线电频率国际协调，积极维护我国频谱权益。

促进无线电事业高质量发展

“未来，我国将不断提升频谱资源管理集约化水平，着力构建现代化频谱治理体系，维护安全有序的电波秩序，促进无线电事业高质量发展。”为此，程建军提出如下建议：

提高频谱资源支撑保障能力。深入贯彻落实国家频谱中长期规划，加强频谱资源统筹优化、合理布局，盘活存量、挖掘增量，超前谋划和布局工业互联网、物联网、车联网和地面雷达系统等行业和领域频率规划，不断增强频谱资源供给的精准性、针对性，夯实数字经济发展的频谱基础。培育更多无线电新应用、新业态、新模式，加快频谱资源开发利用、效率提升、动态共享等关键技术攻关，进一步发挥频谱资源对产业发展的先导作用。

提升电磁空间安全维护能力。坚定不移贯彻总体国家安全观，坚持以新安全格局保障新发展格局，加强维护国家电磁空间安全技术手段建设，最大限度减少和避免无线电有害干扰，确保事关国计民生的重要频率使用安全。

深度参与全球频谱治理。坚持全球视野，坚持合作共赢，深入开展双（多）边合作，积极参与全球频谱治理，努力提升我国在国际无线电频率和卫星轨道资源工作中的整体能力，维护好我国频谱资源国际权益。我本人也将积极履行国际电信联盟无线电规则委员会委员职责，贡献中国人的智慧和成功发展的成功经验，促进各成员国公平、合理、经济、高效地利用无线电频率和卫星轨道资源。

习近平：

要加快科技自立自强步伐 解决外国“卡脖子”问题

中共中央政治局1月31日下午就加快构建新发展格局进行第二次集体学习。中共中央总书记习近平在主持学习时强调，加快构建新发展格局，是立足实现第二个百年奋斗目标、统筹发展和安全作出的战略决策，是把握未来发展主动权的战略部署。只有加快构建新发展格局，才能夯实我国经济发展的根基、增强发展的安全性稳定性，才能在各种可以预见和难以预见的狂风暴雨、惊涛骇浪中增强我国的生存力、竞争力、发展力、持续力，确保中华民族伟大复兴进程不被迟滞甚至中断，胜利实现全面建成社会主义现代化强国目标。

习近平指出，继续深化供给侧结构性改革，持续推动科技创新、制度创新，突破供给约束堵点、卡点、脆弱点，增强产业链供应链的竞争力和安全性，以自主可控、高质量的供给适应满足现有需求，创造引领新的需求。

习近平强调，要加快科技自立自强步伐，解决外国“卡脖子”问题。健全新型举国体制，强化国家战略科技力量，优化配置创新资源，使我国在重要科技领域成为全球领跑者，在前沿交叉领域成为开拓者，力争尽早成为世界主要科学中心和创新高地。实现科教兴国战略、人才强国战略、创新驱动发展战略有效联动，坚持教育发展、科技创新、人才培养一体推进，形成良性循环；坚持原始创新、集成创新、开放创新一体设计，实现有效贯通；坚持创新链、产业链、人才链一体部署，推动深度融合。

习近平强调，新发展格局以现代化产业体系为基础，经济循环畅通需要各产业有序链接、高效畅通。要继续把发展经济的着力点放在实体经济上，扎实推进新型工业化，加快建设制造强国、质量强国、网络强国、数字中国，打造具有国际竞争力的数字产业集群。顺应产业发展大势，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，增强产业发展的接续性和竞争力。优化生产力布局，推动重点产业在国内外有序转移，支持企业深度参与全球产业分工和合作，促进内外产业深度融合，打造自主可控、安全可靠、竞争力强的现代化产业体系。

习近平：

要打好科技仪器设备、操作系统和基础软件国产化攻坚战

2023年2月21日，中共中央总书记习近平在中共中央政治局第三次集体学习时强调，要协同构建中国特色国家实验室体系，布局建设基础学科研究中心，超前部署新型科研信息化基础平台，形成强大的基础研究骨干网络。要科学规划布局前瞻引领型、战略导向型、应用支撑型重大科技基础设施，强化设施建设事中事后监管，完善全生命周期管理，全面提升开放共享水平和运行效率。要打好科技仪器设备、操作系统和基础软件国产化攻坚战，鼓励科研机构、高校同企业开展联合攻关，提升国产化替代水平和应用规模，争取早日实现用我国自主的研究平台、仪器设备来解决重大基础研究问题。

王志刚：

科技政策要聚焦自立自强

2023年1月3日，科技部党组书记、部长王志刚在接受科技日报专访时指出，要围绕“科技政策要聚焦自立自强”举国体制做好六方面工作：一要坚持打赢关键核心技术攻坚战，加快布局实施一批国家重大科技项目，集中优质资源合力攻关；二要有有力统筹教育、科技、人才工作，推动创新链产业链资金链人才链深度融合，加强企业主导的产学研深度融合，依靠创新培育壮大发展新动能；三要统筹推进国际科技创新中心、区域科技创新中心建设，加快国家自创区、高新区高质量发展，加快形成新的经济增长极；四要持续深化科技体制改革，深化科技评价、科研管理、科技经费改革，形成支持全面创新的基础制度；五要完善人才战略布局，自主培养和引进并举，加快建设世界重要人才中心和创新高地；六要积极拓展国际科技合作空间，推动高水平对外开放。

工信部： 三方面发力 加快工业互联网规模化发展

2023年1月18日，工信部新闻发言人、信息通信管理局局长赵志国在国务院新闻发布会上表示，工信部将重点从三个方面发力，加快工业互联网规模化发展。

一要优环境，加强政策引导。要扎实推进《工业互联网创新发展三年行动计划（2021-2023年）》，研究制定促进工业互联网规模化发展的政策举措，进一步完善顶层设计，用好用足财税金融相关政策，加强产融合作、产教结合，进一步营造良好的发展环境。

二要抓创新，增强发展动能。要强化技术创新，深入实施工业互联网创新发展工程，打好技术攻坚战，完善标准体系，破解制约规模化发展的关键短板；要深化产业创新，支持电信企业、互联网平台企业、工业企业等各类市场主体发挥各自优势加强联动协同，大力培育工业互联网龙头企业和“专精特新”中小企业，壮大工业互联网产业联盟，打造健康可持续的产业生态。

三要强应用，加快推广普及。要加快先进工厂培育，加速产业集群升级，深化重点行业拓展。

证监会：

聚焦网络和信息安全领域 网络和信息安全管理

为有效落实《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》相关要求，规范证券期货业网络和信息安全管理，防范化解行业网络和信息安全风险，维护资本市场安全平稳高效运行，证监会于2023年2月27日发布了《证券期货业网络和信息安全管理办法》（以下简称《办法》），并将于2023年5月1日起正式实施。

证监会调整为国务院直属机构，提级保障证券监管行政执法效能。值得注意的是，2023年3月7日，十四届全国人大一次会议，根据国务院关于提请审议国务院机构改革方案的议案，提出组建国家金融监督管理总局，作为国务院直属机构，统一负责除证券业之外的金融业监管，中国证券监督管理委员会的投资者保护职责划入国家金融监督管理总局；中国证券监督管理委员会由国务院直属事业单位调整为国务院直属机构，强化资本市场监管职责，提升金融数据安全保障能力，推动我国金融业开启高质量发展的新征程。

金融事关发展全局，证券期货业安全管理刻不容缓。证券期货业的特点是数据规模大、数据价值高、数据应用场景复杂，客户个人信息、交易、行情、资讯等海量数据在其业务系统中高速流转，其业务持续性和安全性决定着整个交易系统的运转。近年来，针对数据的安全攻击呈现出高频化、高损化、高显化等特征，证券期货业务场景所具有的特殊性与复杂性，也使得监管侧对数据安全和系统自主可控性要求更为严格，而实际安全防护情况是，证券期货业数据安全组织架构图尚不完善，技术手段未能全面覆盖数据全生命周期。构建实战化的数据安全防护和管理体系，对于证券期货业而言重要且紧迫。

恰逢“全国两会”宣布证监会调整为国务院直属机构之际，《证券期货业网络和信息安全管理办法》对证券期货业乃至整个金融行业具有重要意义，聚焦网络和信息安全领域，在总结实践经验的基础上，为上位法在证券期货行业的落地实施明确了路径。《办法》全面覆盖了包括证券期货关键信息基础设施运营者、核心机构、经营机构、信息技术系统服务机构等各类主体，以安全保障为基本原则，对网络和信息安全管理提出规范要求，主要包括：网络和信息安全运行、投资者个人信息保护、网络和信息安全应急处置、关键信息基础设施安全保护、网络和信息安全促进与发展、监督管理和法律责任等。

国家能源局： 多措并举 推进电力行业网络与信息安全

2023年1月17日，国家能源局印发《2023年电力安全监管重点任务》，任务要求，要推进电力行业网络与信息安全工作，组织开展网络安全五年行动计划中期评估，加强网络安全态势感知能力建设，推进国家级电力网络安全靶场建设，组织开展年度攻防演练，修订行业网络安全事件应急预案，建立完善网络安全监督管理技术支撑体系，推动商用密码等在电力行业的应用；要开展电力行业关键信息基础设施安全保护专项监管，制修订电力关键信息基础设施安全保护政策性文件，对电力行业运营者落实关键信息基础设施安全保护要求的有关情况开展专项监管。

市场监管总局标准技术司： 加强国家标准制修订周期管理

2023年2月15日，市场监管总局标准技术司发布《国家标准管理办法》强化国家标准制修订周期管理，自2023年3月1日起实施。重点包括：

一、国家标准制修订工作管理信息系统增加了国家标准计划项目周期管理功能，对国家标准计划项目周期实施全过程管理。

二、自2023年3月1日起，申报单位在系统中申报国家标准计划项目时，应填报工作计划，并根据制修订周期细化标准组织起草、征求意见、技术审查等各阶段时间安排。国家标准计划下达后，可结合工作实际进一步优化调整工作计划。

三、2023年3月1日之前已立项的国家标准，将按照征求意见阶段不少于90天（其中，征求意见60天，意见处理30天），技术审查阶段不少于30天的原则，自动生成工作计划，供参照执行。

四、高度重视国家标准制修订周期管理，科学合理制定工作计划，严格按照工作计划确定的时间安排开展国家标准制修订。将定期对工作计划执行情况进行监督，持续加强国家标准制修订周期管理，提升国家标准供给效率。

北京市政府： 发挥中关村新一轮先行先试改革和创新示范引领作用 打造世界领先科技园区

1月31日下午，新一届市政府召开第一次常务会议，下达部署2023年政府工作报告涉及的300项工作任务，研究《北京市人民政府工作规则》等事项。会议研究国际科创中心建设重点任务2023年工作方案时指出，要狠抓重点任务落实，发挥中关村新一轮先行先试改革和创新示范引领作用，打造世界领先科技园区；加强各类高水平科创人才培养和汇聚，建设高水平人才高地；围绕企业需求做好服务，组织开展科研攻关，发挥好企业在科技创新中的关键作用；聚焦共性技术，释放创新平台催化效应；加强服务保障，丰富场景应用，构建良好生态，促进企业创新发展；坚持开放创新，加强国际科技交流合作。深化央地协同、部市共建机制，共同推动重点任务落地见效，为推动高质量发展、服务国家科技自立自强提供支撑。

湖北省市场监管局等十四部门： 促进团体标准高质量发展

近日，湖北省市场监管局、省教育厅、省科学技术厅等14部门联合印发《关于促进团体标准高质量发展的意见》提出，要加大对社会团体标准化工作的政策支持，指导和帮助团体标准制定组织紧贴重点产业，加强团体标准与科技创新深度融合，聚焦产品质量提升、民生改善、绿色发展和乡村振兴规划构建标准体系，鼓励相关团体标准组织围绕产业链供应链需求联合制定团体标准，带动团体标准化工作水平整体提升。倡导战略规划和产业政策中，要积极采用或引用符合要求的、技术水平高、应用效果好的团体标准，推动产业转型升级，提高团体标准的社会认可度。要推动团体标准内部实施和外部采用，以市场的内生动力来推动团体标准应用发展。要实施团体标准培优计划，采取将优秀团体标准纳入科技成果评价和奖励等多层面政策激励，支持团体标准制定组织开展国内外标准化交流合作。

WAPI产业联盟2项WLAN通信模块团体标准正式立项

WAPI产业联盟 简 练



2022年12月20日，经WAPI产业联盟无线网络安全标准化委员会评审，《传感器类设备专用WLAN通信模块技术要求与测试方法》《工业串口类设备专用WLAN通信模块技术要求与测试方法》2项团体标准正式立项。多家单位积极申请成为参编单位。

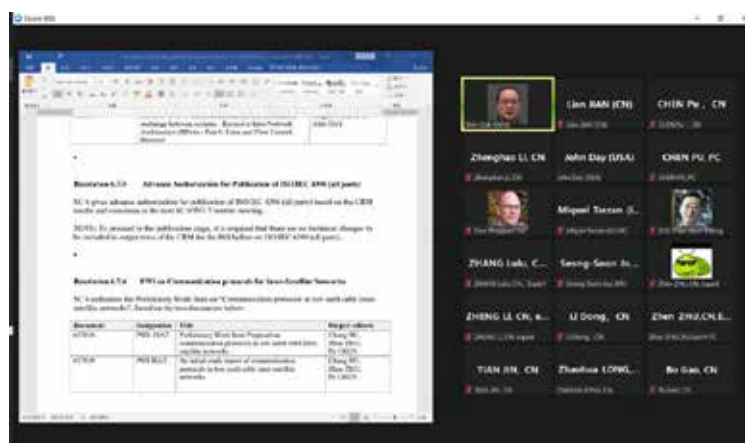
当前WAPI在各行业大规模应用，并快速扩展到工业物联网和行业物联网应用场景中（例如各类传感器设备、工业串口类设备）。在为行业用户数字化、智能化提供安全支撑的同时，如何兼顾行业物联网“功耗足够低、尺寸足够小、唤醒足够及时、具备边缘算力、兼容传统布线式工业串口设备”等需求，成为现下重要课题之一。对此，联盟牵头组织西安芯语慧联信息科技有限公司、北京联盛德微电子有限责任公司、西电捷通公司等多家单位启动了上述2项团体标准的创新工作。

这2项团体标准依据网络安全法、密码法和等保2.0等相关法律法规以及GB 15629.11系列国家标准、GB/T 32420—2015《无线局域网测试规范》等标准，针对计划使用WAPI技术的各种传感器类物联网设备和工业串口类设备，规定了相应的物理接口、工作模式、技术参数、安全能力、测试方法，为行业用户产品选型、部署实施、验收测试等提供了技术支撑，保障了基于WAPI的物联网系统高质量发展。

多年来，为持续推动安全无线局域网的规模应用和发展，WAPI产业联盟联合产学研用单位和国内外标准化组织，以GB 15629.11系列国家标准为基础，围绕“总体、基础技术、组网技术、网络管理技术、产品及测评、应用”六个方面开展规划布局，已构建了较为完整的基于WAPI的无线局域网国家/行业/团体标准体系，发布相关标准69项。

WAPI产业联盟组织专家参加 ISO/IEC JTC 1/SC 6/WG 7中期会议

WAPI产业联盟 简 练



2023年1月10-11日，ISO/IEC JTC 1/SC 6/WG 7召开中期会议，来自中国、韩国、美国、加拿大、西班牙的18位专家参加了会议。WAPI产业联盟秘书处张璐璐、简练等同志和无线网络安全标准化委员会相关同志作为中国代表团专家参会。

本次会议的主要内容是对ISO/IEC 4396系列标准项目在国际标准草案（DIS）投票阶段所收集的意见进行处理，对各成员国提出的意见进行逐条分析和讨论，形成新一版的DIS文本，以便进行新一轮投票。会上，各国长期在该领域开展研究的专家们对技术性意见展开了充分的讨论，取得了良好的效果。对于尚

未讨论确定的意见，会议决定将在2023年2月再组织一次中期会议进行处理。

ISO/IEC JTC 1/SC 6是信息技术领域国际标准化组织重要的分技术委员会，其技术方向为系统间远程通信和信息交换，专注于开放系统之间信息交换领域的技术研究和标准化，涵盖国际标准化组织提出的开放系统互联（OSI）七层模型，是全球网络空间系统信息通信的基础。目前，WAPI产业联盟组织会员单位推进并获发布的15项ISO/IEC国际标准中，有8项是在ISO/IEC JTC 1/SC 6制定的，另有2项未来网络领域的基于智能代理改善QoS的国际标准即将获发布。

深国电无线局域网系列产品通过联盟测试

WAPI产业联盟 王立华



2023年1月17日，深圳市国电科技通信有限公司（以下简称深国电）的无线局域网系列产品通过了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。联盟为上述产品出具了测试报告。

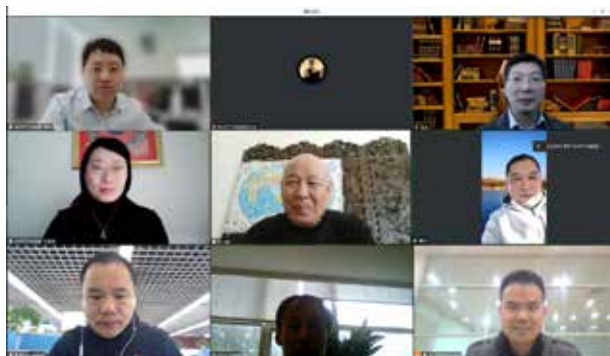
本次通过测试设备包括WAPI鉴别服务器（AS）、室内无线接入点（AP）、WAPI DTU设备和WAPI MCU物联网终端模组。其中AS设备具备证书签发、鉴别、漫游、管理功能；AP设备支持2.4/5GHz双频接入，通信速率支持802.11ac协议；WAPI DTU设备具备RS232/RS485通信转WAPI网络数据收发能力，设备即插即用，无需对现网设备做改造，即可实现安全无线局域网通信；WAPI MCU物联网终端模组体积小、功耗低、接口丰富、方便嵌入各类行业机具，快速实现WAPI通信，有效支撑WAPI在低功耗物联网领域的应用。

联盟测试实验室依据GB/T 32420—2015《无线局域网测试规范》和T/WAPIA 037.2—2021《无线局域网测试 第2部分：设备测试规范》，对上述设备进行了协议互通性、完整性、及功能测试。针对首轮测试中AP设备在WAPI协议完整性存在的部分未通过项，联盟实验室进行了精准定位并提出整改建议，深国电依据联盟建议完成了整改，最终通过全部测试。

深国电表示，作为深耕通信领域多年的企业，我们始终致力于为客户提供安全的整体解决方案。当前公司WAPI全系列产品已通过联盟测试，后续将深度挖掘能源、仓储、安防、交通等领域WAPI网络需求，提供从模组到整机产品、从终端到网络的整体解决方案。

2023年无线网络安全标准化委员会 第一季度主任委员会议（总第4次）顺利召开

WAPI产业联盟 张璐璐



2023年3月2日，WAPI产业联盟无线网络安全标准化委员会（以下简称“标委会”）主任委员曹军主持召开第一季度主任委员会议。副主任委员王立建、张璐璐、黄振海、陶洪波、王宏，及联盟秘书处标准化部、市场与产业部负责同志参加了会议。

会议包括：对上一次主任委员会议精神落实情况进行汇报、2023年标委会重点工作规划汇报、WAPI应用于工业场景等需求分析、新近政策分析和机遇讨论等。

2022年第四季度主任委员会议之后，联盟秘书处结合会议指导意见，推动并落实了“强化更有利于WAPI标准体系实施的氛围，加强组织建设、强化成员参与，采取关键措施、推动应用”，成效显著。

会议邀请标委会WG3张国强组长做《WAPI应用于工业场景等需求分析》汇报，张国强分析了当前工业互联网对通信网络提出的新要求，并按使用范围厘清了通信网络在工厂内和工厂外的网络承载业务，报告了与此相关的国内外技术及标准情况。分析指出，WAPI无线局域网技术产业，可提供大容量、高带

宽、高速率、高安全的无线通信网络，网络时延毫秒级别，可广泛适用于工业应用场景，能满足工业自动化大部分场景的通信要求，包括高可靠、强实时、高安全、高密度、低抖动、低功耗和低成本等等。

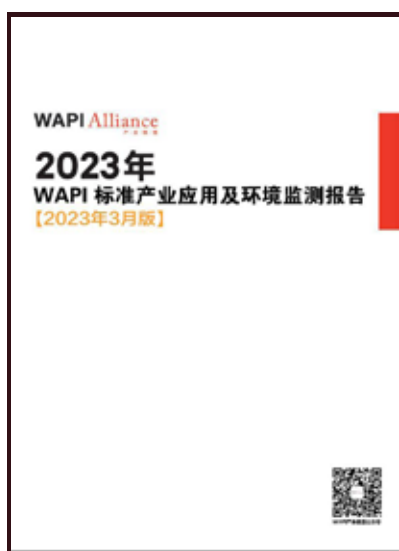
黄振海副主任委员报告了落实标委会2023年重点工作的规划。包括：第一、深入推进制度和组织建设，巩固高水平的标准化可持续发展平台；第二、按流程推进标准化项目，严格进度管理，确保标准质量水平；第三、做好新项目立项工作，加强标准化与产业发展的相互支撑；第四、推进标准实施，提升已发布标准的易用性，充分发挥标准的联通与支撑作用；第五、密切与委员和外部组织的联络关系，构建可持续发展的标准化生态网络；第六、深入落实国家战略，合规、创新、合作保障网络安全。以及上述六方面的具体行动计划。

与会主任委员副主任委员还就新近政策和机遇进行了分析和讨论。

经讨论，形成2023年第一季度联盟标准化工作重点，标准化部将据此落实相关工作。

WAPI产业联盟发布最新版 《WAPI标准产业应用及环境监测报告》

WAPI产业联盟 简 练



近日，WAPI产业联盟发布最新版《WAPI标准产业应用及环境监测报告》。

本期《报告》，重点对报告第二部分中的“WAPI 典型应用案例”进行扩充，加入了一批新的有代表性的WAPI应用。

《WAPI标准产业应用及环境监测报告》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（WAPI）的产业和市场全貌，服务市场建设和示范，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，以电子文档和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。其中，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，均截至2022年3月10日。鉴于产业特性和技术迭代，存在一定动态变化的可能。

《报告》版权归WAPI产业联盟（中关村无线网络安全产业联盟）所有，更多产业咨询或获取本文件授权等事宜，敬请联系：WAPI产业联盟秘书处 010-82351181 staff@wapia.org

《报告》全文可通过扫描下方二维码下载：



WAPI产业联盟再添4家新成员 联盟会员达118家

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。日前，佰才邦、瑞斯康达、莲雾科技、皖通邮电4家单位相继加入WAPI产业联盟，联盟成员增至118家。以下按新成员加入时间进行概要介绍。

北京佰才邦技术股份有限公司

2022年12月19日，经联盟理事会批准，北京佰才邦技术股份有限公司（以下简称佰才邦）正式加入WAPI产业联盟。



佰才邦成立于2014年，是一家专注于无线宽带接入解决方案、业务运营平台的研发和未来无线宽带技术创新的高科技公司。公司在成立之初就开始了WAPI技术标准、芯片与模组、终端、网络侧设备等研发工作。目前，基于WAPI标准的自研AC、AP、AS、CPE等产品已在行业内广泛应用，和国家电网等用户单位在WAPI可信无线网络方面有着深度合作。

此外，作为面向全球的无线网络覆盖解决方案头部企业，佰才邦可提供室内外小型基站、家庭网关、云核心网、网管计费系统、天线等在内的全系列产品，涵盖网络基础设施、移动手持终端和设备、软件、应用程序各个方面，且拥有完全自主知识产权和5G芯片技术，可服务于移动运营商、宽带接入运营商、有线电视运营商、虚拟运营商、政府和企业网络等各类客户。特别是在国际上首次提出全系列创新解决方案，为客户提供包括OpenRAN、SDN、基于IT架构的免授权频谱解决方案，及灵活的低成本建网方案，帮助客户打造“自由连接、触手可及”的新世界。

佰才邦公司总部位于北京海淀区，在深圳、成都、南京、西安、广州、西藏、美国达拉斯和日本东京设有子公司，在英国、巴基斯坦、巴西、泰国、缅甸等近十个国家设有办事处，拥有员工800余人，其中研发人员超过500人，大部分具备硕士、博士学位，在5G等领域申请核心专利超过500件。

瑞斯康达科技发展股份有限公司

2023年2月6日，经联盟理事会批准，瑞斯康达科技发展股份有限公司（以下简称瑞斯康达）正式加入WAPI产业联盟。



瑞斯康达成立于1999年，是国内光纤通信接入领域的领军企业，为客户提供接入层网络的产品、技术服务和综合解决方案，产品覆盖传输、宽带、无线、云网融合等领域，广泛服务国内外电信运营商、广电网络以及政府、交通、石油、电力、金融、互联网等垂直行业。

瑞斯康达自2020年启动WAPI系列产品研发，产品系列涵盖WAPI CPE、室外型WAPI AP、室内型WAPI AP、AC控制器、AS服务器，为电力WAPI覆盖、工业园区WAPI覆盖提供服务。

广州莲雾科技有限公司

2023年2月17日，经联盟理事会批准，广州莲雾科技有限公司（以下简称莲雾科技）正式加入WAPI产业联盟。



莲雾科技成立于2016年，是国家高新技术企业、广东省高新技术企业。作为专业的行业物联网产品、服务和系统解决方案提供商，莲雾科技专注于打造无线传感网络及平台，以“智能网关”和“云接入平台”为核心，配合各类专业传感器，实现传感器数据采集、设备便捷接入、安全可靠通信、智能化运营与管理。让传统行业的设备能方便地连接到云端，采集各种数据进行大数据分析，实现智能化运营管理和服务模式的创新。

莲雾科技的物联网产品多具备无线局域网（WLAN）功能且类型丰富，如WLAN无线工业网关、WLAN工业路由器、WLAN数据采集器（WLAN DTU）、WLAN无线传感器等。据莲雾科技介绍，公司自2021年开始研发WAPI无线通信产品，目前已具有WAPI CPE、WAPI DTU、WAPI通信模块、WAPI卡片机、WAPI温湿度传感器、WAPI水浸传感器等系列WAPI通信产品。

安徽皖通邮电股份有限公司

2023年3月1日，经联盟理事会批准，安徽皖通邮电股份有限公司（以下简称皖通邮电）正式加入WAPI产业联盟。



皖通邮电成立于1997年4月，是深圳市国资委旗下深圳市资本运营集团有限公司的下属企业，是从事通信产品研发、生产、销售及售后服务于一体的专业通信设备及综合解决方案提供商。皖通邮电为全球客户提供一揽子通信解决方案，产品覆盖ICT园区、SD-WAN、政企专线接入、信创等领域。

据皖通邮电介绍，公司在2022年推出了基于WAPI技术的WLAN解决方案，主要服务于高戒备、高安全性场景的无线覆盖。目前，皖通邮电AC、AP产品均支持WAPI，通过三元对等安全架构，使三个物理实体具有独立身份，真正实现了移动终端和无线接入点的直接双向鉴别，有效保证空口安全，从安全机制上防止了假冒AP和钓鱼AP。

皖通邮电目前产品系列涵盖WAPI终端CPE、室外型WAPI AP、室内型WAPI AP、AC控制器、AS服务器，为电力和工业园区的WAPI全覆盖提供整体解决方案。

国网烟台供电公司投运国网首座 “SPN+可信WLAN” 通信新技术应用示范变电站

水母网

2月27日，国网烟台供电公司110千伏建昌变电站将SPN（切片分组网）传输和可信WLAN（可信无线局域网）接入两种新一代自主可控通信技术融合应用，实现电网业务数据传送低时延、大带宽、高可靠承载，这在国家电网有限公司内尚属首次。

“十四五”是国家能源转型战略实施的关键时期，在国家“双碳”战略和国网公司“一体四翼”发展布局的背景下，电网安全生产和经营服务业务持续向IP化、宽带化演进，对电力通信网络的带宽、时延、可靠性以及业务差异化管理提出全新挑战。SPN是我国自主设计、研发的新一代通信传输技术，具有超低时延、超大带宽、集中管控、软硬切片等技术特点，网络业务承载能力较传统设备有了质的提高；可信WLAN是以我国自研的WAPI标准为基础的新一代通信接入技术，采用国产密码算法SM4为准接入技术，独创三元安全架构体系，安全接入更加可靠。

自2022年以来，国网烟台供电公司聚焦通信新技术业务应用，结合变电站电缆火灾隐患专项排查治理等工作，选取110千伏建昌站试点建设“SPN+WAPI”通信新技术应用示范站，探索地下变电站的典型场景应用，全方位匹配各类业务差异化承载和安全隔离需求，同步解决防火和防汛等各类业务信号回传不稳定、业务线缆敷设困难等实际问题，全面支撑、推进公司数字化转型。在组网模式方面，采用“SPN+WAPI”网络架构，实现传输、接入一体化部署，做到业务范围全覆盖、信号传送无盲区。在业务部署方面，简化站内业务承载方案，可实现各类业务的灵活部署，满足未来变电站业务数字化的发展需求。在安全隔离方面，应用通道化切片隔离以及证书鉴权加密方式，仅通过一张物理通信网络即可实现多业务端到端隔离，满足生产控制大区和管理信息大区等多类业务统一承载需求。

目前，烟台供电公司“SPN+WAPI”通信新技术应用成功覆盖110千伏建昌站的在线监测、远程巡视、移动作业等应用场景，接入智能巡视摄像头等11种业务终端形态，完成与安全风险管控监督平台等6套业务系统对接测试，为各专业提供可靠、便捷的高速传输通道。

下一步，烟台供电公司将持续推进“SPN+WAPI”技术深度应用，强化跨专业、跨部门联合协作和专项攻关，促进产学研深度融合，积极探索更多应用场景落地，助力公司数字化转型发展，赋能新型电力系统建设。



电力行业四大厂商联合创新 无线组网标准数字化变电站方案落地德阳

武汉中原电子信息有限公司

由南瑞信通、国网智芯、华为联合打造的F5G（第五代固网通讯技术）全光网络无线接入标准数字化变电站方案在四川德阳落地，电力物联网行业集成商武汉中原电子负责整体集成，德阳成为全国电力数字化变电站、集控站建设标杆。

变电站作为电力系统枢纽节点，在电网运行中占据着重要地位。随着智能电网建设和数字化转型的不断推进，以及设备移动物联网、大数据分析等技术的飞速发展，无线设备应用需求日益增长，而现有无线设备厂商众多、接口繁杂，存在无线网络通信协议、技术路线不统一，“孤立烟囱式”组网模式管理难度大，无线安全防护方案不明确等问题，需要综合适用性、安全性、自主性、经济性等因素制订和推进完备的无线组网整体解决方案，提升变电站（换流站）设备的全面智能感知能力及运检工作效率。

为加快构建现代设备管理体系，提升变电站的网络便捷性、规范性和安全性，提升变电站设备的全面智能感知能力及运检工作效率，自2021年起，北京智芯微电子、华为技术有限公司、南瑞信通等业界大厂与国家电网公司联合制定了标准数字化变电站无线组网方案。

基于2022年9月由武汉中原电子信息有限公司交付的F5G全光变电站项目，2023年2月标准数字化变电站无线组网方案示范站落地德阳。

数字化变电站无线组网方案在变电站内由宽窄一体无线接入与有线回传两部分组成，其中宽带无线接入部分采用全自主可控技术标准WAPI，由WAPI AP、AS鉴权服务器等组成，窄带无线接入部分采用ZigBee或LoRa协议，由内置在传感器中的国产化Zigbee模组和汇聚节点Zigbee AP组成。有线回传部分采用F5G技术，主要部件为OLT、分光器和ONU组成。站内的物联网关和视频网关采用两个独立ONU承载，OLT采用硬管道技术，实现传感器数据和视频数据的物理隔离。视频和物联传感器数据经过变电站OLT汇聚后，经传输设备传输至德阳公司，分别联接到视频平台和物联平台。

国家电网公司和华为等单位还将在IEEE P2413.3 电力IOT标准等方面开展工作。

德阳标准数字化变电站无线方案示范站的落地过程中，在宽窄带无线接入标准、物联网关数据模型和全光硬管道技术等方面做了大量实践：

一、采用全光架构，验证了通过全光网实现变电站内的视频、物联传感器、移动作业终端等高质量灵活接入；

二、实现了物联网关感知数据模型的探索，由北京智芯微电子科技有限公司提供了由其与国网公司共同主导的标准化的变电站感知层设备，按统一SG-CIM 61850 网关物化模型传感接入规约进行数据模型处理并上传数据。

三、全光架构WAPI无线接入提升安全可靠，南瑞信通作为国网变电站安全接入标准制定厂商，在本次标准建设过程中，提供了安全接入方面的标准设备。

四、采用硬管道传输技术OSU，为变电站内的各类传感器、固定视频和移动业务等提供了透明传输的物理管道，对全链路进行了统一网络管理，为后期的运维提供了坚实的网络基础支撑。

德阳标准数字化变电站无线组网方案的顺利试点，为后续大规模建设指明了前进的道路。下一步，国网德阳供电公司立足建设具有中国特色国际领先的能源互联网战略目标，全力以赴推进试点工作，为国网德阳供电公司数字化转型和数字电网建设提供必要的支撑。



WAPI助力电力行业数字化 打造广东茂名首个智慧物资区域仓立体库

太原新闻网

日前，南方电网广东茂名区域仓检储配集成基地项目完成二期建设工作，正式投入使用。作为南方电网首个智慧物资区域仓，该项目与智库智能合作，率先融合运用WAPI通讯、自动化技术、物联网技术、虚拟数字孪生等技术，打破数据壁垒，提升自动化水平，实现检储配高效协同，被列入广东电网“全国最好2021”项目集，项目成果经中国机械行业联合会、中国电器工业协会共同鉴定，整体达到国际领先水平。

茂名检储配一体化集成基地建筑面积约为6636平方米，建筑整体分为1、2号两栋库房。通过自动化仓库的调度监控与管理，该系统既能对仓储设备的整体运行过程进行控制、监控，也能物流信息进行管理跟踪，还能有效管理对作业计划、作业调度、作业过程进行改变，从而提升实现仓储效率的提升。据悉，该仓储方案通过上述管理系统，以及输送线、提升机、重型堆垛机以及四向穿梭车等硬件设备，能使仓储容量提升3倍、效率提升2倍。

该项目仓库充分利用建筑本身的特性，通过提升机打通1号库二楼和2号库一楼物理空间，将堆垛机与四向车系统进行联动控制、统一管理，将不同类型自动化设备贯通融合，实现茂名仓库库区资源一体化管控。

通过充分应用新一代信息技术、机器人技术、检测技术以及先进物流设施设备，立体库基地自动化作业水平得到了全面提升，实现仓储无人化、检测无人化、检储联动无人化。

茂名检储配基地配置AGV无人叉车进行物资出入立体库、装卸、搬运作业，配合智能立库系统进行自动存储，则可实现仓储全过程无人化；端到端联动简化了抽检流程和业务环节，减少了时间、人力成本和外部干扰风险，作业效率提升4倍以上；在南网内首创构建“检储配”一体化平台，整合立体库仓储、检测、配送三大业务系统，能够协调检储资源、动态调整作业策略，并且首次实现了与电网管理平台和全域物联网平台的无缝对接，打通数据交互壁垒，让各环节协同更加高效。

基于此，茂名检储配一体化平台满足物资仓储、检测、配送需求的同时，具备多仓库管理功能，能将各仓库分为若干库区或仓位，通过将各级仓库统一纳入平台中进行仓储管理，实现多仓库协同管控、资源透明化管理。

茂名检储配一体化基地通过创新智能立体库仓储布局、智能规划与控制、智能作业与执行，构建起智能仓库部署架构，成为了以“作业无人化+管控数字化+运营智慧化”为特征的电力仓储行业智能化改造的最佳实践。

智芯公司获评国务院国资委世界一流专精特新示范企业

智芯公司

近日，国务院国资委印发了《关于印发创建世界一流示范企业和专精特新示范企业名单的通知》（国资厅发改革[2023]4号），智芯公司在此次“双示范”创建行动中，获评“创建世界一流专精特新示范企业”。该评选经过企业申报、专家评审和征求意见等环节，全国共有200家企业入选，智芯公司是其中唯一一家芯片设计企业。

创建世界一流专精特新示范企业行动是贯彻落实党中央、国务院关于加快建设世界一流企业决策部署的积极实践，旨在筛选一批专注细分市场、创新水平较高、发展质量较好、未来潜力较大的企业，形成建设世界一流示范企业库，构建分层分类梯度培育体系，加快建设一批专业突出、创新驱动、管理精益、特色明显的世界一流专精特新企业。

芯片产业是一个国家高端制造能力的综合体现，是全球高科技领域的战略必争制高点。近年来，智芯公司坚持服务国家重大战略需求，全面落实国务院国资委及国家电网关于对标世界一流企业管理提升行动部署，聚焦“专精特新”，全力推进芯片产业发展。

智芯公司长期专注于工业芯片领域，围绕工业芯片产业链各环节重点与难点，以应用为牵引，初步构建起了全链条的工业芯片可靠性技术体系，打造了完整的工业芯片产品体系，可为工业应用提供整体解决方案。

智芯公司拥有国家企业技术中心、国家地方联合工程研究中心、国家工业芯片质量检验检测中心、工业芯片产品质量控制和技术评价实验室、院士工作站、博士后科研工作站等科研平台；先后荣获国家科技进步二等奖 1 项、中国专利银奖 2 项等国家级奖项 8 项，北京市科学技术一等奖、北京市发明专利一等奖等省部级奖励 56 项，拥有国内外专利 1000 余项。在高可靠技术、高安全技术等工业芯片领域关键核心技术方面形成了一批重大技术成果。

当前我国工业领域仍有大量的核心芯片依赖进口，且随着“双碳”、“数字中国”等国家战略的实施，工业芯片需求将进一步扩大。智芯公司已组建了一支以院士为引领，以领域专家为核心，以专业技术人员为支撑工业芯片研发队伍；形成了立足电力系统，面向各工业领域，并拓展至海外的市场布局；未来将强化关键核心技术攻关，全面推进各工业领域的芯片国产化替代，加快打造国际一流的工业芯片企业。

下一步，智芯公司将严格按照国资委统一部署，在国家电网公司统一领导下，聚焦提高核心竞争力和增强核心功能，深入做好创建工作，加快建设“专业突出、创新驱动、管理精益、特色明显”的世界一流专精特新企业，为国家电网公司加快实现“具有中国特色国际领先的能源互联网企业”作出积极贡献。

数字认证多项应用方案入选
“工业和信息化领域商用密码典型应用方案名单”

数字认证

日前，北京数字认证股份有限公司作为联合申报单位报送的五项商用密码应用方案入选“工业和信息化领域商用密码典型应用方案”。

工业和信息化领域商用密码典型应用方案名单

一、典型解决方案

序号	方案名称	牵头申报单位	联合申报单位
10.	基于鲲鹏应用的可信密码云解决方案	武汉长江计算科技有限公司	数字认证（武汉）有限责任公司
24.	天津市公安局和平分局智慧平安社区密码保障体系建设方案	天津市公安局和平分局	北京数字认证股份有限公司 天津中网基业智能系统工程有限公司 联通数字科技有限公司天津市分公司
27.	北京市市级政务云太极云平台密码应用方案	太极计算机股份有限公司	北京数字认证股份有限公司
31.	天津市曙光政务云平台密码应用方案	天津中网基业智能系统工程有限公司	北京数字认证股份有限公司 曙光云计算集团有限公司
35.	松原市公共安全视频监控建设联网应用工程商用密码应用解决方案	中共松原市委政法委员会	北京数字认证股份有限公司 长春市博鸿科技服务有限公司 中星智能系统技术有限公司

数字认证本次入选名单

数字认证能够成功入选，源于数字认证多年来在商用密码领域的专注与创新。一直以来，数字认证积极拥抱数字经济和新兴信息技术带来的发展红利和挑战，创新商用密码应用模式和商业模式。一方面深入了解重要领域、关键基础设施的业务场景需求，探索密码创新应用的突破点和推广点；另一方面聚焦密码与大数据、云计算、物联网等新业态的融合需求，持续推进新一代密码技术和产品创新发展，与产业界上下共同携手打造以密码能力一体化、密码供给服务化、密码系统敏捷化为特征的新型密码产业链，厚植商密产业高质量发展新优势。

锐捷网络与佰才邦达成战略合作 助推全球行业数字化进程

锐捷网络



近日，锐捷网络与北京佰才邦达成战略合作。双方将充分发挥各自在科技创新、行业研究、高新技术应用开发等方面优势，在产品研发的多层面、多场景深度合作，实现互惠互利、优势互补，用“新一代信息技术+行业”的解决方案助推全球行业数字化转型。

战略签约现场，锐捷网络总经理刘忠东表示，锐捷网络与佰才邦具备良好的合作基础。在战略签约前，双方已在国际市场展开广泛的技术合作。未来，在全球新一代信息技术建设大发展的背景下，双方夯实合作，不断创新，必将实现携手共赢的目标。

佰才邦董事长孙立新分享了佰才邦聚焦的业务发展及战略方向，希望双方在多行业、多领域、多产品方面展开深度合作。

锐捷网络 and 北京佰才邦均是WAPI产业联盟成员单位，相信它们的深度合作，将推动多行业技术方案创新，为行业数字化转型进程与数字经济发展为创造更多价值。

迈普连续十五年蝉联服务满意度第一

迈 普

2023年2月，“第二十一届中国IT用户满意度大会”在北京召开。大会发布了《2022年中国IT用户满意度报告》，迈普通信凭借“以客户为中心”的服务理念，诚心、贴心、细心、耐心、放心的服务，连续十五年蝉联网络设备服务满意度第一的荣誉。

迈普30年始终将“以客户为中心”作为服务理念，用及时、专业、热情的服务为客户创造价值。33个原厂服务中心、918个认证服务站、6000余名认证技术工程师，迈普服务网络覆盖全国。7×24小时不间断服务，确保需求即时响应，服务零延误。针对不同用户需求，迈普量身定制了数十种服务产品，覆盖从网络规划设计到产品运维保障的全周期。

迈普始终将服务“零延误、零失误、零投诉”作为公司服务准则，构建四级服务保障机制，为客户提供诚心、贴心、细心、耐心、放心的服务，全面助力行业数字化转型。



使用神经网络 NIST抗量子算法第四次被破解

光子盒研究院

近日，瑞典皇家理工学院研究团队发表论文，称其提出一种新的神经网络训练方法“递归学习”(Recursive Learning)，并通过周期性循环旋转信息，实现了对美国国家技术标准研究院(NIST)四种抗量子密码安全算法之一Crystals - Kyber最高5阶掩码的侧信道攻击，以高于99%的概率从中恢复了信息位(message bit)。

Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste

Elena Dubrova, Kalle Ngo, and Joel Gärtner

KTH Royal Institute of Technology, Stockholm, Sweden
(dubrova,kngo,jgartner@kth.se)

Abstract. CRYSTALS-Kyber has been selected by the NIST as a public-key encryption and key encapsulation mechanism to be standardized. It is also included in the NSA's suite of cryptographic algorithms recommended for national security systems. This makes it important to evaluate the resistance of CRYSTALS-Kyber's implementations to side-channel attacks. The unprotected and first-order masked software implementations have been already analysed. In this paper, we present deep learning-based message recovery attacks on the ω -order masked implementations of CRYSTALS-Kyber in ARM Cortex-M4 CPU for $\omega \leq 5$. The main contribution is a new neural network training method called *recursive learning*. In the attack on an ω -order masked implementation, we start training from an artificially constructed neural network M^ω whose weights are partly copied from a model $M^{\omega-1}$ trained on the $(\omega-1)$ -order masked implementation, and then extended to one more share. Such a method allows us to train neural networks that can recover a message bit with the probability above 99% from high-order masked implementations.

随着量子计算机的不断发展，其展现出的算力潜力对当前经典密码体系下的信息安全已经造成巨大威胁。为了抵御未来量子计算机对信息安全领域的冲击，全球密切开展保护数据和加密通信的研究，并从技术来讲总体分为两个方向——基于量子物理原理的量子密钥分发(Quantum Key Distribution, QKD)以及基于经典数学算法的抗量子密码学(Post-Quantum Cryptography, PQC)。

与QKD不同，PQC关注的是可在经典计算机上运行且量子计算机也无法破解的算法。2016年4月，NIST发布抗量子密码报告，宣布启动PQC标准制定项目。2022年7月，NIST完成了第三轮标准化评估，确定了四种标准化候选算法，其中主要的两种为Crystals - Kyber：用于通用加密，保护公共网络交换的信息，和Crystals - Dilithium：用于数字签名，身份认证。

Crystals - Kyber已被NIST选为待标准化的公钥加密和密钥封装机制，同时也被纳入美国国家安全局(NSA)推荐用于国家安全系统的密码算法套件，这使得评估Crystals - Kyber对侧信道攻击的抵抗能力变得非常重要：侧信道攻击利用从物理可测量的非主信道获得的信息，例如运行实现的设备的时序或功耗。

1) 递归学习神经网络

瑞典皇家科学院的研究团队开创性的提出一种使用递归学习的神经网络训练方法(Recursive Learning)，他们从人工构建神经网络开始训练，这一网络的权重是由可破解低阶的神经网络复制而来。其核心思想是将能破解低阶($\omega-1$)掩码的神经网络模型作为破解高阶(ω)掩码神经网络模型的基础，然后循环前进至更高阶。

研究团队调用一个批量归一化层级，首先对输入值使用各自的均值 μ 和方差 σ 进行标准化，然后对结果应用缩放参数 γ 与偏移参数 β 。神经网络在训练过程中通过反向算法学习参数 γ 与 β 。同时， γ 值越大表示输入特征在模型决策中的重要性越高。

ω 阶神经网络批量归一化层级输入值基于 $\omega-1$ 阶神经网络批量归一化层级数值权重构造如下图：

在不使用递归学习训练方法的情况下，对于5阶及以上掩码很难破解。

2) 周期循环信息恢复

研究人员还发现破解掩码过程中信息位(message bit)的泄漏是非均匀的——每个信息位的第一个比特泄漏比最后一个强得多。例如，对于一阶掩码的破解，恢复比特0和比特7的平均成功概率相差9%。为了解决这个问题，他们采用循环旋转信息恢复的方法，将泄漏量较小的信息比特移到泄漏量较大的位置。

对于每组测试信息，他们使用两位循环，对每个字节比特2i和2i+1分别用 和 模型恢复，其中 $i \in \{0, 1, 2, 3\}$ 。如下图所示，信息位(message bit)恢复成功概率有较大提高，平均概率 $p=0.99907$ 。

Byte	Bit position in byte								avg
	0	1	2	3	4	5	6	7	
0	0.99968	0.9984	0.9976	0.9972	0.9980	0.9964	0.9968	0.9988	0.9975
1	0.9996	0.9992	0.9992	0.9988	0.9996	0.9988	0.9996	0.9988	0.9992
2	0.9996	1.0000	1.0000	0.9988	0.9992	0.9988	1.0000	0.9996	0.9995
3	0.9996	0.9992	0.9988	0.9988	1.0000	0.9992	1.0000	0.9996	0.9994
4	0.9996	0.9996	1.0000	0.9996	0.9992	0.9992	0.9996	0.9996	0.9996
5	1.0000	0.9984	0.9992	0.9992	0.9992	0.9992	1.0000	0.9992	0.9993
6	0.9992	0.9992	0.9996	0.9984	0.9996	0.9992	0.9992	0.9992	0.9992
7	0.9992	0.9996	0.9992	0.9992	0.9988	0.9996	0.9988	0.9988	0.9992
8	1.0000	0.9996	0.9996	0.9984	0.9992	1.0000	1.0000	0.9992	0.9995
9	0.9992	0.9988	0.9992	0.9988	0.9988	0.9984	0.9996	1.0000	0.9991
10	0.9992	0.9992	0.9996	0.9992	0.9996	0.9976	0.9996	0.9976	0.9990
11	0.9996	1.0000	0.9992	0.9988	0.9988	0.9976	1.0000	0.9984	0.9991
12	0.9988	0.9996	0.9984	0.9996	0.9988	0.9984	0.9996	0.9996	0.9991
13	0.9996	0.9996	0.9992	0.9988	0.9984	0.9976	0.9996	0.9988	0.9990
14	0.9996	0.9988	0.9992	0.9996	0.9992	0.9984	1.0000	0.9992	0.9993
15	0.9996	0.9984	0.9988	0.9992	0.9980	0.9988	0.9988	0.9988	0.9988
16	0.9996	0.9988	0.9996	0.9980	0.9984	0.9976	0.9996	0.9996	0.9989
17	0.9992	0.9988	0.9996	1.0000	0.9988	0.9992	0.9996	0.9996	0.9994
18	1.0000	0.9988	0.9996	0.9984	0.9992	0.9988	0.9996	0.9992	0.9992
19	0.9992	0.9992	0.9996	1.0000	0.9976	0.9972	0.9992	0.9988	0.9989
20	0.9992	0.9996	0.9996	0.9996	0.9988	0.9988	0.9992	0.9996	0.9993
21	0.9992	0.9984	0.9992	0.9996	0.9984	0.9980	1.0000	0.9992	0.9990
22	0.9996	0.9996	0.9996	1.0000	0.9984	0.9968	0.9984	0.9992	0.9990
23	1.0000	0.9988	0.9992	0.9996	0.9984	0.9988	0.9996	1.0000	0.9993
24	0.9988	0.9988	0.9992	0.9996	0.9988	0.9988	0.9992	0.9988	0.9990
25	0.9992	0.9992	1.0000	0.9984	0.9984	0.9988	0.9988	0.9992	0.9990
26	0.9996	0.9996	0.9984	0.9992	0.9992	0.9988	0.9996	1.0000	0.9993
27	0.9996	0.9984	0.9992	0.9992	0.9972	0.9988	1.0000	1.0000	0.9990
28	0.9992	0.9988	0.9992	0.9980	0.9984	0.9992	0.9976	0.9988	0.9987
29	1.0000	0.9988	0.9996	0.9988	0.9980	0.9984	0.9992	0.9992	0.9990
30	0.9996	0.9984	0.9992	0.9992	0.9992	0.9984	0.9988	0.9988	0.9990
31	1.0000	0.9984	0.9992	0.9992	0.9988	0.9984	0.9992	0.9992	0.9990
avg	0.9994	0.9991	0.9993	0.9990	0.9988	0.9985	0.9993	0.9992	0.99907

研究团队还表示，该方法对Crystals - Kyber不具有特异性，可以应用于其他LWE / LWR PKE / KEM方案。递归学习技术可能具有超越侧信道攻击的意义。

Crystals - Kyber被破解并不是一件坏事，现阶段，众多网络安全公司进军PQC项目研究，但PQC目前还不具备商业化条件，经典密码向量子密码过渡仍存在大量挑战。

并且这已经不是NIST抗量子安全算法第一次被破解，2022年7月，SIKE在被NIST评为抗量子安全算法第四轮候选算法之一一个月后，就被破解了两次。SIKE的主要提出者David Jao表示：“对SIKE的攻击是一个积极信号，表明外界正认真研究这一挑战，并有助于我们将其修复。”

在论文的最后，瑞典皇家理工学院研究团队也表示他们将研究抵御这种递归学习神经网络与循环信息方法的侧信道攻击的对策。

多家科技巨头提醒员工 不要向ChatGPT泄露敏感信息

安全内参

ChatGPT在OpenAI开放测试后风靡全球，仅仅两个月用户便达到1亿，这是OpenAI开发的基于GPT-3.5的AI驱动的聊天机器人，成为互联网发展二十年来增长速度最快的消费者应用程序。但在其备受追捧的同时，ChatGPT也面临数据安全方面的争议。

南都大数据研究院注意到，在科技巨头纷纷整合ChatGPT或布局“类ChatGPT”产品应用的同时，部分企业如微软、亚马逊等还提醒员工不要与ChatGPT分享敏感数据。

ChatGPT训练数据的安全性问题引起各方高度关注。例如，从互联网获取海量数据进行模型训练是否合法？生成的文本是否会被恶意利用？如何阻止人工智能在不良数据上构建和训练？OpenAI是否可以在个人要求时从模型中完全删除数据？对于更多潜在问题，有法律人士甚至呼吁加强AI监管。

年初以来，在发现ChatGPT生成的文本中有疑似商业机密的情况后，不少科技巨头开始提醒自己的员工不要在使用ChatGPT时输入敏感信息数据。

据硅谷媒体报道，在一条从企业内部通信工具Slack泄露的信息中，亚马逊的公司律师称，他们在ChatGPT生成的内容中发现了与公司机密“非常相似”的文本，可能是由于一些亚马逊员工在使用ChatGPT生成代码和文本时输入了公司内部数据信息，该律师担心输入的信息可能被用作ChatGPT迭代的训练数据。

无独有偶，有微软员工曾在内部论坛上询问，能否在工作中使用ChatGPT或其开发商OpenAI推出的产品。微软首席技术官（CTO）办公室的一名高级工程师回应称，只要员工不与ChatGPT分享机密信息，就可以在工作时使用，但不要将敏感数据发送给OpenAI终端，因为OpenAI可能会将其用于未来模型的训练。

复旦大学计算机科学技术学院教授韩伟力表示，无论是个人敏感数据还是企业敏感数据，常理来说大家都不应该分享。

展，对于贯彻和实施国家标准战略具有重要的意义。

2 RFID安全国际标准体系

2.1 RFID国际标准现状

RFID技术作为一项先进的自动识别和数据采集技术，被公认为21世纪十大重要技术之一，也是物联网的主要实现技术。目前，国际上RFID领域的标准主要包括ISO/IEC 18000、ISO/IEC 15693、ISO/IEC 14443、ISO/IEC 15961系列等，以及由全球性行业组织EPCglobal制定的系列标准等，主要涉及连接技术标准、数据内容标准、一致性标准及应用标准四个方面，已制定和正在制定的标准共100多项，涉及RFID系统的多个方面，涵盖空中接口、非接触集成电路卡、测试方法、标识符、集装箱、安全等多个领域。

ISO/IEC JTC1/SC31是负责制定自动识别与数据采集技术领域国际标准的分技术委员会，工作范围涵盖RFID空口标准、测试标准、数据结构标准以及安全标准等领域，近年来相继制定和发布了ISO/IEC 18000系列RFID空中接口标准、ISO/IEC 29167系列RFID空中接口安全标准以及与ISO/IEC 29167对应的ISO/IEC 19823系列RFID空中接口安全符合性测试标准，这些标准互为补充、相互支撑，构建了完整的RFID国际标准技术体系。

2.1.1 ISO/IEC 29167系列国际标准

ISO/IEC 29167系列共包括12项RFID空中接口安全国际标准，该系列标准分别基于不同的密码算法，为RFID空中接口提供不同安全级别的密码套件安全服务，为各类应用场景下的读写器和标签提供了实体鉴别、安全通信、密钥协商等安全协议以及相应的命令。该系列标准包括：

ISO/IEC 29167-1:2014信息技术-自动识别与数据采集技术-第1部分：RFID空中接口安全服务

ISO/IEC 29167-10:2017信息技术-自动识别与数据采集技术-第10部分：用于空中接口通信的AES-128密码套件安全服务

ISO/IEC 29167-11:2014信息技术-自动识别与数据采集技术-第11部分：用于空中接口通信的PRESENT-80密码套件安全服务

ISO/IEC 29167-12:2015信息技术-自动识别与数据采集技术-第12部分：用于空中接口通信的ECC-DH密码套件安全服务

ISO/IEC 29167-13:2015信息技术-自动识别与数据采集技术-第13部分：用于空中接口通信的Grain-128A密码套件安全服务

ISO/IEC 29167-14:2015信息技术-自动识别与数据采集技术-第14部分：用于空中接口通信的AES OFB密码套件安全服务

ISO/IEC TS 29167-15:2017信息技术-自动识别与数据采集技术-第15部分：用于空中接口通信的XOR密

码套件安全服务

ISO/IEC 29167-16:2022信息技术-自动识别与数据采集技术-第16部分：用于空中接口通信的ECDSA-ECDH密码套件安全服务

ISO/IEC 29167-17:2015信息技术-自动识别与数据采集技术-第17部分：用于空中接口通信的cryptoGPS密码套件安全服务

ISO/IEC 29167-19:2019信息技术-自动识别与数据采集技术-第19部分：用于空中接口通信的RAMON密码套件安全服务

ISO/IEC 29167-21:2018信息技术-自动识别与数据采集技术-第21部分：用于空中接口通信的SIMON密码套件安全服务

ISO/IEC 29167-22:2018信息技术-自动识别与数据采集技术-第22部分：用于空中接口通信的SPECK密码套件安全服务

上述标准中，ISO/IEC TS 29167-15:2017和ISO/IEC 29167-16:2022由中国主导，联盟成员单位负责起草。

2.1.2 ISO/IEC 19823系列国际标准

ISO/IEC 19823系列共包括7项RFID空中接口安全符合性测试标准，该系列标准提供了与ISO/IEC 29167系列标准相对应的标准符合性测试方法，包括测试环境、测试条件、测试方法、测试模式、测试参数等。该系列标准包括：

ISO/IEC 19823-10:2020信息技术-密码套件安全服务一致性测试方法-第10部分：AES-128密码套件

ISO/IEC 19823-11:2022信息技术-密码套件安全服务一致性测试方法-第11部分：PRESENT-80密码套件

ISO/IEC 19823-13:2018信息技术-密码套件安全服务一致性测试方法-第13部分：Grain-128A密码套件

ISO/IEC 19823-16:2020信息技术-密码套件安全服务一致性测试方法-第16部分：ECDSA-ECDH密码套件

ISO/IEC 19823-19:2018信息技术-密码套件安全服务一致性测试方法-第19部分：RAMON密码套件

ISO/IEC 19823-21:2019信息技术-密码套件安全服务一致性测试方法-第21部分：SIMON密码套件

ISO/IEC 19823-22:2019信息技术-密码套件安全服务一致性测试方法-第22部分：SPECK密码套件

上述标准中，ISO/IEC 19823-16:2020由中国主导，联盟成员单位负责起草。

2.2中国贡献的RFID安全国际标准

迄今，由中国主导制定并获得ISO/IEC发布的标准共有4项，分别为：ISO/IEC 29167-16:2022及ISO/IEC 29167-16:2015、ISO/IEC 19823-16:2020和ISO/IEC TS 29167-15:2017，该标准均由西电捷通公司、无线网络安全技术国家工程研究中心做主要技术贡献，WAPI产业联盟、国家商用密码检测中心、国家无线电监测中心检测中心、国家信息技术安全研究中心等10余家单位全程参与标准开发工作。虎符国际标准项目组从2005年起启动RFID空中接口鉴别与保护方面的研究工作，至今已近18年时间，项目组对RFID空中接口所面临的威胁和风险进行了深入分析，对其鉴别与保护需求进行归纳和整理，并基于此自主提出了一套完整的RFID空中接口鉴别与保护解决方案（TRAIS）。

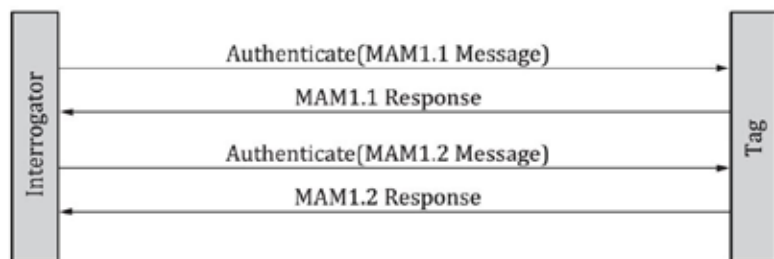
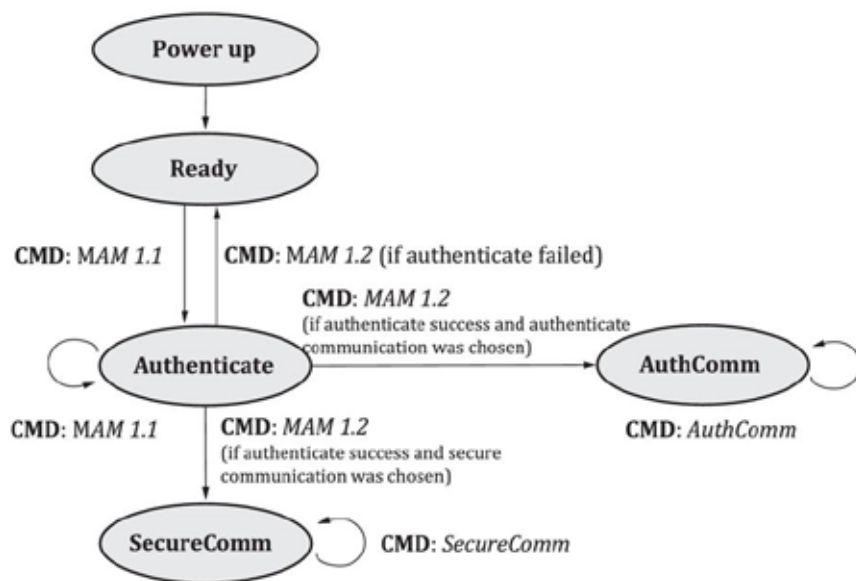
TRAIS技术体系包括针对各等级需求的鉴别与密钥协商协议，以及访问控制协议等，提供实体鉴别、保密通信、访问控制等空中接口鉴别与保护服务。其中，在鉴别机制方面，TRAIS包括基于XOR运算、基于杂凑运算和基于对称以及非对称运算等四个等级的整体性鉴别解决方案，能够提供读写器鉴别、电子标签鉴别、读写器与电子标签双向鉴别等三种鉴别模式的服务；在访问控制方面，TRAIS规范了基于非对称算法的、针对不具备计算能力的电子标签访问控制协议，无需电子标签进行任何的运算即可完整对自身数据的保护；在保密通信方面，TRAIS规范了保密通信机制，为读写器与电子标签之间的保密通信提供基础；在安全符合性测试方面，TRAIS规范了安全标准符合性测试方法与流程。

2.2.1 ISO/IEC 29167-16:2022

ISO/IEC 29167-16:2022 Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA-ECDH security services for air interface communications（信息技术-自动识别与数据采集技术-第16部分：用于空中接口通信的ECDSA-ECDH密码套件安全服务），采纳了TRAIS技术体系中的TRAIS-P鉴别机制，为RFID空中接口规范了一种高安全级别的安全保护套件，包括标签与读写器之间的双向实体鉴别机制和通信保护机制，能够有效抵抗伪造、重放等威胁。

该标准目前是第2版，第1版于2015年发布。

该标准共包含11章。前4章是标准的通用要素，分别为：范围、规范性引用文件、术语和定义、符号和缩略语。第5章为一致性，规范了读写器与标签的一致性要求。第6章介绍了标准所使用的密码算法。第7章给出了密码套件的参数定义。第8章规定了协议的状态转换方法，见图1。第9章规定了协议的初始化和重置方法。第10章规范了读写器与标签之间的双向鉴别协议，见图2。第11章规范了鉴别通信和安全通信方法。附录A、附录B、附录C、附录E、附录F和附录H均是规范性附录：附录A给出了协议的状态转换表；附录B给出了错误码与错误处理方法；附录C给出了密码描述；附录E规定了与特定空中接口协议相应的消息格式；附录F给出了协议消息分片与重组方法；附录H规范了有可信第三方TTP参与的鉴别协议。附录D、附录G均是资料性附录：附录D给出了协议的测试向量；附录G给出了ECC参数示例。



2.2.2 ISO/IEC 29167-16:2015 (已被ISO/IEC 29167-16:2022替代)

ISO/IEC 29167-16:2015 Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA-ECDH security services for air interface communications (信息技术-自动识别与数据采集技术-第16部分：用于空中接口通信的ECDSA-ECDH密码套件安全服务)，为ISO/IEC 29167-16的第1版，发布于2015年。2020年启动修订工作，主要修订内容包括：更新了规范性引用文件；为保持与空中接口标准的一致性，对与空中接口标准相关的内容进行了编辑性和技术性修改。该标准目前已被新发布的ISO/IEC 29167-16:2022替代，主要内容参见2.2.1。

2.2.3 ISO/IEC TS 29167-15:2017

ISO/IEC TS 29167-15:2017, Information technology — Automatic identification and data capture techniques — Part 15: Crypto suite XOR security services for air interface communications (信息技术-自动识别与数据采集技术-第15部分：用于空中接口通信的XOR密码套件安全服务)， 采纳了 TRAIS技术体系中的TRAIS-X鉴别机制，属于轻量级的RFID安全保护套件，包括标签与读写器双向鉴别、读写

器鉴别和标签鉴别三种鉴别模式，具有低开销、高效率、更加适用于无源标签的特性，能够有效抵抗伪造、重放等安全威胁。

该标准目前第1版。

该标准共包含11章。前4章是标准的通用要素，分别为：范围、规范性引用文件、术语和定义、符号和缩略语。第5章介绍了标准所使用的XOR算法。第6章给出了密码套件的参数定义。第7章规定了协议的状态转换方法，见图3。第8章规定了协议的初始化和重置方法。第9章规范了读写器与标签之间的鉴别协议，双向鉴别协议见图4。第10章规范了安全通信方法。第11章规范了鉴别通信方法。附录A、附录B、附录E和附录F均是规范性附录：附录A给出了协议的状态转换表；附录B给出了错误码与错误处理方法；附录E规定了与特定空中接口协议相应的消息格式；附录F给出了协议消息分片与重组方法。附录C、附录D和附录G均是资料性附录：附录C给出了密码描述；附录D给出了协议的测试向量；附录G给出了安全相关的考虑。

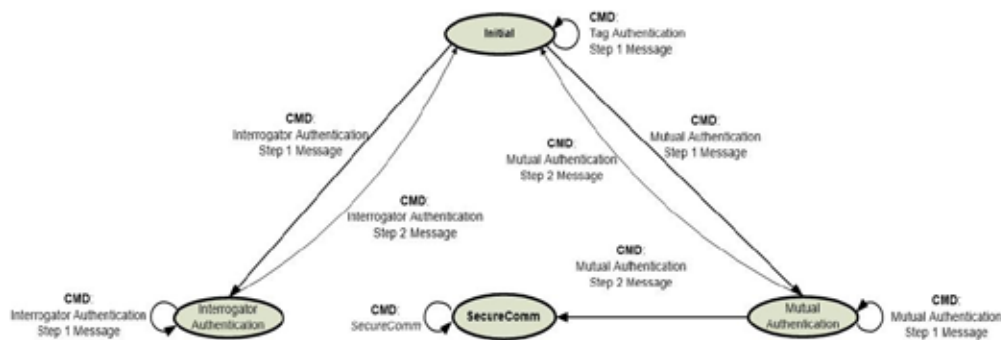


图3 协议状态转换方法

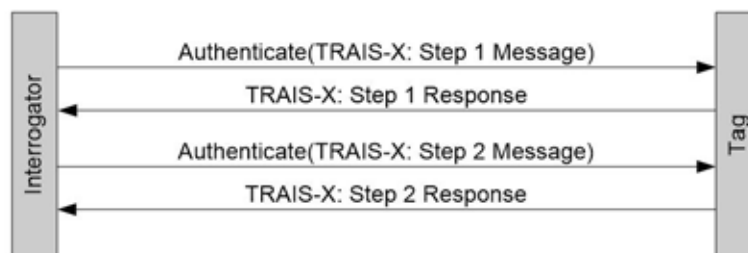


图4 双向鉴别协议

2.2.4 ISO/IEC 19823-16:2020

ISO/IEC 19823-16:2020, Information technology — Conformance test methods for security service crypto suites — Part 16: Crypto suite ECDSA-ECDH (信息技术-密码套件安全服务一致性测试方法-第16部分: ECDSA-ECDH密码套件)，采纳了TRAIS技术体系中的TRAIS-P TEST方法，规范了与ISO/IEC 29167-16对应的标准符合性测试方法。

该标准目前第1版。

该标准共包含11章。前3章是标准的通用要素，分别为：范围、规范性引用文件、术语和定义、符号和缩略语。第4章给出了通用测试算法。第5章给出特定空中接口协议情况的密码套件测试方法。第6章规定了与ISO/IEC 29167-16相对应的读写器和标签安全符合性测试方法。附录A是资料性附录，给出了测试参数示例。

3 NFC安全国际标准体系

3.1 NFC国际标准现状

近场通信（NFC，Near Field Communication）技术是一种方便迅捷的近距离无线通信技术，是物联网的基础连接技术之一。可实现电子设备之间非接触式、点对点的数据传输和数据交换，带宽高、能耗低，是实现物物互联的关键技术，具有广阔的应用前景。近年来，NFC技术正被智能手机等诸多消费类电子产品所集成，用于移动支付、交通、门禁等诸多场景，逐步成为网络空间可信身份最重要的物理存储载体和网络安全基础设施。目前，NFC领域的国际标准主要包括ISO/IEC 18092、ISO/IEC 13157系列、ISO/IEC 21481、ISO/IEC 22536、ISO/IEC 23917、ISO/IEC 22425等，涉及NFC空中接口协议、NFC安全、NFC测试方法等，共计10余项。

ISO/IEC JTC1/SC6是负责制定系统间远程通信和信息交换领域国际标准的分技术委员会，工作范围涵盖以太网、无线局域网、近场通信、磁域网、传感器网络、无人机区域网络等技术领域。近年来，在NFC领域相继制定和发布了ISO/IEC 18092近场通信空中接口标准、ISO/IEC 13157系列NFC空中接口安全标准以及与ISO/IEC 13157对应的ISO/IEC 22425 NFC空中接口安全符合性测试标准，形成了完整的NFC国际标准技术体系。

3.2 ISO/IEC 13157系列国际标准

迄今，ISO/IEC 13157系列共发布了5项NFC空中接口安全国际标准，该系列标准分别基于不同的密码算法，为NFC空中接口提供不同安全级别的鉴别与安全通信服务，为NFC技术在不同场景中的应用提供了实体鉴别、安全通信、密钥协商等安全协议。该系列标准包括：

ISO/IEC 13157-1:2014 信息技术-系统间远程通信和信息交换-NFC安全-第1部分：NFC-SEC NFCIP-1安全服务与协议

ISO/IEC 13157-2:2016 信息技术-系统间远程通信和信息交换-NFC安全-第2部分：采用ECDH与AES的NFC-SEC密码标准

ISO/IEC 13157-3:2016 信息技术-系统间远程通信和信息交换-NFC安全-第3部分：采用ECDH-256与AES-GCM的NFC-SEC密码标准

ISO/IEC 13157-4:2016 信息技术-系统间远程通信和信息交换-NFC安全-第4部分：采用非对称密码算法的NFC-SEC实体鉴别与密钥协商协议*

ISO/IEC 13157-5:2016 信息技术-系统间远程通信和信息交换-NFC安全-第5部分：采用对称密码算法的NFC-SEC实体鉴别与密钥协商协议*

上述标准中，ISO/IEC 13157-4:2016和ISO/IEC 13157-5:2016由中国主导，联盟成员单位负责起草。

3.3 中国贡献的NFC安全国际标准

迄今，在已发布的6项NFC安全国际标准中，由中国主持制定的标准为3项，占50%，分别为：ISO/IEC 13157-4:2016、ISO/IEC 13157-5:2016和ISO/IEC 22425:2017，均由西电捷通公司、无线网络安全技术国家工程研究中心做主要技术贡献，WAPI产业联盟、国家商用密码检测中心、国家无线电监测中心检测中心、国家信息技术安全研究中心等10余家单位全程参与标准开发工作。长期以来，NFC领域的研究和技术创新，在国际上主要是由欧、美等发达国家和地区贡献的，中国产业起步晚、基础薄弱，在上述领域长期处于市场提供者和技术跟随者角色。虎符国际标准项目组在2007年启动NFC空口安全技术研究，经过长期的研发，提出了两种NFC实体鉴别（NEAU）技术：“NFC非对称实体鉴别”（NEAU-A）和“NFC对称实体鉴别”（NEAU-S）来应对NFC多种应用场景的安全挑战，定义了NFC实体间对等双向鉴别、密钥协商及确认协议。NEAU技术体系的突出特点是定义了独立于具体NFC应用的通用空口通信安全，以防止近距离空口窃听、设备假冒、数据篡改等攻击，更为端到端模式下开展高价值交易提供了保障，可取得与高端智能卡比拟的高安全等级。

NEAU技术分别从接入鉴别、安全数据传输、安全管理三个层面确保NFC近场通信的安全，是对现有NFC安全技术ISO/IEC 13157-1(ECMA-385)和ISO/IEC 13157-2(ECMA-386)的有效补充，可以有效应对NFC设备被伪造以及通信过程中的数据被破坏、窃听、篡改和中间人攻击等典型安全威胁，确保NFC设备间数据传输的机密性、完整性、真实性。NEAU技术为NFC近场通信提供了可靠的通信安全解决方案，将为广大NFC用户使用移动支付、信用卡、交通一卡通等服务提供更进一步的安全保障。

3.3.1 ISO/IEC 13157-4:2016

ISO/IEC 13157-4:2016, Information technology — Telecommunications and information exchange between systems — NFC Security — Part 4: NFC-SEC entity authentication and key agreement using asymmetric cryptography（信息技术-系统间远程通信和信息交换-NFC安全-第4部分：采用非对称密码算法的NFC-SEC实体鉴别与密钥协商协议），采纳了NEAU技术体系中的NEAU-A机制，为NFC空中接口规范了一种高安全级别的安全保护方案，包括NFC设备之间的双向实体鉴别机制和通信保护机制，能有效防止伪造、窃听和篡改等攻击。

该标准目前是第1版，共包含11章。前6章是标准的通用要素，分别为：范围、一致性、规范性引用文件、术语和定义、符号和缩略语。第7章为总则，规范了标准的通用要求，以及该标准与ISO/IEC 13157-1协作方法，见图5。第8章规定了NEAU-A协议的字段和协议数据单元。第9章规定了NEAU-A协议的原语。第10章规定了NEAU-A协议的工作流程，见图6。第11章规定了安全通信方法。附录A和附录B均是规范性附录：附

录A给出了协议的UDP端口号和协议封装格式；附录B给出了协议的测试向量。

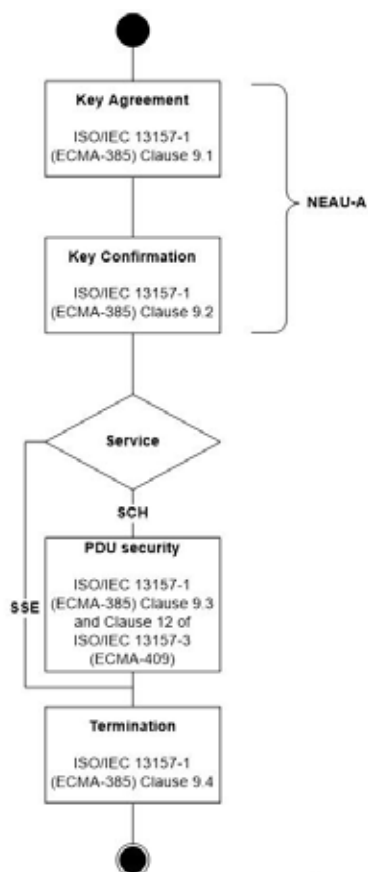


图5 NEAU-A与ISO/IEC 13157-1
的合作方法



图6 NEAU-A机制工作流程

该标准由ECMA 410—NFC-SEC-04: NFC-SEC entity authentication and key agreement using asymmetric cryptography (NFC-SEC-04: 采用非对称密码算法的NFC-SEC实体鉴别与密钥协商协议) 经国际标准快速流程转化而来。ECMA 410是欧洲信息和通信系统标准化协会ECMA于2015年发布的地区性标准，该标准同样由联盟成员单位主导起草。

3.3.2 ISO/IEC 13157-5:2016

ISO/IEC 13157-5:2016, Information technology — Telecommunications and information exchange between systems — NFC Security — Part 4: NFC-SEC entity authentication and key agreement using symmetric cryptography (信息技术-系统间远程通信和信息交换-NFC安全-第4部分: 采用对称密码算法的NFC-SEC实体鉴别与密钥协商协议)，采纳了NEAU技术体系中的NEAU-S机制，为NFC空中接口规范了一种高效的安全保护方案，包括NFC设备之间的双向实体鉴别机制和通信保护机制，能有效防止伪造、窃听和篡改等攻击。

该标准目前第1版，共包含11章。前6章是标准的通用要素，分别为：范围、一致性、规范性引用文件、术语和定义、符号和缩略语。第7章为总则，规范了标准的通用要求，以及该标准与ISO/IEC 13157-1协作方法，见图7。第8章规定了NEAU-S协议的字段和协议数据单元。第9章规定了NEAU-S协议的原语。第10章规定了NEAU-S协议的工作流程，见图8。第11章规定了安全通信方法。

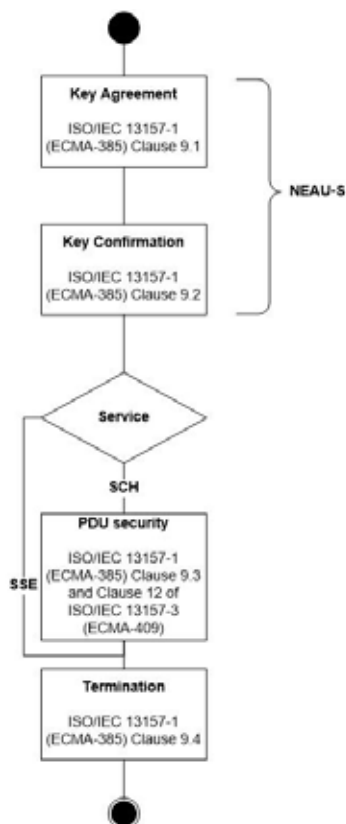


图7 NEAU-S与ISO/IEC 13157-1
的协作方法

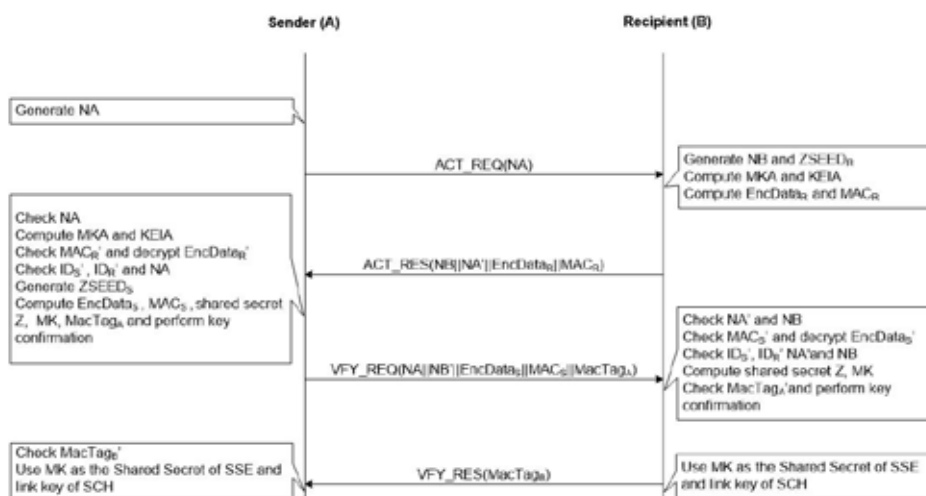


图8 NEAU-S机制工作流程

该标准由ECMA 411—NFC-SEC-05: NFC-SEC entity authentication and key agreement using symmetric cryptography (NFC-SEC-05: 采用对称密码算法的NFC-SEC实体鉴别与密钥协商协议) 经国际标准快速流程转化而来。ECMA 410是欧洲信息和通信系统标准化协会ECMA于2015年发布的地区性标准，该标准同样由联盟成员单位主导起草。

3.3.3 ISO/IEC 22425:2017

ISO/IEC 22425:2017 Information technology — Telecommunications and information exchange between systems — NFC-SEC Test Methods (信息技术-系统间远程通信和信息交换-NFC-SEC测试方法)，规范了ISO/IEC 13157系列标准的符合性测试方法，包括测试装置、测试规则、NFC-SEC协议测试方法等。

该标准目前第1版，共包含12章。前6章是标准的通用要素，分别为：范围、一致性、规范性引用文

件、术语和定义、符号和缩略语。第7章为NFC-SEC测试装置，见图9。第8章为测试规则。第9章规定了NFC-SEC-01的测试方法。第10章规定了NFC-SEC-02的测试方法。第11章规定了NFC-SEC-03（NEAU-A）的测试方法。第12章规定了NFC-SEC-04（NEAU-S）的测试方法。附录A和附录B均是资料性附录：附录A给出了接收方测试报告模板；附录B给出了发送方测试报告模板。

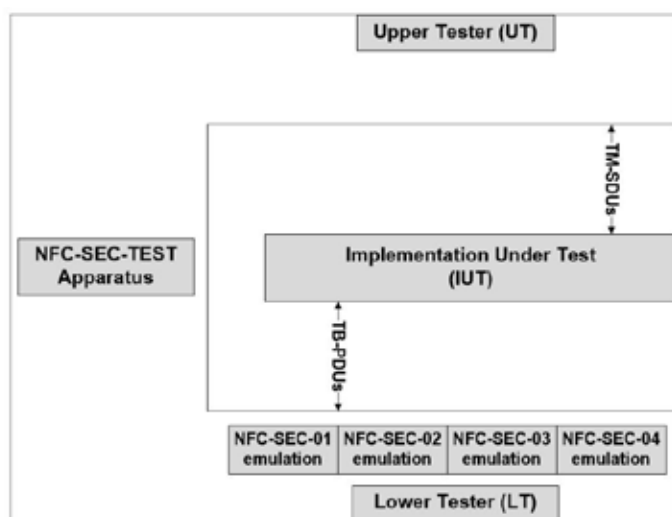


图9 NFC-SEC测试装置

该标准由ECMA 415—NFC-SEC test methods（NFC-SEC测试方法）经国际标准快速流程转化而来。ECMA 415是欧洲信息和通信系统标准化协会ECMA于2016年发布的地区性标准，该标准同样由联盟成员单位主导起草。

4 总结与展望

从全球范围看，欧美是物联网技术和应用的积极推动者，其物联网标准的建立、相关软硬件技术的开发与应用领域均走在世界前列。比较于欧美等发达国家或地区，我国物联网产业起步较晚，但经过近20年的发展，目前已在物联网技术、应用及标准化方面取得了长足发展。随着物联网应用领域的拓展和应用规模的扩大，各种安全隐患也暴露出来，信息安全事件频繁发生，如标签伪造、空中接口数据泄漏等，在一定程度上制约了物联网产业的发展。物联网安全技术研究和标准化成为推动物联网产业发展的关键。

2022年11月发布的国际标准ISO/IEC 29167-16:2022，是我国在物联网安全关键技术领域的创新突破，是WAPI产业联盟在中共中央和国务院印发的《国家标准化发展纲要》、北京市发布关于贯彻落实《国家标准化发展纲要》的实施意见指导下，践行网络强国战略和创新驱动发展战略的又一成功实践，对巩固我国在物联网安全协议关键技术领域的群体创新成果具有重要意义。本文所述包括ISO/IEC 29167-16:2022在内的7项由WAPI产业联盟组织制定的国际标准，已构成了我国主导的物联网安全关键技术标准体系，有助于实现全球物联网系统的互联互通和共享共治，充分体现了我国在网络空间的国际话语权。WAPI产业联盟将持续组织成员单位开展物联网安全技术与标准化工作，支撑我国物联网安全标准化工作迈向全球前列。

WAPI 产业联盟成员单位名录

中国移动通信集团公司	优比无线技术（深圳）有限公司	飞天联合（北京）系统技术有限公司
中国电信集团公司	南京智达康无线通信科技股份有限公司	中国电力科学研究院
中国联合网络通信集团有限公司	上海欣民通信技术有限公司	锐迪科微电子（上海）有限公司
国家密码管理局商用密码检测中心	福建三元达通讯股份有限公司	苏州汉明科技有限公司
国家无线电监测中心检测中心	新华三技术有限公司	神州数码网络(北京)有限公司
西电捷通公司	北京傲天动联技术股份有限公司	北京必虎科技股份有限公司
北大方正集团有限公司	中兴通讯股份有限公司	北京市政务信息安全保障中心
北京中电华大电子设计有限责任公司	武汉虹信通信技术有限责任公司	天津赞普科技股份有限公司
中电科普天科技股份有限公司	广州市卓纪思网络科技有限公司	上海连尚网络科技有限公司
深圳市明华澳汉智能卡有限公司	赛芯电子技术（上海）有限公司	深圳市瑞科慧联科技有限公司
北京数字认证股份有限公司	雷凌科技股份有限公司	深圳市信锐网科技术有限公司
北京六合万通微电子技术股份有限公司	瑞晟微电子（苏州）有限公司	福建新大陆通信科技股份有限公司
无锡中太数据通信有限公司	联发科技股份有限公司	北京比邻科技有限公司
青岛海尔科技有限公司	四川天邑信息科技股份有限公司	天津市电子机电产品检测中心
海信集团有限公司	湖南城市热点无线通信有限公司	高通无线通信技术（中国）有限公司
联想（北京）有限公司	珠海市魅族科技有限公司	中科开创（广州）智能科技有限公司
华为技术有限公司	深圳市雄脉科技有限公司	北京华信傲天网络技术有限公司
大唐移动通信设备有限公司	奥泰尔科技（深圳）有限公司	南京博洛米通信技术有限公司
北京朗波芯微技术有限公司	北京网贝合创科技有限公司	广西新海通信科技有限公司
大唐微电子技术有限公司	网件（北京）网络技术有限公司	上海麓慧科技有限公司
上海鼎芯科技有限公司	上海市数字证书认证中心有限公司	深圳市智开科技有限公司
北京天一集成科技有限公司	北京创原天地科技有限公司	南方电网数字电网研究院有限公司
北京联信永益信息技术有限公司	阿德利亚科技（北京）有限责任公司	深圳航天科创实业有限公司
深圳鑫金浪电子有限公司	深圳市华讯方舟软件信息有限公司	南方电网深圳数字电网研究院有限公司
深圳市普天宜通科技有限公司	迈创智慧供应链股份有限公司	广西电力线路器材厂有限责任公司
北京汉铭信通科技有限公司	科通宽带技术(深圳)有限公司	广西通量能源技术有限公司
西安大唐电信有限公司	邦讯技术股份有限公司	恩智浦（中国）管理有限公司
深圳共进电子股份有限公司	惠州市宝丰信息科技有限公司	南方电网科学研究院有限责任公司
北京华安广通科技发展有限公司	晨星软件研发（深圳）有限公司	山东华辰泰尔信息科技股份有限公司
深圳国人通信有限公司	卓望数码技术（深圳）有限公司	山东思极科技有限公司
东蓝数码有限公司	迈普通信技术股份有限公司	深圳市国电科技通信有限公司
美国安移通网络公司北京代表处	北京汇通融业科技发展有限公司	北京至周科技有限公司
北京五龙电信技术公司	上海寰创通信科技有限公司	北京联盛德微电子有限责任公司
北京同耀通电科技有限公司	吉翁电子（深圳）有限公司	北京市柴傅律师事务所
北京登合科技有限公司	北京汇为永兴科技有限公司	北京佰才邦技术股份有限公司
宇龙计算机通信科技（深圳）有限公司	福建星网锐捷网络有限公司	瑞斯康达科技发展股份有限公司
上海润欣科技有限公司	北京新岸线移动多媒体技术有限公司	广州莲雾科技有限公司
弘浩明传科技股份有限公司	广东欧珀移动通信有限公司	安徽皖通邮电股份有限公司
京信通信技术（广州）有限公司	上海贝尔股份有限公司	
北京城市热点资讯有限公司	成都鼎桥通信技术有限公司	

【注：截至2023年3月，联盟正式成员已达118家，以加入联盟的时间先后排序。】

WAPI Alliance
产业联盟



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>