WAPI 产业发展白皮书

（2021 年）

中关村无线网络安全产业联盟

目录

文件编制说明

习近平总书记在十九大报告中对网络安全及信息化建设工作提出了新的要求：加强应用基础研究，拓展实施国家重大科技项目，突出关键共性技术、前沿引领技术、现代工程技术、颠覆性技术创新，为建设科技强国、质量强国、航天强国、网络强国、交通强国、数字中国、智慧社会提供有力支撑。如何构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系，走出一条中国特色国家安全道路，成为社会和各行各业的共同关注，全国上下“如何在本行业践行总体国家安全观”的工作正在部署和落实。

为进一步贯彻和落实网络强国战略，突破我国网络安全核心技术制约，推动自主可控安全技术在网络和信息化建设中的应用，我们对无线局域网及无线局域网安全技术 WAPI 的发展情况进行了认真研究，深入分析了无线局域网安全面临的突出问题，系统梳理了 WAPI 技术标准与产业化取得的重要进展，提出了加强无线局域网安全管理和产业发展的建议，形成《2021 年 WAPI 产业发展白皮书》。

数据来源及版权声明

本文件中涉及的产品数据与信息，均源自公开媒体或厂商，相关统计数据截至 2021 年 12 月 31 日，鉴于产业特性和产品迭代，存在一定动态变化的可能。

一、无线局域网基本情况

（一）无线局域网基本概念。

无线局域网（英文简称 WLAN）是无线高速数据通信两大主流技术之一（另一个是 3G/4G/5G），具有带宽高、成本低、部署方便等特点，可在局部区域（约 100 米）内为使用者提供高达 9.6Gbps 的高速率数据通信服务。历经二十余年的发展，WLAN 已经成为全球宽带信息基础设施的重要组成部分，是各国网络用户主要的宽带接入方式之一。当前最常见的 WLAN 应用场景主要包括公共接入、行业网络和个人接入等三类。

（二）全球 WLAN 安全技术路线。

目前，全球 WLAN 已形成相对统一的技术架构（包括编码调制、数据交换、访问控制、频段分配等），但在安全协议部分有两条路线：一个是美国主导的 IEEE/Wi-Fi 标准，包括 WEP、WPA、WPA2、WPA3，另一个是中国主导的 WAPI 标准（WLAN Authentication and Privacy Infrastructure，无线局域网鉴别与保密基础结构），其属性是强制性国家标准。基于上述技术路线形成的 WLAN 网络，业界分别称为 Wi-Fi 网络和 WAPI 网络。由于 Wi-Fi 网络架构和协议设计方面均存在设计缺陷和漏洞，所有按照该标准实现的产品都难以幸免。但由于商业公司对短期商业利益的考虑远超对无线安全的关心，导致安全问

题层出不穷：从最初的 WEP 到后来的 WPA，再到 WPA2、WPA3，一次又一次地被曝出安全漏洞， Wi-Fi 安全问题已经无法通过“修补”和“演进”来解决。

全球范围内，中国是除美国之外，唯一有能力且提出了无线局域网安全协议技术标准的国家。自 2000 年起，中国研究团队即开始从网络基础架构安全入手，提出更为先进的三元对等（TePA）网络安全技术架构，并在此基础上开发出了自主的无线局域网安全协议——WAPI,这是中国首个在计算机网络通信领域自主创新并拥有知识产权的安全接入技术（属无线网络通信领域基础和共性关键技术范畴）。目前 WAPI 已经成为全球无线局域网芯片的标准配置，拥有完整的产业链,随着各行业、领域对安全可管可控无线局域网的应用需求,WAPI 处于更大规模的商用时期。

WAPI 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。

（三）全球和我国 WLAN 发展基本情况及趋势。

全球 WLAN 市场从 2014 年开始增长放缓，2015 年至 2021 年继续了这种态势，增长速度均在 7%以下，处于 2010 年以来的较低水平。2019~2021 年，全球 WLAN 市场整体开始显现缓慢复苏态势，市场规模已接近 100 亿美元。其中，消费级 WLAN 市场规模较 2018 年增长幅度不超过 2%、企业级 WLAN 市场增长约 5%。这种增长与复苏主要得益于企业用户对 WLAN 无线接入技术和产品的持续高需求以及与新的先进软件管理和自动化功能相结合的技术趋势。

其中，企业 WLAN 市场中支持 802.11ac 标准的产品占据出货量的 90%以上，消费 WLAN 市场中支持 802.11ac 标准的产品出货量突破市场总量的 70%。这标志着 802.11ac 已经完全占据市场。预计从 2021 年开始，企业细分市场将开始转向采用新的 802.11ax 标准，大型公共场所和其他密集 WLAN 网络的运营商将会是最早的采用者。

当前，我国已成为全球最大的无线局域网产品制造、应用国家，拥有超过 1000 家专业设备商，涉及技术研发、芯片设计、仪器仪表、生产制造等。据不完全统计，全国在网 WLAN 设备数量达到 3 亿台，使用 WLAN 上网用户超过 6 亿人，开展 WLAN 商用热点建设运营服务的企业有数百家，拥有超过 6000 余项 WLAN 技术专利，形成了完备成熟的 WLAN 产业集群与产业生态。

二、无线局域网安全面临的主要问题

（一）Wi-Fi 技术安全问题十分突出。

主要体现在：Wi-Fi 无法实现无线接入点与终端的双向鉴别和访问控制，终端无法判断接入点的合法性，不法分子可以伪造接入点，通过“钓鱼接入”、窃取数据等方式，实施诈骗恐吓、不良信息、造谣传谣等违法犯罪活动，对用户权益、社会稳定等带来严重威胁。特别是，随着无线局域网的应用日益广泛，Wi-Fi 作为美国主导的网络安全技术，其安全问题越来越成为威胁我国网络安全和国家安全的重大隐患。

（二）我国 WLAN 安全市场受制于人。

一方面，ICT 产业核心环节和生态仍被美国巨头所控制，英特尔、思科、微软等企业产品优先采用 Wi-Fi 标准，具有市场先发优势和话语权，造成我国 WAPI 标准的市场应用障碍重重。另一方面，美国政府从自身利益出发，长期打压 WAPI 标准发展，屡屡以政治引导、舆论影响、符号绑架，甚至以“拒签”等手段，进行干扰与阻挠，导致部分国内企业仍存在观望态度，在一定程度上对产业持续健康发展产生影响。

（三）关键领域 WLAN 存在重大安全隐患。

受 Wi-Fi 技术安全漏洞及其广泛应用的影响，我国关键领域的

WLAN 网络安全问题日益凸显。比如，2015 年 3 月，有黑客发布信息称，可通过 Wi-Fi 网络直接获取天河一号计算机集群的控制权；2015、2016 连续两年的 3.15 晚会，现场演示了通过公共 Wi-Fi 网络，窃取在线用户地址、姓名、身份证号、银行卡号等隐私信息；2015 年，广东银监局对广州市 60 多家银行的 1600 个 Wi-Fi 网络进行检测，发现存在非法通过窃取用户信息，实施金融诈骗等风险隐患。

2017 年 11 月，比利时专家在国外社交媒体 Twitter 上曝出一种宣判无线网络 Wi-Fi 最高级别安全协议（WPA2）“死亡”的漏洞——密钥重装攻击（KRACK），建立了专门的网站详述针对该漏洞的攻击过程，并发表了专题论文，文中明确指出该漏洞是由于 Wi-Fi 安全协议技术标准存在严重缺陷所导致的，所有按照该标准实现的产品都难以幸免。该漏洞会导致无线局域网用户（客户端）和基站（接入点/路由器）之间的通信加密数据被重放、被解密甚至被伪造等安全问题，进而产生勒索软件植入、网站劫持等严重后果。由于无线局域网已成为全球宽带网络关键基础设施，消息被披露后，引发全球产业界前所未有的关注。

三、我国安全无线局域网技术 WAPI 发展情况

我国根据国家标准化法和国家商用密码管理条例，于 2003 年以

强制性国家标准形式，发布了拥有自主知识产权的 WAPI 技术标准，并于 2010 年成为 ISO 国际标准。与 Wi-Fi 安全技术相比，WAPI 能够实现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，弥补了 WLAN 技术标准中的严重安全缺陷，填补了我国在网络安全基础技术标准方面的空白。WAPI 突破了发达国家及其跨国公司的网络安全技术垄断，是我国网络科技创新在世界范围内具有重大意义和影响的标志性事件，为我国 WLAN 技术和产业发展赢得了宝贵的主动权。

WAPI 标准发布后，引起美国政府和以英特尔、思科、微软等为代表的美国 ICT 产业跨国巨头的高度关注，认为 WAPI 是“中国作为产业下游代工附属”向其既有霸权秩序发起的首次挑战，**以“我国不公开加密算法从而无法验证技术可行性、不兼容国际标准、不按规定向 WTO 通报”**等为由，通过外交、媒体等多种方式向我国政府施压，混淆事实，反对我国强制实施 WAPI 标准。时逢中国入世不久，我国基于多方面考虑，于 2004 年 4 月做出策略性调整并公告“WAPI 标准延期强制实施”。

但是，我国相关方面没有放弃实施 WAPI 的努力。2005 年，遵照国务院领导批示精神，由国家发展改革委牵头，建立了科技部、工业和信息化部（原信息产业部）、财政部、商务部、国标委、认监委、商密办等八部委参加的部际联席会议机制，统筹推进 WAPI 发展工作，推动开展了公开 WAPI 使用密码算法、继续颁布 WAPI 升级标准（仍为

强制性）并向 WTO/TBT 紧急通报、政府采购和引导电信运营商使用、成立 WAPI 产业联盟、设立 WAPI 产业发展专项等具体措施。

在各方的共同努力下，2009 年之后，WAPI 已经成为全球无线局域网芯片的标准配置。截至 2021 年 12 月，相关芯片产品累计超过 500 个型号，全球累计出货量超过 190 亿颗；移动终端和网络设备等已超过 18000 款。国内三大电信运营商也将 WAPI 作为集采网络设备支持的基本功能。目前，WAPI 产业联盟成员已发展到 109 家，包括三大电信运营商和 ICT 领域骨干企业。除公共 WLAN 网络外，WAPI 在政务、军队、海关、金融、电力、医疗、教育等诸多行业得到应用。

2006 年 1 月，根据 WTO/TBT 有关规则，我国就 WAPI 升级标准向 WTO/TBT 履行了紧急通报义务，并明确了实施时间为 2006 年 2 月 1 日。过程中未收到反对和任何异议。这意味着我国随时可实施 WAPI 标准，无需再通知。

2017 年 11 月 4 日第十二届全国人民代表大会常务委员会第三十次会议修订的《中华人民共和国标准化法》第二条明确规定：**强制性标准必须执行。**第二十五条明确规定：不符合强制性标准的产品、服务，不得生产、销售、进口或者提供。

北京市在采用自主可控安全技术开展政务网络和信息化建设方面一直走在全国前列。早在 2012 年，北京市经信委会同有关部门对 WAPI 技术标准及产业情况进行了深入调研。2014 年，北京市经信委

发布《北京市经信委关于加强政府投资信息化项目前置评审管理的通知》（京经信委发[2014]56 号文）。在政府投资信息化项目建设管理前置评审细则中明确要求：**无线局域网应符合 WAPI 标准，新增无线局域网建设项目应符合无线局域网安全技术标准（WAPI）。**项目涉及的无线局域网产品和含有无线局域网功能的计算机、移动终端、办公设备、专用机具等，应选用支持无线局域网安全技术标准并通过国家有关安全认证的产品。已建无线局域网（WLAN）项目应逐步升级改造。

四、WAPI 标准产业发展情况

（一）WAPI 标准发展概况

我国根据国家标准化法和国家商用密码管理条例，于 2003 年以强制性国家标准形式，发布了拥有自主知识产权的 WAPI 技术标准，其核心技术于 2010 年成为 ISO/IEC 国际标准。

WAPI 技术标准体系包括以下重要组成，其中 5 项为国家强制性标准：

- GB 15629.11-2003《信息技术　系统间远程通信和信息交换　局域网和城域网　特定要求　第 11 部分：无线局域网媒体访问控制和物理层规范》

- GB 15629.1102-2003《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范：2.4GHz 频段较高速物理层扩展规范》
- GB 15629.1101-2006《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范：5.8 GHz 频段高速物理层扩展规范》
- GB 15629.1104-2006《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范：2.4GHz 频段更高数据速率扩展规范》
- GB 15629.11-2003/XG1-2006《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范》第 1 号修改单
- GB/T 15629.1103-2006《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范：附加管理域操作规范》

为持续推动安全无线局域网的深度应用和发展，2006 年国家发展改革委、工信部、科技部指导成立 WAPI 产业联盟，联合会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、

基础技术、组网技术、网络管理技术、产品及测评、应用六个方面规划布局，通过产业界共同努力和持续研发，形成了基于 WAPI 的无线局域网标准体系，包括已发布国家标准、行业标准和团体标准 61 项，产业成果转化成效显著：经过十余年的努力，已形成了完备的 WAPI 产业链与产业生态，WAPI 产业群体完全具备了自主的产品开发与工程化能力以及 WAPI 网络大规模部署能力。WAPI 产业化历程经历了产业化准备阶段、电信运营商 WLAN 网络建设阶段之后，2015 年正式进入行业应用推广阶段。随着行业无线网络应用的普及，用户对无线网络安全的重视程度日益提升。WAPI 正在逐步与物联网、大数据、边缘计算、智能等新兴技术相融合，支撑起我国网络安全基础设施的建设。WAPI 产业化及应用已迈入新阶段。

WAPI 产业联盟密切关注市场需求和无线局域网技术演进，积极推进标准的制定发布和配套产业化。2020-2021 年，已开展产业化推进并发布的标准有《无线局域网产品工程化实现指南 第 10 部分：WAPI 与 IEEE 802.11ax》《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范 第 2 号修改单：管理帧保护技术规范》《无线局域网安全技术规范》《无线局域网接入控制 第 1 部分：组网架构规范》《无线局域网接入控制 第 2 部分：调度平台技术规范》等。

（二）WAPI 产业发展概况

目前 WAPI 已经成为全球无线局域网芯片的标准配置，拥有完整的产业链，截至 2021 年 12 月，支持 WAPI 的无线局域网芯片已超过 500 款型号、全球累计出货量超过 190 亿颗，移动终端和网络侧设备等已超过 18000 款，电信运营商已将 WAPI 作为集采网络设备支持的基本功能，除公共 WLAN 网络外，WAPI 已广泛服务于海关、金融、能源、政务、公安、交通、医疗、教育等行业，成为行业物联网的关键组成部分。

主流 WLAN 芯片厂商高通、博通、联发科（MTK）、美满电子（Marvell）、德州仪器（TI）、赛普拉斯半导体（Cypress）等国外厂商和瑞昱（Realtek）、乐鑫、联盛德微电子、南方硅谷、澜起科技、展讯、华大电子、海思等国内厂商均支持 WAPI。

集成和支持 WAPI 功能的产品包括但不限于：芯片、模组、个人电脑、智能手机、平板电脑、应用软件/APP、无线局域网接入点/路由器、无线局域网控制器、鉴别管理服务器等。集成和支持 WAPI 功能的产品形态越来越丰富、产品体系越来越完善。

（三）WAPI 产品易用性

相较于互联网时代的 PC 和移动互联网时代的智能手机，物联网时代的终端产品形态更加开放，任何设备都可以集成无线功能、接入 WLAN/WAPI 网络，这给各行业专用机具厂商们的 WAPI 产品开发带来

了挑战。针对上述，联盟组织会员单位推出了“WAPI 中间件解决方案”，快速让不同行业、形态各异的设备机具具备了 WAPI 功能，为 WAPI 终端满足泛在物联网时代的需求奠定了基础。轨道交通安防仪器等专用机具，即采用了“WAPI 中间件解决方案”。再如：针对“如何让 WAPI 终端更加易用”的共性问题，联盟从“芯片”这一产业链源头解决问题，通过组织芯片厂商通力合作，推进了 WAPI 证书应用接口的技术研发与升级。这些芯片厂商在 2018 年完成了相关产品解决方案的开发，第三方应用厂商可以直接调用这些芯片厂商提供的接口，开发出集成 WAPI 功能的 APP 应用。例如“一键 WAPI”APP，实现了用户终端 WAPI 证书申请、下载、安装和管理功能，满足了各行各业用户移动终端的 WAPI 网络便捷接入需求。

（四）WAPI 产业测试服务平台

WAPI 产业联盟测试实验室为产业和市场提供公共技术支撑服务，在多年服务产业市场过程中，在技术研发、咨询、测试等服务实践中，联盟测试实验室积累了丰富的经验。目前所开展的各项服务，具有“紧密贴合市场及产品需求、前瞻性强、技术服务全面精准、服务颗粒度精细、高效协助厂商完成产品整改”等特点。WAPI 产业联盟自身公共社会组织特征和优质高效的服务能力，让越来越多的行业用户愿意信任和选择联盟，纷纷采用“委托联盟开展测试”或“采信联盟测试报告”等形式，协助其 WAPI 产品选型和应用建设。

WAPI 产业联盟测试实验室持续提供标准符合性测试服务，并且对测试不通过的产品提供整改技术咨询,任何一家厂商如果希望做好 WAPI 产品，这些支撑服务都是可以利用的资源，并且是公开可以获得的。

目前联盟开展的无线局域网鉴别与保密基础结构(WAPI)测试，主要包括：WAPI 协议互通性、WAPI 协议完整性、功能与性能测试。其中，WAPI 协议互通性测试主要用于检验设备实现 WAPI 协议的一致性和正确性，以及设备与其他 WAPI 设备之间的互联互通性；被业界俗称为“WAPI 负面测试”的协议完整性测试，主要用于检验设备所实现 WAPI 协议的健壮性，以及是否能够正确处理异常协议报文等特殊状况，能够有效验证各行业 WAPI 产品是否能正确处理特殊场景下的异常报文，是否能有效抵御非法设备接入网络；在测试过程中，联盟会紧密结合用户需求，关注除协议之外的功能与性能测试。这些对保障 WAPI 网络系统运行的稳定性和健壮性，十分必要。

在测试过程中，联盟会紧密结合市场用户需求，融合共性技术和市场通用问题去开发新的测试项目。2020 年，联盟已两次升级了《无线局域网产品鉴别与保密基础结构（WAPI）功能测试项目》，并依据最新版本实施相关服务。

在服务全国 WAPI 检测机构方面，自 2019 年起，联盟在广泛调研并征求全国范围内检测机构意见的基础上，启动了 WAPI 检测系统比对服务，开发出多款比对样品，并依据最新《无线局域网产品鉴别

与保密基础结构（WAPI）功能测试项目》开展比对业务。比对输出的结果，已被 CNAS 等权威机构采信。

五、WAPI 应用概要及典型应用

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的在安全可管可控的无线网络中运行。特别是自 2016 年国家连续出台了《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 因其产业成熟度高、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。

如下给出若干典型应用方案的案例。

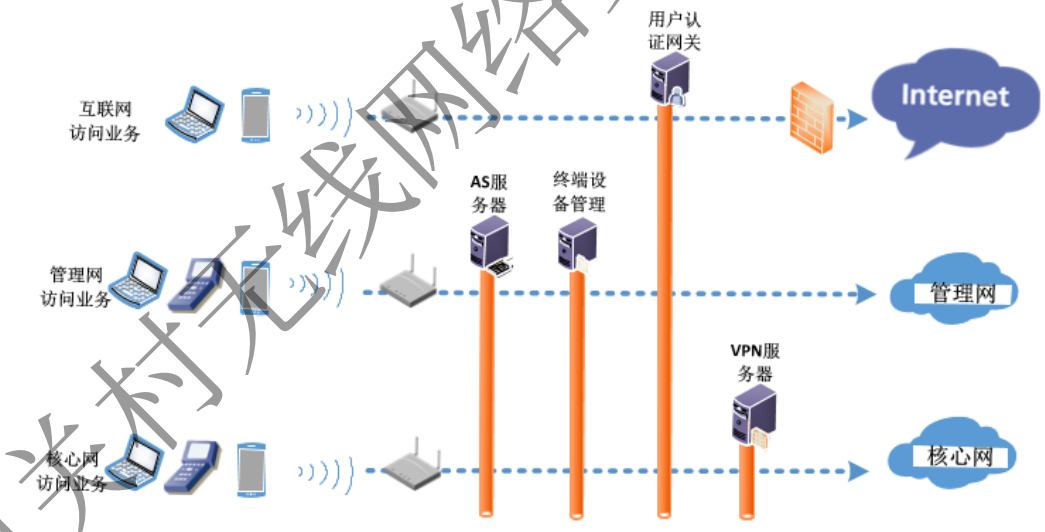
【案例 1】全国海关 WAPI 无线局域网应用示范项目（一期）

2015 至 2017 年，国家海关率先采用 WAPI 技术产品实施本行业无线局域网络建设，成为 WAPI 全国性大规模行业应用的首发单位，也综合考验了 WAPI 的网络安全性、易用性、规模组网能力、运行管理能力。在海关总署信息中心的统筹下，在 WAPI 产业联盟的组织下，顺利完成了中国海关十余个关区的 WAPI 应用示范项目建设。该项目能容纳近 30 万用户接入 WAPI 网络，保障了海关信息化系统的无线业务安全和数据资产安全。全国海关信息中心在项目建成后表示：“经检验，WAPI 是非常好的技术，具有技术先进性，产业化成熟度高，满足了海关信息化业务运行最后一公里的路径安全问题，具有规模化应用能力。”

全国海关 WAPI 无线局域网项目特点是：海关是国家重要信息系统的组成部分，在满足“必须使用安全可靠网络”的同时，还要满足“信息化业务丰富多样、建设环境复杂多样、不同用户对安全等级有不同需求、接入和使用网络要具备灵活方便性”等许多高标准要求。但因为海关信息化建设起步早、执行力强，是“有要求、严要求”的好用户，因此很多行业的共性问题在海关项目中被一一发现和解决，项目的可复制性非常高。该项目建成后，很多行业用户以此为模板和参考，实施本行业的 WAPI 规划和建设。

- WAPI 网络部署要求及总体架构

在网络部署架构方面，充分考虑无线网络可靠性、接入用户身份差别、接入设备访问业务差别等需求，采用符合国家规定的安全措施，分区分域管理，做到网络可管可控，保障数据资产安全；实现基于 WAPI 的接入，做到互联网、局域网的互通；确保基于 WAPI 网络实现移动终端等业务机具接入内部业务网络，能够使用 WAPI 开展海关内部办公和日常业务。应用中将业务划分为互联网业务、管理网业务、核心网业务三个层面，在终端设备接入内部业务网络时，不仅通过 WAPI 三元对等实体鉴别机制进行鉴别，还验证了数字证书绑定的设备硬件信息，进一步提升安全访问控制。



图：海关 WAPI 网络总体系统架构逻辑图

【案例 2】新疆乌鸟鲁木齐地铁 1 号线 WAPI 应用示范项目

2017 年 8 月至 2018 年 6 月，WAPI 产业联盟组织数字认证、瑞科慧联、华为等成员单位，开展了新疆乌鲁木齐地铁 1 号线 WAPI 项目建设。该项目于 2018 年 10 月顺利完成验收并投入运营，WAPI 成为乌鲁木齐地铁通信网络系统的重要组成部分。

乌鲁木齐地铁 1 号线北起国际机场站，南至三屯碑站，线路全长 27.6 公里，共 21 座车站。基于其安防系统、服务平台等无线业务和管理的需要，采用 WAPI 实施应用部署，保护地铁业务和信息数据网络的安全。

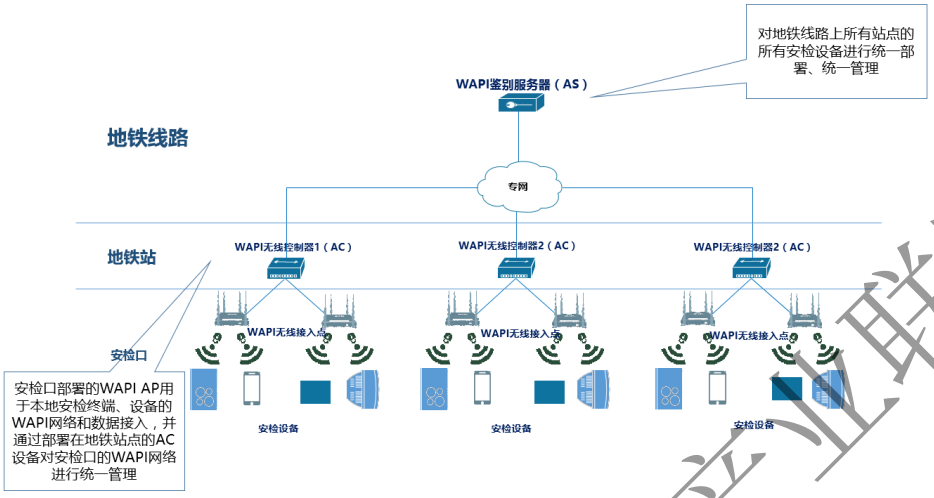
在该项目规划建设过程中，联盟和成员单位结合 WAPI 行业建设经验和新疆地铁的业务特点，迅速推出了综合应用解决方案，通过嵌入免驱动 WAPI 物联网终端模组，使地铁专用终端机具（如：行李检查机、液体检查仪、智能安全探测仪等）快速实现了对 WAPI 的支持。

- WAPI 网络部署要求及架构

本项目的特点是：应用中涉及了诸多安防设备和专用机具，由于其管理地位特殊、数据传输必须具备实时和保密能力、设备机具必须可管理可追溯，故要求独立采用 WAPI 组网。

该项目采用独立的 WAPI 网络进行覆盖；地铁全线设置一台鉴别服务器（AS）用于安防等设备机具的网络身份鉴别和管理；在业务过程中，通过 WAPI 网络将实时的业务状态数据上传至服务器进行备份、

汇总；通过专用机具为安防设备预置 WAPI 证书。



图：部分地铁安防业务 WAPI 网络部署架构图

【案例 3】公安系统 WAPI 室外高清视频设备及接入网络建设

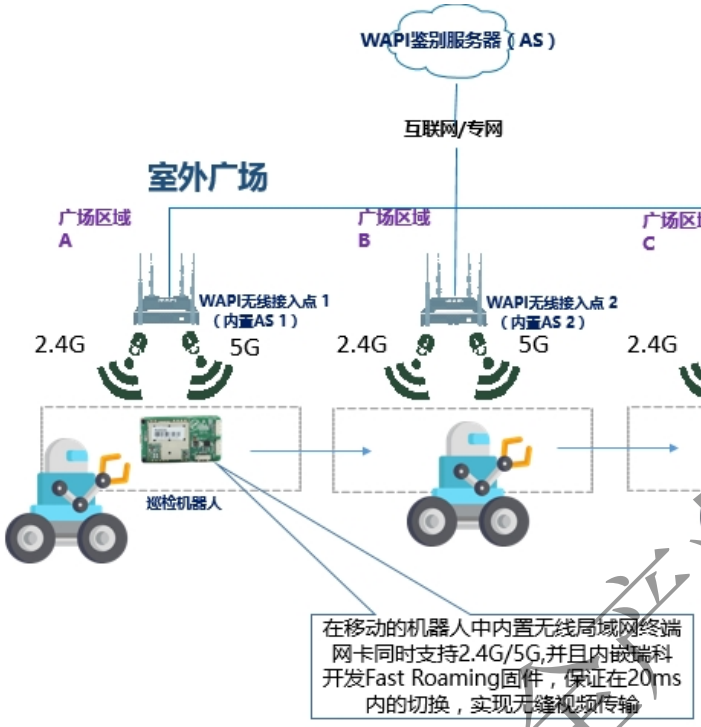
2017 年，按照公安部相关单位对室外高清视频无线传输的技术与应用需求，联盟组织西电捷通、瑞科慧联、数字认证、北京比邻等成员厂商，从公安系统的业务特性与应用特点出发，开展了具针对性的 WAPI 产品与解决方案的研发、设备改造、网络部署和试点示范工作。

在 2018 年“两会”期间北京某重点地区警用机器人示范项目中，采用 WAPI 技术打造的“公安系统室外高清视频接入网络”，有效满足了公安系统“专网专用、安全可控”等业务要求，突破性实现了现场专用移动机具的高清视频回传功能，达到了“高数据实时传输、网络快速切换”的管理要求，实施效果受到北京市公安局某分局认可与

表彰。该项目也因此成为公安系统的重要示范样板，以此为模板开展“WAPI 智慧警务”规划与建设。此类基于 WAPI 安全局域网的室外无线视频无缝切换和传输业务，也推动了公安、政务领域全面导入安全的无线局域网技术实现智慧安防应用。

- WAPI 网络部署要求及架构

项目要求：全网络覆盖区域须达到稳定的信息传输带宽（可按分级的可保证稳定数据传输带宽参数来设计）；移动端在多个 AP 之间漫游时，传输视频流没有明显卡顿。因此在网络架构设计上，终端和 AP 侧都采用了双 Radio 架构，可以保证永远有一路处于连接状态，默认连接走在 5GHz,当出现漫游区域切换时，优先让 2.4GHz 的终端跟 2.4GHz 的新 AP 建立连接，这样可以满足公安高清安防不会出现断和卡的问题。本架构经过项目检验之后，能有效满足公安用户更多室外场景的需求。



图：WAPI 视频布设及传输接入架构逻辑图

【案例 4】北京大兴国际机场 WAPI 无线局域网建设项目

2017 年，基于对安全无线网络建设和管理的需要，北京大兴国际机场选择采用安全自主可控的 WAPI 技术产品建设其无线局域网络，构建综合、绿色、安全、智能的立体化现代化城市交通系统。投运后大兴机场航站楼业务区域实现 WAPI 全覆盖，为各部门工作人员日常办公和开展海关、边检、运维等业务提供支撑保障。

机场规划和建设期间，WAPI 产业联盟高度重视并充分发挥组织协调和公共技术支撑服务作用，组织数字认证、新华三、瑞科慧联等成员单位，积极配合北京新机场建设指挥部工作，全面参与了技术论

证、网络规划、应用方案制定、行业机具开发、业务融合及优化、测试验证等工作，并与中国电信集团系统集成有限责任公司一起，高质高效的推进 WAPI 网络建设、设备调试、工程验收等。

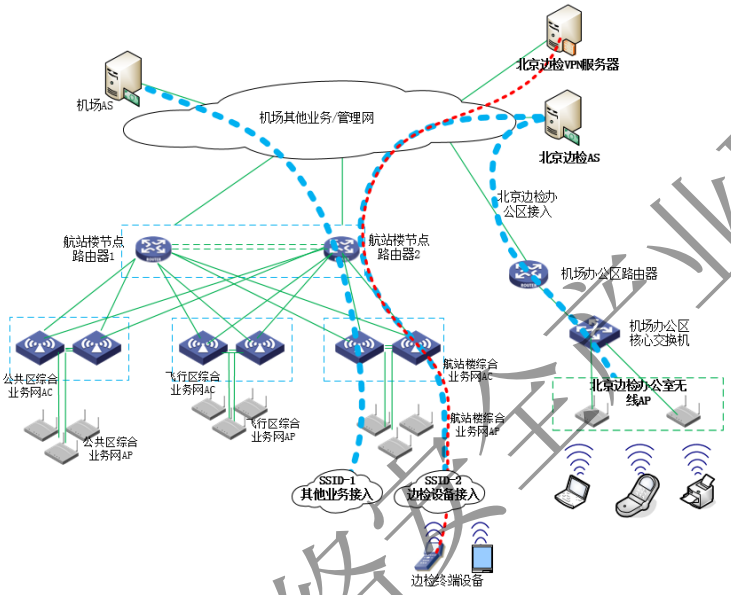
受承建方委托，联盟测试实验室预先模拟机场业务场景搭建了仿真测试环境，给予了高效的配套支持服务：一方面，为机场的 WAPI 无线网络建设方案以及多业务运行提供超前模拟验证，及时修正和完善建设方案，提高了建设效率，确保了建设质量；另一方面，根据机场建设需要，随时帮助参建厂商完成各种 WAPI 通用产品和机场专用机具的测试、整改、调优，完善各产品之间的互联互通性、互操作性、易用性，确保上述产品能在机场异构网络中良好稳定的运行。

2019 年 9 月 25 日，随着北京大兴国际机场正式投运，由 WAPI 产业联盟组织成员开展的北京大兴国际机场 WAPI 无线网络也同步投入使用。项目承建方中国电信集团系统集成有限责任公司表示：WAPI 技术产品成熟，在安全可控、高效运营管理等方面优势显著，为北京大兴国际机场开展无线业务提供了安全保障和管理便利。

● WAPI 网络部署要求及架构

北京大兴国际机场根据以往无线网络建设经验，为避免不同业务单位私自搭建无线 AP 接入点，造成 AP 间的信道同频干扰，规定：无线终端设备须接入机场统一建设的 WAPI 无线网络中。针对这种多业务类型、数据密度高、多终端并发接入等特征，WAPI 网络部署方

案采取在 AP 上创建多个 SSID，不同业务的终端设备接入专用 SSID，配置相应的 SSID 安全策略。鉴别方式采取“不同业务类型使用各自的 AS 鉴别服务器进行鉴别”，保障了多业务独立性和工作效率。



图：大兴机场 WAPI 无线局域网多业务接入架构逻辑图

【案例 5】电力行业 WAPI 无线局域网建设项目

随着智能电网、数字电网建设的推进，出现了以机器人巡检、可视化作业、变电状态在线监测为代表的新型业务，这些业务总体呈现出高带宽、移动性、大连接的特点，有线通信方式往往无法满足。为适应电网业务快速发展的数据采集需求，实现电网移动业务、高带宽业务的灵活接入，实现“最后一公里”热点覆盖，南方电网公司采用了 WAPI 技术进行变电站、配电房无线覆盖，为其提供安全、灵活、泛在的无线接入。

自 2019 年起，联盟组织数字认证、新华三、信锐技术、瑞科慧联等会员单位，积极配合南方电网总调开展 WAPI 技术应用可行性分析和论证、部署规划以及方案设计等工作。

2020 年 7 月，由南网数研院承建的 WAPI 系统在广东电网公司中山供电局 220 千伏光明变电站上线应用，已顺利完成机器人巡视任务，实现机器人巡检数据无线回传。该网络主要应用于 35 千伏及以上电压等级变电站或电厂，实现了厂站室内外无线信号的全方位深度覆盖，为南方电网公司数字化转型和智能电网建设提供通信支撑。

图：光明变电站项目现场

2020 年 12 月，由广西电网公司自主研制建设的南方电网首个变电站 WAPI 网络覆盖项目顺利通过验收。该项目在南宁供电局本部和 220kV 琅东变电站进行试点部署及应用，成功接入室外轮式巡检机器人、室内轨道式机器人、智能巡视摄像头、动环监控、移动办公等多

项业务，试运行 6 个月，系统运行情况良好，业务通信稳定。该项目有效支撑了南方电网变电站数字化转型，对各行业关键信息基础设施部署安全的无线网络具有良好示范作用。

图：琅东变电站项目现场

【案例 6】2022 北京冬奥会综合管廊 WAPI 应用示范项目

京投交通科技是2022北京冬奥会综合管廊项目的建设方，在综合评估了多种无线通信技术和方案后，选择应用WAPI开展冬奥会无线网络建设，并委托WAPI产业联盟组织厂商落实管廊专用机具全面支持WAPI，结合行业特点和应用需求开展测试，确保项目高效高质量推进。

结合管廊行业特征和项目核心业务需求，联盟积极配合京投交通科技工作，组织多倍通、华为等单位，对参建设备机具等进行了具针对性的产品性能优化和整改，通过了WAPI协议符合性测试、互操作测试、管廊行业系统测试等。目前该项目已正式投入运营。

图：北京冬奥会综合管廊项目现场

六、有关建议

1、加强政务及重要行业的无线局域网的规划与建设，依据《网络安全法》、《密码法》、《标准化法》等法律法规实施。

WAPI 是我国系列强制性国家标准，多年来，国家到地方及多个重要行业相继出台一系列法律法规，明确了对 WAPI 安全技术的使用要求。2017 年 11 月 4 日《中华人民共和国标准化法》（修订版）：第二条明确规定：强制性标准必须执行。

建议：**第一**、依据国家和北京市经信委等网络安全方面政策要求，北京市政府在政务网络安全信息化建设和数据资产管理方面，与网络安全国家战略接轨、与国际网络安全管理接轨。践行总体国家安全观，在符合国家标准化法（修订版）、政府采购管理规定要求等方面走在全国前列。发挥北京在信息化建设方面的示范和龙头作用，积极与其他省市开展技术和产业合作。**第二**、加强统筹协调和顶层设计，推动重要行业和社会化网络的安全无线局域网络建设和应用。

- 2014 年，北京市经信委发布[2014]56 号《北京市经信委关于加强政府投资信息化项目前置评审管理的通知》。**在政府投资信息化项目建设管理前置评审细则中明确要求：无线局域网应符合 WAPI 标准，新增无线局域网建设项目应符合无线局域网安全技术标准（WAPI）。**项目涉及的无线局域网产品和含有无线局域网功能的计算机、移动终端、办公设备、专用机具等，

应选用支持无线局域网安全技术标准并通过国家有关安全认证的产品。**已建无线局域网（WLAN）项目应逐步升级改造。其目的是采用自主可控技术标准产品，满足政府信息化建设和业务需求的同时，确保政府数据资产安全。**

- 2018 年 1 月，财政部印发了《政务信息系统政府采购管理暂行办法》，其中明确规定，政府信息系统采购须满足国家、行业相关标准的要求，鼓励使用市场自主制定的团体标准。**这意味着：1、WAPI 属我国颁布的系列强制性国家标准，按上述要求须体现在采购需求中；2、与 WAPI 产业化实施相关的团体标准可纳入采购需求。**

- 此前，财库[2005]366 号《关于印发无线局域网产品政府采购实施意见的通知》和《关于信息安全产品实施政府采购的通知（财库[2010]48 号）》中，也**对政府采购无线局域网产品有符合 WAPI 标准的要求。**

- 国际环境：2017 年 8 月，美国《物联网网络安全改进法案》要求：政府的网络（物联网）设备供应商要保证其设备采用政府认可的标准协议，不能含有已知的安全漏洞，法案建议“禁止使用硬编码”——联邦政府的物联网设备供应商要保证其设备采用政府认可的标准协议，不能包含硬编码密码，不能含有已知的安全漏洞，并且是不可以打补丁的。

2、利用标准，在一带一路、中东欧、中非等国家战略带动产业走出去方面发挥作用。

在开展一带一路建设、通过标准带动技术、产业“走出去”方面，WAPI 产业联盟有长期的项目组织经验，且事实证明：联盟组织产业群体实施标准输出，效果优于企业单打独斗。

下一步，WAPI 产业联盟将重点开展如下两个方面工作：

（一）多渠道促进我国牵头制定且具有自主知识产权的国际标准在“一带一路”沿线国家的实质性应用，以标准带动技术和产业走出去。

WAPI 产业联盟组织产业群体形成了创新领先的、面向网络基础架构一体化安全的 TePA（三元对等）网络安全技术架构，包括 IP 安全可信、无线和有线通信一体化安全、近距离通信安全、移动支付应用等在内的 40 余项创新安全协议。截至目前，这些技术已被 12 项国际标准和 32 项国家标准采纳。其中，在已成为关键信息基础设施的无线局域网领域，WAPI 产业联盟群体提出的 WAPI（无线局域网鉴别和保密基础结构）是国际上唯一一个与美国主导的 Wi-Fi 竞争无线局域网安全技术，而 Wi-Fi 因设计缺陷和安全问题已频繁被攻破，WAPI 必将在全球获得广泛应用。另外，在世界各国激烈竞争的物联网领域，WAPI 产业联盟群体已形成了 5 项国际标准的群体创新突破。

下一步，WAPI 产业联盟将抓住“标准联通一带一路行动计划（2018-2020）”中“深化基础设施标准化合作，支撑设施联通网络建设”的历史机遇，交流融通，强化“一带一路”沿线国家对 WAPI、TRAIS、NEAU 的认同，在充分了解中国牵头制定的国际标准在这些国家使用前景的基础上，积极促进这些国际标准的落地，以及向本国国家标准转化，促进更多自主创新技术在“一带一路”国家的应用，带动相关技术和产业的发展，从而扩大需求，提升技术和装备出口。

（二）在我国已形成突破和具备优势的领域，积极引导并促进“一带一路”沿线国家联合参与国际标准化工作。加强优势领域海外标准化应用示范推广行动，强化与沿线国家的合作，带动技术和装备出口。

WAPI 产业联盟长期在国际标准化组织 ISO/IEC 内开展技术提案工作，填补了我国在信息技术三个分技术领域的国际标准提案的空白（网络通信、信息安全、自动识别）。2017 年 11 月，无线网络安全标准化委员会副主任委员黄振海同志全票当选 ISO/IEC JTC 1/SC 6/WG 1 召集人，全面负责数据通信物理层和数据链路层国际标准制修订的总体工作，在网络通信国际标准化活动中取得了主导权。WAPI 产业联盟将充分利用上述工作基础，积极引导并促进“一带一路”沿线国家，欧洲、非洲相关国家联合参与国际标准化，在

巩固我国已经形成的网络安全国际标准体系的同时，促进更多自主创新技术在“一带一路”国家、欧洲、非洲的应用，带动相关技术和产业的发展，从而扩大需求，提升技术和装备出口。

前期，WAPI 产业联盟积极响应中关村管委会号召，曾成功协办了商务部“新一代无线通信与数字电视技术官员研修班”和“亚洲国家下一代网络建设研修班”，向包括“一带一路”沿线国家在内的 30 多个国家、上百位商务官员及信息主管官员进行了无线网络和网络安全接入领域的培训，收到良好反响。2014 年，WAPI 产业联盟响应中古两国元首共识，援助古巴形成客观可控的 WAPI 标准及其测试技术能力，协助古巴形成本国的无线网络安全技术能力。

后续，WAPI 产业联盟重点工作包括：落实“一带一路”倡议，推动 WAPI 技术标准走出去。将根据一带一路相关国家获取无线局域网的技术、标准能力的需求，协助这些国家逐步建立无线局域网技术标准体系，掌握通过检测认证等手段对无线局域网产品进行认证管理，培训并协助建设小型试验网络，逐步掌握 WAPI 无线网络的建设和运行管理能力。

3、加强 WLAN 安全宣传，推动 WAPI 标准走出去。

一是根据《中华人民共和国国家通用语言文字法》等有关规定，要求政府部门、行业企业和各类媒体规范使用“无线局域网/WLAN”中英文学名，严禁用“Wi-Fi”简单代替；同步工信部可制定通信网

络领域名词术语标准以供遵循。明确要求将将包括但不限于公共场所的“Wi-Fi”标志全部替换为“无线局域网”或者“WLAN”。二是采取有效措施，加强 WLAN 安全知识的宣传报道，将“Wi-Fi 不安全”形成一种社会共识。