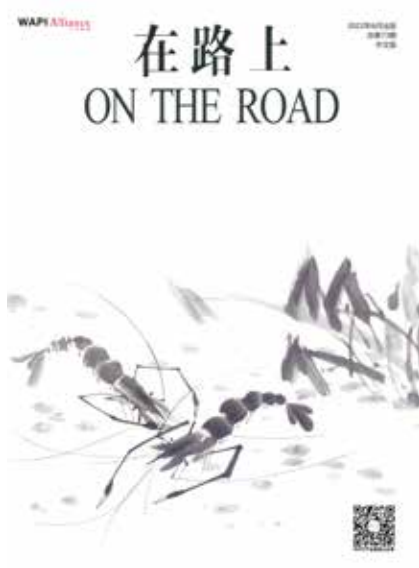


在路上

ON THE ROAD





理事成员：

中国移动通信集团公司
中国电信集团有限公司
中国联合网络通信集团有限公司
国家密码管理局商用密码检测中心
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
北京六合万通微电子科技股份有限公司
广州杰赛科技股份有限公司
深圳市明华澳汉智能卡有限公司

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 JTC1/SC6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：



WAPI产业联盟公众号

媒体聚焦 Media Focus

- 05 中国电子报等：芯语慧联发布新一代全国产WAPI MCU无线终端模组TH6180
- 07 飞象网等：恩智浦推出双模式WAPI模组并通过联盟测试
- 09 中国标准化等：WAPI产业联盟对发布实施3年以上的63项团体标准进行复审检验

特别报道 Special Report

- 11 维护网络安全推进网络强国建设 中国成为世界网信“引领者”
- 13 网络安全工作需要示范和验证 示范和验证即要公正、要权威，又要有能力、有水平

联盟关注 Alliance Concerns

- 16 我国电信设施曾遭网络窃密 部分数据传至境外
- 17 中国国际化现状与发展形势分析
- 21 重要行业的密码应用政策要求
- 23 走出认知误区 医疗机构如何迎接“密评”挑战

政经要闻 Policy News

- 26 中央军委主席习近平：签署命令发布《军队非战争军事行动纲要（试行）》
- 26 中共中央办公厅 国务院办公厅：推进实施国家文化数字化
- 27 国务院：强化气象基础能力建设中的信息网络安全保障
- 27 刘鹤：加强网络信息技术研究 确保网络技术体系可控性
- 28 外交部：美不择手段阻碍中国网络和数字发展
- 28 外交部：美国已成为网络安全领域的威胁
- 29 庄荣文：加强数字中国建设整体布局 全面赋能新时代高质量发展
- 29 国家药品监督管理局：要加强密码应用夯实网络安全
- 30 国家文物局：强化科技支撑 全面提升文物安全防控和应急管理水平
- 30 北京市经信局：安全已纳入北京市数字经济促进法规制度范畴
- 31 张晓刚：用标准为人类文明发展贡献力量

联盟工作 Alliance Work

- 32 WAPI产业联盟发布 最新版《WAPI标准产业应用及环境监测报告》
- 33 WAPI产业联盟召开 2022年无线网络安全标准化委员会第二季度主任工作会议
- 34 WAPI产业联盟召开 2022年第二次标准工作及项目组会议（总第122次）
- 37 WAPI产业联盟完成 2022年度中关村产业技术联盟诚信建设工作
- 39 WAPI产业联盟组织会员单位参加 2022科创中国·科技创新创业大赛
- 40 WAPI产业联盟参加 2022年国际标准化第一期视频培训会
- 41 新华三“智原生”系列产品通过WAPI产业联盟测试

新成员 New Member

- 42 北京至周科技有限公司加入WAPI产业联盟

成员与市场 Member & Marketing

- 43 南网深圳数研院“基于WAPI技术的大功率远距离无线数据传输装置”
获国家实用新型专利权
- 44 博洛米与WAPI可信无线局域网通信系统
- 46 MTK发布全新智能物联网AIoT平台Genio 1200
- 47 国家无线电监测中心检测中心荣获“北京2022年冬奥会、冬残奥会北京市先进集体”
荣誉称号
- 48 联盟成员发挥创新优势 筑科技抗疫坚强防线
- 50 数字认证：“雪亮工程”密码也是应用C位
- 51 地缘政治使欧洲风电行业成网络攻击主要目标

产业技术论坛 Industry & Technology Forum

- 52 方舱医院WAPI无线网络安全解决方案

中国电子报等：

芯语慧联发布新一代全国产WAPI MCU无线终端模组TH6180

【编者按】2022年6月17日，西安芯语慧联信息科技有限公司联合北京联盛德微电子有限责任公司、西电捷通公司，发布了新一代旗舰版WAPI MCU（微控制单元）物联网终端模组——TH6180。TH6180是TH6160的升级，具有全国产化、高安全、低功耗、小尺寸、免驱动、高可靠、易扩展等特点。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。

2022年6月，西安芯语慧联信息科技有限公司联合北京联盛德微电子有限责任公司、西电捷通公司，发布了新一代旗舰版WAPI MCU（微控制单元）物联网终端模组——TH6180。TH6180是TH6160的升级，具有全国产化、高安全、低功耗、小尺寸、免驱动、高可靠、易扩展等特点。

2022年2月，WAPI产业联盟发布了首套WAPI MCU物联网终端模组系列产品TH6160，迅速引发市场关注。据用户方反馈，TH6160上市后，满足了“低功耗物联网设备无需二次开发就能快速实现WAPI连接”的需求。

本次新发布的TH6180系列产品，是结合用户使用和反馈，对TH6160产品进行了全面升级改进，主要创新点集中在三方面：



图：TH6180物联网终端模组

第一、功耗更低。低功耗是WAPI MCU类型模组有别于WAPI CPE类型产品的重要特性，也是物联网类应用场景所必备的能力。更低的功耗，让更多物联网场景应用WAPI安全无线局域网成为可能。TH6180比TH6160在最低功耗上降低了30%，实测功耗小于10uA。

第二、性能更高、数据吞吐更加稳定。TH6180数据加解密运算采用了硬件方式（WLAN芯片内置WAPI加解密算法寄存器），在办公环境下的实测性能比TH6160提升了60%。更值得一提的是，由于数据加解密不再占用MCU运算资源，因此即便在多业务并发运算导致MCU负荷较高的时候，WAPI数据吞吐性能也不会出现波动。

第三、硬件设计和生产工艺提升、无线信号更强。相比上一代TH6160采用的二层板设计，TH6180采用了工业级四层板设计方案，模组的无线信号射频收发能力更强、硬件扩展能力和抗电磁干扰能力更好。



图：TH6180物联网终端模组应用示意图

据联盛德微电子CEO李庆介绍，TH6180基于全国产WLAN SoC低功耗芯片和国家权威机构认证的硬件安全密码模块研制，内部运行高可靠实时操作系统（RTOS），支持2.4GHz 1T1R射频收发，支持IEEE 802.11 b/g/n速率集，提供WAPI、TCP/IP、MQTT、HTTP等多种网络协议通信能力和丰富的AT指令集，提供串口、SPI、SDIO、IIC、GPIO等多种物理接口，能轻松实现诸如串口转无线、IIC转无线等常用模式，可广泛服务于传感器远程监测、工业自动化、智能电网、智慧交通、可穿戴设备、智能语音设备、智能安防设备、智慧仓储无线系统、智能开关、无线继电器、仪器仪表监测等物联网应用场景，帮助用户更高效便捷地部署实施“WAPI+”安全应用解决方案。

据芯语慧联CEO童伟刚介绍，作为新一代高安全低功耗WAPI MCU物联网终端模组，TH6180符合GB 15629.11系列国家标准，解决了此前电池供电类设备因功耗问题无法使用WAPI的难题。目前TH6180已通过WAPI产业联盟的WAPI协议符合性、协议完整性、产品互通性测试。后续芯语慧联将在WAPI技术产业上投入更多资源，为更广的物联网应用场景服务，发挥安全无线局域网的可管、可控、可追溯作用。

部分媒体新闻链接：

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20220617/116579.html>

飞象网：<http://www.cctime.com/html/2022-6-17/1621509.htm>

通信世界：<http://www.cww.net.cn/article?id=564061>

飞象网等：

恩智浦推出双模式WAPI模组并通过联盟测试

【编者按】2022年6月27日，恩智浦委托WAPI产业联盟开展了双模式WAPI模组的无线局域网鉴别与保密基础结构（WAPI）测试，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W9098模组进行了协议互通性、完整性、功能及性能测试并出具测试报告。该产品的推出，让物联网专业设备机具无需二次开发即可实现WAPI安全接入，解决了各厂商独立开发WAPI产品周期长、成本高、质量差异大的难题，满足了物联网市场对产品成本控制和接入安全的要求。飞象网、中国电子报/电子信息产业网等媒体对此进行了报道。

以下是飞象网的报道。



日前，恩智浦（中国）管理有限公司（以下简称恩智浦）推出双模式WAPI模组W9098，并通过了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、功能及性能测试。联盟为该产品出具了测试报告。

当前，物联网专业设备机具中模块化集成WAPI功能是大势所趋。恩智浦W9098模组，让物联网专业设备机具无需二次开发即可实现WAPI安全接入，解决了各厂商独立开发WAPI产品周期长、成本高、质量差异大的难题，满足了物联网市场对产品成本控制和接入安全的要求。

W9098模组具有如下产品特点：支持2.4/5GHz双频接入；通信速率支持802.11ac协议；支持双模式切换，既可工作在终端（STA）模式，也可工作在无线接入点（AP）模式，多个模组之间无需其他设备即可直接连



图：恩智浦WAPI模组W9098

接；可通过USB/PCIE/SDIO等接口与任意的设备/机具连接，无需安装驱动程序、无需做任何硬件改动即可具备WAPI能力。这些特点，高效满足了当前智能家居、互联汽车和工业机械等领域对WAPI的需求。

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W9098模组进行了协议互通性、完整性、功能及性能测试，恩智浦依据联盟实验室建议完成产品整改。目前，该模组已应用于车载互联网、IOT设备中。

恩智浦是全球半导体核心厂商，也是嵌入式应用安全连接解决方案的领跑者。2021年9月加入WAPI产业联盟之后，在WAPI芯片与模组方面与联盟成员展开协同创新与合作，推动更便捷、更智能、更安全的物联网应用。

部分媒体新闻链接：

飞象网：<http://www.cctime.com/html/2022-6-27/1622487.htm>

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20220628/116684.html>

中国标准化等：

WAPI产业联盟对发布实施3年以上的63项团体标准进行复审检验

【编者按】为规范团体标准管理，有序推进团体标准复审工作，推动团体标准复审常态化和制度化，WAPI产业联盟于2022年6月20日完成了63项团体标准的复审工作，复审结论为49项标准继续有效，9项标准需要修订，5项标准因随着技术发展被新版标准代替而予以废止。通过本次标准复审工作，对WAPI产业联盟实施满3年的团体标准进行了一次系统的检验评判，确保了联盟团体标准的适用性、规范性、时效性和协调性，对联盟的标准化体系建设亦有积极作用。中国标准化、中国电子报、电子信息产业网、飞象网、搜狐网等媒体对此进行了报道。

以下是中国标准化的报道。



据2022年6月20日WAPI产业联盟发布的《WAPI产业联盟关于63项团体标准复审结论的公告》显示，联盟完成了T/WAPIA 011—2012《无线网络访问控制技术规范》、T/WAPIA 001—2008《WAPI密钥管理实施指南》等63项团体标准的复审工作。

为规范团体标准管理，有序推进团体标准复审工作，推动团体标准复审常态化和制度化，WAPI产业联盟于2022年4月至6月期间，依据国标委《团体标准管理规定》、《WAPI产业联盟团体标准制修订工作程序》等要求，对本联盟已发布实施3年以上的63项团体标准进行复审，复审标准类别涉及技术要求、产品实现、测试规范、应用规范等。复审期间，联盟标准化部组织总体工作组、网络安全工作组、无线网络工作组、产品与解决方案工作组、互操作测试工作组以及相关领域专家，从团体标准的技术内容、实施应用情况、与现行国家政

策法规和其他标准的协调性、标准文本质量等维度对标准进行了审查并形成标准复审意见，经总体组审议复核并提交无线网络安全标准化委员会审定，复审结论如下：

一、T/WAPIA 011—2012《无线网络访问控制技术规范》等23项团体标准目前已转化为国家标准，复审结论为“继续有效”。

二、T/WAPIA 001—2008《WAPI密钥管理实施指南》等32项标准正在实施且效果良好，复审结论为“继续有效”。

三、T/WAPIA 002—2010《无线局域网接入点技术要求与测试方法》等9项团体标准，复审结论为“修订”。后续将从进一步符合《中华人民共和国网络安全法》《中华人民共和国密码法》等法律法规最新要求，满足市场对证书管理、TePA接入控制、AS/CIS/AC/AP/STA测试方法需求等方面，进行修订。

四、T/WAPIA 006—2010《无线局域网WAPI安全协议符合性测试规范》等5项团体标准，因随着技术发展已被新版标准代替，复审结论为“废止”。

通过本次标准复审工作，对WAPI产业联盟实施满3年的团体标准进行了一次系统检验评判，确保了联盟团体标准的适用性、规范性、时效性和协调性，对联盟标准化体系建设和标准高质量发展有积极作用。

WAPI产业联盟自2006年成立起，充分发挥标准对技术产业市场的创新牵引力，取得了丰硕成果。截至2022年6月，联盟已牵头组织成员开展了160余项标准的制修订，其中已发布（获发布）国际标准（ISO/IEC）14项，国外标准3项，国家标准41项，国家军用标准4项，行业标准7项，团体标准87项。

在组织团体标准创新和先试先行方面，WAPI产业联盟亦走在前列：联盟于2015年获批成为国家标准委首批团体标准试点单位；2017年和2019年分别荣获工信部百项团体标准应用示范项目；《关键信息基础设施无线局域网》等系列团体标准已在北京冬奥会、综合管廊、南方电网、国家电网等重大项目中广泛应用，创造了可观的经济效益和社会效益。市场用户评价表示：“WAPI产业联盟团体标准内容科学，要求定义合理，对行业无线局域网产品的采购、网络规划和建设部署具有积极指导意义，多项团体标准已成为行业标准制定的重要依据。”

部分媒体新闻链接：

中国标准化：https://mp.weixin.qq.com/s/bMt_n5JJfZ7QZEm_5zvwpPg

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20220620/116607.html>

飞象网：<http://www.cctime.com/html/2022-6-20/1621810.html>

搜狐网：https://www.sohu.com/a/559187064_121117464



图：2022年WAPI产业联盟团体标准复审公告

维护网络安全推进网络强国建设

中国成为世界网信“引领者”

中国信息安全

党的十八大以来，习近平总书记高度重视网络安全和信息化工作，从信息化发展大势和国际国内大局出发，就网信工作提出了系列新思想、新观点、新论断，深刻回答了系列方向性、根本性、全局性、战略性重大问题，形成了内涵丰富、科学系统的习近平总书记关于网络强国的重要思想，为做好新时代网络安全和信息化工作指明了前进方向、提供了根本遵循。

习近平总书记关于网络强国的重要思想是站在时代前沿和战略全局的认识和判断。当今世界，中华民族伟大复兴的战略全局与世界百年未有之大变局同步交织、相互激荡、交融交汇。以习近平同志为核心的党中央高瞻远瞩，准确把握人类历史发展机遇，深刻洞察新一轮科技革命和产业变革先机，坚持马克思主义立场观点方法，系统阐述网络强国战略思想，擘画中国网络强国建设之路，引领中国紧紧抓住千载难逢信息革命的历史机遇。

党的十八大以来，中国网信事业取得系列历史性成就：确立网络强国建设战略目标；切实维护网络意识形态安全；进一步巩固网络安全屏障；新基建“拔地而起”；数字经济迎风速长；中国“智”造享誉全球，开始成为世界网信的“引领者”，肩负起时代赋予的重大历史使命，这些彰显了大国领袖的深邃历史眼光、宏阔全局视野和非凡远见卓识。

习近平总书记关于网络强国的重要思想是中国维护网络安全的思想武器。随着万物互联和智能化时代的到来，网络空间发展所面临的安全威胁和风险日益突出，正向政治、经济、文化、社会、生态、国防等领域传导渗透，成为世界性难题。面对世界各国普遍感到棘手的难题，习近平总书记明确提出“没有网络安全就没有国家安全”“网络安全和信息化是一体之两翼、驱动之双轮”，把网络安全提升到国家安全的层面，为推动中国网络安全体系的建立，树立正确的网络安全观指明了方向。

习近平总书记以哲学视野和辩证思维提出网络安全观，精辟论述了网络安全的几大重要关系，言简意赅地指出“正能量是总要求，管得住是硬道理，用得好是真本事”，在把握互联网规律、引导网络舆论、驾驭信息化发展和保障网络安全等方面提出具体要求。在习近平总书记关于网络强国的重要思想指引下，中国一面推出《网络安全法》《个人信息保护法》《数据安全法》《关键信息基础设施安全保护条例》，搭起网络安全顶层设计的“四梁八柱”；一面健全网络综合治理体系，加强和创新互联网内容建设，落实互联网企业信息管理主体责任，全面提高网络治理能力，营造清朗的网络空间，构建网上网下同心圆，在维护网络安全方面不断出台新举措，迈出筑牢网络安全屏障新步伐，开辟管网治网新境界。

习近平总书记关于网络强国的重要思想是中国推进网络强国建设的行动指南，它明确了党的领导是网信事业沿着正确方向发展的坚强政治保障，明确了网信工作为人民的崇高使命，明确了网信工作在党和国家事业全局中的重要地位，明确了构建网络强国的基本原则要求和具体路径，体系严整、逻辑严密、内涵丰富、博大精深，正展现着实践伟力。目前，中国已建成全球最大光纤网络，信息基础建设规模全球领先；在5G、人工智能、高性能计算、量子计算等基础性、通用性新兴技术领域取得一大批重大科技成果，信息技术创新能力持续提升；数字经济体量位列全球第二，增速居全球第一，数字经济发展活力不断增强；全国中小学互联网接入率达100%，健康码等互联网应用不断向老年群体普及，信息技术不断增强人民群众获得感、幸福感、安全感；不断推动构建网络空间命运共同体，为推动全球互联网治理体系变革贡献了中国智慧、提供了中国方案、体现了中国担当。中国网络强国建设正在习近平总书记关于网络强国的重要思想指引下取得积极进展和瞩目成就。

在信息革命时代潮流与“两个大局”历史进程交汇之际，习近平总书记关于网络强国的重要思想指引中国网信事业取得历史性成就，展现着马克思主义真理的力量。遵循习近平总书记关于网络强国的重要思想，中国网络强国建设定将赢得光辉未来。

作者周宁南 系中国现代国际关系研究院科技与网络安全研究所助理研究员

网络安全工作需要示范和验证

示范和验证即要公正、要权威，又要有能力、有水平

公众号 与智慧做朋友 作者 李志勇

网络安全工作需要示范和验证。

网络安全成为当下要做且必须要做好的工作，并且要坚持持续做。另外，随着信息化系统的成熟，以及国家对网络安全的政策驱动，当下的网络安全工作也成为必须马上要开展的工作。但是，鉴于网络安全特有的专业技术性、应用相关性、效果不可见性、监管复杂性、政策标准严谨性等特点，对于建设单位来讲能在短时间搞清楚并做出正确的选择是一件很困难的事情。建立网络安全应用示范和验证，为建设单位输出建议并提供最直观、最多样的参考和选择成为一项解决当前问题比较有效的办法。当下，这样的机构已经存在不少，有的是官方的、有的是民办的、有的是院校的、有的是混合的，形式各异，出发点也不尽相同，其效果还有很大的提升空间。

网络安全工作示范、验证还有很大的空间。

示范和验证的意义明显：示范和验证无论对于网络安全建设单位、组织单位、供应商、主管单位都意义深远：

对于建设单位：

- 1、通过示范和验证做出快速选择，应对网络安全工作的特殊性和紧迫性
- 2、通过示范和验证做出正确选择，应对网络安全技术的复杂性和产业的多样性
- 3、通过示范和验证提升整体感观效果，应对审、选、建、评、用、升等复杂的全流程工作
- 4、通过示范和验证提升能力的交付性，应对本单位网络安全能力缺失问题

对于网络安全企业：

- 5、通过示范和验证为企业构建展示和提升自己的平台
- 6、通过示范和验证为网络安全上下游企业形成产业链奠定基础
- 7、通过示范和验证为企业上知政策、下得需求提供帮助

对于组织单位：

8、通过示范和验证更好的对接各方，更能发现行业中的问题，并给予针对性解决

9、通过示范和验证的深度参与，能更好的掌握实用信息，通过实践不断提升自己，从“智库”转化成“智能库”（有智慧并且有能力）

10、通过示范和验证促使单位站在全局角度看待和解决问题，更能为行业的发展助力

对于主管单位：

11、通过示范和验证保障政策有效落实，并能获取实践效果信息

12、通过示范和验证能和所有行业单位进行连接，更好地发挥众人之力

示范和验证对于网络安全工作的落实有着重要的意义，是一项必须认真做好的事情。

当前，各个有示范和验证功能的单位，整体表现还算可以，各有各的特点，但还是有一些问题需要解决，简单列举几个：

1、成了众多厂商的展厅、成了产品的货架，整体营养性不够

2、成了大厂商的招牌，示范了品牌，缺失了自身定位

3、成了厂商的聚集地，缺失了建设单位的参与度，整体客观性不够

4、成了检测机构，发证、出报告成为主业，缺失全局性

5、成了组织协调者，缺失业务能力和独立分析能力，主动牵引性和纠偏性不够

6、成了关注技术的场所，缺失政策、产业、场景、能力、落地等多维度示范和验证，完整性不够

7、成了一个利益体，缺乏开放性、公正性

8、成了“拿来用”，缺失自己分析和特殊贡献，无法对多方进行引导

当下，示范和验证存在的问题还是不少的，以上任何一个问题发展下去都会直接让示范和验证失去意义，请大家思考。

示范和验证问题列举。

对于提供示范和验证服务的机构而言，重点做到有权威、有能力，缺一不可。建议如下：

1、通过政府支持、效果展示、实际行动、口口相传等方式，提升自身公信力和可信度

2、自身不能仅仅定位管理和组织的职能，必须建立自己的能力体系（分析、咨询、设计、研判、评价、落地、纠偏、预言等）

3、不要紧紧聚焦技术层面，还要在思想、认识、逻辑分析、理论与方法、方案与抓手等多个维度提供示范和验证

4、在工作形式上可以考虑借鉴“揭榜挂帅”的方式，建设单位提供需求，大家群策群力

5、在职责上要肩负“正本清源”，产生错误不要紧，只要不一直错下去就行

6、在业务开展上考虑对建设单位人力的使用培养工作，这对建设单位意义重大

7、发布的报告、证照尽量控制在定向范围，并保持审慎态度，如果可以要提高监督力度8、充分考虑对行业“管、用、产、引”四个维度的衔接和催化作用9、积极整合公正机构/人士，审慎使用利益单位/人士，加强专家管理，保障全局思维

总之：示范和验证单位，最需要被认可的权威性和被认可的能力，才能成为促进行业发展可信赖、可依赖重要部分。

示范和验证单位有权威、有能力才是王道。

示范和验证对网络安全工作的开展意义重大，但当下的示范和验证所发挥的作用还远远不够，还有很多地方需要提升，应该围绕自身公正权威性和能力提升两个维度，其中能力欠缺、思想认识范围有限是当下制约示范和验证发挥作用的最主要问题。

澎湃新闻

2020年以来，国家安全机关工作发现，我国有关电信运营商、航空公司等单位内网和信息系统先后多次出现越权登录、数据外传等异常网络行为，疑似遭受网络攻击。国家安全机关依法开展技术检查，确认部分骨干网络节点设备、核心业务系统服务器等被植入特种木马程序，已有部分数据被发送至境外。通过进一步深入调查证实，相关攻击活动是由某境外间谍情报机关精心策划、秘密实施的。该机构调集强力网络攻击力量，使用全球多地网络资源和先进网络武器，妄图实现对我国关键信息基础设施战略控制的目的。

近年来，国家安全机关持续加大国家安全法律法规和12339举报受理电话宣传力度。随着宣传教育的不断深入，公民自觉主动举报危害国家安全线索显著增多，其中有一些是悬崖勒马、主动自首的情况。在我国某重要军事基地周边，2021年1月至6月间，先后有4人主动向国家安全机关自首。其中2人是被他人“引荐”给境外间谍情报机关，另外2人是在使用某知名网络交友软件时被境外间谍情报机关实施了网络勾连。

《中华人民共和国国家安全法》第七十七条规定，公民和组织应当履行下列维护国家安全的义务：一是遵守宪法、法律法规关于国家安全的有关规定；二是及时报告危害国家安全活动的线索；三是如实提供所知悉的涉及危害国家安全活动的证据；四是为国家安全工作提供便利条件或者其他协助；五是向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；六是保守所知悉的国家秘密；七是法律、行政法规规定的其他义务。

国家安全机关提醒，维护国家安全没有“局外人”，每个人都应该参与其中，贡献一份力量。国家越安全，人民就越有安全感；人民越有安全意识，国家安全也就越有依靠。

中国国际标准化现状及发展形势分析

国防标准化前沿

1 国际标准化背景分析

1.1 主要国际标准化组织分析

ISO(国际标准化组织)、IEC(国际电工委员会)、ITU(国际电信联盟)是全球公认的三大国际标准化组织, ISO 和IEC 制定了85%的国际标准, 其余15%则由ITU、WHO(世界卫生组织)、ICAO(国际民航组织)、WIPO(世界知识产权组织)等几十个国际机构制定。各大国际标准化组织均依托成员国平等合作运行, 原则上没有特权国。但一国在国际标准化组织中的参与度、影响力, 是其综合实力和国际话语权的重要体现, 在特定情况下, 标准话语权可以表现为个别国家对行业全球技术产品走向的强大控制力。

1.2 主要国家国际标准化战略分析

美国统筹部署国内和国际, 全方位展开美国标准化活动, 积极推行“标准国际化战略”。2020年版《美国标准化战略》^[1], 直接表明要推广美国标准, 并进一步细化了美国标准的全球推广措施, 专门要求“标准制定者要继续实施一致的程序来验证有关翻译, 并促进标准在全球的快速传播。”

德国作为出口型经济大国, 为提高产品和技术在全球市场竞争力, 启动“标准化研究2030”^[2], 鼓励本国企业、标准化机构参与国际标准化活动, 使德国标准在全球范围得到认可和应用;将国内80%资源投入欧洲标准和国际标准, 只有20%投入本国急需的国家标准工作上, 使德国的标准始终保持在国际先进水平。

日本提出《标准化官民战略》, 核心举措包括提高标准制定过程中利益相关方的参与程度, 提升技术标准市场适用性和透明度;积极参与ISO、IEC 国际标准审议, 承担更多的秘书处工作, 积极参与国际标准审议, 培养熟悉国际标准制订规则的高层次专业人才和标准化专家。在制定涉及日本利益的国际标准时充分反映日本的诉求和意见, 标准化战略聚焦于日本优势产业及国际空白领域。

1.3 中国在国际标准化组织中的参与情况

目前我国加入了21 个认证认可国际组织, 对外签署多边互认协议13 份、双边合作互认协议117 份。中国是ISO 创始成员国, 担任72 个TC/SC秘书处, 占总数的9.5%, 并在733 个TC/SC 中作为P 成员参与标准化活动, 共有142 名专家担任工作组召集人;是IEC 的89 个技术委员会和107个分委员会的P 成员以及IEC 理事局、执委会和合格评定局的成员, 担任了10 个TC/SC 的秘书处工作, 约占总数的5%, 并在180 个TC/SC 中作为P 成员参与标准化工作;是ITU 行政理事会理事, 国内三大电信运营商以部门成员身份参加国际电信联盟三大部门的活动。

2 我国标准化工作现状分析

2.1 政策体系情况

中国标准化战略尚处于建设进程中，国家标准化战略实施专家咨询委员会于2020年成立，先后发布了《国家标准化体系建设发展规划（2016—2020年）》以及《标准联通“一带一路”行动计划》，旨在推动标准国际化。《国家创新驱动发展战略纲要》着重突出了标准化工作，支持大力实施标准战略，提出加强技术创新和标准化融合发展。

2.2 工作开展情况

国际标准化工作主要包含两方面，一是积极参与国际标准化活动，加强我国在国际标准化活动中的影响，推动我国标准成为国际标准；二是提高国内标准与国际标准的一致程度，通常以“采标率”来表示。我国产品国际采标率已达80%以上，但主导制定的ISO、IEC国际标准仅占其标准总数的1.8%，与我国世界第二大经济体的地位极不匹配，难以适应“一带一路”背景下中国产品加速走出去的战略需要。

2.3 面临的主要问题

第一，未形成明确的国际标准化战略。重国内、轻国外，我国的国内标准数量庞大，远超过国际标准的数量。资源分配不均衡造成我国对国际标准化工作的参与度仍低于发达国家。

第二，技术标准化研究人才匮乏。具有较高理论修养和业务能力的标准化人员不足，特别是缺乏熟悉国际标准组织工作语言并能代表国家参与国际标准制定的高素质复合型人才。国内开设标准化学科或专业的高等院校少，严重影响标准化发展。

第三，对国际标准组织参与度不足。发达国家大量专家参加了大部分的国际标准会议，尤其是美国，参与度达到80%。而中国国际标准会议参与度、承担国际标准组织要职、承担国际标准活动主办数量方面，都处于弱势地位。

第四，企业在国际标准工作中参与度与贡献度低^[3]。在不断追求合格率提高情况下，多数企业采取保底线策略制定标准，没有提升标准的动力和压力。龙头骨干企业参与标准国际化的意愿不够强，仅40%左右的企业采用国际标准，企业的技术标准参数与国际对标达标不够。

3 ISO/TC306 案例剖析

国际标准化组织铸造机械技术委员会（ISO/TC306）于2016年由ISO批准创建。目前由7个P成员国和17个O成员国组成，秘书处设在济南铸锻所检验检测科技有限公司。

3.1 ISO/TC306 组织情况分析

虽然我国在306中占据较为主动的地位，但标委会组织能力、国际协调能力、国内行业统筹能力必须同时

具备，才能促成我国提案顺利通过，实现既定目标。在投票时，组织方对P 成员国的引领力和影响力，至关重要。从组织机构上说，秘书处设于我国，主席由国内教授担任；从专家比例来说，中国专家占比达35%以上。但是，在标准推动中，仍需要成员国支持以实现既定目标。虽然中国在TC306 中处于组织者地位，但当标准制定提议投票和标准审议投票时，必须有足够的赞成票才能通过立项和发布。

3.2 ISO/TC306 国际合作分析

标准联合制定过程中，由于欧洲标准化委员会框架下要求欧洲标准与国际标准同步制定，导致德国工作组出现延后情况。这一情况体现了欧洲国际标准化工作的协同性和一致性加强，但ISO 标准总体进度受到影响。面对疫情及其他复杂情况导致难以协调多国进度时，科学高效处理问题、达到既定目标，是树立国家标准化工作威信、取得国际支持和话语权的重要基础。

3.3 国内标准国际化情况

TC306 秘书处与“全国铸造机械标准化技术委员会（SAC/TC186）”同步开展工作。国标委既是国际标委会的支撑机构，也是国内产业与国际标准衔接的重要桥梁。TC306 在2020 年完成了《GB/T25711-2010 铸造机械通用技术条件》等2个标准外文版项目报批工作。国家标准外文版对我国标准国际化具有重要意义，对于类似中、美等体量的产业大国，将本国标准国际化、通用化、并最终上升为国际标准，是推进国内产业持续发展、走向世界的重要环节，亟需通过培育专门人才、搭建高水平平台，加快国家标准外文化、国际化的步伐。

4 对策建议

4.1 从国家战略高度重视标准化工作

我国亟需在国家层面、产业层面提出面向全球竞争的国际标准化发展战略规划布局，“谁制定标准谁就拥有市场”，要坚定不移地深入推进标准化工作，树立“标准先行”理念，以标准化战略，助推高质量发展。工业领域标准化长远战略重心应转向标准国际化，按照ISO 倡议的“一个标准、一次检测、全球通行”，以标准国际化增强中国制造海外渗透性。

4.2 改革现行的标准化管理机制体制

加快推进标准化体制改革，划清政府与市场参与标准的边界，凡是企业主体、社会组织、行业协会能有效供给的标准，政府逐步退出。政府主导制订的标准，侧重于守底线、保安全；市场自主制订的标准，应侧重于强优势、拓市场、时效快。深化标准化运行机制改革，进一步简化标准制修订流程，缩短标准制修订周期。

4.3 搭建平台并提供标准化支持

建设覆盖全国各行业各领域的标准化信息平台,通过平台向企业免费提供行业标准、国家标准和国际标准检索服务，鼓励企业踊跃采用国际标准。培育标准化咨询服务平台和机构，鼓励行业协会等社会团体协调领军企业、高校院所、中介组织组建标准化信息咨询服务平台，及时向社会各界提供全球各国技术标准和法规情

况，强化企业对贸易战、反倾销、国际法律与规则的学习与理解。

4.4 培养标准化复合型人才

人才是开展国际标准化工作的基础。政府、行业机构、企业均应积极组织开展标准化工作相关培训和继续深造，在外语、技术及国际标准制定规则方面全面深入，加强标准国际化人才培养与交流，提高人才综合能力。通过优选在校生及从业人员定向培训，鼓励大学设立标准化本科和研究生课程，培养懂专业和标准化、英语流利的复合型人才。

4.5 积极参与国际组织活动

全力争取国际标准化组织技术委员会稀缺席位，加强与标准化组织合作，深度介入国际标准制修订，在重点领域承担更多的召集人和秘书等职务，拓宽中国标准走出去通道。同时，积极参加国际标准制修订工作，及时了解最新动向和技术信息，促进国内标准和国际标准同步。

4.6 着力增加必要专利数量

“技术专利化、专利标准化、标准国际化”是产业知识产权发展走向。以美国为首的发达国家掌握95%以上的必要专利，在多个领域处于垄断地位，并将其转化为技术贸易壁垒，严重影响我国产业成长和参与国际竞争。目前国际标准必要专利产业分布不均匀，绝大多数必要专利来自信息产业，其他产业正处于国际标准与专利结合的起步阶段，我国可以以此为契机，有重点地拓宽我国必要专利涉及领域。

4.7 聚焦主业领域深入挖掘

企业围绕自身主营业务，积极研究开展对口领域国际标准化工作。关注相关标准委员会工作计划、组织架构、委员会内各国家参与情况。统筹企业内部资源，坚持自主制定标准和采用国际标准“两条腿”走路。掌握国内外标准制定情况，寻找国际标准空白领域开展国际标准提案前期准备。固定团队跟踪对应领域国际技术委员会工作进展，积极参与国际标准研讨会议，分析企业国际标准提案的可行性、合理性和市场需求度，提升国际立项成功率。

参考文献:

- [1] 高倩倩, 梁丽, 董衍磊, 等. 美国标准化战略[J]. 中国标准化, 2021(05): 26-37.
- [2] 肖洋. 西方科技霸权与中国标准国际化——工业革命4.0 的视角[J]. 社会科学. 2017(07): 57-65.
- [3] 王欢, 王庆华. 中国企业开展国际标准化工作的思考[J]. 中国标准化. 2020(06): 112-116.

作者:

程琳¹, 李尚达¹, 宋鹏飞¹, 辛海明², 卢军³

1. 山东省工业和信息化研究院; 2. 潍坊职业学院; 3. 济南铸锻所检验检测科技有限公司

重要行业的密码应用政策要求

商密君

为增强金融和重要领域网络与信息系统的的风险防控能力，充分发挥密码在维护网络与信息安全方面的重要作用，切实加强行业和地区的密码应用工作，近年来许多行业主管部门和地方陆续出台了一系列政策文件，对密码应用提出了明确的要求。

1 金融行业密码应用政策要求

中国人民银行对银行机构使用的密码基础设施、金融 IC 卡、网上银行、移动支付、关键信息系统提出了密码应用要求，要求采用符合国家密码法律法规和标准要求的密码算法和密码产品，构建安全可控的密码保障体系。2016年，中国人民银行会同原中国银行业监督管理委员会发布《银行卡清算机构管理办法》，要求银行卡清算业务基础设施应满足国家信息安全等级保护要求，使用经国家密码管理部门认可的商用密码产品。

中国证券监督管理委员会明确提出逐步在网上证券、网上期货、网上基金等业务中规范密码应用，按照国家法律法规和标准的要求，推广使用合规有效的密码算法和密码产品。

原中国保险监督管理委员会要求逐步在电子保单、电子认证、办公系统，以及各类保险业务系统中规范密码引用，使用符合国家密码法律法规和标准要求的密码算法和密码产品，加强密码应用的检测评估，确保密码应用合规、正确、有效。

2 其他重要行业密码应用政策要求

教育、公安、住建、交通、水利、卫生计生、工商、能源等领域主管部门，均制定了本领域密码应用总体规划或工作方案，明确要求使用符合国家密码法律法规和标准规范的密码算法和密码产品，实现密码在本领域的全面应用。

教育部要求，在教育和科研计算机网、教育管理、教育资源、电子校务、教育基础数据、教育卡等信息系统，以及面向社会服务的教育政务系统中加强密码应用。

公安部要求，在信息安全等级保护第三级及以上的网络信息系统、国家级信息化项目、全国或跨地区联网的网络与信息系统、公安信息网基础设施、面向社会服务的政务信息系统中加强密码应用。

财政部印发《政务信息系统政府采购管理暂行办法》，要求采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

住房和城乡建设部要求，在城市基础设施信息系统、面向社会服务的政务信息系统、行业性业务系统和

办公系统中加强密码应用。

交通运输部要求，在高速公路不停车电子收费系统（ETC）、交通一卡通系统、联网售票系统、出行服务系统、运政管理系统、地理信息系统等领域加强密码应用。中国铁路总公司要求，在铁路基础网络、重要信息系统、公众服务平台等领域加强密码应用。

水利部要求，在重要水利枢纽、重要水文水利系统中加强密码应用。国务院三峡办要求，在三峡水利枢纽工业控制系统中加强密码应用。

原国家卫生计生委要求，建设卫生计生行业密码应用基础设施，在人口健康信息平台、卫生计生行业重要信息系统中加强密码应用。

原国家工商总局要求，在工商部门面向社会服务的信息系统中，加快推进基于密码的网络信任、安全管理和运行监管体系建设，规范密码应用。

国家能源局要求，在电力系统、核电厂、石油天然气、油气管道等重要信息系统和重要工业控制系统中加强密码应用。

原国家测绘地理信息局要求，在卫星导航基准站、面向社会服务的测绘地理信息政务系统中加强密码应用。

走出认知误区，医疗机构如何迎接“密评”挑战

HIT专家网

“正确认识密码应用与密评工作，帮助医疗机构奠定网络与信息系统安全的基础，维护好最后一道防线。”

2022年4月19日，在由中国医院协会信息专业委员会（CHIMA）指导、HIT专家网主办、北京数字认证股份有限公司（简称数字认证）承办的“卫生健康行业商用密码应用线上研讨会”上，中国科学院信息工程研究所副研究员、中国密码学会密评联委会副主任委员马原对医疗机构普遍关注的商用密码应用安全性评估工作（也即密评）进行了详细介绍，并针对业内对密评的认知误区进行了剖析与澄清。

1 了解密评体系及测评要点

“商用密码应用安全性评估”，是对采用商用密码技术、产品和服务集成建设的网络和信息系统的密码应用的合规性、正确性、有效性进行评估的活动。自国家密码管理局开展密评试点工作至今，已完成密评体系的构建设计、标准和指导性文件的制定、密评试点机构的认定、密评结果的备案等工作。当前，全国范围内对重要信息系统的密评活动也正在有序开展过程中，这有力促进了密码应用的合规性、正确性和有效性。

“密评工作的整体思路是‘三同步一评估’，也即围绕密码应用方案，项目建设单位应当同步规划、同步建设、同步运行密码保障系统，每一个阶段都需要开展密评。”马原对密评体系进行了介绍：

首先是GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称《基本要求》），这是密码应用的纲领性、框架性标准，也是安全性评估的顶层准则。《基本要求》在给出总体性要求的基础上，对密码应用提出了4个方面的技术要求，分别为：物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全，以及4个方面的管理要求，分别为：管理制度、人员管理、建设运行、应急处置。

《基本要求》对每一个密码应用的要求项，采用“应”“宜”“可”来表达不同的约束程度。以等保三级系统为例，《基本要求》制定了49条指标，其中“应”30条、“宜”14条、“可”1条，另外还包括“GB/T 37092-2018《信息安全技术 密码模块安全要求》中关于二级及以上密码产品要求”4条。

其次是GM/T 0115-2021《信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》，这是为配合《基本要求》的贯彻实施、更好地指导和规范密评工作而制定的两部行业标准，已于2022年5月1日起正式实施。马原说：“在一项完整的密评任务中，GM/T 0115自下而上地提出了对测评活动的要求，GM/T 0116从测评准备、方案编制、现场测评、分析和报告编制全过程对测评活动进行指导。”

此外，中国密码学会密评联委会还组织制定了密评工作的系列指导性文件，包括《信息系统密码应用高风险判定指引》（以下简称《高风险判定指引》）《商用密码应用安全性评估量化评估规则》（以下简称《量化评估规则》）《商用密码应用安全性评估报告模板（2021版）》等。

其中，《高风险判定指引》基于当前密码产品的发展现状，聚焦安全问题被威胁利用后对信息系统（主要是数据资产）造成的影响程度，给出信息系统密码应用过程中可能存在的高风险安全问题、可能的缓解措施和风险评价。《量化评估规则》的主要内容是如何对各应用点进行打分判定并给出定量评估结果，其编制原则是：鼓励使用密码技术，特别鼓励使用合规的密码算法/技术/产品/服务；优先在网络和通信安全、应用和数据安全层面推进密码技术应用。

“系统中是否存在高风险项，以及各应用点的分值情况，这两者共同决定了密评结果。特别是高风险项，具有‘一票否决’的关键作用。”马原介绍，如果量化评估的分数为100分，且风险分析为“无风险”，则评估结论为“符合”；如果量化评估分数大于等于阈值（目前量化评估的阈值设置为60分），且风险分析为“无高风险”，则评估结论为“基本符合”；如果量化评估分数小于阈值，或风险分析为“有高风险”，评估结论则为“不符合”。

2 对密评工作的几个常见错误认识

“在密评工作试点过程中，通过与用户单位和主管部门的反复沟通，在形成部分共识的同时，我们也发现关于密评存在一些认知误区，需要及时厘清。”马原对几个常见的密评问题进行了总结与解答。

问题1：信息系统里没有使用密码技术，可以不做密评吗？

马原认为，之所以会有这样的疑问产生，根源在于误以为“密评是围绕密码产品来测密码”。实际上，密评的目的是围绕信息系统应该保护的重要数据等来测试密码应用的合规性、正确性和有效性。

“信息系统是否需要进行密评，不在于是否使用了密码技术，而取决于系统内需保护对象的重要程度。”马原说。根据《密码法》《商用密码管理条例》等法律法规以及地方和行业的要求，应对重要信息系统开展密评。

问题2：没有使用商用密码或国产密码，在密评中会导致“一票否决”吗？

马原介绍，决定密评结果的两个因素：一个是“质”，也即不能存在高风险项；一个是“量”，也即量化评估的分数要超过阈值。只要严格对标《高风险判定指引》与《量化评估规则》，确保量化评估分数大于等于阈值，且风险分析为“无高风险”，即可通过密评。

问题3：不使用认证合格的密码产品会导致“一票否决”吗？

“在实际的密评试点过程中，确实会遇到某些业务场景暂时未能找到现成的、认证合格的密码产品，只能转而使用其他产品做支撑的现象。”马原介绍，密评时对此的原则是“有用则用、能用则用”，同时注重“风险评估”。

问题4：等保和密评要求的部分条款相同，是否能够复用？

从顶层设计的角度来看，密评与等保工作是相互衔接、相互补充的关系。“密评的部分条款虽然与等保的内容相同，但在具体测评要求上有所不同。”

马原以“数据传输机密性指标”为例对此进行了说明，并通过对比分析指出，密评的测评实施覆盖从底层密钥到上层业务应用的全部方面，目的是切实打牢密码的基础性作用。“从这一点上说，密评测试实施的力度和深度是很大的。”

3 医疗机构如何推动密评工作？

当前，从行业调研情况来看，医疗机构对于密评工作的认识深度与重视程度还不足；在密码应用方面，除部分医疗机构在部分业务场景中引入CA系统外，缺乏整体密码应用规划与设计。另一方面，作为与国计民生息息相关的重点领域，医疗行业面临的数据安全与隐私保护难度正日益加大，医疗机构未能采用密码技术，或仅采用不安全的密码技术对重要业务数据和患者隐私数据进行防护，在数据泄漏与防护层面存在较大缺口。

“随着密评工作在医疗行业的逐步开展，这些情况将有很程度的改观。”马原认为，医疗机构应系统性推进密码应用，通过关键节点的密码应用与风险控制相结合的手段，在密评工作的推动下守牢网络与信息安全的底线。针对医疗机构密评工作的实施推进环节，马原给出以下具体建议：

首先，确定密评的系统边界，一般遵照等保定级边界即可。

第二，确定系统保护的主体，也即密评对象，一般包括机房、网络通道、设备、重要数据、重要用户身份等。“保护对象的覆盖应尽可能全面，避免盲区。”马原说，比如同一应用面向不同用户、存在不同类型的重要数据时，在系统设计中应考虑全面，避免遗漏对高风险项的处理。

第三，关键指标的密码应用要尽可能合规、正确、有效。重点关注《基本要求》中“应”的指标，尽可能选用二级密码模块，重视应用层的密码应用。“应用层的权重高达30分，做得不好可能就无法及格。”

最后，高风险项是“一票否决项”，坚决不能有。应格外注意应用存储加密等无缓解措施的条款；梳理密钥体系，避免密钥泄露、篡改等问题。

中央军委主席习近平： 签署命令发布《军队非战争军事行动纲要（试行）》

中央军委主席习近平日前签署命令，发布《军队非战争军事行动纲要（试行）》，自2022年6月15日起施行。

《纲要》坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平强军思想，坚持总体国家安全观，着眼有效防范化解风险挑战、应对处置突发事件，保护人民群众生命财产安全，维护国家主权、安全、发展利益，维护世界和平和地区稳定，创新军事力量运用方式，规范军队非战争军事行动组织实施，对有效履行新时代军队使命任务具有重要意义。

《纲要》共6章59条，认真总结以往遂行任务实践经验，广泛汲取军地相关理论成果，主要对基本原则、组织指挥、行动类型、行动保障、政治工作等进行了系统规范，为部队遂行非战争军事行动提供法规依据。

中共中央办公厅 国务院办公厅： 推进实施国家文化数字化

2022年5月22日，中共中央办公厅、国务院办公厅印发《关于推进实施国家文化数字化战略的意见》指出，要在数据采集加工、交易分发、传输存储及数据治理等环节，制定文化数据安全标准，强化中华文化数据库数据入库标准，构建完善的文化数据安全监管体系，完善文化资源数据和文化数字内容的产权保护措施。加快文化数字化建设标准研究制定，健全文化资源数据分享动力机制，研究制定扶持文化数字化建设的产业政策，落实和完善财政支持政策，在文化数字化建设领域布局国家技术创新中心、全国重点实验室等国家科技创新基地，支持符合科创属性的数字化文化企业在科创板上市融资，推进文化数字化相关学科专业建设，用好产教融合平台等。

国务院：

强化气象基础能力建设中的信息网络安全保障

2022年5月23日，国务院印发《气象高质量发展纲要（2022—2035年）》指出，要加强气象基础能力建设，打造气象信息支撑系统。要求在确保气象数据安全的前提下，建设地球系统大数据平台，推进信息开放和共建共享。要健全跨部门跨地区气象相关数据获取、存储、汇交、使用监管制度，研制高质量气象数据集，提高气象数据应用服务能力。要研究建设固移融合、高速泛在的气象通信网络。要强化气象数据资源、信息网络和应用系统安全保障。

刘 鹤：

加强网络信息技术研究 确保网络技术体系可控性

2022年5月30日，中共中央政治局委员、国务院副总理刘鹤出席中国工程院第十六次院士大会开幕式中强调，要按照“疫情要防住、经济要稳住、发展要安全”的要求，在做好现有工作基础上，加强几方面的研究力度。其中包括：加强网络信息技术研究，确保网络技术体系可控性，加强人工智能技术研发，重视区块链、数字货币等技术创新。立足资源禀赋提升能源保障水平，提高资源勘探和开发水平，重视煤制油制气、智能电网等技术研发。确保产业链供应链畅通，补齐基础软件、核心硬件、基础原材料等突出短板。探索科技助力城市管理，探索更科学的城市规划布局和智慧城市技术路径，结合疫情防控研究极端情况下的城市运营调度。

外交部：

美不择手段阻碍中国网络和数字发展

2022年5月6日，外交部发言人赵立坚在例行记者会上表示，为了保持自己领域优势和垄断地位，美国不守规则，不择手段，不负责任地阻碍中国的网络和数字发展。

赵立坚表示，为了限制中国的发展，美国不守规则，不惜分裂互联网，裹挟部分国家发表所谓“互联网未来宣言”，抛弃多边主义和联合国等平台，企图以小圈子的“帮规”取代多边规则。美国多年来在全球范围实施了大规模系统性、无差别的数据和网络窃密。美还向其他国家扩散进攻性网络技术和武器，极力整合盟友的网络进攻力量，并散布“中国黑客攻击”的虚假信息，试图在中国周边国家前沿部署网络军事力量。这些都是极其不负责任的行为。美国在网络问题上为“一己之私”不惜制造分裂，挑动对抗，胁迫其他国家，严重破坏了国际社会的团结，也严重阻碍了国际社会推动网络空间全球治理的努力。网络空间是我们所有人的家园。维护网络空间的开放与包容，顺应网络经济和技术发展客观规律是大势所趋。维护网络空间的和平与安全，在公平、公正、非歧视性环境中共享网络和数字发展红利是人心所向。美方应站在历史正确的一边，多从国际社会的共同利益出发，立即停止不负责任的言论和做法。

外交部：

美国已成为网络安全领域的威胁

2022年6月15日外交部发言人汪文斌主持例行记者会时表示，对全世界而言，美国已经成为网络安全领域的首要威胁。有报告披露的材料表明，英国等“五眼联盟”和部分欧洲国家的网络机构协助并参与了美国在全球范围内的网络窃密行动，这表明美国正在打造一个以美国为核心的网络窃密轴心。值得关注的是，报告指出，部分美国互联网软硬件公司全程参与美国网络武器研发制造。前不久，中国国家计算机病毒应急处理中心也发布报告指出，现有国际互联骨干网和世界各地的重要关键信息基础设施中，只要包含美国公司提供的软硬件，就极有可能被内嵌各类的后门程序，从而成为美国政府网络攻击的目标。

汪文斌表示，不难看出，美国以所谓的国家安全为借口，抹黑打压中国的企业，真实目的是为美国不负责任的网络窃密活动大开方便之门。我们敦促美方立即停止针对全球的恶意网络活动，在网络空间采取负责任的态度。

庄荣文：

加强数字中国建设整体布局 全面赋能新时代高质量发展

2022年5月，中央宣传部副部长、中央网络安全和信息化委员会办公室主任、国家互联网信息办公室主任庄荣文在《中国网信》杂志发表署名文章中表示，要加强数字技术自主创新，立足关键核心技术高水平自立自强，加快基础性技术、通用性技术突破，提升关键软硬件技术创新能力；要夯实数字基础设施根基，统筹推进通信网络基础设施等建设，聚焦工业互联网、物联网等重点领域，大力推进体系化建设、规模化部署、产业化应用，加快建设高速泛在、天地一体、云网融合、智能敏捷、绿色低碳、安全可控的数字基础设施；要筑牢数字安全防护屏障，树牢总体国家安全观，深入实施《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》等法律法规。全面加强网络安全保障体系和能力建设，加强关键信息基础设施安全保护。

国家药品监督管理局：

要加强密码应用夯实网络安全

2022年5月11日，国家药品监督管理局发布《药品监督网络安全与信息化建设“十四五”规划》，把夯实网络安全综合保障能力作为重点任务。

任务要求：一要加强网络安全保障管理。完善网络安全保障体系，开展信息系统安全等级保护备案与信息安全等级保护测评、关键信息基础设施安全保护、密码应用安全性评估等工作，依据《网络安全法》《密码法》等法规，落实《关键信息基础设施安全保护条例》。二要推进数据安全保障建设。要提升数据的存储安全、传输安全、访问安全和使用安全。三要升级安全管理运维平台。要从关键基础设施安全、业务系统安全、数据资源安全三个维度建立安全运维一体化体系，确保信息系统安全管理的机密性、完整性、可用性、可控性和不可否认性。

国家文物局：

强化科技支撑，全面提升文物安全防控和应急管理水平

2022年5月5日，国家文物局印发《文物安全防控“十四五”专项规划》指出，要全面提升文物安全防控和应急管理水平。要健全文物安全技术标准，出台文物安全监管平台建设技术指导标准，实现文物安全防护智能化和标准化。要建设安全监管平台，推动文物资源纳入公共安全视频建设联网应用工作。要推动文物安全防控专用和关键技术研究，建设安全监测、电子巡查等安全防控设施，利用智能监控装备等提升文物安全预警能力和效率，实现精准化预警、智能化防控、信息化管理。

北京市经信局：

安全已纳入北京市数字经济促进法规制度范畴

2022年5月7日，北京市经济和信息化局发布《北京市数字经济促进条例（征求意见稿）》，《条例》共九章五十八条，从数字基础设施、数字产业化、产业数字化、数字经济安全等方面对北京市的数字经济工作进行法规制度设计。

在数字基础设施方面，要坚持安全可信，加快建设信息网络基础设施。支持建设移动通信网络等网络基础设施，形成高速泛在、天地一体、云网融合、安全可控的网络服务体系。

在数字产业化方面，要通过政策支持、标准制定等方式，支持数字产业基础研究和关键核心技术攻关。支持网络安全等技术和软硬件产品的研发应用，鼓励安全咨询设计、安全评估、检测认证等数据安全服务业发展。要适当提高公共机构、重点行业企事业单位的数字安全投入水平。

在产业数字化方面，要支持农业、制造业、建筑、能源、金融、医疗等领域产业互联网发展，建立健全安全保障体系和产业生态。

在数字经济安全方面，要对关键信息基础设施实行重点保护，建立信息基础设施网络安全保障体系。

张晓刚： 用标准为人类文明发展贡献力量

2022年5月10日，原国际标准化组织（ISO）主席张晓刚在“2022品牌强国论坛”演讲中表示，中国高质量发展转型要解决三个主要问题。

一要解决经济发展模式的问题。要从过度追求速度和数量的增长方式，而转向追求质量。标准是质量的技术基础。要想抓质量，必须抓标准。要想有高质量，必须有高标准。

二要解决制造业大而不强、中国制造技术含量中低端的问题。这是中国品牌的基础，更是中国品牌国际化的前提。

三要实现国家治理体系和治理能力现代化的问题。积极地参与全球治理，为全球治理提供中国解决方案和中国智慧，是最重要的基础。

在如何实现中国制造的品牌与世界共享方面，他认为企业应让自己的标准为全球消费者认同，标准会成为国际市场竞争的制高点。国力之争主要是市场之争，而市场之争主要是企业之争，是技术之争。而技术之争，归根到底是标准之争。过去中国企业只是全球技术的追随者、国际标准的使用者。未来通过制造高质量发展，中国最优秀的企业如何用标准为人类的文明发展，贡献我们的聪明才智和力量，这一定是今天中国最优秀的企业的价值思考。

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 周 园

WAPI Alliance
2022年
WAPI 标准产业应用及环境监测报告
【2022年6月版】



2022年6月23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》，增添了“新一代旗舰版WAPI MCU（微控制单元）物联网终端模组、WAPI网络摄像机、方舱医院WAPI无线网络安全解决方案”等新机具新方案，同时也推出了覆盖“产品选型、设计、施工、验收、监督检查”全过程的WAPI安全协议检测系统、携行式WAPI网络验收测试工具、便携式WAPI网络运维检查工具，充分满足用户建设WAPI网络赋能数字化转型的产品选型需求。

《WAPI标准产业应用及环境监测报告》是联盟帮助政府、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。主要包括：无线局域网及WAPI政策及配套监管、国家标准符合依据、全产业链厂商及其产品统计分析、市场应用示范案例、公共关键技术和解决方案、技术标准体系介绍等，以电子文档或印刷品形式面向政府、产业、公众公开。《报告》中涉及的产品数据与信息，均源自公开媒体或厂商。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6月22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产业联盟召开

2022年无线网络安全标准化委员会第二季度主任工作会议

WAPI产业联盟 米东

2022年6月16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二季度主任工作会议。副主任委员王立建、张璐璐、黄振海、陶洪波、王宏、刘科伟，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。

曹军主任首先介绍会议背景。目前WAPI标准产业共同体已有近200家成员单位，已成为国内最大的专注于无线网络安全的标准产业创新平台。截至2022年6月，联盟共发布团体标准87项，团体标准被采纳发布的国家标准45项、行业标准7项，国际标准14项、欧洲标准3项。新形势下，如何进一步凝聚力量集思广益，促进联盟标准化工作高质量发展、落实优质标准的实施和应用，需要标委会全体专家共同努力。结合上述，联盟启动了主任季度工作会议机制。

标委会副主任委员、WG1工作组组长黄振海做《标准体系建设和标准实施工作报告》，围绕规划并完善WAPI标准体系、推动标准实施、挑战与计划三方面和与会专家分享最新情况，并向与会专家报告了2022年WAPI产业联盟63项团体标准的复审情况。

联盟标准化部负责人米东从“组织发展、标准创制、标准复审、标准实施与服务”四方面，汇报了1至6月联盟标准化重点工作。截至目前，联盟标委会委员共计81人，其中主任委员1人、副主任委员7人，单位委员18人，专家委员55人，覆盖政产学研用各个环节。今年2月，联盟加强了标准化部专业化人员建设，强化了标准化部的组织协调职责；结合内外部情况和变化，对联盟标准化工作管理文件和流程文件



进行了修订和流通；进一步明确并强化了各工作组组长和项目编辑的工作职责和牵头作用；鼓励标委会主任副主任和专家认真履职，严格执行三稿三审；对已实施三年的63项团体标准完成了复审等。结合当前企业参加标准化工作热情日益高涨的实际，联盟愿意结合标准化工作的先行优势，发挥标准产业平台的公益作用，尝试将WAPI产业联盟锻造成为我国无线网络安全标准化协同创新的一个实践基地，以实际行动推动我国企业标准化创新能力的提升。在标准实施方面，WAPI相关标准正广泛服务国防、政务、能源、交通、金融等行业，成为这些行业深耕数字化转型的重要组成。近期，联盟将重点围绕WAPI标准应用过程中的新技术创新和标准化展开工作，同时也将根据市场用户和检测机构的实际需求，推动深入行业业务的安全无线局域网测评解决方案。上述工作获得了与会专家的肯定和鼓励。

会上，与会专家围绕联盟标准高质量发展进行了深度交流和探讨，形成了第三季度联盟标准化工作重点。会后将根据重点，细化工作方案，推动相关工作的落实。

WAPI产业联盟召开2022年第二次标准工作及项目组会议 (总第122次)

WAPI产业联盟 米 东

2022年6月23日，WAPI产业联盟组织召开2022年第二次标准工作及项目组会议（总第122次）。会议包括：2022年第二季度标委会主任工作会议情况通报、2022年第二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、标准国际化专题讨论、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、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、中国电信研究院、华为技术有限公司、西电捷通公司、深圳市国电科技通信有限公司、国网四川电力信息通信公司、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、山东思极科技有限公司、新华三技术有限公司、深圳市信锐网科技有限公司、深圳市智开科技有限公司、紫光展锐（上海）科技有限公司、瑞晟微电子（苏州）有限公司、北京市政务信息安全保障中心、陕西省网络与信息安全测评中心、西安芯语慧联信息科技有限公司、北京兴汉网际股份有限公司、巷子科技(北京)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、重庆邮电大学、金陵科技学院网络与通信工程学院等单位代表，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，目前WAPI标准产业共同体已有近200家成员单位，成为国内最大的专注于无线网络安全的标准产业创新平台。截至2022年6月，联盟共发布团体标准90项，团体标准被采纳发布的国家标准45项、行业标准7项，国际标准14项、欧洲标准3项。联盟标准的数量、质量和应用成效被业界广泛认可，并屡获国家主管部门肯定。我们认为，联盟标准化工作的成功很大程度上取决于现实中不同利益相关方的技术洞察和实现经验能在标准制定过程中得到充分反馈和协商。当前新形势下，作为创新型产业标准开发平台，如何在鼓励技术创新支撑产业的原则下，创造公平、公正、公开的技术贡献和评议机会，如何进一步围绕市场需求集思广益，落实更多优质标准的立项、发布和实施，是我们标准化工作的重中之重，需要标准产业共同体一起努力。

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分享了近期标准化工作新进展。本季度，在国家标准化管理委员会、中央网信办、科技部等十七部门联合印发《关于促进团体标准规范优质发展的意见》的要求下，WAPI产业联盟在“制定原创性、高质量的团体标准，填补标准空白”“建立标准制定、检验、检测、认证一体化工作机制，推动团体标准在招投标、合同履行等市场活动中实施应用，…提高社会对团体标准的认知度和认可度”，以及“提升团体标准组织的诚信和影响”等方面持续努力提升，工作呈现三个突出特点：第一，熟悉产业的机构和专家不断充实标准化队伍。3个成员单位加入，4位专家成为标委会委员，新成员的加入为团体标准的制定和应用提供了新的能力基础，有利于凝聚共识，共促产业。第二，团体标准的组织机制和运行体系得到进一步优化。建立起更“有规划，有支撑，有保障”的机制，开展了标龄3年以上的63项团标的复审工作，确认了标准的技术和应用现状，使标准体系保持提供“引导、规范、市场监管支撑”的现行有效状态，提升了团体标准组织的诚信和影响力。第三，团体标准的联通和支撑作用得到进一步体现。作为我国网络安全领域的新型产业标准开发平台，联盟将继续充当好行业管理、企业、科研机构、用户的桥梁作用。WLAN信息系统密评标准的推进，为WAPI产业在重要行业应用步伐不断加快、关键信息基础设施落地奠定了重要基础。

黄振海还向与会人员报告了第二季度团体标准和国际标准工作情况：在团体标准方面，发布了团体标准3项，组织开展编制草案稿3项，完成了63项团体标准复审。在标准国际化方面，SC6国内技术对口工作稳步推进，第二季度共对内流通国际提案文件101份，向国际上反馈投票/意见44份；我国主导/参与的2项“无线局域网接入控制”完成委员会草案（CD）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”完成国际标准草案（DIS）投票，正在进行意见处理和文本更新工作。在国际标准推进方面，电子四院、西电捷通等单位参加了ISO/IEC JTC 1/SC 27（信息安全、网络安全和隐私保护）全会和工作组会议，会上黄振海作为SC 27和SC 6双向联络官提交了联络组织报告，杜志强作为中国代表团委派的WG 2工作组中方负责人，协调成员参会及提案推进，为我国提出的多方安全计算、机密计算等提案提供支撑。据黄振海介绍，国际标准化组织/国际电工委员会第一联合技术委员会第六分技术委员会第一工作组（ISO/IEC JTC 1/SC 6）2022年全会和工作组会议将于2022年6月27日-7月1日举行，目前SC 6国内技术对口单位正按流程组织中国代表团参会。

WAPI产业联盟标准化部总监米东报告了2022年6月16日召开的无线网络安全标准化委员会2022年第二季度主任工作会议情况：会议由标委会主任委员曹军主持，副主任委员王立建、张璐璐、黄振海、陶洪波、王宏、刘科伟，及联盟秘书处标准化部、市场与产业部负责同志参加。黄振海做《标准体系建设和标准实施工作报告》，围绕“规划并完善WAPI标准体系、推动标准实施、挑战与计划”三方面和与会专家分享最新情况，并向与会专家报告了2022年WAPI产业联盟63项团体标准的复审情况。米东从“组织发展、标准创制、标准复审、标准实施与服务”四方面，汇报了1至6月联盟标准化重点工作。经与会专家讨论，形成了第三季度联盟标准化工作重点。会后将根据重点，细化工作方案，推动相关工作的落实。

WAPI产业联盟市场总监简练报告了2022年第二季度标准产业市场应用阶段性进展，重点包括：围绕市场需求和卡脖子难题，联盟发布《无线局域网系统规范 第1部分：工程设计》《无线局域网系统规范 第2部分：工程施工》《无线局域网系统规范 第3部分：

验收测试方法》3项联盟团体标准，用以规范和提升各行业WAPI部署和建设质量；组织编制了《无线局域网产品高数据吞吐量工程化实现指南》；芯语慧联、联盛德、西电捷通公司协同创新并发布了新一代旗舰版WAPI MCU（微控制单元）物联网终端模组，在功耗、性能、稳定性、硬件工艺、信号质量等方面进行了全面升级；联盟测试实验室推出终端实体证书管理（CMEE）检测服务，解决当前WAPI安全无线局域网规模建设中的数字证书高效集中管理问题，保证不同厂商产品间的证书管理能够互联互通。对上述标准产业市场成果和企业阶段性进展，多家媒体进行了报道。

在技术产业新动态分享环节，来自电力行业一线的2家联盟成员介绍了能源电力WAPI可信网络建设应用情况。深圳市国电科技通信有限公司工业物联事业部总经理王学良在《深圳市国电科技通信有限公司简介和产品介绍》报告中，重点介绍了电力行业多种类业务需求和深国电WAPI系列产品开发情况：目前，在网络侧，深国电已经开发了AP、AC、AS、网管系统等全系列WAPI产品；在终端侧，深国电的WAPI产品类型已涵盖了CPE、MCU模组、摄像头、断路器、安全帽、融合终端、传感器等，能满足多种类型、多种场景的电力业务应用需求。山东思极科技有限公司市场开发部郭平杰做《直击新型电力系统“痛点”实现分布式光伏“四可”》报告，据介绍，由于分布式光伏布局分散、大量接入后消纳困难，对电力系统的稳定性提出了挑战，需要安全可信的通信链路保障系统的集中管理控制。经综合评估安全、速度、灵活、成本等诸多因素后，分布式光伏领域选择使用

“5G+WAPI”混合组网方式。对此，山东思极迅速开发了多款高性能室外型WAPI AP产品，以及配套的AC和终端等。这些WAPI产品还可用于电动汽车充电桩、智能园区等更多场景。

会上，西电捷通公司产品经理张国强、无线网络安全国家工程研究中心贺焱对最新发布的T/WAPIA 047.1—2022《无线局域网系统规范 第一部分：工程设计》、T/WAPIA 047.2—2022《无线局域网系统规范 第二部分：工程施工》、T/WAPIA 047.3—2022《无线局域网系统规范 第三部分：验收测试方法》3项联盟团体标准进行了宣贯。根据用户单位反馈，在当前WAPI无线局域网系统建设和工程验收方面，行业普遍缺乏明确统一专业的指导规范。结合上述需求，联盟迅速组织厂商制定并发布了上述3项团体标准，为无线局域网的建设单位、施工单位、监管部门提供了必要的技术标准指导，保障其在“工程设计、工程施工、验收测试”相关环节的科学规范性，该系列团标还填补了国内外针对无线局域网系统工程建设部署方面的标准空白。

会上，与会专家对已立项标准《无线局域网信息系统密码应用基本要求》《无线网络安全 术语》《WAPI规模组网技术规范》进行了集中讨论和协商一致，形成了相关决议。对复审结果中需修订的T/WAPIA 002—2010《无线局域网接入点技术要求与测试方法》等9项标准和《极高速WLAN与WAPI团体标准体系融合研究》进行拟立项讨论。

会议期间联盟还进行了标准国际化专题讨论和标准化知识交流与培训，发布了2022年6月版《WAPI标准产业应用及环境监测报告》。

WAPI产业联盟完成 2022年度中关村产业技术联盟诚信建设工作

WAPI产业联盟 刘剑昕

日前，WAPI产业联盟积极响应国家建设社会主义市场经济和诚信社会的要求，连续第4年完成了中关村产业技术联盟诚信建设工作，从“自身建设、管理规范、创新发展、诚信自律”等方面，就联盟情况向社会主动完整详实地进行公开。

中关村产业技术联盟诚信建设工作是强化社会组织规范发展和能力提升意识、提高社会组织服务质量和作用发挥水平、推动社会组织高质量发展并引导所属行业加强自律的重要手段，它有力支撑了北京市科委、中关村管委会对产业联盟的评价和研究工作。

WAPI产业联盟于2006年3月7日经国务院批准成立，是国内首家专注于网络安全且目前最具规模的产业联盟，是国内首家自成立之日起秘书处采用专职人员、不依托任何单位独立运作的新型社会组织

和协同创新载体。目前，联盟是国家首批A类产业技术创新战略联盟、国家首批团体标准试点单位、北京市5A级社会组织，也是国家网络安全防御产业技术基础设施——无线网络安全技术国家工程研究中心的发起单位。

在自身建设方面，16年间，“联盟秘书处专职化、专业化”的定位，“立足产业，标准引领，技术标准研制与产品验证同步进行，产业与市场互为促进和谐发展”的工作指导思路，保障了各项工作顺利开展。联盟测试实验室等技术实体和公共服务平台，可以高效组织无线网络安全技术创新和标准化开发，提供标准符合性、互联互通等测试服务，解决了市场和产业的公共技术短板，降低了用户与厂商之间的沟通成本和费用成本。



在规范管理和诚信自律方面，早在2010年，WAPI产业联盟就开始主动探索并尝试用国际质量管理体系（GB/T19001-2008 idt ISO 9001:2008和GB/T19001-2016 idt ISO 9001:2015）开展业务管理和内部管理，规范自身业务和管理，加强自律和运行透明度，形成了“重策划、讲规矩、按流程、强落实、擅风控、持续改进”的工作作风。联盟平台的专业、规范、高效服务能力，获政府管理部门、会员单位、市场用户的广泛认可。期间，联盟积极响应国家科技部、北京市科委和中关村管委会对社会组织健康有序发展的要求，积极参与科技部产业技术创新战略联盟活跃度评价、中关村产业技术联盟诚信建设等工作，为中关村社会组织诚信长效机制的建设和中关村示范区创新创业营造和谐守信环境做出自身努力。

在联盟和产业链上下游的共同努力下，创新成

果显著：截至2022年5月，WAPI产业联盟会员数量为112家，包括三大电信运营商和ICT领域骨干企业。在标准化方面，已开展了180余项标准的制修订，为构建最基础最共性的网络安全架构体系提供有效支撑，其中发布（获发布）国际标准（ISO/IEC）14项、欧洲标准3项、国家标准41项、国家军用标准4项、行业标准7项、团体标准87项。在产业化方面，WAPI已经成为全球无线局域网芯片的标准配置，支持WAPI的芯片已达500多个型号，全球累计出货量已超过190亿颗；支持WAPI的移动终端和网络侧设备已超过18000款。在服务市场应用方面，除电信运营商公共无线局域网之外，WAPI已广泛服务海关、能源、政务、公安、交通等行业，在这些应用实践中形成了WAPI物联网、WAPI移动互联网、WAPI社会化网络等综合解决方案。

WAPI产业联盟组织会员单位参加 2022科创中国·科技创新创业大赛

WAPI产业联盟 刘剑昕

近日，WAPI产业联盟组织多家会员单位积极参加2022科创中国·科技创新创业大赛。

科创中国·科技创新创业大赛是中国科协企业创新服务中心、北京市科学技术委员会、中关村科技园区管理委员会、北京市科学技术协会、中关村科学城管委会的指导支持的全国性科创大赛。大赛通过BP线上评选、现场路演等系列赛程安排，搭建先进技术与产品的展示平台，促进投资机构与先进技术产品的对接，挖掘富有创新活力、具备发展潜力、深具影响力与号召力的创新企业。大赛旨在以赛事活动促进创新创业企业的交流互通，鼓励优秀企业与投资机构、众

创空间、孵化器对接；鼓励与各个行业领军企业接洽实现产创融合。大赛依托多方优质资源及创投机构专业经验，为参赛项目精准匹配最合适的融资服务，推动产、学、研、融协同发展，切实帮助科技创新企业做大做强。

多年来，WAPI产业联盟持续发挥创新联合体作用，搭建政府与企业间的桥梁，日常通过国家部委、地方政府机构官方网站、微信等公开信息渠道，整理国家、地方相关政策和支持项目，第一时间通报全体会员，并根据会员需求提供支持和服务。此外，联盟在国家重点研发计划等项目中也具有推荐权。



WAPI产业联盟参加 2022年国际标准化第一期视频培训会

WAPI产业联盟 刘剑昕



为落实北京市国际交往建议要求，进一步推动北京市国际标准化人才队伍建设，2022年6月16日，北京市市场监督管理局举办2022年国际标准化第一期视频培训会，WAPI产业联盟组织标准化团队参加培训会。

本次培训会围绕国际标准化发展形势，针对如何有效开展国际标准化工作、如何开展技术性贸易措施工作以及相关案例分析等内容展开，并对国际标准提案技巧与案例分享、技术性贸易措施应对结合企业案例展开介绍。会后，WAPI产业联盟组织联盟标委会工作人员进行了深入学习和研讨。

自2006年起，WAPI产业联盟组织成员积极参与标准国际化工作。目前，联盟已与国际标准化组织（ISO）和国际电工委员会（IEC）第一联合技术委员会（JTC1）第六分技术委员会（SC6）、（ISO）和国际电工委员会（IEC）第一联合技术委员会（JTC1）第二十七分技术委员会（SC27）、（ISO）和国际电工委员会（IEC）第一联合技术委员会（JTC1）第三十一分技术委员会（SC31）建立了广泛

的联络关系；在国标委的指导下组织成员参与无线网络安全标准的国际化创新工作。截至2022年6月，联盟已牵头组织成员开展了160余项标准的制修订，其中已发布（获发布）的国际标准（ISO/IEC）14项，国外标准3项；联盟标委会十余位技术专家和联盟秘书处工作人员相继成为相关工作组注册专家，部分专家还担任了工作组、咨询组、特设组的召集人和联络员；联盟多次承办了ISO/IEC JTC1 SC6年会并获好评；ISO/IEC JTC 1/SC 6主席在访问联盟秘书处时，对联盟取得的成绩给予了高度赞扬。



新华三“智原生”系列产品通过WAPI产业联盟测试

WAPI产业联盟 王立华



2022年6月，紫光股份旗下新华三集团（以下简称新华三）的“智原生”无线接入点系列产品通过了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。

上述WAPI无线接入点型号为：WA6620、WA6620X、WA5630X、WA6630X，均采用瘦架构组网方式，产品支持集中转发与本地转发模式，支持2.4/5GHz双频接入。

上述通过WAPI协议互通性测试的四款产品，具有覆盖广、速率高、安全稳定、实用美观等特点，能

够满足现下电力行业“大带宽、大连接、移动性强”的WAPI网络建设要求，同时也适用于教育、金融、能源、交通、制造等行业，助力用户开展WAPI数字化建设/改造工程。

据新华三介绍，“智原生”无线接入点系列产品的技术优势是：通过云网边协同新华三创新的iRadio、iStation、iEdge和iHeal技术，有效实现智能射频管理、智能终端接入、智能业务保障和智能网络治愈，让无线接入用户体验获得质的提升，业务服务获得更快速及时的保障，让网络管理者无忧运维。

北京至周科技有限公司加入WAPI产业联盟

WAPI产业联盟 周 园



2022年6月2日，经联盟理事会批准，北京至周科技有限公司正式加入WAPI产业联盟，联盟会员单位增至112家。

北京至周科技有限公司（以下简称至周科技）成立于2014年，是服务物联网领域的高新技术企业，将IT（信息技术）、CT（通信技术）和OT（操作技术）融合为新数字化技术，在对物联网、数据网络和视频监控网络实现一体化管理的基础上，针对行业应用，提供智能网络数字化服务解决方案。

据至周科技介绍，其自主研发的无线控制器、无线接入点均支持WAPI，适合批量部署和管理。至周科技通过打造轻量化、自动化、智能化的业务建模平台，为企业提供工具化生产服务和网络平台，高效低成本地实现企业核心技术产品化。目前至周科技已与浪潮、清华同衡、东土科技等公司达成战略合作，服务医疗、教育、政府、金融、交通等多个行业领域。

产品全家福



南网深圳数研院

"基于WAPI技术的大功率远距离无线数据传输装置"

获国家实用新型专利权

龙图腾网

日前，南方电网深圳数字电网研究院有限公司的《基于WAPI技术的大功率远距离无线数据传输装置》专利，获国家实用新型专利权，专利号为：202122182766.4，由童玲、何涵、陈欢、沈通桥、赖丽燕设计研发完成。此实用新型的无线数据传输装置具有较高的安全性能以及较大的射频覆盖范围。

据说明书显示：本实用新型公开了一种基于WAPI技术的大功率远距离无线数据传输装置，包括：WAPI芯片以及连接WAPI芯片的存储单元；射频前端，其具有至少两条用于接收和发射A频段信号的第一射频收发链路，各条第一射频收发链路的拓扑结构相互一致，每条第一射频收发链路中均设有用于选通接收状态或发射状态的第一选通开关，各个第一选通开关之间相同的控制端共接后连接WAPI芯片；以太网物理层，其具有用于扩展路由的LAN口，以及可支持POE的WAN口，LAN口和WAN口分别与WAPI芯片连接；电源管理单元，用于给WAPI芯片、存储单元、射频前端、以太网物理层提供电源。

博洛米与WAPI可信无线局域网通信系统

博洛米通信



局域网技术（以下简称WLAN）在全球范围内发展至今20多年，WLAN技术体系由数据（编码、调制、交换、分段/重组、帧格式等）、管理（媒体访问控制、会聚无线控制、初始化配置、网络同步、功率管理、服务质量、快速切换、漫游、频段分配、MAC地址分配等）和安全（鉴别、密钥交换、保密、加密模式、证书管理等）三个技术层面构成。全球WLAN技术体系，在数据和管理层面形成了相对统一的技术架构，但在安全层面有两条路线：一个是美国主导、Wi-Fi产业联盟主推的IEEE 802.11i（WEP/WPA/WPA2/WPA3）技术，另一个是中国发展主导的WAPI技术。

Wi-Fi虽然几乎家家户户都在使用，但Wi-Fi在网络架构和安全协议设计方面均存在设计缺陷和漏洞，其芯片和软件协议基本由美欧日等国公司控制，加之商业公司对短期商业利益的考虑远超对信息安全的关心，导致Wi-Fi网络安全问题和隐患层出不穷，一次又一次地被曝出安全漏洞。正因如此，我国政府部门、国防、大型国有企业等都明令禁止在工作和业务中使用Wi-Fi网络。

WAPI（无线局域网鉴别与保密基础结构）是中国自主研发提出的WLAN安全协议技术，2003年被采纳并发布为国家标准GB 15629.11，实现了终端和网络的对等访问，在双向身份鉴别、防范非法接入、防钓鱼等方面具有明显优势。迄今，WAPI所基于的三元对等安全架构，较之Wi-Fi所基于的二转三元过渡架构仍具有显著技术优势，解除了接入点缺乏独立鉴别身份、依赖于与网络服务器额外建立安全传递通道、无法直接实现与终端的直接双向鉴别的安全隐患。依据标准化法，目前国内上市的手持终端和政府采购的无线局域网产品都必须支持WAPI。

在典型的WAPI系统中，WAPI终端STA通过WAPI无线接入点（AP）接入互联网。首先，STA与AP进行网络发现协商并开启WAPI功能，STA和AP启动身份鉴别过程，利用AS完成双向身份鉴别。当身份鉴别通过后，STA和AP进行密钥管理，协商用于保护通信数据的密钥，并利用协商出的密钥加密通信数据。

从全球无线局域网安全技术发展和应用来看，加强源头安全技术标准治理，通过采用安全可控技术标准和产品保障重要行业生产、办公网络安全是切实可行的路径。当前，越来越多的行业用户基于法律法规规章合规性及自身需求，规划建设WAPI无线局域网络，以保障其业务和数据资产在安全可控的无线网络中运行。自2016年国家相继出台了《网络安全法》、《密码法》、等保2.0等法律法规之后，各重要行业对于安全可控的无线网络需求愈发强烈。

WAPI因产业成熟度高、不增加采购成本、建设配套条件丰富、对行业的信息通道安全和数据资产安全能形成有效的保护，受到行业用户的青睐，已在全国海关的信息化系统、重要仓储物流管理信息系统、公安重要部位和重大活动智能监控管理系统、南方电网变电站综合数据网接入系统，以及北京大兴国际机场、重庆机场海关口岸、新疆地铁、城市地下综合管廊等国家地方重点项目中广泛应用。

目前，博洛米的WAPI服务包括：解决方案（完整的“交钥匙”工程解决方案）；技术合作（方案设计、项目咨询、项目合作、技术改造等）；产品设备（终端、嵌入式模块、无线接入点AP、接入控制器AC、鉴别服务器AS等）。

MTK发布全新智能物联网AIoT平台Genio 1200

通信世界

2022年5月11日，MediaTek（以下简称MTK）发布Genio智能物联网AIoT平台新品Genio 1200，助力设备制造商打造高端智能物联网产品。

Genio提供从概念、设计到制造全流程硬件、软件 and 开发资源，客户可根据不同的产品需求匹配芯片，并使用MediaTek开发者资源和开放平台SDK进行定制设计。同时，客户可以访问MediaTek合作伙伴的系统硬件和软件，并使用其网络和销售渠道。通过集成式、易于使用的Genio平台，可降低产品开发成本、缩短产品上市周期，同时为操作系统更新和安全补丁提供长期支持，延长产品生命周期。

MTK高级副总裁兼计算、连接和元宇宙事业群总经理游人杰表示：MediaTek为市场上广受欢迎的智能物联网AIoT设备提供全面支持，MediaTek Genio平台是具备灵活性、可扩展性的解决方案，并提供开发支持，满足日益变化的市场需求。我们期待设备制造商借助Genio 1200强大的AI能力、4K显示支持和先进图像功能，为用户升级体验。

Genio提供强劲的多核性能和出色的能效，可优化计算密集型AI应用程序的用户体验。CPU、GPU和AI处理单元APU协同工作，增强边缘计算的智能自主能力，支持高清显示器、摄像头等多媒体界面。此外，支持新的WLAN和蓝牙协议，实现无缝网络连接。

MediaTek Genio系列包括旗舰、中端和入门级SoC和模块，可满足不同市场和应用需求：

Genio 1200适用于高端智能物联网AIoT应用，拥有4.8 TOPs的强劲AI性能，支持新的多媒体标准和4K显示，兼具出色能效。

Genio 500适用于零售和商用物联网应用，提供高性能边缘计算和先进的多媒体功能。

Genio 350为便携式、智能家居应用提供解决方案。

Genio 130适用于thin-OS操作系统和支持云端的语音助手设备，满足音频和麦克风导向平台的需求。

国家无线电监测中心检测中心荣获 “北京2022年冬奥会、冬残奥会北京市先进集体” 荣誉称号

中国无线电检测

4月19日，北京冬奥会冬残奥会北京市·北京冬奥组委总结表彰大会召开，会议全面总结冬奥成功经验，隆重表彰先进集体和先进个人。国家无线电监测中心检测中心（以下简称检测中心）荣获“北京2022年冬奥会、冬残奥会北京市先进集体”荣誉称号。

北京冬奥会、冬残奥会完美落幕，冬奥会和冬残奥会无线电安全保障工作实现“零干扰、零失误、零瑕疵”。作为冬奥会无线电安全保障检测组主力单位，检测中心坚决落实习近平总书记关于冬奥办赛的重要指示批示精神和工信部党组对冬奥会无线电保障工作的部署要求，提高政治站位，胸怀国之大者，把保障北京冬奥会/冬残奥会无线电安全作为2021年工作的头等大事，坚决扛起国家级技术机构的政治责任和时代使命，全力以赴把好冬奥会无线电安全第一道关口，助力呈现了一届简约、安全、精彩的冬奥盛会。

在冬奥会筹办举办过程中，检测中心坚持以“一刻也不能停，一步也不能错，一天也误不起”的工作状态，周密部署、精益求精，扎实推进各项保障工作。统筹配置保障力量150余人，仪表50余台套、检测车6辆，在北京、延庆、河北赛区共设置8个固定检测点和6个移动检测组，实现用户检测需求全覆盖。提前编制中英文服务指南加强宣传引导，抓住宝贵时间窗口赴海关物流中心、国家体育场等场馆为境外奥运转播商、开闭幕式演出团队等重要用户开展上门检测服务。冬奥期间，检测中心共为近200家国内外重要用户提供设备检测核验服务并发放无线电发射设备专用标签14.5万枚。在冬奥会、冬残奥会开闭幕式及演练的12次活动中，组织475人次赴安检口对进入核心区的无线电设备进行查验，全力保障开闭幕式活动无线电安全。此外，检测中心积极发挥自主研发能力优势，为冬奥会定制开发检测信息系统、现场快速检测仪表等专用装备，开展同频段多业务技术仿真和压力测试，为“科技冬奥”保驾护航。在冬奥会无线电安全保障指挥中心、TOC及张家口分指挥中心部署重大活动无线电安全保障平台，为无线电安全保障工作提供强有力的技术支撑。

联盟成员发挥创新优势 筑科技抗疫坚强防线

当前疫情防控工作正处于“逆水行舟、不进则退”的关键时期和吃劲阶段，WAPI产业联盟成员单位发挥网络强国主力军作用，全力做好通信、服务、防疫“三个保障”，抓实抓细疫情防控各项工作，为坚决筑牢疫情防控屏障、实现疫情防控和经济社会发展的双胜利贡献了数智力量。

中国移动

每当疫情来袭，中国移动的通信保障队伍都第一时间冲锋在前，筑起疫情防控的信息化屏障。

3月下旬的吉林，疫情防控形势依然严峻。新冠肺炎定点收治医院长春市传染病医院通信需求猛增，亟需网络升级。中国移动迅速派出多业务骨干，勘测、引电、布缆、建站……仅用5个小时就开通了5G网络，保障了医疗救治信息的高效稳定传递。4月初的上海，方舱建设刻不容缓。在国家会展中心（上海）方舱医院，中国移动承担了约50%的总体通信保障工程量，保障团队竭尽全力抢进度，最快最早完成工程项目交付。在浦东临港，面对正常情况下需要1个月标准工期的网络建设任务，中国移动在58小时内完成方舱医院所有无线网络的建设开通任务。5月上旬的北京，疫情仍处于高位平台期。针对朝阳区严峻的防控形势，中国移动第一时间与45个区政府部门及43个街乡政府取得联系，连夜将500余台防疫终端紧急送到街道工作人员手中，并提供电子门磁500个、防疫摄像头100余个，同时一支由青年员工组成的志愿者团队迅速下沉重点区域抗疫一线展开流动人口统计工作。在天津的疫情防控中，中国移动利用大数据技术每日对全市约3000万次扫码关键信令进行汇聚分析，精准识别“津心办”APP、微信小程序、支付宝小程序以及核酸检测登记二维码等对网络的需求，通过智慧网络运维体系进行实时动态监测、评估以及快速专项优化，在扫码业务量增加一倍的情况下，确认时延大幅缩短，平稳保持在55毫秒以下。基层街道社区的排查监测是防控的重要环节，但传统人工走访式排查不仅耗时耗力，还面临交叉感染的风险。中国移动云客服智能外呼可同时拨打100个电话，实现每天（8小时）15万通电话的智能呼叫和数据采集，并可一键生成外呼数据分析报告、全量存储、调用通话录音等，在降低接触风险的同时筑牢社区疫情防控线。30分钟内实现1000人次的触达和信息收集工作，相当于20个社区工作人员一整天工作量的“数字社工”也在浙江抗疫中上岗。“数字社工”机器人可以在极短时间内为社区提供及时、准确的人员活动轨迹信息并汇总成流调信息表，解决了基层疫情流调工作面临的数据量大、工作时间长、跨系统信息不同步等难题，显著提升了社区基层防疫工作效率。核酸检测样本量大、时间紧，移动5G技术的应用大幅提升了检测的能力和速度。在西安邮电大学长安校区2.5万名师生集中核酸检测过程中，中国移动部署的4台5G“御兔号”移动核酸检测车开进了校园，该车采用“有线100M宽带+无线5G CPE”的解决方案，保障了更快更准地录入样本信息。

中国电信北京公司

针对疫情形势，北京市朝阳区严格管控风险点位，连日来每天依据最新流调排查和核酸检测结果，划定封控区、管控区，同时对部分区域采取临时管控措施。中国电信北京公司对朝阳区健康云及相关网络进行重点保障，实时监控、弹性扩容，确保朝阳区健康云平台畅通使用。在昌平区，中国电信北京公司已累计为昌平区多个街道提供、补充疫情防控终端并开通号卡85个。据工作人员介绍，通过安装标本采集APP，检测人员可直接扫描居民身份证信息，实现核酸检测快速、精准且高效。在这场没有硝烟的战“疫”中，通信“黑科技”成为战场上默默无闻却又不容小觑的坚强力量，在信息传递、智能识别、社区管理等各个领域都彰显出优势。智

能门磁作为防疫“黑科技”，在疫情防控中为居家医学观察、健康监测人员筑起智能“安全网”。4月26日晚10点，中国电信北京房山区分公司接到当地政府来电，须紧急开通2000个门磁。当晚，房山区分公司党员先锋队连夜赶回办公楼，齐心协力通宵完成首批2000个智能门磁的安装激活，第二天一早准时交付。在随后的3天时间里，房山区分公司争分夺秒、连续奋战，累计为多个街道开通1.2万个门磁，有力支撑了房山区疫情防控工作。2022年4月25日凌晨3点，中国电信北京昌平区分公司接到紧急搭建热线电话坐席的需求。昌平区分公司快速响应，仅用6小时帮助街道搭建完成10个热线坐席，保障街道及时响应居民服务需求和问题反馈。截至26日，该批坐席累计接听处理居民相关诉求和反馈1000余人次。“提高脆弱人群疫苗接种率是走出疫情关键的科学手段”，中国电信北京公司协助西城区政府，向在西城区全域范围内单日驻留8小时以上人群定向发送疫苗接种宣传短信，累计发送疫苗接种宣传短信46万余条，实现疫苗接种宣传精准触达。

国网北京电力公司

国网北京电力及时建立了“统一指挥、运转高效、反应灵敏、资源共享、保障有力”指挥体系，统筹开展疫情防控供电保障整体工作。该公司各专业严格落实疫情防控要求，在防控期间按照“四个一”（一在岗、一接班、一备用、一应急）原则，优化部署资源力量、落实人员防控措施。期间，公司动态更新防疫保障客户范围，及时跟进疫情防控供电保障服务工作，坚决贯彻落实北京市和国家电网公司相关部署，全力做好疫情防控工作，确保首都电网安全稳定运行，保障各级党政机关、防疫重点客户和广大居民可靠供电。目前，北京电网整体运行平稳，电力供应可靠。

在运行管理上，国网北京电力安排调控人员在“双场所值班、不见面交接”的基础上，采取“半封闭”管理措施，确保值班体系正常运转；将市公司层面反外力监控业务、电缆监控业务转为集中封闭办公业务；在北京电力工程公司、国网北京电力华商远大公司组建50人变电抢修队伍和150人配电抢修队伍，负责市公司层面应急支援，严格落实人员集中住宿、“两点一线”工作要求。各单位运维人员、抢修人员、发电车及带电作业人员等按照分散布置原则，携装备在不同地点驻守并开展工作，确保突发状况下能够快速反应、及时处置。

信锐技术

今年以来，全国多省市积极准备方舱医院。信锐技术在2020年武汉方舱医院建设交付的基础上，形成了快速响应、快速建设、快速交付为目标的方舱方案，快速响应各地建设要求。3月19日，山东烟台，2000个床位，次日到货，4天时间全网交付开通；3月22日，辽宁沈阳，一期1000个床位，次日到货，4天时间全网交付开通；二期1000个床位，继续支持；安徽合肥、安徽马鞍山、山东威海、浙江绍兴等多个方舱医院也仍然在持续交付中。目前，信锐已开通方舱医院绿色通道，使用成熟可靠的方舱方案，由精兵强将组成的专业交付以及保障团队，全流程保障快速交付，随时响应各地的号召，站在全国抗疫的第一线。

在协助制造企业数字化转型方面。北京科兴中维生物技术有限公司携手信锐完成厂区网络改造，实现产能提升和产线升级。针对科兴中维网络改造需求，信锐为其设计了如下多分支组网解决方案：构建厂区统一认证体系，厂区员工认证可实现网随人动，业务随行，与员工物理位置解耦，打造员工安全认证体验。开放办公部署吸顶AP，实现无线信号覆盖，保障流畅的无线上网体验；生产场景部署高密AP，确保能接入足够多的终端，满足无线快速漫游。

数字认证：“雪亮工程” 密码也是应用C位

数字认证

作为被纳入国家“十三五”规划和国家安全保障能力建设规划的重要工程，“雪亮工程”自身的系统安全运营也需要得到足够的保障。随着GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》于2021年10月1日起正式实施，在不少市县区的前期设计规划阶段，都开始探索利用商用密码技术来保障“雪亮工程”的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等多个层面。

北京数字认证股份有限公司（以下简称数字认证）凭借在密码领域多年的技术创新研究与大型项目实践，不久前打造了全国首个“雪亮+密码”建设项目，通过详尽周密的规划、严格规范的审核，成功完成“雪亮工程”密码应用方案的设计编写及评审工作，帮助用户顺利通过项目立项并进行密码应用体系建设，为其维护国家和社会稳定、预防打击违法犯罪、服务经济社会发展、辅助科学决策、开展智慧治理提供了有力支撑。

数字认证融合35114标准和39786标准要求，为“雪亮工程”建设了三大体系：

统一数字证书应用体系建设 解决各类设备及用户身份真实性问题。由于“雪亮工程”涉及大量前端监控设备、应用终端、安全设备和用户，因此数字认证构建了统一的数字证书应用体系，用以标识各类用户、设备的网络身份，并保证雪亮工程项目网络空间中的用户、设备身份真实性，有效防止身份被冒用，从源头避免安全威胁。

多级网络安全通信体系建设 解决纵横双向多级网络通信安全问题。“雪亮工程”网络结构非常复杂，横向看会交叉互联网、公安专网及综治专网，纵向看则连接地市、区县网络。数字认证基于35114及39786的标准体系，为“雪亮工程”配套专用密码设备，实现控制信令认证，防止摄像头被控制、替换，同时基于IPSec及SSL双重协议支持构建安全通信通道，保证通信过程中数据的机密性、完整性。

多类数据安全保护体系建设 解决各类数据机密性及完整性保护问题。“雪亮工程”汇聚海量重要隐私和业务数据，为此数字认证构建了全方位的数据安全管理体系，基于加解密及电子签名技术实现各类数据在应用及存储过程中的机密性及完整性保护。

地缘政治使欧洲风电行业成网络攻击主要目标

安全内参

4月中旬，风力涡轮机维护公司Deutsche Windtechnik AG遭遇勒索软件攻击，德国约2000台风力涡轮机的远程控制系统瘫痪了一天左右。这是自俄乌冲突全面爆发以来，欧洲第三家风能公司遭到网络攻击。有专家认为，欧美制裁俄罗斯能源入口使得风电行业受益，站队俄罗斯的黑客组织试图在这一行业制造混乱。

自俄乌冲突全面爆发以来，已有三家欧洲风能公司遭遇网络攻击，这引发了人们的警觉。欧美制裁俄罗斯能源入口使得风电行业受益，站队俄罗斯的黑客组织试图在这一行业制造混乱。安全专家称，这类针对工业设备的严重网络攻击并不常见，需要提前搜集大量知识以做好筹备。

近期陆续遭遇网络攻击的3家风能公司均位于德国。4月中旬，专门从事风力涡轮机维护的Deutsche Windtechnik AG公司遭遇黑客攻击。该公司表示，攻击发生之后，德国约2000台风力涡轮机的远程控制系统瘫痪了一天左右。涡轮机制造商Nordex SE表示，他们在3月31日发现一起安全事件，导致IT系统被迫关闭。曾宣布支持俄罗斯的Conti勒索软件团伙本月放话称，对此次攻击负责。另一家涡轮机制造商Enercon GmbH提到，今年2月，他们在一起针对某家卫星通信企业的攻击中沦为“附带受害者”，而且此次攻击“俄罗斯对乌发起军事行动的时间完全相同”。这次攻击破坏了Enercon公司共5800台风力涡轮机的远程控制系统，好在设备仍能在自动模式下保持运行。（详情见：美国“卫星网中断”事件复盘：管理后台遭入侵，数万Modem被下发破坏指令）

有分析指出，风电行业将成为网络攻击主要目标。埃森哲公司的Guinn指出，随着欧洲国家逐渐摆脱对俄罗斯传统化石燃料的依赖，接下来的替代能源将主要来自德国和北海区域的风电场。而亲俄派黑客肯定会把这些替代能源企业当成攻击目标，“这将是一场漫长的对抗——骚扰、蚕食，就如同棋盘上的厮杀。”

挪威风险管理公司DNV GL网络安全常务董事Trond Solbert表示，只要成功感染风力涡轮机的工业控制设备，黑客就能操纵制动器以阻止正常发电。这可能会扰乱客户服务体验，影响运营收入。Solbert还说，对当地互联网连接服务的攻击，往往也能干扰到风电农场的远程监控系统。

方舱医院WAPI无线网络安全解决方案

本文由北京数字认证股份有限公司、深圳市信锐网科技有限公司联合供稿

WAPI产业联盟编辑整理

一、方案背景

方舱医院是指以医疗方舱为载体，医疗与医技保障功能综合集成的可快速部署的移动医疗平台，具备机动性好、展开部署快、环境适应性强等优势，能够快速响应突发的应急医学救援任务。新冠疫情期间，方舱医院主要用于针对无症状感染者和轻症患者实行集中治疗与监测管理，在疫情处置中有效缓解了当地医疗资源紧张的压力并保障了正常的医疗服务需求。

为了保障方舱医院各类IT设施、医疗设备、检测仪器的安全稳定运行，同时保障医生、护士和患者就诊治疗业务信息安全性和保密性，方舱医院需要构建安全可信的网络环境，进而保障方舱医院LIS系统、PACS系统、HIS系统、重症系统、护理系统等核心诊疗系统的安全运行。

WAPI技术可以提供安全、便捷的无线接入，十分适合方舱医院应用场景和业务需求。目前，北京数字认证股份有限公司和深圳市信锐网科技有限公司针对方舱医院“无线安全接入”和“电子病历签名”两个需求点，提出了“WAPI无线安全接入方案”和“可信电子签名应用方案”，以期方舱医院网络建设提供安全、高效、合规的解决方案。其中：

1、无线安全接入：为了便于各类诊疗设备和仪器、医生就诊终端、护士诊疗PAD、智能监控摄像头安全高效的接入网络，需要构建安全、便捷、灵活、可靠的无线网络接入机制，支撑医院监控、患者诊疗、医生办公等各种应用场景的开展。



2、电子病历签名：采用电子病历替代纸质病案，避免纸质病案传输带来的疾病传播风险，保障人民生命健康安全。电子病历需采用合法合规的电子签名技术，确保电子病历的签署行为可信以及病历数据的可信归档。

二、解决方案

（一）WAPI无线安全接入方案

方舱医院网络接入解决方案基于WAPI技术实现各医疗服务单元的网络覆盖和多业务接入，相较于Wi-Fi，WAPI技术标准采用三元对等安全架构进行双向鉴别，具备更高的安全性和可控性，更适合方舱医院网络建设应用场景。该方案提供统一的凭证管理与身份认证服务，其中：凭证管理能够实现终端身份凭证（数字证书）的签发和管理，方舱医院覆盖的无线医疗终端均需要预先获取WAPI证书作为入网身份凭证；身份认证支持利用鉴别服务器实现无线医疗终端与无线控制器、无线接入点的双向认证，并进行业务端的身份认证与授权。

根据方舱医院污染区、半污染区、洁净区的划分，在WAPI网络规划方面也相应的分为三个区域，分别部署网络接入设备和无线AP，各类移动终端和智能设备需支持WAPI网络协议并下载WAPI认证证书，进行实现终端基于WAPI的网络安全接入认证。

鉴别服务器（AS）部署在核心网络区，实现对整个方舱医院的WAPI证书管理及身份认证；无线控制器（AC）也部署在核心网络区，实现对所有AP的集中管理，并与AS的对接实现认证策略的统一下发。

该方案解决了方舱医院对无线网络“搭建速度快、扩容简单、移动终端灵活接入、运维难度低”的需求，具有高安全、高带宽、高并发、易运维、能感知等特点。

- 高带宽：支持WAPI与802.11ac的双频无线AP，单AP速率可达1.6Gbps，带宽充裕，可满足隔离区多用户观看视频和医生视频会议、隔离病房远程探视的需求。

- 高并发：单AP并发用户数量大（理论可达1024用户），可满足患者手机等大量的终端接入，优化高密场景的上网体验。

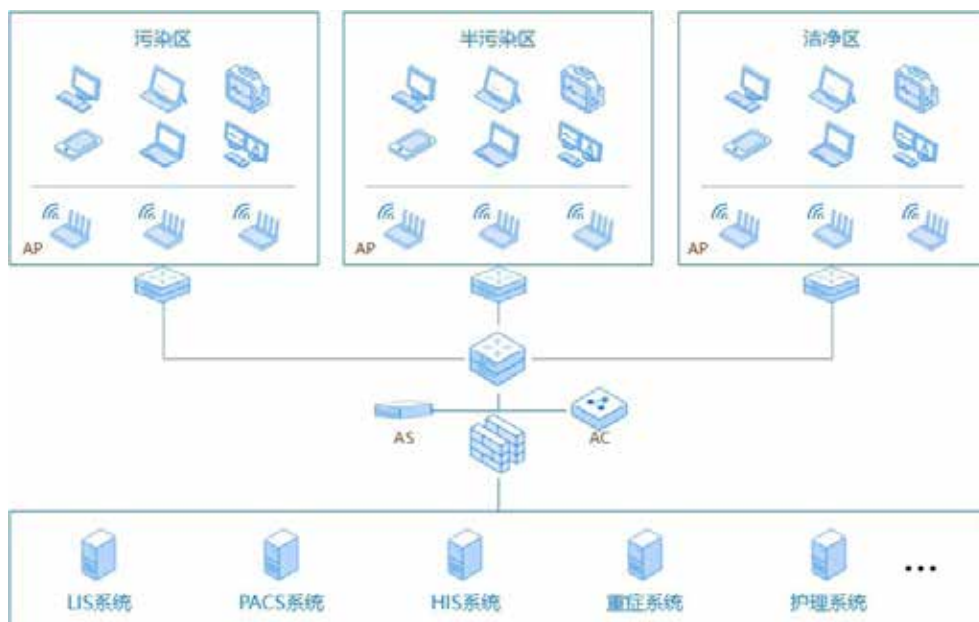
- 易运维：设备集中管理，上线快、扩容简单、运维难度低，零配置可急速完成网络部署，全程远程化运维，快速完成故障恢复。

- 能感知：系统支持智能业务感知和智能环境感知，可实时监测终端到业务系统间的链路状态，根据无线环境的变化实现无线网络整体优化。

（二）可信电子签名应用方案

根据方舱医院无纸化建设需求和污染区工作特点，选用基于USB Key的电子签名方案。开展诊疗工作前，医护人员需要预先通过鉴别服务器（AS）对各类诊疗终端进行网络接入认证，确保网络接入的安全性。开展诊疗工作时，医护人员基于USB Key完成电子病案签署，实现诊疗全流程无纸化，有效阻断潜在的疫情传播风险。

无线医疗终端接入认证的业务流程如下图所示：



三、方案优势

（一）提升方舱医院无线网络安全性

基于WAPI安全无线接入技术，为各地方舱医院相关医疗业务提供安全、灵活、泛在的网络接入服务。WAPI采用数字证书的身份鉴别机制，在协议中通信方使用自己的私钥生成签名，身份无法伪造，具备PFS（完善前向保密）、non-KCI（非密钥泄露伪装）、non-UKS(未知密钥共享)等性质，提高了网络接入的安全性。

（二）基于无纸化降低病毒传播风险

针对方舱医院清洁区、半污染区、污染区的特殊情况，在不同环境下为医护人员提供了灵活便捷的电子签名应用方案，有效防止因诊疗导致的病毒扩展风险。

（三）符合网络安全政策和标准要求

符合《网络安全法》《密码法》《电子签名法》等法律法规，采用公钥密码技术，使用国密对称密码体制的SM4算法，核心密码模块实现安全自主可控。

WAPI 产业联盟成员单位名录

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

【注：截至2022年6月，联盟正式成员已达112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>