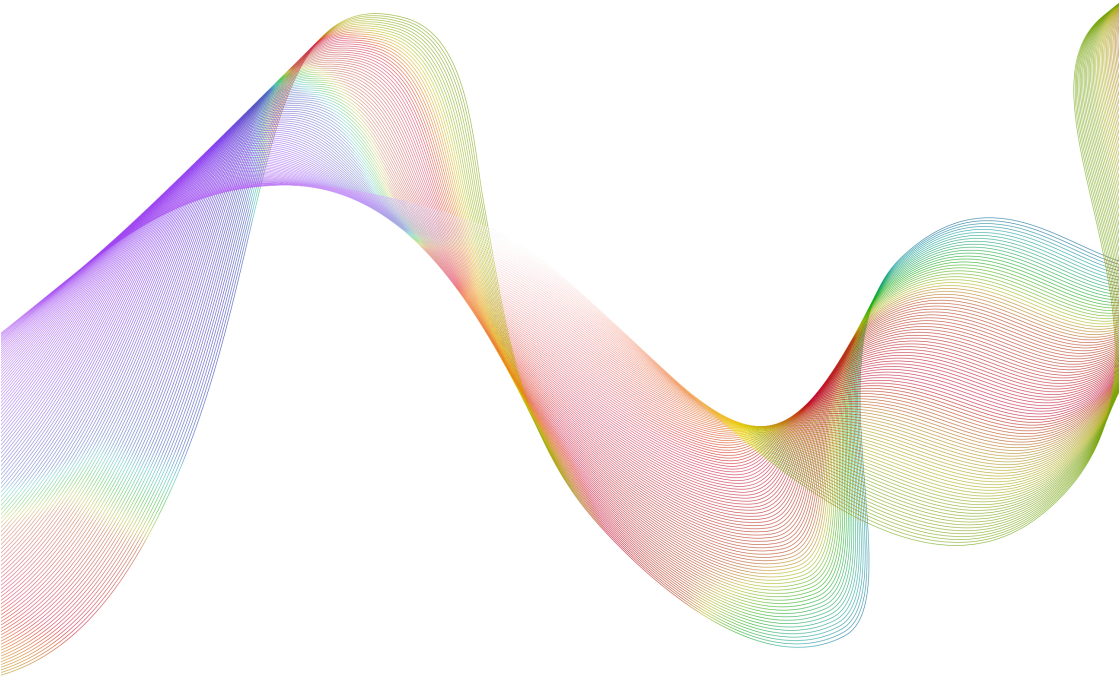
FAQ

WAPI Alliance
产 | 业 | 联 | 盟

WAPI 问答

中关村无线网络安全产业联盟
（WAPI产业联盟）
2025年12月



目录

编制说明

在 WAPI 服务各行各业及关键信息基础设施建设的过程中，中关村无线网络安全产业联盟（WAPI 产业联盟）总结了业界关注的常见问题，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 的解释存在不准确乃至错误之处，开设 WAPI 问答（系列连载）栏目，帮助业界更加客观准确地了解 WAPI。

截至 2025 年 12 月 WAPI 问答已发布 17 期，覆盖 WAPI 技术、标准、产品、应用、检验检测、联盟与会员等各方面焦点问题。为响应市场和厂商要求特集结成册，并分为“基本情况与业界关注、技术标准与演进、产品与工程化实现、市场建设与应用、WAPI 检测与服务、联盟与会员服务”等六部分，供参考使用。

本文件中涉及的数据与信息，均源自公开信息。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 2025 年 11 月。鉴于产业特性和技术迭代，存在一定动态变化的可能。

更多需求，欢迎和联盟交流探讨。

联盟秘书处联系方式：010-82351181，staff@wapia.org

【第一部分 基本情况与业界关注】

1. 问：什么是无线局域网？

答：无线局域网（WLAN）是无线高速数据通信两大主流技术之一（另外一个是 4G/5G/6G），使用无需授权的 ISM 频段中的 2.4GHz 或 5GHz 射频波段等进行无线连接，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。当前最常见的 WLAN 应用场景主要包括公共接入、个人接入和行业专网等。

2. 问：WLAN、WAPI、Wi-Fi 的关系和区别是什么？

答：目前，全球 WLAN 在数据和管理层面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、切换漫游等），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）标准，另一个是中国主导发展的 WAPI 标准。网络安全之外的其他部分是统一的、互通的，产品具备网络安全能力大都采用双模方式，产品可以互连互通。

从技术角度，WAPI 和 Wi-Fi 的区别，大的层面有三个：

（1）安全架构不同。WAPI 采用三元对等安全架构（对应全球安全架构演进的第三阶段），Wi-Fi 采用二转三元过渡架构（对应全球安全架构演进的第二阶段）。在不同架构下，核心区别是无线接入点（AP）有没有独立身份，这决定了无线局域网终端和接入点的双向鉴别是直接还是间接（三元是直接，二转三元是间接），也导致 Wi-Fi 容易遭受中间人攻击（假基站）。

（2）安全协议设计不同。WAPI 采用五次传递过程确保安全，Wi-Fi 采用的安全协议设计，已被全球业界揭示出容易遭受 KRACK、dragonblood 等攻击。

（3）使用的密码算法不同。WAPI 使用的对称密码算法是中国自主研发的 SM4，Wi-Fi 则采用美国提出的 AES。

3. 问：把 Wi-Fi 作为无线局域网的代名词使用，对吗？

答：把“无线局域网（WLAN）”称为“Wi-Fi”是不正确的，犯了以偏概全的错误。

（1）Wi-Fi 产品/系统，特指符合美国主导的 Wi-Fi 联盟标准的产品/系统，它只是无线局域网实现的部分形式，把“无线局域网（WLAN）=Wi-Fi”，相当于把“篮球=NBA”，把“卫星导航系统=GPS”，形式上是以偏概全，实质上是抹杀中国产业界“安全无线局域网”相关的自主创新技术成果。

（2）有可能侵权了美国 Wi-Fi 产业联盟组织的商标名称。使用“Wi-Fi”标记的前提是：产品符合美国 Wi-Fi 联盟标准（美 IEEE 标准+Wi-Fi 联盟互操作标准），并通过了 Wi-Fi 联盟收费的产品认证。

（3）这种错误使用涉嫌违法。违反了《中华人民共和国国家通用语言文字法》中“需要使用外国语言文字的，应当用国家通用语言文字作必要的注释”的规定。

（4）应合法、规范使用正确中英文学名。在描述“无线局域网”这种网络形态时，使用正确表述——“无线局域网”或者“WLAN”。

在描述“符合中国标准的安全无线局域网”时，使用正确表述——“符合 GB 15629.11 系列国家标准和相关行业/团体标准的安全无线局域网”或者“采用 WAPI 技术的安全无线局域网”。

（5）急需纠正目前国内的一些典型错误表达。包括但不限于：政府或行业在公开会议、下发文件、采购要求中，把无线局域网（WLAN）称为“Wi-Fi”；把 WLAN 覆盖（包括支持 WAPI 服务）的区域，标记为 Wi-Fi 等。

4. 问：Wi-Fi 技术有什么安全问题？

答：问题主要体现在：Wi-Fi 无法实现无线接入点（AP）与终端（STA）的对等双向鉴别和访问控制，STA 无法判断 AP 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，美国主导发展的 Wi-Fi，其安全问题越来越成为威胁我国网络空间安全和国家安全的重大隐患。

5. 问：Wi-Fi 安全机制也在不断升级，它的最高安全机制能否保证安全？

答：Wi-Fi 安全技术演进从 WEP 到 WPA、WPA2，再到当前最高等级的 WPA3，它的安全核心架构并未升级，仍然沿用 20 多年前设计的 IEEE 802.1x，即二转三元架构模式，无线接入点（AP）没有独立身份，容易导致中间人攻击。并且，密钥需要在 AP 和鉴别服务器之间传递，而传递密钥的安全通道在 Wi-Fi 标准中并未明确，仅仅依赖于厂商自行选择，安全通道存在的漏洞给整个 WLAN 系统带来非常严重的安全威胁。

WPA3 虽然在密码算法和预共享密钥机制等方面安全强度有所加强，但因安全架构并未提升，之前业界发现的安全问题未能完全消除，仍然存在安全隐患，因此，目前 Wi-Fi 最高安全机制并不能保证安全。网络安全等级保护国家标准也明确禁用 Wi-Fi 的相关模式。

6. **问：WAPI 比 Wi-Fi 更加安全，仅仅是因为使用了国产密码算法吗？**

答：这种说法是错误的。

Wi-Fi 自诞生起，就被不断披露存在安全漏洞，最近的包括：针对 WPA2 的 KRACK 攻击、针对 WPA3 的 dragonblood 攻击等等。相对而言，WAPI 迄今未被业界提出有安全漏洞。从技术层面剖析，主要是因为：

（1）WAPI 安全架构更优。WAPI 采用三元对等安全架构（对应全球安全架构演进的第三阶段），Wi-Fi 采用二转三元过渡架构（对应全球安全架构演进的第二阶段）。两者的核心区别是无线接入点（AP）有没有独立身份，这决定了无线局域网终端和接入点的双向鉴别是直接还是间接（三元是直接，二转三元是间接），间接双向鉴别导致 Wi-Fi 容易遭受中间人攻击（假基站）。

（2）WAPI 安全协议设计更完备。WAPI 采用具备原子性的五次传递过程确保安全，Wi-Fi 采用的安全协议设计，已被全球业界揭示出容易遭受 KRACK、dragonblood 等攻击。

（3）WAPI 采用国产密码算法。国产 SM 系列密码算法是经过我

国密码学界长期研究提出的，目前已被发布成为国家标准和ISO/IEC 国际标准，采用国产密码算法是 WAPI 高安全性的基础之一。

7. **问：有人说，WAPI 底层通信协议使用的是 Wi-Fi 技术。这种理解正确吗？**

答：不正确。

WAPI 和 Wi-Fi 使用的均为国际标准 ISO/IEC 8802-11 定义的底层通信协议，两者底层通信协议技术相同，但使用的安全协议不同，底层通信协议技术并不单独“属于”任何一者。

全球 WLAN 技术发展近 30 年，在底层通信协议（数据和控制）层面形成了相对统一的技术架构，这种技术格局的形成，能最大限度地利用全球和中国产业链多年发展的成果（一颗芯片可以同时支持 WAPI 和 Wi-Fi），技术和产业成熟度高，市场竞争充分。

8. 问：有人说，WAPI 产品只能“对标 Wi-Fi 5”、不能“对标 Wi-Fi 6”。这种说法对吗？

答：这种说法不对。在用户数据通信速率集等 WLAN 技术层面，WAPI 标准体系建设、产品研发、市场应用，和全球包括美国均是同步的。

WAPI 和 Wi-Fi 使用相同物理层技术。与 Wi-Fi 5 对应的物理层技术标准是 IEEE 802.11ac，与 Wi-Fi 6 对应的物理层技术标准是 IEEE 802.11ax。

多年来，在联盟组织下，持续以团体标准方式推动 WAPI 的技术演进和标准化，以确保在数据和管理层面全球保持统一技术架构和互通性。

早在 2016 年联盟就发布了 T/WAPIA 007.8《无线局域网产品工程化实现指南 第 8 部分：WAPI 与 IEEE 802.11ac》，目前市场上绝大多数产品均支持该标准。

2020 年联盟发布了 T/WAPIA 007.10《无线局域网产品工程化实现指南 第 10 部分：WAPI 与 IEEE 802.11ax》，目前市场上包括终端和 AP 的多种产品均支持该标准，其中还包括多款全国产的产

品。

目前，“对标 Wi-Fi 7”的 T/WAPIA 007.11《无线局域网产品工程化实现指南 第 11 部分:WAPI 与 IEEE 802.11be》标准已经发布，相关产业化工作已在同步推进中。

9. 在中短距离无线通信技术路线方面，WAPI 无线局域网和其它技术相比，有哪些优势？

答：正在演进的中短距离无线通信技术丰富多样，包括 WAPI、NB-IoT、LoRA、EUHT、WIA-FA、星闪、蓝牙等，它们各具特点和优劣势，适用于不同的应用场景和需求。

在选择采用具体中短距离无线通信技术路线时，需遵循五项基本原则，即：法律合规性、标准符合性、功能/性能匹配性、产业成熟度、可持续发展性。具体详见《WAPI 市场应用洞察报告——工业网络选择中短距离无线通信技术路线的基本原则》。

10. **问：行业用户使用 WAPI 与使用 Wi-Fi 相比有哪些优势？**

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

（1）更加安全。

（2）具有法律合规性——符合网络安全、密码、无线电管理等法律法规。

（3）具有标准符合性——符合 GB 15629.11 等百余项中国标准。

（4）中国自主安全协议，符合国家自主可控发展战略。

11. **问：目前有一些先进的物理层技术，例如毫米波、大规模 MIMO、TDMA 调度技术等，为什么没有被无线局域网国际标准 ISO/IEC 8802-11 采纳？**

答：物理层技术的选择并非追求理论最优，而是在现实约束下寻求最大化的实用价值。其演进路径反映了技术可行性、商业逻辑与用户需求的动态平衡。

返回目录

纵观无线局域网国际标准 ISO/IEC 8802-11 的发展历史，每次升级都是逐步引入新技术，比如 OFDM、MIMO、OFDMA 等。但为什么没有直接采用更激进的技术呢？因为需要平衡性能和现有产业发展、生态系统的稳定。

每一种技术都不是完美的，将新技术纳入标准需要各方的共识，涉及众多厂商和利益相关者。例如，毫米波虽能提供极高吞吐量，但覆盖范围小、穿墙能力差，仅适合特定场景，难以取代主流频段；又如，大规模 MIMO 可能增加功耗，手机、平板电脑等设备对续航敏感，物理层设计需在性能和能效间平衡；再如，TDMA 调度技术需要精确的时间同步，对硬件时钟精度要求极高，增加复杂调度模块会显著提高芯片成本和功耗，低成本、低功耗设备难以接受。所以某些在特定场景下表现优秀的技术，在另一些场景中可能效果不佳，需要综合考虑。同时，新技术的引入还需要经过长时间的论证和测试，确保互操作性和稳定性。

技术改进是为了解决实际问题，而不是单纯追求理论上的最优。未来，随着芯片工艺进步和频谱政策优化，更先进技术将逐步融入无线局域网标准，但可以预见仍将遵循渐进式而非激进创新的原则。

12. 问：区别于 Wi-Fi，WAPI 所采用的三元对等（TePA）网络安全技术架构是什么，先进性在哪里？

答：三元对等架构（TePA）是引入在线可信第三方，实现两个实体对等鉴别的架构。以三元对等安全架构为核心，包括网络空间可信身份识别不可或缺的基础安全机制（实体鉴别、群签名、密钥管理等）和网络基础连接所需的网络通信安全协议，如无线局域网安全（WAPI）、光/电以太网安全（TLSec）、射频识别空中接口安全（TRAIS）、近场通信安全（NEAU）等，共同构成了三元对等网络安全技术体系，为网络连接和互联提供了原子性基础安全能力。

全球范围内基础网络连接架构演进至今，一共经历了三个阶段：二元架构、二转三元过渡架构（Wi-Fi 所基于的基础架构）、三元对等安全架构（WAPI 所基于的基础架构）。第二和第三阶段的核心区别是架构是否支持无线接入点（AP）有独立身份，这决定了无线局域网终端和接入点的双向鉴别是直接还是间接——三元是直接，二转三元是间接，这也是 Wi-Fi 易遭受中间人攻击（假基站）的根本原因。

TePA 加强了可信实体的参与，确保了正确而全面的验证。TePA 已经是 ISO、IEC 等国际安全标准中的一个组成部分，同时已经被国

际标准化组织 ISO/IEC、欧洲标准化组织 ECMA 以及中国国家标准的许多主要网络通信协议所采纳。

13. 问：除 WAPI 之外，基于三元对等（TePA）安全架构的网络安全协议技术还有哪些？

答：三元对等架构（TePA）可以应用于有线、无线、近距离通信、IP 网络等多种网络，目前已形成了二十多项网络安全协议技术，并已被国际标准（ISO/IEC）、欧洲标准、中国国家标准、行业标准、团体标准采纳，构建了新一代网络四层安全协议，为 TCP/IP 四层互联网协议提供基础安全架构。这些协议技术及标准已广泛服务于能源、通信、金融、交通枢纽工程等关键基础设施，以及国防、公用事业等多行业和领域。

除无线局域网安全 WAPI 之外，基于三元对等架构（TePA）的典型网络安全协议技术及标准还包括：

（1）以太网安全——TLSec：GB/T 15629.3；

（2）射频识别安全——TRAIS：ISO/IEC 29167-16，ISO/IEC TS 29167-15，ISO/IEC 19823-16，GB/T 28925，GB/T 28926，GB/T 29768，

GB/T 35102，GJB 7377.1，GJB 7377.2 等；

（3）近场通信安全——NEAU：ISO/IEC 13157-4，ISO/IEC 13157-5，ISO/IEC 22425，ECMA 410，ECMA 411，ECMA 415，GB/T 33746，GB/T 30001.1，GM/T 0101 等；

（4）IP 安全可信——TISec：GB/T 25068.5 等。

14. 问：在合规性要求方面，与 WAPI 相关的国家法律法规规章和技术标准有哪些，其内在要求的关系是什么？

答：党的十八大以来，我国网络安全和信息化事业取得重大成就，网络安全保障体系和能力持续提升，网信领域科技自立自强步伐加快，网络空间法治化程度不断提高，网络空间国际话语权和影响力明显增强，网络强国建设迈出新步伐。国家正加快构建大网络安全工作格局，筑牢国家网络安全屏障。

法律是由全国人民代表大会及其常委会制定的规范性文件，是以国家强制力保证实施的规范体系；行政法规是由国务院制定的具有全国通用性的规范性文件，是对法律的补充，在成熟的情况下会被补充进法律；部门规章是由国务院各部、委员会和具有行政管理

职能的直属机构发布的规范性文件，在本部门/行业的权限范围内有效；标准则是由国务院标准化行政主管部门（国家市场监督管理总局 国家标准化管理委员会）批准或者授权批准的，农业、工业、服务业以及社会事业等领域需要统一的技术要求。

判断安全无线局域网（WLAN）产品和系统是否合规，最基础的依据是应符合相关的法律、行政法规、部门规章和技术标准。安全无线局域网相关的法律包括《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国标准化法》《中华人民共和国数据安全法》《中华人民共和国国家安全法》《中华人民共和国个人信息保护法》等，行政法规和部门规章包括《中华人民共和国无线电管理条例》《中华人民共和国电信条例》《中华人民共和国计算机信息系统安全保护条例》《商用密码管理条例》《关键信息基础设施安全保护条例》《网络安全审查办法》《网络产品安全漏洞管理规定》等，支撑上述法律法规规章实施的技术标准包括 GB 15629.11 无线局域网国家标准（系列标准）、GB/T 32420《无线局域网测试规范》、T/WAPIA 040 关键信息基础设施无线局域网技术要求（系列标准）、T/WAPIA 041 关键信息基础设施无线局域网测试方法（系列标准）、T/WAPIA 046《无线局域网安全技术规范》、T/WAPIA 047 无线局域网系统规范（系列标准）、T/WAPIA 048《信息系统无线局域网密码

应用基本要求》,以及 GB/T 22239 网络安全等级保护基本要求、GB/T 39786 信息系统密码应用基本要求等。

与无线局域网相关的法律、行政法规、部门规章和技术标准，共同构成了完整的无线局域网产品和服务合规性要求体系。具体见下图。

15. 问：针对关键信息基础设施领域的无线局域网，网络安全等级保护标准是如何规定的？

答：《网络安全法》第三十一条“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国

家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”其中明确要求关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护——在网络安全等级保护标准 GB/T 22239 中，明确规范了在密码管理上应遵循密码相关的国家标准和行业标准，在 WLAN 领域，GB 15629.11 系列国家标准（WAPI）是密码相关的国家标准，应依法遵循。

Wi-Fi 标准不是中国国家或行业标准，且未经国家密码管理部门认证核准，因此使用 WAPI 符合网络安全法，使用 Wi-Fi 产品、提供 Wi-Fi 服务不合法。

16. 问：在信息系统网络安全等级保护方面，涉及到安全无线局域网时，产品和系统应符合哪些标准？

答：安全无线局域网产品和系统应符合现行有效的 WAPI 标准体系，共计 80 余项标准。

（1）GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》规定了网络安全等级保护的第一级到第四级等级保护对象的安全通用要求和安全扩展要求。

（2）针对安全无线局域网，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，构建了完整的基于 WAPI 的无线局域网标准体系，截至 2025 年 11 月，标准体系共计 89 项标准。标准清单详见 WAPI 产业联盟发布的《WAPI 标准产业应用及环境监测报告》（2025 年 12 月版）。

17. 问：在信息系统密码应用安全性保护方面，涉及到安全无线局域网时，产品和系统应符合哪些标准？

答：安全无线局域网产品和系统应符合 WAPI 标准体系。

（1）GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》规定了信息系统第一级到第四级的密码应用的基本要求，从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面提出了第一级到第四级的密码应用技术要求，并从管理制度、人员管理、建设运行和应急处置四个方面提出了第一级到第四级的密码应用管理要求。

（2）T/WAPIA 048—2023《信息系统无线局域网密码应用基本要求》规定了信息系统中 WLAN 网络的密码应用通用要求，并针对 WLAN 网络的通信主体、通信信道及提供通信保护功能的设备提出了第一级到第四级的密码应用基本要求，适用于应用 WLAN 网络的信息系统的规划、建设、运行及测评。

（3）安全无线局域网的密码应用安全性评估涉及 GB 15629.11 系列国家标准、GB/T 37092《信息安全技术 密码模块安全要求》、T/WAPIA 046《无线局域网安全技术规范》。

18. 问：什么样的场景下，更适合使用 WAPI？

答：在所有应用无线局域网（WLAN）的地方，均适合使用 WAPI。

符合 WAPI 标准体系的 WAPI 无线局域网系统，符合国家网络安全法、密码法、标准化法、国家安全法、数据安全法、个人信息保护法等法律；符合网络安全等级保护、密码应用安全性评估、网络安全审查、关键信息基础设施安全保护、商用密码管理等法规；符合国家、行业、团体技术标准的要求。

符合 WAPI 标准体系的安全无线局域网系统，和 Wi-Fi 系统相

比，建设成本相同。

符合 WAPI 标准体系的安全无线局域网系统，保障了无线局域网用户的数据传输安全。

19. 问:为什么有些地方部署了 WAPI 网络,但用手机却搜不到 WAPI 信号?

答:WAPI 网络部署后，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。

20. 问：WAPI 目前的产业生态和应用情况如何？

答：WAPI 已经得到了广泛的应用。已成为全球无线局域网芯片的标准配置，正在为关键信息基础设施提供安全保障。

截至 2025 年 11 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 320 亿颗，移动终端和网络侧设备等已超过 24000 款，为电信运营商集采网络设备提供了安全能力，并广泛部署于海关、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。

目前，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。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、办公机具、各类行业专用机具等等。

21. 问：目前 WAPI 产品的国产化情况如何？

答：目前 WAPI 国产化已覆盖全系列产品。

包括 WAPI 终端（STA）、无线接入点（AP）、鉴别服务器（AS）在内的各类产品均已实现多厂商供货，有多款采用国产芯片的产品

已通过了 WAPI 产业联盟测试，符合 WAPI 标准体系。在此基础上，有多家厂商已推出了 AS、AC、AP、STA 全系列国产解决方案，供市场用户选择。

22. 问：建设和使用 WAPI 的成本比 Wi-Fi 如何？会不会增加额外成本？

答：WAPI 产业成熟度高，市场竞争充分，不会增加用户的采购和建设成本。具体如下：

（1）网络设备方面：所有主流厂商产品全部支持 WAPI，大多采用安全能力双模方式，售价与 Wi-Fi 产品相同。

（2）智能移动终端（Android、iOS）方面：全部支持 WAPI（双模方式），不仅限于手机和平板电脑，也包括所有使用了类似芯片/操作系统方案的产品，如音视频记录仪、移动布控球、智能安全帽等。

（3）非智能终端：绝大部分可通过软件升级支持 WAPI，不增加成本。

23. 问：前期已经部署的 WLAN 网络，要达到启用 WAPI 服务的效果，需要花多少钱？

答：绝大部分 WLAN 网络设备通过软件升级，均可支持并启用 WAPI 安全服务，升级的直接费用可以忽略不计。

（1）对于运营商部署的 WLAN 网络，在采购时即已经要求所有设备必须支持 WAPI 功能，因此实际上这类网络使用的设备已在功能上支持了 WAPI，仅仅是在网络配置上没有启用 WAPI 服务而已。因此，这属于网络配置工作，没有成本。

（2）对于非运营商部署的 WLAN 网络，由于硬件芯片都已在物理上具备了 WAPI 功能，只需要软件配合启用 WAPI 服务，而不需要升级任何硬件。具体方式是：设备厂商提供支持启动 WAPI 服务的升级包对设备进行升级。(而对于网络设备来说，经常在运营中会发现设备存在缺陷或者功能更新需求，因此厂家本身会经常发布新的升级包，来解决问题和改进，这属于设备厂商对产品生命周期正常管理的范畴。)

（3）为了给用户提供 WAPI 安全服务，按照标准要求，一个无线局域网需要配置一个具备鉴别服务单元（ASU）功能的实体，ASU 单元的形态有如下三种：**一是**内置在无线接入点（AP）中，软件升

级 AP，无硬件成本；**二是**内置在现有的其他网络服务器设备中，软件升级设备即可，无硬件成本；**三是**在一些关键基础设施中以独立设备——鉴别服务器（AS）方式部署。

24. 问：工业场景下的瘦 AP 产品选择，应该如何平衡成本和质量？

答：在工业场景中，瘦 AP 的成本应综合考量“可靠性、安装成本、后期运维费用”等全生命周期成本，而不应一味追求一次性低价采购。工业环境通常具有高温、高湿、粉尘多等严苛条件，低成本的 AP 可能无法满足长期稳定运行的需求，导致频繁故障和更高的维护成本。

在很多场景中（例如变电站、输电线路），维修/更换一台 AP 的费用，可能大大高于 AP 本身的设备采购价格。因此，选择高可靠性、适应工业环境的 AP 设备，虽然初期投入略高，但能够减少故障和停机时间、降低运维费用，保证生产系统的连续性和安全性，从长远来看更具经济效益。

25. 问：WAPI 技术标准在国外有应用吗？

答：WAPI 技术标准已在全球广泛应用。

在产业化层面，WAPI 已成为全球无线局域网芯片的标准配置。截止至 2025 年 11 月，支持 WAPI 技术标准的芯片已达 500 多个型号，全球出货量已超过 320 亿颗，移动终端和网络侧设备等超 24000 款。

在标准国际化层面，WAPI 的核心技术架构已于 2010 年被发布为 ISO/IEC 国际标准。美国、英国、韩国、捷克、意大利、哈萨克斯坦、乌克兰、中国等 8 个国家确认等同采用了该标准；比利时、法国、德国、爱尔兰、日本、墨西哥、挪威、波兰等 8 个国家确认在本国使用了该标准，本国产品是基于该标准的；日本确认其法规中引用了该标准。

26. 问：使用 WAPI 是否涉及版权、专利授权？

答：WAPI 技术涉及的标准、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》《著作权法》等相关法律法规，具体而言：

（1）标准版权：应用标准（包括设备厂商和最终用户等）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：最终用户使用 WAPI 网络服务不涉及软件版权问题。

（3）专利授权：最终用户使用 WAPI 网络服务不涉及专利授权。最终用户产品制造商需要为其 WAPI 设备取得专利许可。

27. 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 技术至少在未来 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）内为使用者提供高达数十 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 和 5G/6G 协同，提供包含短距离无线

通信和长距离移动通信在内的，完整的网络通信服务。

WLAN 技术和标准体系的不断演进——速率的不断演进，应用方式的不断革新，模块化技术的不断发展，安全技术的发展，均推动 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，是一条显性的主线。当前，在 100-300 米局部区域通信方式上，WLAN 没有可直接匹敌的竞争者；在 100 米之内短距离通信，WLAN 与蓝牙、RFID、NFC、Lora 等技术相比有明显优势。

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。

目前，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完善和发展，将具有机密性、完整性、可用性、抗量子攻击、可运营可管理等特性，有效支持人工智能、区块链、物联网、大数据、万物互联等应用。

【第二部分 技术标准与演进】

28. 问：“强制性标准必须执行”，但“推荐性标准”就可以不执行，这种说法对吗？

答：这种说法是错误的。

《标准化法》第二条“本法所称标准（含标准样品），是指农业、工业、服务业以及社会事业等领域需要统一的技术要求。国家标准分为强制性标准、推荐性标准，行业标准、地方标准是推荐性标准。强制性标准必须执行。国家鼓励采用推荐性标准。”据此，有人认为推荐性标准可以不执行，这种说法是错误的。

（1）合规性体系是指包括法律、行政法规、部门规章和技术标准在内的，以国家强制力保证实施的完整的规范体系。强制性标准是《标准化法》赋予自身具有强制力保障实施的规范性文件，推荐性标准虽不具备《标准化法》赋予的自身强制力，但其通过其他法律（如《网络安全法》《密码法》等）的引用，被赋予了强制力实施的属性，如《网络安全法》第十条“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要

求采取技术措施和其他必要措施，保障网络安全、稳定运行”，此处所述依照标准的强制性要求（包括了推荐性标准中的必备项，满足这些必备项要求是判定产品/服务符合标准的前提）即由《网络安全法》赋予了强制力实施的属性。

（2）标准是由国务院标准化行政主管部门（国家市场监督管理总局 国家标准化管理委员会）批准或者授权批准的，农业、工业、服务业以及社会事业等领域需要统一的技术要求。标准是对重复性事物和概念所做的统一规定，以科学技术和实践经验的结合成果为基础，以特定形式发布作为共同遵守的准则和依据；只有统一的高标准才能引领高质量发展。网络的基本属性是互联互通，除强制性标准外，推荐性标准即为事实上的引导建设高质量网络、提供高质量网络服务的统一要求，是应该要使用的。

29. 问：建设无线局域网只需要遵守国家或者行业标准，团体标准则可以忽略，这种说法对吗？

答：这种说法是错误的。

合规性体系是指包括法律、行政法规、部门规章和技术标准在

内的，以国家强制力保证实施的完整的规范体系，在安全无线局域网建设中应符合相关国家、行业、团体标准。

（1）《标准化法》第十八条“国家鼓励学会、协会、商会、联合会、产业技术联盟等社会团体协调相关市场主体共同制定满足市场和创新需要的团体标准，由本团体成员约定采用或者按照本团体的规定供社会自愿采用。”按照上述法律要求，WAPI 产业联盟制定 WAPI 相关团体标准是国家法律鼓励的行为，团体标准对产品和服务的要求高于国家或者行业标准，是对促进国家和行业标准实施的必要补充，运营者或者产品制造商不应排斥采用 WAPI 团体标准，而应积极采用以提升产品质量和服务水平。

（2）2022 年 7 月 6 日，国家市场监督管理总局等 16 个部门印发了《贯彻实施〈国家标准化发展纲要〉行动计划》，明确了 2023 年重点工作，要求有序推进任务落实，更好发挥标准化在推进国家治理体系和治理能力现代化中的基础性、引领性作用。其中明确要求“探索推进… …推荐性国家标准采信团体标准… …等机制创新。”

（3）2023 年 2 月，中共中央、国务院印发了《质量强国建设纲要》，其中第 22 条明确要求优化质量基础设施管理，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，进一步从政策层面支持和鼓励团体标准的制定和实施。

（4）2024 年 3 月，国家市场监管总局、中央网信办等 18 个部门联合印发了《贯彻实施〈国家标准化发展纲要〉行动计划（2024—2025 年）》，明确要求要深入实施团体标准培优计划，培育一批优秀的团体标准组织，推进团体标准应用示范，促进团体标准规范优质发展，制定一批填补空白、引领发展的高水平团体标准。

30. 问：团体标准是不是一定要转化为国际标准、国家标准才能体现出价值？

答：不是。

国家标准化管理委员会和民政部联合印发的国标委〔2019〕1 号文《团体标准管理规定》第 3 条明确规定，“**团体标准是依法成立的社会团体为满足市场和创新需要，协调相关市场主体共同制定的标准。**”其核心价值在于应用。在应用过程中，可以根据实际需要，转化为国际标准、国家标准或者行业标准。这些

转化从一定程度上会促进团体标准的应用实施，但不是团体标准取得应用的前提条件。

从实践看，WAPI 产业联盟团体标准对技术、产品和服务的要求，均高于本领域的国家标准、行业标准，是对促进国家和行业标准实施的重要补充，起到强有力的支撑作用。

对于技术内容具有先进性、引领性的标准提案，联盟会同步规划和推动国际标准、国家标准、团体标准的制定。以《无线局域网接入控制》系列标准为例，该标准提案自 2020 年 5 月立项，就同步开展了国际标准制定工作，于 2021 年 11 月发布为联盟团体标准，2023 年 8 月获发布为国际标准。

31. 问：国家标准委印发的《团体标准组织综合绩效评价指标体系》和企业有什么关系？企业要关注哪些具体要求和指标？

答：2024 年 8 月 14 日，国家标准化管理委员会印发《团体标准组织综合绩效评价指标体系》，旨在深入贯彻落实《国家标准化发展纲要》，发挥市场对团体标准的优胜劣汰作用，促进“制定好、管理好、应用好”团体标准。《指标体系》从组织管理能力、专业技术

能力、标准编制能力、推广应用能力 4 个维度提出了具体要求。其中对企业参与团体标准工作提出了具体要求，建议企业关注和落实相关工作。包括：

（1）在“2.3 参编单位相关技术创新成果”中，鼓励制定含有标准必要专利的团体标准，鼓励科研成果、新产品、新技术、新服务转化为团体标准；

（2）在“4.5.3 市场应用”中，鼓励在招投标文件或商业合同中实施应用团体标准；鼓励企业依据团体标准进行生产经营活动时，在“企业标准信息公共服务平台 https://www.qybz.org.cn/”上公开执行团体标准的相关信息；

（3）在“4.5.6 合格评定应用”中，鼓励在检验检测、评价、认证认可中应用团体标准。

32. 问：现有的国家标准体系是 2003 年和 2006 年发布的，十几年过去了，WAPI 是否还具有先进性？

答：WAPI 技术标准体系具有先进性，且在持续演进。

（1）WAPI 技术最初于 2003 年被采纳并发布为 GB 15629.11 国

家标准，之后 2006 年多模并存增强机制被采纳并发布，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 技术体系不断得到发展。

（2）2015 年国家发布了 GB/T 32420《无线局域网测试规范》：不仅针对 2006 年之前国家标准的技术内容，也针对后续演进的团体标准（对应 11n、11ac、11ax 等增强模式）等内容。在 WAPI 产业联盟组织下，持续推动 WAPI 的技术演进和标准化，截至 2025 年 11 月已形成了包括国家标准、行业标准、团体标准和国际标准在内的 89 项 WAPI 标准体系。

（3）目前，WAPI 标准产业共同体正开展高质量安全无线局域网技术体系研发和标准制定。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完善和发展，将具有机密性、完整性、可用性、抗量子攻击、可运营可管理等特性，有

效支持人工智能、区块链、物联网、大数据、万物互联等应用。

33. 问：有人说，WAPI 产品不能防范解除链路验证攻击。这种理解正确吗？

答：不正确。

启用 WAPI 管理帧保护功能的产品均可以防范解除链路验证攻击。

WAPI 在安全身份鉴别和密钥建立基础上，采用国家批准的密码算法对管理帧进行保护，相关标准包括 T/WAPIA 010.3 和 T/WAPIA 046。目前符合团体标准 T/WAPIA 010.3 或 T/WAPIA 046 的产品，均具备防范解除链路验证攻击能力。

34. 问：WAPI 协议和产品支持 STA 在 AP 间快速切换吗？

答：支持。

STA 在同一 AS 域内跨 AP 快速切换是 WLAN 应用中的常见需求。无线局域网国家标准（GB 15629.11—2003/XG1—2006）已定义了预鉴别机制和 BKSA 缓存机制来降低切换时延，团体标准 T/WAPIA 046

也进一步定义了 WAPI 快速切换协议，进一步降低了跨 AP 切换对低时延业务的影响。符合上述标准的 STA 产品，可以实现高效快速安全切换，满足切换时业务不中断。

另据了解，此前一些厂商已在产品工程化方面通过“双发选收”等优化设计方案实现了 WAPI 终端产品跨 AP 的无缝切换，实测切换时间小于 20ms，能满足流媒体等实时业务数据的不间断传输需求。

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

答：通过“双发选收”实现快速切换的 STA，对网络侧设备没有特殊要求。

实现“双发选收”的 STA 有射频 A 和射频 B 两组射频，在 AP 间切换类似于两只脚走路，但总有一只脚不离地面——当 STA 在 AP1 与 AP2 之间切换时，射频 A 保持与 AP1 稳定连接，同时射频 B 开始连接 AP2，连接稳定后，射频 A 与 AP1 断开，以此类推——始终保持有一组射频处于稳定连接状态，从而实现“无感”切换。早在 2021

年就有相关（两组射频）CPE 产品通过了 WAPI 产业联盟测试，实现了移动高清视频等业务无间断、不卡顿、实时传输，实测切换时间小于 20ms。

36. 问：WAPI 技术是否适用于物联网（IoT）设备？

答：适用。

WAPI 技术不仅完全适配物联网设备，更在安全性、场景兼容性及合规性等核心维度，精准解决了物联网规模化应用中的关键痛点，已在多领域应用。

（1）筑牢物联网安全防线：物联网“端-边-云”链路中，智能家居传感器、工业监控终端、医疗设备等常涉及敏感数据采集与远程控制，数据泄露、篡改及非法接入风险突出。WAPI 通过终端设备与接入点的双向鉴别机制及国密算法加密，有效抵御了“非法设备接入”“数据窃听”等风险。

（2）适配复杂物联网场景：物联网设备常处于海量终端并发、移动物联网终端动态连接切换等场景，WAPI 技术的部署应用可直接复用现有网络架构，无需额外改造。WAPI 产业群体已结合物联网应

用场景需求，开发出低功耗模组、毫秒级快速切换技术和产品，适配工业实时通信、智慧城市等规模化部署需求。

（3）符合关键领域的合规性要求：政务、工业、医疗等核心领域明确要求：物联网设备应符合《网络安全法》《密码法》对网络安全与密码应用的强制性要求。WAPI 物联网完全满足上述要求。

37. 问：WAPI 技术用于物联网（IoT）设备时，需要考虑哪些特殊因素？

答：物联网设备与消费电子（如手机、电脑）相比，具有低功耗、资源受限、场景碎片化、长期在线等特性，因此在集成 WAPI 时应重点关注以下因素：

（1）适配低功耗：应优先采用芯片自带的硬件加密引擎（如支持 SM4 硬件算法的低功耗 WLAN 芯片），避免软件加解密占用 CPU 资源、增加功耗。

（2）资源受限设备的协议栈轻量化：由于多数物联网设备的硬件资源有限（如：RAM<1MB、Flash<16MB、CPU 主频低），需使用轻量化的 WAPI 协议栈。

（3）证书管理的简化：物联网设备通常不具备人工操作的证书管理界面，需考虑“在线证书管理”功能。

38. 问：无线局域网技术可用于民用无人驾驶航空器的相关通信吗？

答：可以。

无线局域网 WLAN 已成为全球宽带信息基础设施的重要组成部分，并作为基础模块被其它行业设备集成，为海量行业设备提供了中短距离高速通信能力。

近年来，我国民用无人驾驶航空器产业取得了巨大发展，广泛应用于个人消费、植保、测绘、应急等领域，在国民经济各个领域发挥着重要作用。目前，微型、轻型和小型民用无人驾驶航空器在飞行过程中采用无线局域网信标帧广播协议，通过无线电方式周期性主动对外广播其唯一产品识别码，实现了远程识别与动态监控，保障了实时监管与空域安全。

此外，在民用无人驾驶航空器的遥控遥测数据传输、低空自组网及协同飞行等应用场景中，无线局域网技术均为典型的技术实现方案。

返回目录

39. 问：2024 年 1 月，国际标准化组织(ISO) 和国际电工委员会(IEC)宣布成立量子技术联合技术委员会——ISO/IEC JTC 3，这对 WAPI 技术标准体系的影响是什么？

答：WAPI 产业联盟高度重视量子技术发展对 WAPI 标准体系带来的新挑战和新机遇，自 2015 年即组织开展了相关标准化项目的研究，以满足身份保护需求和应对潜在量子计算攻击威胁，联盟团体标准 T/WAPIA 046《无线局域网安全技术规范》即是 WAPI 产业群体的贡献，为向量子安全时代过渡的安全无线局域网产品提供了架构及协议支持。

2024 年 1 月 11 日，国际标准化组织和国际电工委员会在日内瓦宣布成立 ISO/IEC JTC 3 量子技术联合技术委员会，负责量子技术领域的标准化工作，包括量子信息技术（量子计算和量子仿真）、量子计量学、量子源、量子探测器、量子通信和基础量子技术等领域。目前，该技术委员会有包括中国国家成员体/国家委员会在内的 24 个积极成员国（P-Member）和 8 个观察员国（O-Member），并已与欧洲电信标准化协会（ESTI）、国际电联电信标准化局（ITU-T）以及 12 个 ISO、IEC 技术委员会建立了联络关系。JTC 3 由英国标准协会（BSI）担任秘书处，韩国全州大学碳和纳米材料工程系教授

Haeseong Lee 担任主席。

量子技术是指利用量子力学原理来设计、制造和操控器件与材料的技术，通过利用量子叠加态、纠缠态和隧道效应等奇特性质实现更高的信息处理和通信能力，在人工智能、量子计算、生物医药、通信传输、石油勘探等方面应用前景广泛。以量子信息科学为代表的量子技术，可以在保障信息安全、提高运算速度、提升测量精度等方面突破经典技术的瓶颈，成为信息、能源、材料、生命等领域重大技术创新的源泉，将引领新一轮科技革命和产业变革方向。

JTC 3 的成立，标志着国际社会对量子技术发展的高度重视，以及应对量子时代网络信息安全新威胁的全球协同行动正在加速。

后续，WAPI 产业联盟和无线网络安全标准化工作委员会将结合量子技术的发展和全球的标准化进展，持续创新、提升和发展 WAPI 标准体系。

40. 问：面向量子时代，WAPI 技术标准体系将如何演进和发展？在为无线局域网络提供抗量子攻击能力方面，进展如何？

答：自 2003 年 WAPI 1.0 技术标准体系形成迄今，80 余项国

家、行业、团体标准陆续得到发布，标准体系不断完善，联盟测试实验室的产品和系统测试项目，已演进四个版本，持续支撑产业创新发展。

随着量子技术逐步取得突破及商业化进展的加快，使用传统密码算法的网络安全协议体系面临重大挑战，迫切需要形成新一代WLAN安全技术标准体系。因此WAPI 2.0技术标准体系的演进目标是：面向量子时代安全需求，逐步提供抗量子攻击能力，并在身份保护、防范离线字典攻击等方面提供更高安全性，支持快速切换、确保承载的多媒体业务传输具备更高质量。2021 年 12 月 28 日，WAPI 产业联盟、无线网络安全标准化工作委员会发布了 T/WAPIA 046《无线局域网安全技术规范》，这是WAPI 2.0技术标准体系的第一项标准。

T/WAPIA 046在安全性、隐私保护、应对量子计算攻击威胁和防范离线字典攻击等方面，对现有 WAPI 1.0 技术标准体系进行了升级与增强，主要包括：

（1）升级采用面向量子安全的安全协议方案缓解量子威胁，降低WLAN通信系统数据“当前存储，以后破解”风险；

（2）新增支持身份保护功能，在保障通信安全的同时保护用户

隐私；

（3）新增支持快速切换机制，满足音视频等流媒体业务无中断传输；

（4）升级支持防范离线字典攻击，提供可靠前向安全性（PFS），防范窃听者暴力破解获得密码和通信数据；

（5）全面适配通用国密算法，提供更高强度安全。

同时，T/WAPIA 046 兼容 WAPI 1.0 技术标准体系，为实际部署中提供了向新安全方案的有序过渡，适应了平滑演进、兼容互通的产业需求。

41. 问：目前已经发布的基于 WAPI 的无线局域网技术标准有 80 多项，从技术演进角度看，分为几个标准体系？

答：WAPI 从技术演进角度，目前分为两个技术标准体系——WAPI 1.0 技术标准体系和 WAPI 2.0 技术标准体系。

2000 年，为弥补无线局域网（WLAN）国际标准 ISO/IEC 8802-11 存在的严重安全缺陷，中国业界在多年技术积累基础上，自主研

发提出了全新的安全架构和 WLAN 安全协议——WAPI（无线局域网鉴别与保密基础结构），2003 年被采纳入国家标准 GB 15629.11/1102。WAPI 所基于的三元对等安全架构，较之 ISO/IEC 8802-11 所基于的二转三元过渡架构具有显著技术优势，解除了接入点缺乏独立鉴别身份、依赖于与网络服务器额外建立安全传递通道，无法实现与终端的直接双向鉴别、易遭受“假基站”“蹭网”等安全隐患。GB 15629.11/1102 标准的发布，标志着 WAPI 1.0 技术标准体系的形成。

2006 年国家密码管理局发布第 7 号公告，批准了 WLAN 产品须采用的密码算法，包括对称密码算法 SM4，签名算法 ECDSA、密钥协商算法 ECDH 的指定椭圆曲线和参数，杂凑算法 SHA-256。上述 WLAN 专用商密算法的发布，为 WAPI 技术标准体系持续演进提供了重要支撑。GB 15629.11—2003/XG1—2006、GB 15629.1101—2006、GB/T 15629.1103—2006、GB 15629.1104—2006 四项国家标准发布后，基础安全技术、安全组网技术、网络管理技术、产品与解决方案、测试评价技术、创新应用等持续演进发展，80 余项国家、行业、团体标准陆续得到发布，WAPI 1.0 技术标准体系不断完善，联盟测试实验室的产品和系统测试项目，已演进至第四个版本。标准体系的深入实施推动了产业发展，支持 WAPI 1.0 技术标准体系的 WLAN 芯

片超过 500 款型号、全球累计出货量超过 320 亿颗，移动终端和网络侧设备等超过 24000 款，为能源、海关、金融、政务、公安、交通、医疗、教育等行业提供着安全网络服务。

随着本世纪初迄今量子技术逐步取得突破及商业化进程的加快，使用传统密码算法的网络安全协议体系正面临重大挑战，迫切需要新一代 WLAN 安全技术标准。2021 年 12 月，WAPI 产业联盟、无线网络安全标准化工作委员会发布了 T/WAPIA 046《无线局域网安全技术规范》，这是中国 WLAN 业界面向量子时代的网络安全挑战，结合适配通用商密算法 SM2、SM3 需求，使用更高性能密码套件 WPI-SM4-GCM，满足身份保护需求和应对离线字典攻击、潜在量子计算攻击威胁，为向量子安全时代过渡的安全 WLAN 产品提供架构及协议支持的新贡献，安全 WLAN 技术标准体系也因此得到新的发展，标志着进入了 WAPI 2.0 技术标准体系阶段。

42. 问：联盟团体标准 T/WAPIA 046《无线局域网安全技术规范》的实施情况如何？

答：T/WAPIA 046 实施正稳步进行中。目前已有多家联盟成员发布了符合 T/WAPIA 046 标准的 STA、AP/AC、AS 等系列产品，联盟

测试实验室已经建设了相关测试能力。

值得关注的是,T/WAPIA 046 适配了通用商密算法 SM2 和 SM3，并持续使用 SM4，对 WAPI 1.0 技术标准体系中 WLAN 安全协议内容进行了扩展，增加了适配后的机制选项，包括新增 WAI2 协议、快速切换机制等，在密码算法强度、身份保护、抗离线字典攻击和应对量子计算攻击等安全性方面有显著增强，使 WLAN 设备持续满足合规要求、支持形成可信赖 WLAN 网络和服务，适用于更高安全要求的应用环境，将有效应对量子时代的新安全威胁。在实际部署方面，T/WAPIA 046 兼容 WAPI 1.0 技术标准体系，满足实际部署中 WAPI 1.0 向 WAPI 2.0 技术标准体系的有序过渡，适应了平滑演进、兼容互通的产业需求。

T/WAPIA 046 发布实施后，因其结合和兼顾了面向量子时代安全和使用通用商密算法的需求，得到业界的关注和响应。多厂商多类别产品开发、联盟测试平台能力建设，稳步推进。同时，联盟不间断地收集和响应产业应用实施过程中成员单位和业界各方提出的意见、建议，持续追求在不降低安全性的前提下，进一步减少技术演进升级的投入，将芯片等硬件系统升级的工作减至最少，在满足合规性需求的前提下，进一步保护投资。例如：标委会已针对

T/WAPIA 046 中 WAI2 协议封装及以太类型字段标识的改进，发布了修改单。

根据联盟产业调研，实施 T/WAPIA 046 的典型方式是采用软件升级方式（作为软件补丁部署在 WAPI 1.0 标准符合性设备上），目前已有多家联盟成员发布了符合 T/WAPIA 046 标准的 STA、AP/AC、AS 等系列产品，为行业和产业应用提供合规、兼顾面向量子时代安全和通用商密算法应用需求的产品和网络系统解决方案，联盟测试实验室已经建设了相关测试能力。同时联盟将继续做好和产业、行业决策机构以及采购政策的衔接，使产业、行业能及时采用合规、具有更高安全性、面向量子时代安全需求的产品，支持保障网络服务的安全性。

43. 问：依据 T/WAPIA 046 团体标准实现的产品，是否意味着就支持了 WAPI 2.0 功能？

答：是的。

严格依据 T/WAPIA 046《无线局域网安全技术规范》团体标准实现的产品，意味着不仅支持 WAPI 2.0 功能，还同时支持 WAPI 1.0

功能，即“WAPI 1.0 功能和 WAPI 2.0 功能兼容模式”。

44. 问：在 WAPI 1.0 和 WAPI 2.0 两种技术标准体系中，安全服务可以在同一网络 SSID 内启用吗？

答：不可以。

在产品测试和示范应用中，存在同一网络 SSID 内，不同版本 WAPI 机制并存，以及同一版本机制中证书鉴别和预共享密钥鉴别混用的情况。由于预共享密钥鉴别面临的安全管理风险较大、仅适用于满足短时间临时组网的需求，与证书鉴别机制安全性差异大，以及不同版本 WAPI 机制的安全等级不同，为防止降维攻击，联盟建议：应用中应避免不同版本 WAPI 机制，以及同一版本机制中证书鉴别和预共享密钥鉴别在同一网络中同时启用服务的做法。

45. 问：在 WAPI 1.0 技术标准体系基础上，直接将密码算法替换为 SM2/3。这种做法是否合规，为什么？

答：这种做法不合规。

目前业界存在“在现有 WAPI 1.0 技术标准体系的基础上，在产品开发中直接替换原有 WLAN 专用商密算法、使用通用商密算法”的做法。这种做法，不是现有标准体系支持的合规方式，以这种方式开发的产品，不具备技术标准体系演进形成的新的安全能力。

WAPI 产业联盟在 2024 年 11 月 14 日发布的《关于安全无线局域网高质量发展的通告》中，对此已做了警示和剖析。详见联盟官网 http://www.wapia.org.cn/yaowen/detail_342490.shtml。

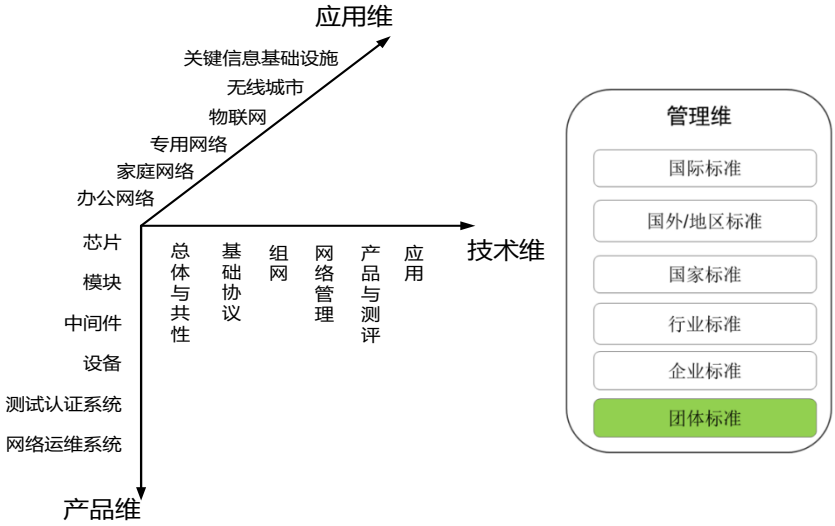
46. 问：目前 WAPI 标准体系情况是怎样的？

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 80 余项。

WAPI 标准体系由无线网络安全标准化工作委员会总体工作组（WG1）规划和更新维护，现行有效的标准体系文件已在 2022 年第

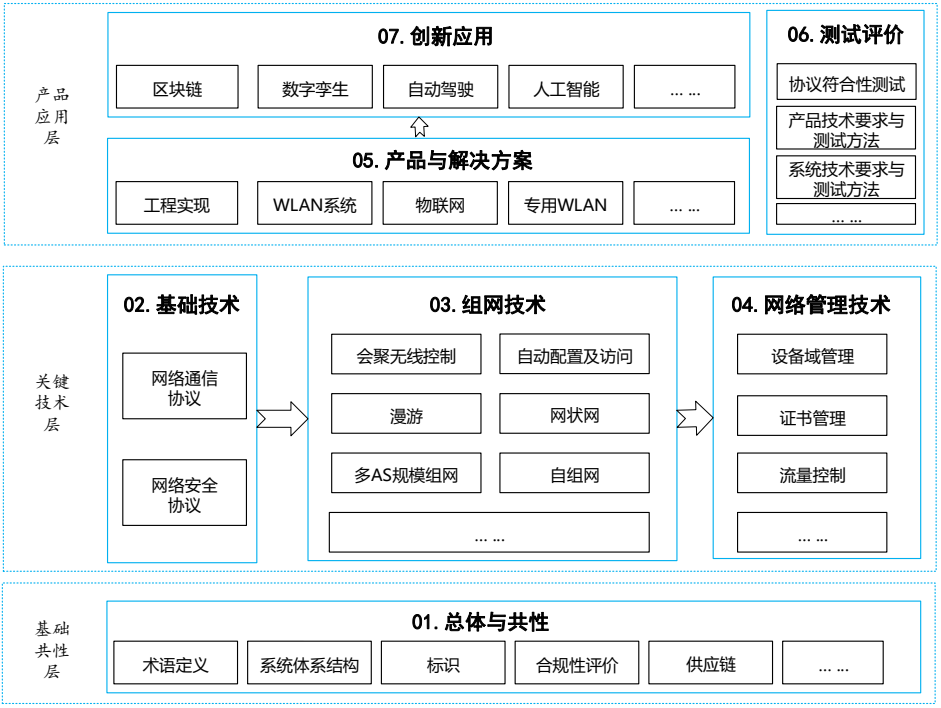
3 次标准工作会议上发布。

WAPI 标准体系价值链见下图。



返回目录

WAPI 标准体系架构见下图。



47. 问：每项团体标准中都要有标准必要专利吗？

答：不是。

团体标准中可能存在标准必要专利，但不是每一项标准都包含标准必要专利。本联盟鼓励创新和技术进步，鼓励标准和专利融合，

已依据《中华人民共和国标准化法》、《中华人民共和国专利法》和《国家标准涉及专利的管理规定（暂行）》等相关法律、法规、标准和规章，发布了知识产权政策，提出“参与标准制修订的组织或个人应尽早向联盟标准化部披露自身及关联者拥有的标准必要专利，宜尽早披露其所知悉的他人（方）拥有的必要专利”等相关要求，用以保护社会公众和专利权人及相关权利人的合法权益，保障 WAPI 产业联盟标准的有效实施。同时，在联盟团体标准的引言中，会披露该标准可能涉及的专利信息。

48. 问：如果正在制定的团体标准中涉及到了专利，应当如何操作？

答：以 WAPI 产业联盟为例：

在团体标准制定过程中，联盟遵守《国家标准涉及专利的管理规定（暂行）》（2013 年 12 月 19 日，国家标准化管理委员会、国家知识产权局发布）和 GB/T 20003.1—2014 的规定，主张公平有序的知识产权处置，提倡企业之间依据市场规律处置相关事务。联盟秉持中立原则，不对标准涉及专利的真实性、有效性和范围持有任何立场；不涉足评估专利对标准的相关性或必要性；不参与解决有关标准中所涉及专利的纠纷等。

参与该项团体标准制修订的单位和个人，有义务尽早披露其拥有和知悉的标准涉及专利。

同时，联盟也鼓励利益相关方以及未直接参与该项团体标准制修订的单位和个人，尽早披露其拥有和知悉的标准涉及专利。如团体标准中的某些内容涉及到专利，专利信息披露者（个人/单位）可随时联系联盟，填写《必要专利信息披露表》和《必要专利实施许可声明表》并签字/盖章后报联盟备案。联盟将在团体标准文本从当前阶段到正式出版的“引言”中给出相应说明。

49. 问：WAPI 产业联盟团体标准的作用和特点是什么？

答：作为市场自主制定标准，WAPI 产业联盟组织制定的团体标准是形成“安全无线局域网”的关键基础，是对政府颁布标准（国家标准、行业标准）的重要补充。

（1）2021 年 10 月，中共中央、国务院印发《国家标准化发展纲要》，2022 年 7 月，国家市场监管总局等印发《贯彻实施〈国家标准化发展纲要〉行动计划》，要求“优化标准供给结构。充分释放市场主体标准化活力，优化政府颁布标准与市场自主制定标准二元

结构，大幅提升市场自主制定标准的比重。大力发展团体标准，实施团体标准培优计划，推进团体标准应用示范，充分发挥技术优势企业作用，引导社会团体制定原创性、高质量标准”。

（2）WAPI 产业联盟自 2006 年 3 月成立起，即与工信部宽带无线 IP 标准工作组、国际标准组织 ISO/IEC JTC 1/SC 6 国内技术对口单位形成了 WAPI 标准产业共同体，除按国家标准计划要求完成相关国家标准、行业标准的起草外，也积极探索开展了市场自主制定标准——联盟标准的组织制定工作，对国家和行业标准的实施起到重要的支撑作用。2015 年 5 月，国家标准委批准 WAPI 产业联盟成为开展团体标准的首批试点单位之一。

（3）WAPI 产业联盟的团体标准制修订过程完全公开，任何感兴趣的单位都可以报名参加，做出技术贡献或者只是提出疑问。标准征求意见阶段，主流产业链厂商都会被通知到，确保最终发布的标准符合各方一致意见和利益。

（4）在 WAPI 产业联盟组织下，持续推动 WAPI 的技术演进和标准化，截至 2025 年 11 月已形成了包括国家标准、行业标准、团体标准和国际标准在内的 89 项 WAPI 标准体系。

50. 问：WAPI 产业联盟在团体标准转化方面有何经验和成果？

答：在国家标准方面，2023 年 8 月 18 日国家标准化管理委员会发布了《推荐性国家标准采信团体标准暂行规定》，结合我国现有推荐性国家标准和团体标准特点，在推荐性国家标准工作机制基础上，畅通渠道、简化程序、缩短时间，规范了国家标准采信团体标准的程序。目前 WAPI 产业联盟的团体标准已被 21 项国家标准采信。

在行业标准和企业标准方面，联盟认为：团体标准的核心在于“用起来、活起来”。在日常工作中，联盟会协调相关市场主体共同制定满足市场和创新需要的团体标准，由本团体成员约定采用或者按照本团体的规定供行业、企业自愿采用；或基于联盟团体标准，为行业标准企业标准提供必要的支持和服务。

例如：目前《关键信息基础设施无线局域网系列团体标准》及其它多项联盟团体标准已转化成为行业标准或企业标准，包括但不限于：《南方电网 WAPI 无线局域网技术规范》《南方电网 WAPI 无线局域网综合管理系统技术规范》《南方电网 WAPI 无线局域网接入控制器北向接口技术规范》《铁路基础设备设施监测检测数据通信技术要求 专用无线网络承载技术要求》等。

51. 问：如何参与 WAPI 产业联盟团体标准的制修订？

答：标准化工作的成功，很大程度上取决于现实中不同供应商技术洞察和实现的经验能反馈到标准制定过程中。WAPI 产业联盟欢迎任何单位和个人加入到标准产业协同创新中来，并不遗余力地创造和维护公平、公正、公开的技术贡献和评议机会。

WAPI 产业联盟团体标准的制修订过程完全公开。首先，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协商一致。

52. 问：如何申请参与 WAPI 产业联盟团体标准项目工作？

答：以单位名义和个人名义，均可以申请参与联盟团体标准项目工作。

以单位名义申请参与项目工作的，须填写《项目参与单位申请表》并加盖本单位公章，每家单位参与人数原则上不超过 3 名。

以个人名义申请参与项目工作的，须填写《项目参与专家申请表》并由专家本人签名，由推荐单位加盖公章。

根据联盟标准化管理要求，申请方须将纸质盖章/签名原件交付联盟标准化部。

53. 问：专家个人，是否可以成为无线网络安全标准化工作委员会委员，参加 WAPI 标准制定工作？

答：可以。

无线网络安全标准化工作委员会（WNSSC）是在无线网络和网络安全专业领域内，从事标准起草、技术审查、标准实施等标准化工作的技术组织，负责 WAPI 产业联盟团体标准的制定、发布、实施，推动团体标准被国际、国外、中国、行业以及其他团体标准的采用和引用，具有最广泛的代表性。标委会由委员组成，委员分单位委员和专家委员两类，来自生产者、经营者、使用者、消费者、公共利益方等相关方。WAPI 产业联盟和标委会欢迎关注和支持无线网络和网络安全技术、标准、产业发展的组织和个人参加标准制定和实施工作，并对他们开放。

关注 WAPI 技术、标准、产业的专家个人，可以通过如下方式申请加入标委会：（1）所在机构是联盟会员的，可由所在机构提名为

单位委员或专家委员；（2）所在机构不是联盟会员的，可由联盟会员单位推荐为专家委员。

54. 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，会上传至全国团体标准信息平台（http://www.ttbz.org.cn/），提供在线阅读服务。此外，会员单位可凭会员账号/密码在联盟网站“标准资料”栏目(http://www.wapia.org.cn/Down/Standard/list.shtml)下载标准文本。

55. 问：联盟正在建设的高质量安全无线局域网标准体系，其发展背景和进展情况是怎样的？

答：19 年来，WAPI 产业联盟组织会员单位，并与其他标准化组织协同，以 GB 15629.11 系列国家标准为基础，构建了完整的基

于 WAPI 的无线局域网国家、行业、团体、企业标准体系，对安全无线局域网产品和系统，及其在关键信息基础设施的应用均给出了要求。WAPI 标准体系在产品研发、检验检测、认证认可、产业应用等环节得到了广泛采信和实施，对规范、引导和服务市场起到重要作用。

当前，在满足提供基本的安全无线局域网连接需求的基础上，如何建设和运行高质量的安全无线局域网，成为安全无线局域网产业链各方的共同需求，包括产品提供者关心自己研发的产品是否有“高质量”，网络建设者关心使用的产品和建设过程本身是否有“高质量”，网络运营者和网络服务提供者关心自己网络运行的状态，以及提供的网络服务是否有“高质量”。所有网络利益相关者追求“高质量”的目标，是希望自身的产品、系统和服务的质量可被显性识别，从而更好满足客户和发展需求，赢得市场先机。这也是建设“高质量安全无线局域网”标准体系以满足上述需求的出发点。

针对上述需求，联盟和无线网络安全标准化工作委员会分析了在现有 WAPI 标准体系基础上，过渡和发展到高质量安全无线局域网标准体系的演进路径，提出了高质量安全无线局域网的范围、内涵、要求，并且立项了一项基础共性团体标准《高质量安全无线局

域网 总体要求》，将给出高质量安全无线局域网的基本定义、总体架构、所涉及对象的基本要求和高质量指标体系，该标准已进入报批阶段，计划于 2025 年 12 月正式发布。

56. 问：最新发布的联盟团体标准《无线局域网安全技术规范 第 1 号修改单》，其项目目标是什么？

答：2021 年，WAPI 产业联盟发布了团体标准 T/WAPIA 046—2021《无线局域网安全技术规范》。这是中国无线局域网业界面向量子时代的网络安全需求，结合适配通用商密算法 SM2、SM3 需求，使用更高性能密码套件 WPI-SM4-GCM，满足身份保护需求和逐步应对潜在量子计算攻击威胁，继承既有安全技术架构的安全功能和属性，新增抗离线字典攻击的安全特性，为向量子安全时代过渡的安全无线局域网产品提供架构及协议支持的新贡献，使得安全无线局域网技术标准体系得到新的发展。

伴随产业界对 T/WAPIA 046—2021 应用实施的不断深入，在产品开发和产业实施过程中，联盟成员针对规范中 WAI 增强协议的封装和承载的以太类型字段提出了修订需求。希望结合当前产业现状，进一步降低技术演进升级的投入，将芯片等硬件系统设计升级的工

作减至最少。

为提供更便捷的技术升级路径，标委会于 2024 年 9 月立项了《无线局域网安全技术规范 第 1 号修改单》,对 T/WAPIA 046—2021 中 WAI 增强协议中的封装格式和以太类型字段等内容进行修订，以指导厂商更快速地实现高安全等级的产品，并为相关的检测活动提供规范。

57. 问：2025 年修订发布的联盟团体标准《管理帧保护技术规范》，其项目目标是什么？

答：WAPI 产业联盟于 2012 年发布 T/WAPIA 010.3《管理帧保护技术规范》，通过加密与完整性校验机制为关键管理帧保驾护航。2020 年，联盟结合产业实践与技术发展，启动标准修订工作，扩大管理帧保护范围，细化针对不同无线局域网络及管理帧类型的保护策略，并于 2021 年发布修订版标准。

近年来，随着技术应用的深化，业界对管理帧中的信标帧安全保护的需求日益凸显。为完善 WAPI 标准体系，联盟于 2024 年 4 月再次启动修订项目，并于 2025 年 7 月正式发布新版《管理帧保护

技术规范》，重点强化信标帧安全策略协商机制、完整性保护能力及集合组播密钥通告协议设计等，不仅显著提升了无线局域网产品安全防护水平，还优化了密钥建立协议效率。

58. 问：最新发布的联盟团体标准《无线局域网产品工程化实现指南 第 11 部分：WAPI 与 IEEE 802.11be》，其项目目标是什么？

答：2025 年 7 月，WAPI 产业联盟发布《无线局域网产品工程化实现指南第 11 部分：WAPI 与 IEEE 802.11be》团体标准。该标准的发布，是对《无线局域网产品工程化实现指南》团体标准的更新完善，将助力安全无线局域网产品在支持超高吞吐量和低延迟的同时，更有效地兼顾安全性与高效性，通过多链路传输技术增强复杂网络环境下的兼容性与稳定性，提升抵御网络攻击能力，为用户提供更安全、稳定、高速的无线连接体验。

无线局域网技术在全球范围内发展至今 20 多年，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）三个层面的技术，构成了无线局域网本身的技术体系。全球 WLAN 技术体系，在数据和管理层面具有相对统一的技术架构，但在安全层面仅有两条路线：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；另一个是中国主导发展的 WAPI 技术。

结合无线局域网技术演进，在符合 GB 15629.11 系列国家标准、采用 WAPI 安全协议保障无线局域网安全的基础上，确保应用 IEEE 相关物理层增强规范时，持续实现 WLAN 产品在数据和管理层面统一技术架构和互通性，WAPI 产业联盟组织制定并发布了《无线局域网产品工程化实现指南》系列团体标准，给出技术规范。目前该系列已发布的标准还包括：

（1）T/WAPIA 007.1《无线局域网产品工程化实现指南 第 1 部分：WAPI 与 IEEE 802.11n》

（2）T/WAPIA 007.2《无线局域网产品工程化实现指南 第 2 部分：WAPI 与 IEEE 802.11e》

（3）T/WAPIA 007.6《无线局域网产品工程化实现指南 第 6 部分：WAPI 与 IEEE 802.11p》

（4）T/WAPIA 007.8《无线局域网产品工程化实现指南 第 8 部分：WAPI 与 IEEE 802.11ac》

（5）T/WAPIA 007.9《无线局域网产品工程化实现指南 第 9 部分：WAPI 与 IEEE 802.11ad》

（6）T/WAPIA 007.10《无线局域网产品工程化实现指南 第 10 部分：WAPI 与 IEEE 802.11ax》。

59. 问：正在修订的联盟团体标准《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》系列团体标准，项目目标是什么？

答：2021 年，系列团体标准 T/WAPIA 045《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》获得发布。该系列标准规范了实体鉴别与密钥管理的融合技术，基于国家/国际标准规范的三元对等安全架构，具备身份保护能力、抗字典攻击能力等，促进了网络安全连接技术在有线局域网、无线局域网、近场通信、射频识别、移动通信、TCP/IP 等基础通信网络中的规模部署和应用实施。

量子计算、区块链等新技术的快速发展和演进，对现有的鉴别与密钥管理技术体系提出了新挑战和新需求。针对上述，无线网络安全标准化工作委员会于 2024 年 11 月立项了《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》系列标准（修订），该项目欢迎所有联盟成员单位、标委会委员和社会公众积极参与。

60. 问：正在制定的联盟团体标准《信息安全技术 数字证书管理 第 3 部分：证书颁发》和《信息安全技术 数字证书管理 第 4 部分：证书撤销》，其项目目标是什么？

答：2024 年 8 月 14 日，无线网络安全标准化工作委员会批准《信息安全技术 数字证书管理 第 3 部分：证书颁发》和《信息安全技术 数字证书管理 第 4 部分：证书撤销》立项，该 2 项标准将规范 WAPI 证书颁发和撤销技术，旨在减少因证书管理不当而引发的安全风险，提高网络通信的安全性和稳定性。

其中，《信息安全技术 数字证书管理 第 3 部分：证书颁发》将规范证书在线颁发、自动更新的技术实现，通过自动化管理流程，实现证书到期前的自动检测、生成、分发和更新，保障在自动更新过程中数据的完整性和机密性。

返回目录

《信息安全技术 数字证书管理 第4部分：证书撤销》将确保无线局域网中的证书撤销机制能够有效组织被撤销证书的继续使用，防止未授权访问、数据泄露等安全威胁；通过减少撤销过程中的计算量和传输开销，提高撤销效率；保障WAPI证书撤销机制能够与其他安全协议和标准兼容，促进不同设备和系统间的互操作性，为安全无线局域网提供更灵活和广泛的安全支持。

61. 问：正在制定的联盟团体标准《应用于抽水蓄能领域的 WAPI 终端电力物模型》，其项目目标是什么？

答：随着电力行业的数字化、智能化、智慧化发展，在业务通信领域面临着高安全性、大带宽、高度移动性以及大规模连接等需求与挑战。抽水蓄能作为能源行业重要的储能和调节手段，对电力系统的稳定运行起着至关重要的作用。但目前在抽水蓄能领域存在物模型不统一的情况，不同厂家设备的数据结构、信息表示和通信协议存在差异，导致信息交互与数据兼容性差，容易出现信息解析错误。此外，由于缺乏统一的信息表达，严重制约了电力物联网系统间的高效协同。

本次立项的《应用于抽水蓄能领域的 WAPI 终端电力物模型》，

从基本信息、技术参数、量测参数等维度，规定了抽水蓄能领域 WAPI 终端在电力物模型中有关通信能力和量测方面的基础信息模型，用于支撑各物联网 WAPI 终端信息在业务应用、物联网平台、智能网关之间的交互应用。

该项目将有助于实现抽水蓄能领域 WAPI 终端在电力物模型层面的无缝对接，通过统一的信息表达提高系统的兼容性和互操作性，为抽水蓄能电力系统的规划、建设、运营和管理提供规范支撑，保障行业的健康有序和可持续发展。

【第三部分 产品与工程化实现】

62. 问：目前符合 IEEE 802.11ac、802.11ax 等更高速率集的 WLAN 产品依据什么标准支持 WAPI？是否已有成熟产品？

答：符合 802.11ac、802.11ax 等更高速率集的 WAPI 产品，依据的是联盟团体标准 T/WAPIA 007.8《无线局域网产品工程化实现指南 第 8 部分：WAPI 与 IEEE 802.11ac》和 T/WAPIA 007.10《无线局域网产品工程化实现指南 第 10 部分:WAPI 与 IEEE 802.11ax》。

市场上已有许多产品支持了上述标准。因为 WAPI 产业链通常由上游芯片厂商提供技术供给，所以大多下游设备厂商无须自己从零开始对照标准开发产品，可以无障碍地推出符合标准的最终用户产品。

63. 问：笔记本电脑如何升级支持并启用 WAPI？

答：目前主流 WLAN 芯片均已具备 WAPI 安全能力，笔记本电脑厂商可以通过软件升级支持让用户选择使用 WAPI 功能。具体方式是：笔记本厂商发布对应机型的支持 WAPI 的安装包，用户进行安装

后，即可以使笔记本具备 WAPI 安全服务能力，无需更换硬件。

据不完全统计，戴尔、惠普等笔记本厂商均发布过此类安装包。

64. 问：对于瘦 AP 厂商来说，将瘦 AP 升级至支持 WAPI，需要投入多少研发人员，多长时间？

答：WAPI 的标准和相关算法都是公开的，任何厂商均可按照标准开发产品，也可以选择与有开发经验的厂商合作。据了解，在成熟的瘦 AP 产品上增加 WAPI 功能，投入 2-3 人约 1-3 个月可完成升级。

65. 问：工业场景下瘦 AP 是否需要集中转发功能？

答：在电力等工业场景中，瘦 AP 通常不需要集中转发功能。原因是：工业现场对实时性和本地化处理的要求较高。

集中转发会将所有数据流量汇聚 AC 进行处理，可能增加网络延迟并影响实时系统的性能。而工业场景中的数据传输通常需要在本地快速处理，例如设备状态监控、传感器数据采集和自动化控制

等，因此瘦 AP 在工业网络中更倾向于采用本地转发模式，直接将数据发送到本地服务器或边缘计算设备，以确保低延迟和高可靠性，满足工业物联网（IIoT）的需求。

66. 问：为什么“把鉴别器实体（AE）实现在 AC 上”是不合理的？

答：在 WLAN 集中控制模式下，AC 负责集中控制 AP，AP 和 AC 协同实现 STA 的接入和管理。在这种集中控制模式下，理论上 AE 既可以完全驻留在 AP 中，也可以完全驻留在 AC 中，两种方式均可实现 WAPI 鉴别和保密的完整过程。

但在产品工程化实现上，出于保障加解密性能等目的，加解密过程必须在 AP 上实现，因此，将 AE 完全驻留在 AC 中（WAPI 鉴别和保密的完整过程都在 AC 上实现）实际是无法实现的。

当前，有些厂商把 AE 的鉴别功能在 AC 上实现，把保密功能在 AP 上实现，这就意味着要在 AC 与 AP 之间传输加解密密钥，也因此引入了新的安全风险。

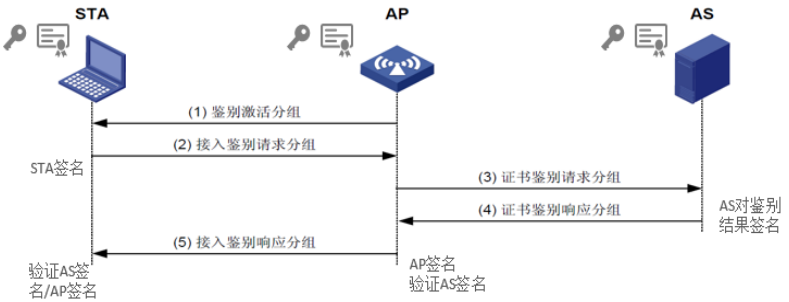
针对上述，最合理的方式是：AE 要完全驻留在 AP 中，WAPI 鉴别和保密的完整过程应完全由 AP 实现。具体详见《WAPI 市场应用

洞察报告——瘦 AP 组网架构下的 WAPI 产品工程化实现与部署》。

67. 问：WAPI 协议“五次传递”具体传递的是什么信息，会传递密钥吗？

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

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



返回目录

68. 问：WAPI 鉴别过程需要传输私钥吗？会传输公钥吗？

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

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

69. 问：WAPI 数据加解密传输过程中需要使用公钥/私钥吗？

答：不需要。

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

70. 问：为什么要协商加解密密钥？直接用公钥/私钥加解密数据可以吗？

答：不可以。原因是：

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

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

71. 问：加解密密钥多久会更新一次？密钥更新过程中还需要再次鉴别吗？

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

（2）密钥更新需要重新进行身份鉴别。密钥更新过程不会引起通信中断。

72. **问：适用于物联网场景的低功耗 WAPI 终端，例如电池供电的各种传感器设备/终端模组，现在有没有相关的产品和标准？实际功耗情况是什么水平？**

答：早在 2019 年，WAPI 产业联盟就关注到物联网低功耗 WAPI 模组的需求增长，并组织多家厂商进行了技术研发攻关。2022 年初首款 WAPI 低功耗物联网模组面世，它标志着打通了 WAPI 低功耗物联网场景应用之路。之后，多家厂商采用此类 WAPI 低功耗模组做出了各种物联网终端产品，例如：温湿度传感器、GIS 局放传感器、微水密度传感器、避雷器监测设备、可穿戴定位设备等等，让 WAPI 能更广泛地服务物联网和工业互联网场景。同期，联盟组织相关单位和专家制定并发布了《传感器类设备专用 WLAN 通信模块技术规范》团体标准。

目前此类模组休眠功耗约 10uA;上电/唤醒所需时间约 100ms，平均功耗约 60mA;发送业务数据时瞬间最大功耗约 180mA;一个“唤醒→连接 WAPI→建立 socket 连接→发送 2MB 数据→休眠”的周期，持续时间只要几秒钟；使用一块 1000mAh 的电池，按照每天发送 4 次数据的典型应用，可支持模组工作 1-2 年。

73. **问:据业界反馈,部分低功耗 WAPI 模组以及集成了低功耗 WAPI 模组的终端产品,产品设计和使用中存在密钥泄露的安全风险,对此联盟是否有解决方案?**

答:是的,WAPI 产业联盟对此高度重视,已有应对和解决方案,并逐步实施。

低功耗 WAPI 模组通常以单片机(MCU)为核心单元,算力和资源受限,这类产品无法像运行 Windows、Linux、Android 等操作系统的产品那样具备一定的软件安全防护能力。因此,针对低功耗 WAPI 模组,应采用具有符合国家密码主管部门批准算法能力的安全芯片对密钥进行安全存储、执行密码运算,让密钥产生、密码算法运算、密钥销毁等与 WAPI 协议实现紧密相关的基础要素工作在安全芯片内部完成,确保密钥不出安全芯片。

针对上述,联盟一方面向行业管理部门沟通示警,并加强对厂商的宣贯;另一方面,联盟测试实验室迅速开展了“WAPI 协议基础要素”测评能力建设,为市场和产业提供具针对性的测评支撑服务。详细情况,可联系联盟测试实验室:staff@wapia.org。

74. 问：联盟 2024 年 8 月推出的 WAPI 协议基础要素测评服务具体指什么？解决什么问题？测试对象是什么？

答：WAPI 协议基础要素测评服务用于：检验被测产品是否采用了具有符合国家密码主管部门批准算法能力的安全芯片，对密钥进行安全存储、执行密码运算，以及让密钥产生、密码运算、密钥销毁等与 WAPI 协议实现紧密相关的基础要素工作，是否在安全芯片内部完成，保证了“密钥不出安全芯片”的原则。

目前 WAPI 协议基础要素测评服务对象主要是：低功耗 WAPI 模组，以及集成了低功耗 WAPI 模组的终端产品。

75. 问：为什么 WAPI 协议基础要素测评主要针对低功耗 WAPI 模组？

答：低功耗 WAPI 模组以单片机（MCU）为核心单元，算力和资源受限，这类产品无法像运行 Windows、Linux、Android 等操作系统的产品那样具备一定的软件安全防护能力。如果低功耗 WAPI 模组不采用硬件安全芯片存储密钥、执行密码运算，软件存储、执行运算的密钥就非常容易被非法获取，会导致“非法设备获取合法身

份”，由此带来安全风险。

因此需要通过 WAPI 协议基础要素测评，检验低功耗 WAPI 模组是否采用了具有符合国家密码主管部门批准算法能力的安全芯片，对密钥进行安全存储、执行密码运算。

76. 问：厂商为什么要参加 WAPI 协议基础要素测评？

答：随着 WAPI 在各行业广泛应用，传感器、手持终端等类业务终端产品，大多通过集成低功耗 WAPI 模组快速具备了 WAPI 功能。但市场上有一部分低功耗 WAPI 模组以及集成了低功耗 WAPI 模组的终端产品，它们没有采用具有符合国家密码主管部门批准算法能力（包括国家密码管理局第 7 号公告发布的无线局域网专用商密算法 ECDSA、ECDH 的指定椭圆曲线和参数，SHA-256，以及通用商密算法 SM2/3/4）的安全芯片对密钥进行安全存储和执行密码运算，因此存在密钥泄露的安全风险，易导致“非法设备获得合法身份”。这种风险与 WAPI 安全协议技术本身无关，属于产品工程实现层面的问题，但却会影响用户整体使用方案的安全性，给行业网络带来安全风险。

厂商参与 WAPI 协议基础要素测评，可以验证产品是否采用了

具有符合国家密码主管部门批准算法能力的安全芯片对密钥进行安全存储、执行密码运算，避免密钥泄露、非法设备获得合法身份等安全风险，也为行业网络选用产品提供了参考和依据。

77. 问:现在被市场用户广泛关注的“硬件安全模块(安全芯片)”，是做什么用的？

答：硬件安全模块（安全芯片）可以进一步提升 WAPI 产品工程实现层面的安全性，它通常以安全芯片的物理形态存在，适用于对系统安全性要求更高的场景。

硬件安全模块（安全芯片）不同于通用的存储芯片，存储芯片属于操作系统软件调用范畴，仅提供数据存储保障。硬件安全模块属硬件安全技术范畴，不仅提供了密钥、WAPI 证书及敏感参数的安全存储环境，而且提供了 WAPI 所需密码算法独立安全运行环境。硬件安全模块能进一步提升 WAPI 产品的安全性和增加产品其他安全功能，为加强无线局域网设备的管理带来更多便利。例如：基于硬件安全模块，扩展实现对无线局域网设备的统一鉴别管理等等。

78. 问：为什么使用硬件安全模块（安全芯片）比纯软件方案在安全性上具有显著优势？

答：在物理安全性方面，硬件安全模块（安全芯片）采用物理防护机制（如防拆外壳、自毁电路），一旦检测到非法入侵（如物理拆卸、电压异常），会自动擦除敏感数据（如加密密钥），密钥生成、存储和运算均在专用安全芯片内完成，无法通过物理手段直接提取。而纯软件方案的密钥可能存储在存储芯片或内存中，易被物理攻击窃取。

在密钥安全性方面，硬件安全模块的密钥在其内部生成、存储和使用，始终处于加密或硬件隔离状态，永远不会以明文形式暴露在外部环境；软件中的密钥可能在内存、缓存、日志或临时文件中残留，易被恶意进程（如内存抓取工具）窃取。

在性能方面，硬件安全模块有专用硬件加速密码运算，处理加解密任务更快，不会占用主系统资源，这在单片机（MCU）等算力和资源有限的设备上很有意义。

此外，使用硬件安全模块也是网络安全等级保护等国家网络安全法律法规中明确要求的更高级别的安全措施。例如：等保国家标准 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

中“9.1.2.2 通信传输”明确要求“应基于硬件密码模块对重要通信过程进行密码运算和密钥管理”。

79. 问：为什么 WPI-SM4-GCM 密码套件可有效提升安全无线局域网产品性能？

答：随着安全无线局域网（WAPI）的大规模应用，面对海量的用户和海量的数据，对 WAPI 产品性能提出了更高的需求，包括：应使用更高效的密码套件 WPI-SM4-GCM。

此前市场中 WAPI 产品，其 WPI（无线局域网保密基础结构）部分大多使用的是 WPI-SM4-OFB+CMAC 密码套件。该套件需要将每一分组计算的输出反馈到下一分组计算的输入中，无法进行多分组并行计算，并且该套件仅提供加解密功能，数据完整性校验需结合 CBC-MAC 组件实现，性能虽能满足千兆网络需要，但不适应网络更高速率的发展。

WPI-SM4-GCM 是一种新增的密码套件，提供多分组并行加解密特性，可通过多核并行处理提升性能，提供加解密功能的同时还能提供数据完整性校验功能，无需结合额外组件，效率更高，满足万

兆网络或更高性能网络需要。

80. 问：WPI-SM4-OFB+CMAC（以下简称 OFB+CMAC）密码套件对应 WAPI 1.0 功能，WPI-SM4-GCM（以下简称 GCM）密码套件对应 WAPI 2.0 功能，这样理解对吗？

答：不对。

OFB+CMAC 密码套件与 GCM 密码套件是 SM4 加密算法的两种不同工作模式，它们既可用于 WAPI 1.0 功能，也可用于 WAPI 2.0 功能，而不是分别对应其中之一。

81. 问：WAPI AP 支持 OFB+CMAC 和 GCM 密码套件时，如何与 STA 协商确定单播密码套件和组播密码套件？

答：AP 和 STA 在建立安全连接前需要先进行安全策略协商，当 AP 和 STA 的 WAPI 安全策略同时支持 OFB+CMAC 和 GCM 时，在工程实现上，安全策略协商应遵循以下处理逻辑：

（1）若 AP 同时支持 OFB+CMAC 和 GCM 密码套件，可通过配置

WAPI 信息元素（WAPIE）通告多个单播密码套件,但组播密码套件只能通告一个；若优先考虑兼容性，则组播密码套件建议选择 OFB+CMAC。（通常 AP 在信标帧或探询响应帧中包含 WAPIE 字段，用于标识它支持的 WAPI 安全策略。）

（2）若 STA 和 AP 发现双方单播密码套件或组播密码套件没有相同项，则关联失败。

（3）若 STA 和 AP 发现双方单播密码套件均支持 OFB+CMAC 和 GCM，则应优先选择 GCM。

（4）若 STA 和 AP 发现 AP 支持 OFB+CMAC 和 GCM，而 STA 仅支持 OFB+CMAC，则应选择 OFB+CMAC；

OFB+CMAC 和 GCM 密码套件用于 WAPI 保密通信过程。2003 年 GB 15629.11 定义了 OFB+CMAC 密码套件，随着 WAPI 技术向更高速率的演进发展，2016 年发布的《WAPI 与 IEEE 802.11ac》团体标准中新增支持了 GCM 密码套件。

82. 问：在实现 WAPI 保密通信时，OFB+CMAC 和 GCM 两种密码套件在工程实现方面有哪些区别？

答：OFB+CMAC 和 GCM 在 WAPI 保密通信中提供了满足不同速率需求的数据保密性与完整性保护能力，为 WAPI 应用于多样化场景（如企业无线接入、工业控制、物联网等）提供了可灵活选用的安全方案，确保了网络通信在高效与安全之间的平衡。

OFB+CMAC 和 GCM 两种密码套件在工程实现方面，在密钥、初始向量（IV）、完整性校验码计算三方面有显著区别：

（1）使用 OFB+CMAC 时，应使用 2 个密钥，分别为加密密钥和完整性校验密钥；使用 GCM 时，仅使用 1 个密钥即可完成加密和完整性校验。

（2）使用 OFB+CMAC 时，IV 取值为 128 位（16 个八位位组）的数据分组序号（PN）值；使用 GCM 时，IV 取值为 128 位 PN 值的低 96 位。

（3）使用 OFB+CMAC 时，在计算完整性校验码时，若完整性校验数据的第一部分的长度或第二部分的长度不足 16 个八位位组的整数倍，则应分别在后面补零至 16 个八位位组对齐后，再参与完整

性校验计算；使用 GCM 时，在计算完整性校验码时，完整性校验数据的第一部分作为算法的附加认证数据（AAD）直接参与运算，不需要补零处理。

83. 问：使用 GCM 密码套件时，GCM-SM4 算法在计算 TAG 时已经包含了 PDU 数据的长度 L，AAD 数据构造是否还需包含 PDU 数据的长度 L？

答：需要。

使用 GCM 时，完整性校验数据的第一部分作为 AAD，具体字段包括帧控制（FC）、地址 1、地址 2、序列控制、地址 3、地址 4、服务质量控制、KeyIdx、保留和 PDU 数据的长度 L。完整性校验数据定义见《无线局域网安全技术规范 第 1 号修改单》标准的 6.5.3.1。

GCM 的特点是高效与安全并重，具备并行处理能力；WPI 使用 GCM 实现了加密与完整性保护一体化，使 WAPI 在高速通信环境下仍能保持强大的数据完整性与抗篡改能力。

84. 问：WAPI 中针对单播管理帧的保护与单播数据帧的保护，在实现处理方面有哪些异同？

答：相同点：使用相同的单播密码套件，即：均使用单播加密密钥、单播完整性校验密钥和 IV。

不同点：单播管理帧在完整性校验码计算时，帧控制（Frame Control）字段的位 4、5、6 参与完整性校验；单播数据帧在完整性校验码计算时，FC 字段的位 4、5、6 置 0，不参与完整性校验。上述处理方式与无线局域网国际标准所定义的方式一致，最大程度减少了厂商的开发工作量。

2025 年 7 月发布的新版《管理帧保护技术规范》标准，为 WAPI 安全无线局域网产品提供了清晰可操作的安全能力指引，增强了管理帧抵御仿冒、重放等攻击能力，提升了复杂环境下无线连接的安全性。

85. 问：在实现 WAPI 组播管理帧保护时，完整性校验数据如何处理？

答：通过对组播管理帧的协议数据计算完整性校验码（MIC），

实现 WAPI 组播管理帧的防篡改保护。参与完整性校验的字段包括帧控制、地址 1、地址 2、地址 3、MAC 管理协议数据单元（MMPDU）和管理 MIC 信息元素（MMIE）。其中，在计算前应将 MMIE 中的 MIC 字段置零，以确保校验结果的正确性。

使用 WPI-SM4-CMAC-128 时，若组播管理帧协议数据不足 16 个八位位组的整数倍，应在数据后面补零至 16 个八位位组对齐，补零后的数据作为完整性校验输入进行计算。

使用 WPI-SM4-GMAC-128 时，组播管理帧协议数据直接作为附加认证数据（AAD）参与完整性校验计算，无需进行扩展补零操作。

综上，针对组播管理帧的完整性校验机制，无论采用 WPI-SM4-CMAC-128 还是 WPI-SM4-GMAC-128，均在《管理帧保护技术规范》标准中进行了规范。该标准最新版本已于 2025 年 7 月发布，进一步强化了信标帧的安全策略协商机制、管理帧的完整性保护能力以及组播密钥通告协议的设计，显著提升了无线局域网产品的安全防护水平，优化了密钥建立与协商的效率。

【第四部分 市场建设与应用】

86. 问：如何理解“网络安全”？

答：《网络安全法》第七十六条规定，“网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。”

网络安全涵盖传统意义上的信息安全、互联网安全、通信安全、计算机安全等方面，包括互联网、通信网、计算机系统、自动化控制系统安全，同时包括这些网络和系统承载的应用、数据和信息内容的安全。

87. **问：网络安全法第十条规定，“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性”。执行过程中，如何保障上述在无线局域网领域的落地？**

答：法律是由全国人民代表大会及其常委会制定的规范性文件，是以国家强制力保证实施的规范体系。建设、运营的无线局域网及其提供的服务想要做到“安全”“合法”，应做到如下两点：

（1）确保选用的产品及工程建设符合标准

在无线局域网领域，支撑上述法律法规规章实施的技术标准包括：GB 15629.11 无线局域网国家标准（系列标准）、T/WAPIA 040 关键信息基础设施无线局域网技术要求（系列标准）、T/WAPIA 046《无线局域网安全技术规范》、T/WAPIA 047 无线局域网系统规范（系列标准）、T/WAPIA 048《信息系统无线局域网密码应用基本要求》以及 GB/T 22239 网络安全等级保护基本要求、GB/T 39786 信息系统密码应用基本要求等。在建设和运营无线局域网时，应采用符合上述标准的 WAPI 技术产品。

（2）无线局域网产品、系统和服务，均应通过规范检测

上述检测应严格依据标准并使用专业的检测工具实施检测，杜绝“简易测试”、“简化测试项”等不科学、不规范的检测和评估。检测依据的标准包括：GB/T 32420《无线局域网测试规范》、T/WAPIA 041 关键信息基础设施无线局域网测试方法（系列标准）、T/WAPIA 037.2—2021《无线局域网测试 第 2 部分：设备测试规范》等。

具体应实施并通过三个层面的检测或风险评估，包括：在产品采购前，开展产品型式检验：对拟采购的无线局域网产品，实施并通过 WAPI 标准符合性测试。在网络建设中，开展系统验收检测：对无线局域网系统，实施并通过系统工程竣工验收测试。在运行管理时，开展系统运维检测：对无线局域网系统，实施并通过安全服务状态测试。

88. 问：什么是关键信息基础设施？

答：依据《网络安全法》和《关键信息基础设施安全保护条例》规定，“关键信息基础设施，指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领

域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。需要在网络安全等级保护制度的基础上，实行重点保护。”

89. 问：在关键信息基础设施领域，为什么采购和使用 WAPI 产品合法合规，而采购和使用 Wi-Fi 产品、提供 Wi-Fi 服务涉嫌违法？

答：我国现行的法律体系，明确了在关键信息基础设施领域，符合 WAPI 技术标准体系的设备、系统和服务具有合规性，采购和使用 Wi-Fi 产品、提供 Wi-Fi 服务则涉嫌违法。

以《中华人民共和国网络安全法》和《中华人民共和国密码法》为例，说明如下：

（1）《网络安全法》第十条“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。”其中明确要求应依照国家标准的强制性要求—

—GB 15629.11 系列标准以及对应的测试标准是国家标准，其中 WAPI 安全协议是国家标准内容中的强制性要求，因此建设、运营 WLAN 网络如不采用 WAPI 则涉嫌违法；明确要求维护网络数据的完整性、保密性和可用性——GB 15629.11 系列标准是迄今为止全球唯一的、可保障 WLAN 网络达到上述三性要求的，不符合则涉嫌违法。

（2）《网络安全法》第二十二条“网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。”其中明确要求发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施——全球已经大量披露了 Wi-Fi 安全机制（包括 WPA2/WPA3）的安全缺陷，若不采取补救措施，仍在建设 WLAN、提供 WLAN 服务中使用 Wi-Fi 安全机制、提供 Wi-Fi 服务，涉嫌违法。

（3）《密码法》第二十七条“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密

码应用安全性评估。”其中明确要求关键信息基础设施应当使用商用密码进行保护——符合 GB 15629.11 系列国家标准即满足了使用商用密码进行保护的要求，使用 Wi-Fi 机制、提供 Wi-Fi 服务则不符合上述规定，涉嫌违法。

90. 问：目前等保标准中没有使用 WAPI 的具体要求，是否意味着在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。

91. 问：在行业无线网络部署中，选 WLAN 还是选 5G？

答：WLAN 和 5G 之间不是非此即彼的关系。但从实际建设和应用看，WLAN 较之 5G 专用网络，更符合行业应用工程“大带宽、大连接、移动性”的需求。

（1）WLAN 是现有行业专网的自然延伸，自建自营，独占网络资源，数据自己掌握，完全自主可控。

（2）在已部署有线网络/光纤的区域使用 WLAN 完成“最后一公里”覆盖，性价比非常高。一次建成后，可以不断承载新增业务。例如，电网变电站等应用场景的场地特性基本排除了外部同频干扰的可能，可在局部区域实现“饱和式”覆盖，网络连续性、安全性、性能冗余等目标可自主设计实现。

（3）相对而言，5G 专用网络无论是设备物理专用，或者是切片逻辑专用，本质上仍是“行业租用了运营商的服务”，行业难以达到真正的自主可控：行业 5G 专用网络中设备由运营商所有，由运营商运维；数据通过运营商，运营商做数据分析（注：原则上不查看用户数据内容，只看数据头用于分析业务质量，但存在未授权获知用户数据内容的可能）。

（4）目前阶段，WLAN 产业链成熟度高于 5G 专网，且建设费用和运维成本较低。我国 5G 正式商用时间还不长，尚未经受大流量、大连接、高可靠、低时延的充分考验，网络切片等大规模组网技术尚未充分验证。相比而言，WLAN 自 1997 年发展至今，最新一代速率可达数十 Gbps，技术不断演进、产业高度成熟、成本更低。

92. 问：如何判断一款产品是否已经支持了 WAPI？

答：对于无线电发射设备，如无线接入点（AP）、终端（STA）等产品，依据国家法律法规，上市前应取得《无线电发射设备型号核准证》。如果厂商在型号核准阶段申请测试了 WAPI 功能，在《型号核准证》“设备名称”一栏上会标注“WAPI”。

相关信息可登录工信部网站查询：https://zwfw.miit.gov.cn/miit/resultSearch?wd=WAPI&categoryTreePid=&categoryTreeId=313

对产品的标准符合性，以及多厂商间产品的互操作最优化性能，目前市场用户通常采用委托 WAPI 产业联盟测试或采信联盟测试报告的方式。

此外，国内多家检测机构也具备 WAPI 相关测试能力，市场用户也可采信这些机构出具的报告。主要机构包括：国家无线电监测中心检测中心、上海无委无线电检测实验室有限公司、工业和信息化部电子第五研究所、辽宁信鼎检测认证有限公司、江苏省电子信息产品质量监督检验研究院、广州通导信息技术服务有限公司、国家无线电频谱管理研究所有限公司、国家信息技术安全研究中心。

93. 问：市面上的无线局域网产品支持 WAPI 和 802.11i（Wi-Fi）双模能力情况如何？

答：目前，绝大部分终端（STA）和接入点（AP）均具备支持 WAPI 和 802.11i（Wi-Fi）双模的能力。

（1）无线终端具备 WAPI 和 11i 安全能力。比如国内的智能手机已同时支持 WAPI（WAPI-PSK/WAPI-Cert）和 11i（WEP/WPA/WPA2/WPA3）安全机制，使用无问题：无线终端在进入提供 WAPI 服务的网络时，无线终端会自动判断，弹出 WAPI 相应的界面来供用户操作。针对提供 11i 服务的网络，情况相同。当然，在一些行业无线终端应用情况下，行业网络运营者会有意屏蔽不安全的 11i 模式，不让行业无线终端去连接提供 11i 服务的无线接入点，以降低网络安全风险。

（2）无线接入点同时支持 WAPI 和 11i 也完全没有问题。支持 WAPI 的 AP，可以同时支持 11i，并且可以在一个 AP 上建立多个“虚拟 AP”，每个虚拟 AP 提供的是 WAPI 或 11i 安全服务是可以配置的，这些功能在市场上已非常成熟。

94. 问：WAPI 使用数字证书有哪些安全性优势？

答：安全性优势包括：

（1）强身份鉴别。

（2）防止中间人攻击。

（3）不可否认性。

（4）易于集中管理。

（5）易于网络规模的扩展。

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

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

答：有价值和意义。原因如下：

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

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

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

96. 问：启用 WAPI 的预共享密钥模式，是否对保障网络安全就已经足够了？

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

组合的字符同样很困难。

（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）。

97. 问：有些家用/餐厅/酒店的无线局域网采用的是口令方式（预共享密钥模式），适用于工业场景吗？

答：不适用。

（1）口令方式是所有网络用户共用一个密钥。口令极易外泄，并且无法追查。

（2）即使网络用户实施了一些违法违规行为，但因为使用的是同一口令，行为无法追溯到该用户。

口令方式面临的安全管理风险大、仅适用于满足短时间临时组

网的需求，是绝不能用于能源电力等工业场景的。

98. 问：在行业瘦 AP 应用场景中，AC 的部署位置怎样最合理？

答：在行业瘦 AP 应用场景中，AC 的部署位置（本地部署或远端部署）应取决于管理和业务的需求。

如果网络对实时性、低延迟和本地化控制要求较高（例如在需要快速响应的关键设备监控场景中），AC 应当选择本地部署，以减少网络延迟并确保业务连续性。再如：在大型变电站/换流站、大型仓库等业务相对独立，且本地具备运维人员的场景中，AC 也应当选择本地部署，以满足业务管理逻辑的完整性。

但在需要集中管理多个分散站点的场景中，远端部署 AC 则更为适合，可通过云端或数据中心实现统一管理和运维，降低管理复杂度并提高资源利用率。

因此，应结合业务和管理需求，灵活决定 AC 部署位置，采取本地部署或远端部署，而不应一味追求大型化、集中化。对业务相对独立的大型变电站/换流站、大型仓库之类的应用场景，建议采用小型化本地部署的 AC 产品（包括 AC、AS 一体化的产品）。

在本地部署的 AC，因管理 AP 区域集中、数量有限，暂不必过度关注与异品牌 AP 的互联互通。

99. 问：某分布式光伏场站，一款实验室测试合格、在变电站场景也工作正常的 AP/AC 产品，用户方反馈无线信号断断续续，WAPI 终端有时候连不上，感觉像是信号覆盖不足，这是什么原因？

答：无线通信的故障成因很复杂，不同的原因可能导致相似的症状，需要具体问题具体分析。

以本案例为研究样本，表象上是无线信号覆盖不足，但现场进行信号强度测试后却排除了该原因。经调查，该项目的 AP 部署在光伏场站，AC 部署在远端的主站，由于该光伏场站较为偏远，现场没有有线网络资源（如光纤等）可通主站，只能用 4G 网络与主站通信，即 AP 与 AC 之间的链路通过运营商 4G 网络连接，而地处偏远的光伏场站 4G 网络信号很差，从而导致 AP 与 AC 间通信极其不稳定，加之该项目所用的 AP/AC 其鉴别器实体（AE）错误的驻留在 AC 上，终端每次入网都需要连接主站的 AC，所以表现为终端经常连不上。

针对这种情况，可采用 AC 本地部署方式，避免 AP 与 AC 之间的链路不稳定导致终端入网失败。本案例也说明，应结合业务和管理需求，灵活决定 AC 部署位置，采取本地部署或远端部署。

100. 问：WAPI 应用解决方案工作组是做什么的？目前主要开展的项目有哪些？

答：2023 年，WAPI 产业联盟组织成立了 WAPI 应用解决方案工作组（以下简称方案组）。方案组的核心作用是：快速响应市场需求，组织产学研用协同开发针对各细分行业、细分应用场景的 WAPI 解决方案，支持高质量安全无线局域网建设和发展。

方案组属于联盟专项工作范畴，由联盟统一管理，方案组下设若干项目组。所有 WAPI 相关企业和用户单位，可随时向联盟秘书处申请参与现有项目组工作或发起成立新的项目组，为高质量安全无线局域网建设赋能。项目组运行期间，联盟给予充分的组织协作支持、企业间业务合作支持、公共技术服务支持、测试验证支持，为企业科技创新和技术研发提速，并择优向市场用户推荐 WAPI 解决方案和配套产品。

目前正在开展的项目包括：变电站 WAPI 应用解决方案、安全以太网解决方案、WAPI 网络业务隔离解决方案、基于 WAPI 的智能仓储解决方案、基于终端预置工程证书的 WAPI 证书在线管理解决方案等。

101. 问：变电站 WAPI 应用解决方案项目组的目标是什么？

答：该项目组聚焦电力行业用户“变电站”应用场景，聚合 WAPI 产业生态，为用户提供场景化解决方案，降低用户使用门槛、助力大规模数字变电站智慧应用。通过生态共创，形成变电站场景的 WAPI 能力集、输出场景化解决方案和《变电站 WAPI 生态图谱》。同时深挖场景需求、探索 WAPI 在变电站场景的更多应用潜力。

目前的应用场景包括但不限于：在线监测（设备的运行环境等状态监测）、远程巡视（安全监控、人员监控，包含巡检机器人、布控球、无人机）、运维管理（手持终端、智能安全帽）等。

102. 问：如何获得《变电站 WAPI 生态图谱》？

答：《变电站 WAPI 生态图谱》于 2024 年 6 月首次发布，并将持

续更新发布新的版本。《图谱》为国家电网、南方电网和地方电网公司等提供可快速落地的“菜单式”WAPI 建设方案。

您可登录 WAPI 产业联盟网站，在“重要通知”栏目下载：http://www.wapia.org.cn/Down/notify/default.shtml

103. 问：WAPI 网络业务隔离解决方案项目组的目标是什么？

答：通常行业网络会要求专网专用，满足网络安全隔离要求。当前，需要研究如何架构和部署 WAPI 网络，构建多个业务隔离的专网（即一张物理网络承载多个互相隔离的业务），实现不同业务的 WAPI 无线终端无法跨网“直接”访问。

该项目组以 WAPI 基础设施（含 WAPI 网络设备、AS 和 WAPI CPE/终端等）为核心，结合行业网络业务隔离的具体要求（如电力行业对安全Ⅲ区和安全Ⅳ区隔离要求），从部署结构、设备要求、网络管理等方面进行方案研究、验证环境搭建等，形成《WAPI 网络业务隔离解决方案》。

该方案实现了使用同一台 AS 完成不同安全区设备的证书颁发和接入鉴别；不同安全区共用同一套 AC+AP 的无线网络接入系统，

通过虚拟局域网（VLAN）隔离等技术实现了不同安全区无线终端专网专用。满足了行业通过一张 WAPI 物理网络承载多个互相隔离业务的应用需求。

104. 问：针对无线局域网系统工程，业内有无相应的标准体系和验收测评方法？

答：有。

T/WAPIA 047 无线局域网系统规范系列标准，在 GB/T 32420—2015《无线局域网测试规范》基础上，对无线局域网系统工程设计、工程施工、竣工验收等环节提供了规范要求和测试方法。其中，第 1 部分“工程设计”确立了适用于无线局域网系统的工程设计需要遵守的总体原则和相关要求；第 2 部分“工程施工”确立了适用于无线局域网系统的工程施工需要遵守的总体原则和相关要求；第 3 部分“验收测试方法”为无线局域网系统验收确立了可操作、可追溯、可证实的测试程序。

目前，WAPI 产业联盟测试实验室已经具备依据上述标准判断无线局域网系统工程建设是否合规的能力。

【第五部分 WAPI 检测与服务】

105. 问：WAPI 产业联盟测试实验室是政府机构吗？通过了工信部相关检测后，是否需要再到联盟实验室检测，两者有什么区别？

答：WAPI 产业联盟测试实验室是为产业链上下游服务的公共机构，所提供的测试服务是对工信部基础合规性检测的良好补充。

在 WAPI 应用建设中联盟发现，市场用户对 WAPI 检测有更高更精细的要求，需要检测的项目已远超基础合规性检测。为此，联盟持续跟进无线局域网技术创新和标准演进，持续更新并发布《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》，并依据最新版《测试项目》实施 WAPI 产品测试，为市场用户的 WAPI 采购、验收、监督检查等提供支撑。

相较于 WAPI 基础合规性测试，联盟测试具有更加贴合市场对产品的需求、测试项目更加全面准确、测试颗粒度更高、可依据市场要求定制化等特点。联盟出具的测试报告是当前市场用户 WAPI 建设的重要采信依据。

106. 问：在 WAPI 产业联盟通过测试的产品，送工信部认证的时候可以直接引用联盟的测试报告吗？

答：联盟测试不能代替行政许可合规类测试。对于厂商来说，委托联盟测试主要有以下三方面好处：

（1）WAPI 产业联盟的测试项目已完全覆盖 WAPI 合规类测试，在联盟测试通过的产品技术上完全满足 WAPI 合规类测试要求。

（2）目前行业用户 WAPI 建设中，通常会采信 WAPI 产业联盟出具的测试报告。因此通过联盟测试并取得报告的产品，会更具市场竞争力。

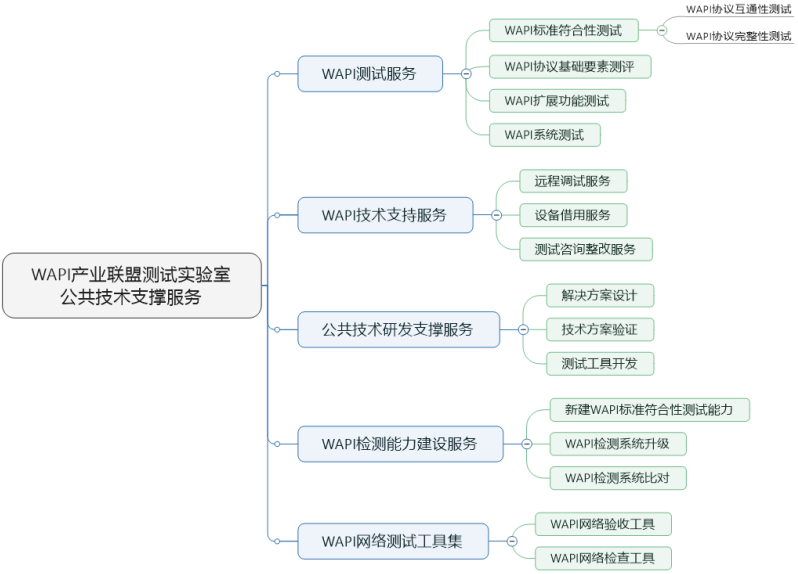
（3）WAPI 产业联盟测试服务的目的是“以测促建”。通过测试，完善产品性能、提升产品质量。在测试过程中，帮助厂商快速定位技术问题，协助厂商完成产品整改。

107. 问：WAPI 产业联盟测试实验室的定位是什么，能提供哪些服务？

答：WAPI 产业联盟测试实验室（以下简称联盟测试实验室）是公平、公正的第三方公共技术支撑服务平台，十余年来持续为产业

群体提供与 WAPI 技术、标准、产品和应用相关的公共技术支撑服务，满足市场和企业不同阶段的需求，解决“厂商和市场用户想做、做不了、但又迫切需要有人做”的技术产业难题。联盟测试实验室开展的公共技术支撑服务具有紧密贴合市场需求，服务专业全面，服务颗粒度精细，能够快速协助厂商完成产品整改等特点。由于自身公共社会组织特征和优质高效的服务能力，获得了产业上下游和市场用户的信任和认可。

目前联盟测试实验室围绕无线局域网鉴别与保密基础结构（WAPI）开展的公共技术支撑服务见下图。



返回目录

（1）WAPI 测试服务：包括 WAPI 标准符合性测试、WAPI 扩展功能测试和 WAPI 系统测试，用于检测产品之间的兼容性与互通性。

（2）WAPI 技术支持服务：包括远程调试服务、设备借用服务、测试咨询整改服务，帮助厂商在开发阶段验证 WAPI 接入功能，缩短产品研发周期。

（3）公共技术研发支撑服务：针对行业应用中的难点问题，提供共性关键技术研发支持、WAPI 应用解决方案设计、技术方案验证和测试工具开发等配套服务。

（4）WAPI 检测能力建设服务：面向市场用户、市场建设方和检测机构等，提供配套技术咨询与培训、WAPI 检测系统搭建、WAPI 检测系统升级、WAPI 检测系统比对服务等，以满足上述单位在 WAPI 检测能力建设方面的需求，满足在 CNAS 等资质能力认可、期间核查中的要求。

（5）WAPI 网络测试工具集：为用户方、建设单位提供 WAPI 网络验收工具和 WAPI 网络检查工具。

108. 问：目前有用户反馈，已取得联盟 WAPI 测试报告的产品在供货、建设、交付中出现了质量问题。有可能是什么原因造成的？如何加以防范？

答：联盟 WAPI 测试，均严格依据标准开展，并对被测样品保留每一个测试项数据包交互过程，做到可查询、可追溯。和其他检测机构一样，联盟出具的 WAPI 测试报告仅对被测样品负责。

针对用户反馈“取得联盟 WAPI 测试报告的产品，在供货、建设、交付中出现的质量问题”，经调研，可能出问题的环节和解决建议如下：

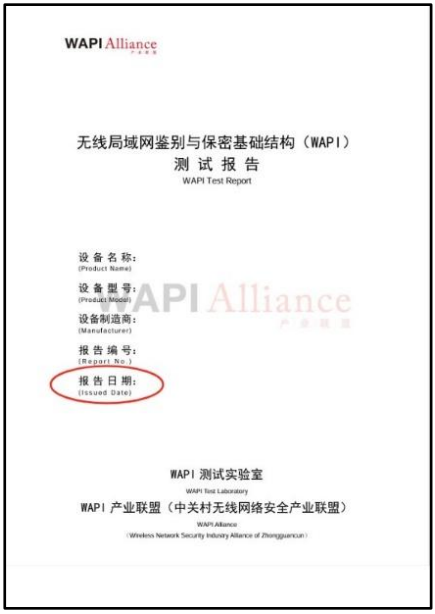
（1） 个别厂商 “同一型号产品，送联盟测试的样机与交付用户的产品不一致”。

针对此，建议：建设单位自建与 WAPI 产业联盟同等的 WAPI 检测能力。这样就可以在厂商供货、建设和验收阶段，随时检测/抽检供货产品是否和送测产品一致，并与联盟保持协同校验，保障供货产品一致性和质量。

（2） 厂商老型号产品未及时升级和检测，不满足市场应用新需求。联盟每年会根据市场需求，对《无线局域网鉴别与保密基础

结构（WAPI）功能测试项》进行增项、调整、升级，目前最新版测试项为：2025 年 4 月版。因此，拿 2022 年或之前更早版本测试报告去投标供货的产品，可能不能完全满足当下的建设和采购需求。

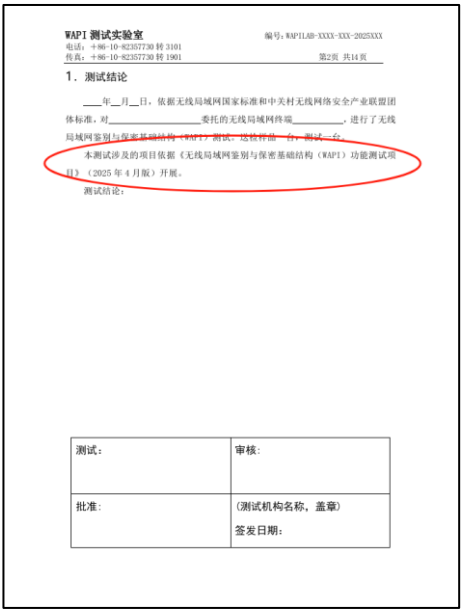
针对此，建议：持有 2022 年（含）之前测试报告的产品，如继续参与 2025 年（含）之后的 WAPI 建设，厂商须及时申请重新测试，测试通过后联盟将为其更换新版本测试报告。用户单位应关注厂商持有测试报告的出具日期（见封面）和测试项版本（见测试结论）。


WAPI Alliance

无线局域网鉴别与保密基础结构（WAPI）
测 试 报 告
WAPI Test Report

设备名称：
(Product Name)
设备型号：
(Product Model)
设备制造商：
(Manufacturer)
报告编号：
(Report No.)
报告日期：
(Issued Date)

WAPI 测试实验室
WAPI Test Laboratory
WAPI 产业联盟（中关村无线网络安全产业联盟）
WAPI Alliance
(Wireless Network Security Industry Alliance of Zhongguancun)


WAPI 测试实验室 编号：WAPILAB-XXXX-XXX-2025XXX
电话：+86-10-82357730 转 3101
传真：+86-10-82357730 转 1901 第2页 共14页

1．测试结论

____年__月__日，依据无线局域网国家标准和中关村无线网络安全产业联盟团体标准，对_____委托的无线局域网终端_____，进行了无线局域网鉴别与保密基础结构（WAPI）测试。送检样品 一台，测试 一台。

本测试涉及的项目依据《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》（2025 年 4 月版）开展。

测试结论：

测试：	审核：
批准：	（测试机构名称，盖章） 签发日期：

测试报告出具日期（封面）　　测试项版本（测试结论）

返回目录

（3） 厂商获得测试报告之后，又对产品进行了升级改造。任何硬件设计改动或软件版本升级，都有可能对既有功能产生影响。

针对此，建议：厂商在同型号产品升级改造后，进行重新测试。

109. 问：联盟测试实验室具备哪些无线局域网监测和风险评估手段？

答：为服务高质量安全无线局域网，联盟测试实验室依标为用户开发了 WAPI 全系列测评工具，包括：针对无线局域网产品的产品型式检验系统、针对无线局域网系统的工程验收检测系统、针对无线局域网服务的网络运维检查系统。

上述系统，符合 GB 15629.11、T/WAPIA 007 系列标准，并严格依据 GB/T 32420、T/WAPIA 037.2、T/WAPIA 041 等标准开展测评，支持市场用户在安全无线局域网产品选型、设计施工、工程验收、监督检查的全过程中，对产品和网络实施标准符合性、安全性、互联互通性测评。测评项目的种类、系统性、精准度均高于行政许可类检测。

110. 问：目前 WAPI 有哪几类测评工具，它们之间是否能够相互替代使用？

答：目前 WAPI 有三类测评工具，它们之间不能相互替代。

这三类 WAPI 测评工具，均有特定的适用范围，在适用范围之外的不当使用，会导致测试充分性不足、完整性缺乏、结论不可信、风险未获得正确评估等风险，埋下安全事故隐患。

三类 WAPI 测评工具的区别如下：

（1）针对无线局域网产品的产品型式检验系统——安全无线局域网（WAPI）协议检测系统。面向检测机构、市场用户、网络建设实施单位，对独立的 WAPI 产品（如：鉴别服务器、无线接入点、无线网卡等），集成或内置了 WAPI 模块的产品（如：手机、平板电脑、各类办公设备、无线行业机具、机器人等），提供 WAPI 功能的软件产品，进行标准符合性、协议完整性、互联互通性测试，验证产品是否全面符合国家标准要求、产品是否好用易用。本检测系统是实施行政许可类（如：电信设备进网许可）检测的必备工具，也是市场用户在 WAPI 产品选型环节用到的必要测评工具。

（2）针对无线局域网系统的工程验收检测系统——WAPI 网络

验收测试工具。主要面向网络建设单位和管理单位，是在 WAPI 网络建设完成后、正式投运前，在网络工程现场实施自动化随工测试、初步测试、试运行阶段测试、竣工验收测试等。核心是从“网络部署合规性、安全配置差异度、安全接入可用性、网络性能质量、网络设备安装工艺”等维度，去检查 WAPI 网络工程是否符合设计要求，评定网络建设的质量及相关功能、性能、可用性和安全性。

（3）针对无线局域网服务的网络运维检查系统——WAPI 网络检查评估工具。主要面向网络管理和运维单位，适用于对已投入运行的 WAPI 网络进行日常运维检查，以非介入式测试手段从网络部署合规性、安全配置差异度、安全接入可用性等方面，实时地判定网络的合规性、工作状态、是否存在安全隐患、与管理配置要求的偏离度等。尤其在应急故障排查时，能快速判断网络运行状态，快速定位问题、快速修复。

111. 问：联盟测试实验室的 WAPI 测试对象包括哪几类？

答：目前联盟测试实验室的 WAPI 测试对象主要包括：终端（STA）、无线接入点（AP）、鉴别服务器（AS）、证书签发服务器（CIS）四大类。

（1）STA 包括：移动终端、传统终端、物联网终端三大类。其中,移动终端指的是手机、PAD 等具备 WLAN 功能的移动类应用设备；传统终端指的是具有 WLAN 网卡的传统非移动类连网设备，如 PC、CPE 等；物联网终端指的是各类传感器、可穿戴设备、状态监测设备、车载设备等物联网设备。

（2）AP 包括：胖 AP（Fat AP）与瘦 AP（Fit AP）两类。其中，瘦 AP 需要接入控制器（AC）配合才能够实现无线接入点功能。在测试过程中，AC 是作为 AP 的辅助测试设备，不单独进行测试。

（3）AS 指的是：能提供 AP 和 STA 身份鉴别功能的服务器。

（4）CIS 指的是：提供对 STA、AP 和 AS 的证书签发管理的服务器。对于 AS 与 CIS 集成在一起的设备，分别按照 AS 和 CIS 测试项目进行测试。

112. 问：在 WAPI 测试中，是否会对接入控制器（AC）单独检测并出具测试报告？

答：不会对接入控制器（AC）单独检测，也不会单独出具测试报告。

原因是：在无线局域网网络部署中，仅瘦 AP 需要 AC 配合才能完成完整的无线接入点功能。由于 AE 只适合在 AP 上实现，AC 是作为辅助设备，所以既不会单独测试也不会出具测试报告。

目前联盟出具的瘦 AP 测试报告,有关 AC 的信息,如设备名称、型号、软件版本、制造厂商等，会在“支持或辅助设备描述”中予以体现,“附件（样品照片)”中也会展示 AC 的外观照片。

113. 问：目前联盟测试实验室有哪些 WAPI 测试项目？

答：联盟测试实验室依据 GB 15629.11 系列标准、GB/T 32420—2015《无线局域网测试规范》以及 WAPI 产业联盟团体标准，为产业市场提供 WAPI 标准符合性测试、WAPI 扩展功能测试和 WAPI 系统测试。

（1）WAPI 标准符合性测试：检验产品是否按照 WAPI 标准实现相关功能，包括：WAPI 协议互通性测试和 WAPI 协议完整性测试两部分。其中，WAPI 协议互通性测试主要测试产品实现 WAPI 协议的一致性和正确性，以及该产品与其他 WAPI 产品的互联互通性。WAPI 协议完整性测试主要检验产品所实现 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。

（2）WAPI 扩展功能测试：是除了 WAPI 标准符合性测试之外，各行各业在 WAPI 建设和应用过程中，所涉及其他功能的测试验证。目前主要包括：管理帧保护（单播）连通性测试、WPI-SM4-GCM-128 工作模式连通性测试、同一 ASU 域内 AP 间切换时延测试，等等……

（3）WAPI 系统测试：通过模拟实际应用环境，进行建设方案验证测试、设备间互联互通互操作测试、业务运行压力测试，为建设方案的可行性和提升用户体验提供保障。

114. 问：如何获得联盟测试实验室最新产品测试项？

答：WAPI 产业联盟依据 GB 15629.11 系列国家标准、GB/T 32420—2015《无线局域网测试规范》以及 WAPI 产业联盟团体标准开发的测试项目已达 300 余项，并根据市场建设需求保持动态更新。可联系联盟实验室获取最新版《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》，电话：010-82351181；邮箱：staff@wapia.org

上述测试项目，始终贴合用户高质量安全无线局域网建设需求，

具有严格依据标准、测试项目更全面、测试颗粒度更细、测试结果更精准、定制化程度更高、支持技术产品持续演进等特点。覆盖了对无线局域网终端（STA）、无线接入点（AP）、鉴别服务器（AS）和证书签发服务器(CIS)设备的 WAPI 协议互通性、WAPI 协议完整性、功能及性能测试。

目前国防、电力等用户单位在 WAPI 产品选型时，采用“委托联盟开展测试”或“直接采信联盟测试报告”的方式。

115. 问：相较 2024 年 3 月版《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》，2025 年 1 月版测试项目有哪些新增和变化？

答：《测试项 2501》重点增设了以下测试项目：

（1）对终端（STA）、无线接入点（AP）、鉴别服务器（AS）的 WAPI 2.0 功能测试；

（2）AP、STA 的 WPI-SM4-GCM-128 工作模式连通性测试；

（3）STA 的 WAPI 协议基础要素测评。

116. 问：目前联盟 WAPI 2.0 功能测试是如何开展的，和 WAPI 1.0 功能测试是什么关系？

答：目前联盟的 WAPI 2.0 功能测试和 WAPI 1.0 功能测试是并行开展的。

对于目前的送测产品，厂商可以选择以下三种模式中的任何一种（3 选 1）进行申请：

（1）仅支持 WAPI 1.0 功能；

（2）仅支持 WAPI 2.0 功能；

（3）支持 WAPI 1.0 功能和 WAPI 2.0 功能兼容模式。

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

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

（2)对于 AP，需要测试其能否支持两种模式的 STA 同时接入。

（3）对于 AS，需要测试其能否同时鉴别两种模式的证书。

118. 问：相较 2025 年 1 月版《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》，2025 年 4 月版测试项目有哪些新增和变化？

答：《测试项 2504》重点增设了“瘦 AP 模式下鉴别器实体（AE）是否完全驻留在无线接入点（AP）中”等测试项目。

119. 问：《测试项 2504》发布之日前通过测试的 AP 产品，如果已经实现了“AE 完全驻留在 AP 中”，还需要重新测试吗？

答：需要。

厂商通过重测获得联盟最新测试报告，更有利于满足市场建设采购需求，提升厂商在市场中的竞争力。

从支持厂商产品质量跃升、服务市场建设出发，联盟在启动“针对 AE 驻留位置启动 WAPI 瘦 AP 产品重新测试专项”时，已发布鼓励政策如下：

（1）2024 年 4 月 26 日至 2025 年 4 月 15 日期间通过联盟测试的 AP 产品（以签订测试协议的日期为准，下同），可以申请免费重新测试。

（2）2021 年 6 月 18 日至 2024 年 4 月 25 日期间通过联盟测试的 AP 产品，可以申请半价重新测试。

不满足上述条件的 AP 产品，按照新产品测试受理。

120. 问：委托联盟测试实验室开展 WAPI 测试需要那些流程？

答：相关流程如下：

（1）委托测试受理

第一、委托单位发起测试申请，致电或发送邮件：010-82351181，staff@wapia.org。

第二、委托单位填写《测试委托书》和《待测设备详细信息》，将文件邮件发送至：staff@wapia.org，进入审核流程。

第三、审核通过后，委托单位与联盟测试实验室签署《委托测试协议》。

（2）测试与整改

第一、联盟测试实验室收到送测设备和全部服务费用，进入设备测试环节，按约定时间完成相关测试工作（设备厂商须安排技术

人员现场协同)。

第二、如发生测试未通过项，涉及调试或整改，则测试周期顺延，直至完成所有测试项整改。

（3）出具报告

联盟测试实验室依据测试结果出具测试报告，委托单位可通过快递或自取的方式获取测试报告。

121. 问：在联盟 WAPI 测试中产品如有未通过项，整改后再次提交测试还要另行收费吗？

答：联盟测试实验室会针对测试未通过项目，提供未通过原因定位以及未通过项原始数据包交互日志信息等，协助厂商完善产品功能。

为兼顾测试平台的公共服务效率、减轻厂商负担，联盟测试实验室对整改周期不超过 1 个月、提交整改测试次数不超过 2 次的产品，不另行收费。

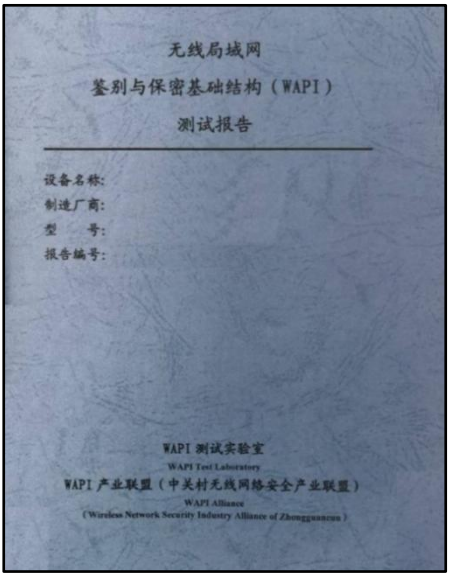
122. 问：通常委托测试受理完成后多久能拿到报告？

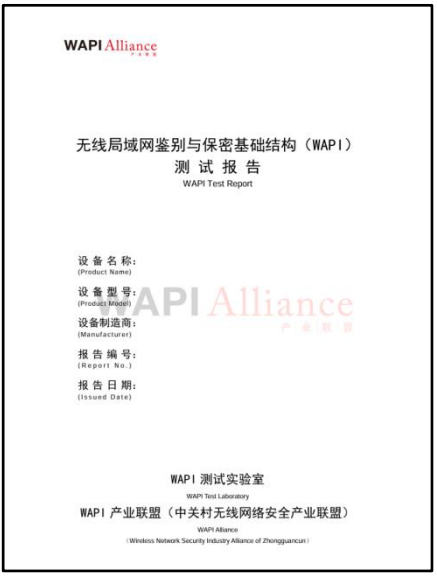
答：完成委托测试受理之后，在不考虑排期的情况下，通常一款设备在一周之内可完成测试并取得报告（如设备涉及整改，则测试周期顺延）。

如存在测试排期情况，联盟会员优先于非会员。

123. 问：依据 2025 年 1 月版（或之后版本）《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》测试并出具的报告，在辨识度上和之前有什么区别？

答：应市场采信要求，WAPI 产业联盟围绕视觉辨识度、防伪辨别等，对新旧测试报告进行了显著区分。依据 2025 年 1 月版（或之后版本）《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》开展测试的产品，已按新版出具测试报告。





旧版测试报告示例　　新版测试报告示例

124. 问：为什么有些网络搭建中采用了具备型号核准证书的 WAPI 产品，但在实际运行中却未达到预期效果？有什么解决办法？

答：一方面，伴随 WAPI 广泛服务各行各业，产品型号核准所涉及的 WAPI 互通性测试项目，不能完全满足行业 WAPI 规模建设和业务运行的发展需求，需在 WAPI 协议互通性测试、WAPI 协议完整性测试等方面，依据最新标准增加精细化测试项目。

另一方面，市场用户对 WAPI 的测评要求，大多已贯穿了“产品采购前、网络建设中、运行管理时”全阶段。伴随所处阶段的不同、检测场景的不同，对测评工具的要求也不同，之前传统形态和功能的 WAPI 合规性检测系统（工具）已不能满足要求。

综上，解决办法是：既要对 WAPI 产品进行更加精细化的测试，又要增加对 WAPI 网络功能性能的测试。

125. 问：为什么要开展 WAPI 协议完整性测试（俗称“负面测试”）？

答：WAPI 协议完整性测试是 WAPI 标准符合性测试中重要的组成部分。目的是检验产品所实现 WAPI 协议的健壮性，以及应用中是否能够正确处理异常协议报文等特殊状况。

据用户单位反馈，未通过 WAPI 协议完整性测试或者测试项目不完整的产品，在网络应用和提供服务过程中，会引发连接不稳定乃至网络瘫痪的风险，给用户方造成巨大的经济损失和影响。

开展 WAPI 协议完整性测试(负面测试) 能有效避免在网络部署完成后才发现因设备缺陷引起的互联互通故障：

（1）负面测试可以发现产品在 WAPI 协议实现上是否有潜在的

不完整，可以检查产品在一些特殊极端情况下的表现。打个比方来说，对于一辆汽车，踩油门前进，踩刹车停止，这是正向的测试项目。但如果同时踩下刹车和油门，会发生什么情况？是否“刹车优先”？这个测试就属于负面测试的范畴。

（2）WAPI 协议互通性测试是按照协议约定格式、字段属性构造、数据报文，对待测设备进行正确性、一致性检测。WAPI 协议完整性测试则包含 7 大类负面测试项目，分为异常 WAI 子类型、异常 WAI 头部字段、异常指定字段、异常完整性校验字段、异常 WPI 数据、异常组播密钥更新、异常 AE 签名属性字段。每一类分为若干项，每一项有一至两个测试用例。此功能旨在设计一簇“错误”的 WAPI 协议程序库，并通过发送这类异常的 WAPI 数据报文与待测设备进行 WAPI 鉴别和加解密处理的过程，从而甄别设备是否能正确处理异常情况的过程。

（3）负面测试还有助于设备厂商和行业网络建设方尽快定位设备的安全风险，并指导设备的开发优化。

126. 问：为什么“WAPI 简易测试”不可取？

答：“依据标准严格测试”是保障网络安全的基础和关键。采用专业的检测系统依标进行严格测试的产品，意味着更低的故障率、更低的运维成本、更好的用户体验。

所谓“WAPI 简易测试”，通常包括两方面：一是检测系统和工具不专业，二是简化测试项目。上述做法，仅能测试网络是否连接成功，无法保证检测结果的准确性、一致性和可靠性，也无法从协议层面去验证产品的标准符合性、健壮性。这种低质量产品一旦流入市场，会给网络质量和用户带来巨大的安全隐患。

围绕上述问题，WAPI 产业联盟已依据 WAPI 国家标准 GB 15629.11 系列、GB/T 32420—2015、WAPI 团体标准 T/WAPIA 007.1 系列和 T/WAPIA 037.2—2021，开发并持续更新《无线局域网产品鉴别与保密基础结构（WAPI）功能测试项目》，目前 2025 年 1 月版总计有 300 余项测试项目。此外联盟还开发了配套测试工具“安全无线局域网（WAPI）协议检测系统”，使用上述工具测试并通过了上述测试项目的产品，具有良好的符合性、互通性和兼容性。此外，联盟还面向检测机构、用户单位和有意向的企业提供 WAPI 检测系统能力建设服务。

127. 问：国标 GB/T 32420 已经规定了 WAPI 产品应通过的测试项目，团标 T/WAPIA 047.3 在实践中的意义是什么，能否把这个测试省去？

答：依据 T/WAPIA 047.3 开展的测试不可以省去。

GB/T 32420—2015《无线局域网测试规范》给出了符合 GB 15629.11（所有部分）的无线局域网系统的工程和设备的测试方法，促进了无线局域网设备测试技术的发展。

为进一步促进无线局网系统规范部署和应用，在 GB/T 32420—2015 基础上，制定了 T/WAPIA 047.3—2022《无线局域网系统规范 第 3 部分：验收测试方法》。内容上，T/WAPIA 047.3—2022 结合网络实际部署环境，新增了工程验收、工程终验等要求，提供了验收测试项目及结果记录表，为无线局域网系统验收确立了可操作、可追溯、可证实的测试程序。如果只参照 GB/T 32420—2015 测试，对现网环境的网络质量以及验收作业的规范性都无法保障。

128. **问：与已通过联盟测试厂商合作开发的同类型产品，为什么还有测试不通过的现象？**

答：无线局域网产品软件系统都比较复杂，任何修改，哪怕是看似与 WAPI 功能无关的修改，都有可能导致最终功能的瑕疵。例如页面的更换有可能导致证书无法正常导入和安装；新增的配置策略（黑白名单、VLAN、防火墙等）有可能导致数据的无法正常通信；软件版本的更新会导致密钥更新无法正常生效等等问题，都有可能引发某些测试项不通过。这也是为什么联盟测试实验室针对任何新型号的产品都需要重新测试，哪怕是同型号产品的迭代更新，也建议重新测试，以确认 WAPI 功能的正确和完整。

129. **问：不同型号的两款产品，只是外观不同，软硬件配置都一样，能否体现在一份测试报告中？或者仅测试一次直接出两份测试报告？**

答：以上均不可以。

联盟测试实验室的每一份测试报告，只对应一个型号的产品，产品照片等信息均会体现在报告中。依据联盟测试实验室的管理制

度，每一项测试，均会留存原始测试记录和全部流程记录，确保测试工作的可追溯性。

130. 问：已经通过联盟测试的产品，在升级迭代后仍使用原型号，是否可以继续使用原测试报告，或不经测试直接获得新报告？

答：不可以。

一是产品的任何软硬件修改，哪怕是看似与 WAPI 功能无关的修改，都有可能导致产品功能的瑕疵，因此升级迭代后需要重新测试。二是产品升级迭代后外观等特征可能发生了变化，原测试报告不再适用。三是联盟不断更新测试项目以保障最佳的 WAPI 功能和互通性，多年前的测试报告肯定不如新的测试报告全面。

此外，鉴于联盟测试实验室的每一份测试报告与产品型号均有一一对应关系，建议厂商委托测试升级迭代产品时，可以添加括号说明以区别于旧款，例如在型号后添加“（2025 款）”、“（第二代）”等方式。

131. 问：委托联盟开展 WAPI 测试期间，需要厂商技术人员现场支持吗？

答：推荐技术人员现场支持。

目前联盟测试实验室的 WAPI 测试对象涵盖了终端（STA）、无线接入点（AP）、鉴别服务器（AS）、证书签发服务器（CIS）四大类产品，测试时需要对设备进行相关配置。一方面，由于各厂商功能实现存在差异，配置命令等不尽相同，需要技术人员现场配置和必要操作；另一方面，有厂商技术人员在场，可以对测试过程中出现的问题以及测试未通过项第一时间处理和整改，提高测试效率。

132. 问：厂商的产品（设备）达到什么标准，可以纳入联盟测试床？

答：纳入联盟测试床的产品（设备）有严格的判定程序和依据，体现了厂商 WAPI 技术能力先进性和合规性。厂商的设备被纳入联盟测试床后，可以获得联盟专家团队更加高效技术协同，参与最新的 WAPI 技术开发，优先获得专业技术和测试资源等等。纳入联盟测试床的设备，首先必须通过联盟测试实验室 WAPI 标准符合性测试和扩展功能测试；其次，需要厂商开放该设备的相关配置端口，提

供相关驱动及说明文档。

133. 问：目前除了联盟测试实验室之外，还有那些机构能提供 WAPI 标准符合性测试服务？

答：随着各行各业采用 WAPI 技术产品实施本行业无线局域网关键信息基础设施，国内已有多家检测机构相继开展了 WAPI 检测能力建设，为产业和市场提供 WAPI 检测服务。

联盟测试实验室面向检测机构定期提供 WAPI 检测系统比对服务，保障检测系统的准确性、一致性、可靠性。

目前，已与联盟测试实验室完成至少一次比对的检测机构包括：

（1）国家无线电监测中心检测中心

（2）上海无委无线电检测实验室有限公司

（3）工业和信息化部电子第五研究所（中国赛宝实验室）

（4）辽宁信鼎检测认证有限公司

（5）江苏省电子信息产品质量监督检验研究院（江苏省信息安全测评中心）

WAPI 产业联盟会及时发布通过 WAPI 检测系统比对校验的机构名单，供厂商和用户单位参考。

134. 问：市场用户或市场建设单位，如果想要自建 WAPI 检测能力，联盟可以提供哪些支持？

答：（1）测试规范支持：一方面可配合建设单位提供已有 WAPI 相关技术规范和测试规范；另一方面可根据建设单位实际需求，合作制定特定领域的测试规范。

（2）测试工具支持：可根据建设单位实际需求，提供在安全无线局域网建设过程中，从产品测试到网络测试的三类测试工具。

（3）技术支持：WAPI 检测能力建设完成后，可根据建设需求和测试技术演进，提供技术支持和软件升级服务。

（4）其它支持：可提供技术/测试培训、实验室间比对等服务。

135. 问：比对是什么？哪些单位需要做 WAPI 比对？

答：在实验室计量术语范畴，比对指的是：在规定条件下，对

相同准确度等级的同类基准、标准或环境进行比较，考核量值的一致性。

实验室间比对通常指的是两个或多个检测机构（实验室），依据统一的条件，对相同或类似的测试样品实施测试之后，就测试的结果进行比对。当测试结果一致或差值在一定范围内，即为“满意”；当测试结果不一致且差值超出一定范围，即为“不满意”。

具备 WAPI 检测能力的检测机构、行业建设方、用户单位，应定期对 WAPI 协议检测系统、WAPI 网络现场测评工具进行比对，一方面为检测系统测试结果的可靠性和准确性提供保障，另一方面为上述机构获得和保持诸如 CNAS、CMA 等资质提供必要支撑。

136. 问：为什么比对服务需要联盟测试实验室来开展？

答：此前，在 WAPI 检测系统比对方面，没有合适的第三方机构开展相关服务，这项工作只能靠检测机构和检测机构之间相互完成，由于缺乏第三方“公平秤”性质的存在，公正性较弱，比对数据和报告在 CNAS、CMA 等资质能力认可、期间核查中效力不足。

十几年来，联盟测试实验室在公共技术支撑和服务中积累了丰

富的经验，技术能力、测试能力、组织能力获业界高度信任。更重要的是，联盟这类产业组织，既不是企业，也不是检测发证机构，具有天然的“公平、公正、第三方”公共服务属性和立场，最适合承担产业“公平秤”角色。因此联盟测试实验室在广泛调研和征求各检测机构意见的基础上，开展了公益性质的比对服务。

通过检测系统间比对，一方面可以判断和监控检测机构（实验室）的基建质量和持续能力，是这些机构（实验室）获得和保持诸如 CNAS、CMA 等资质的必要条件。另一方面也践行了国家鼓励联盟社会组织依据国家标准、团体标准去提高产品和服务质量。

137. 问：联盟测试实验室开展比对服务有哪些？

答：目前联盟测试实验室开展了 WAPI 协议检测系统比对服务、WAPI 网络现场测评工具比对服务，其中 WAPI 网络现场测评工具包括了 WAPI 网络验收测试工具和 WAPI 网络检查评估工具。

（1） WAPI 协议检测系统比对服务，比对样品涵盖了 WAPI 专用标准终端（STA）、WAPI 专用标准无线接入点（AP）及 WAPI 专用标准鉴别服务器（AS），能够覆盖所有设备类别的测试项目。比对项

目包括WAPI协议互通性测试、WAPI协议完整性测试及功能测试等。尤其是被业界俗称为“负面测试”的协议完整性测试，此前在各测试建构之间的互相比对中很少涉及。WAPI协议完整性测试能更加有效地提高WAPI网络运行的稳定性、互操作性，降低用户使用风险，特别是满足了当前各重要行业异构网络环境下设备之间的互联互通和复杂业务运行。

（2）WAPI 网络现场测评工具比对服务所使用的“比对样品”是一个“实境环境”。通过不同的测评工具对同一个实境环境测试所得出的结果进行比对，从而判断测评工具测试结果的准确性。目前涉及的比对项目包括基本功能、安全功能及性能等。

138. 问：申请开展比对服务需要哪些流程？

答：联盟测试实验室服务流程如下：

（1）申请测试受理

第一、申请单位发起比对申请，致电或发送邮件至：010-82351181，staff@wapia.org。

第二、申请单位填写《比对服务申请书》，将文件邮件发送至：

staff@wapia.org，进入审核流程。

第三、审核通过后，申请单位与联盟测试实验室签署《比对服务协议》。

（2）比对样品测试

第一、联盟测试实验室在收到全部服务费用后，进入比对样品测试环节，按要求完成比对样品的测试工作并出具报告单 1。

第二、联盟测试实验室将比对样品及《作业指导书及报告单》发送至申请单位，申请单位对比对样品进行测试，将测试结果填写至报告单 2 并邮寄回联盟测试实验室。

（3）比对并出具报告

联盟测试实验室对报告单 1 和报告单 2 中测试内容进行比对，依据比对结果出具比对报告，申请单位可通过快递或自取的方式获取比对报告。

139. 问：申请联盟测试实验室比对服务多久能够拿到报告？

答：申请单位在比对样品完成测试并填写完报告单邮寄联盟后，

预计一周之内可以取得比对报告。

如存在测试排期情况，联盟会员优先于非会员。

140. 问：对通过了联盟测试的产品，联盟是否会对外发布，从哪里能够查到？

答：已通过联盟测试实验室测试的产品，会在联盟微信公众号、联盟网站、月刊《在路上》等媒体，以及《WAPI 产业联盟产品名录》发布。

此外，厂商还可选择在联盟网站首页“自我声明”中展示（http://www.wapia.org.cn/public/include/Hot341233.shtml）。该“自我声明”，是生产者（制造商）为确认产品能够满足适用标准相关要求所做出的承诺。任何厂商对已经实现 WAPI 功能的产品都有选择自我声明的权利。

141. 问：《WAPI 产业联盟产品名录》是做什么用的？如何获得？

答：为方便市场用户查询，WAPI 产业联盟对已通过了联盟测试

实验室 WAPI 功能测试的产品信息进行汇总，形成了《WAPI 产业联盟产品名录》，面向公众公开。您可登录 WAPI 产业联盟网站，在“测试服务”栏目下载 http://www.wapia.org.cn/Down/Testing/list.shtml

142. 问：《WAPI 产业联盟产品名录》为什么不发布更早期（2021 年 6 月以前）通过测试的产品信息？

答：联盟测试实验室会根据技术产业演进和市场建设需求，持续完善和更新《WAPI 产业联盟产品名录》。

据摸底统计，2021 年 6 月之前通过测试的产品，在功能、性能上大多已无法满足高质量 WAPI 建设需求，且有相当一部分产品已经停产，因此这些产品信息不再纳入发布范围。

如果厂商仍在销售 2021 年 6 月之前通过联盟测试的产品，可申请重新测试。获得最新版测试报告后，将补录到最新版《产品名录》中。

143. 问：什么是“自我声明”，对于企业来说“自我声明”有什么好处？

答：“自我声明”是生产者（制造商）为确认产品能够满足适用标准相关要求所做出的承诺。由生产者（制造商）采用“自我声明”的方式，证明和公示其所提供的产品能够持续符合适用标准相关要求，有助于快速市场对接，营造公平市场环境，提升市场管理效率，促进产业群体健康、有序、高效发展，也有利于强化企业主体责任意识，推动企业质量诚信体系建设。

自我声明是按照市场化要求、国际化方向进行的改革措施。它改变的是评价方式，而对产品质量安全的要求并没有改变。随着评价方式的改变，生产企业产品上市准入的费用和时间成本降低了，有助于企业产品研发、生产、上市的提速增效，可以有效降低制度性交易成本，激发企业自主创新，快速响应市场需求，加快产品提质升级，为市场和产业高效提供合规产品。

144. 问：目前针对无线局域网产品的标准符合性自我声明，都要符合哪些标准？

答：首先，无线局域网产品应符合 GB 15629.11 系列无线局域网国家标准的要求，包括：

（1）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》

（2）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

（3）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》

（4）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》

（5）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》

其次，对于支持更高通信速率的 STA、AP 类产品，还应符合以下团体标准（一个或多个）：

（1）T/WAPIA 007.1—2010《无线局域网产品工程化实现指南 第 1 部分：WAPI 与 IEEE 802.11n》

（2）T/WAPIA 007.1—2010/XG1—2014《无线局域网产品工程化实现指南 第 1 部分：WAPI 与 IEEE 802.11n》第 1 号修改单

（3）T/WAPIA 007.1—2010/XG2—2022《无线局域网产品工程化实现指南 第 1 部分：WAPI 与 IEEE 802.11n》第 2 号修改单

（4）T/WAPIA 007.8—2016《无线局域网产品工程化实现指南 第 8 部分：WAPI 与 IEEE 802.11ac》

（5）T/WAPIA 007.8—2016/XG1—2022《无线局域网产品工程化实现指南 第 8 部分：WAPI 与 IEEE 802.11ac》第 1 号修改单

（6）T/WAPIA 007.10—2020《无线局域网产品工程化实现指南 第 10 部分：WAPI 与 IEEE 802.11ax》

（7）T/WAPIA 007.10—2020/XG1—2022《无线局域网产品工程化实现指南 第 10 部分：WAPI 与 IEEE 802.11ax》第 1 号修改单

（8）T/WAPIA 007.11—2025《无线局域网产品工程化实现指南 第 11 部分：WAPI 与 IEEE 802.11be》

再次，对于鉴别服务器（AS）类产品，还应符合以下团体标准：

（9）T/WAPIA 010.2—2012《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 补篇 2：无线局域网证书漫游规范》

145. 问：无线局域网产品标准符合性自我声明的信息如何发布？

答：为方便市场用户等需求方集中查询无线局域网产品标准符合性自我声明信息，WAPI 产业联盟建设并面向全社会免费开放了“无线局域网产品标准符合性自我声明信息服务平台”。目前已有南方电网数字电网研究院有限公司、深圳市信锐网科技术有限公司、深圳市智开科技有限公司、西电捷通公司、深圳市瑞科慧联科技有限公司、深圳航天科创实业有限公司、广西新海通信科技有限公司、广西电力线路器材厂有限责任公司、南京博洛米通信技术有限公司、

南京才华科技集团有限公司、北京华信傲天网络技术有限公司、北京至周科技有限公司、北京联盛德微电子有限责任公司、西安芯语慧联信息科技有限公司、山东华辰泰尔信息科技股份有限公司、锐捷网络股份有限公司、北京佰才邦技术股份有限公司、安徽皖通邮电股份有限公司、北京数字认证股份有限公司、长园共创电力安全技术股份有限公司、帕孚（上海）电气设备有限公司、北京锐云通信息技术有限公司、广州莲雾科技有限公司、朗松珂利（上海）仪器仪表有限公司等厂商通过该平台发布了上百个型号的产品自我声明信息。

您可登陆联盟官方网站查询，链接如下：

http://www.wapia.org.cn/public/include/Hot341233.shtml

146. 问：在 WAPI 产业联盟 “无线局域网产品标准符合性自我声明信息服务平台”上进行自我声明，需要提供哪些信息？

答：需要提供包括但不限于如下信息：

（1）产品类型：目前包括 STA、AP、AS、CIS 四类

（2）产品名称

（3）产品型号

（4）支持的速率集（模式）：目前包括 GB 15629.1101、GB 15629.1102、GB 15629.1104、11n(2.4GHz) 、11n(5GHz) 、11ac、11ax (2.4GHz) 、11ax (5GHz)

（5）相关测试报告：可以是 WAPI 产业联盟测试报告，也可以是其他机构的测试报告，如果没有可以写“无”。

147. 问：WAPI 产业联盟官方网站“自我声明”专栏的展示效果是怎样的？可以免费查询吗？

答：联盟定期整理并在官网发布无线局域网产品标准符合性自我声明信息，所有单位和个人均可免费查阅。

http://www.wapia.org.cn/public/include/Hot341233.shtml

网站展示效果见下图。

无线局域网产品自我声明信息

以下单位以自我声明的方式声明，该单位生产的产品符合GB 15629.11系列国家标准要求（GB 15629.11及XG1、GB 15629.1101、GB 15629.1102、GB 15629.1104）。以下信息由WAPI产业联盟收集整理并定期发布。

当产品支持11n模式时，同时符合T/WAPIA 007.1－2010《无线局域网产品工程化实现指南 第1部分：WAPI与IEEE 802.11n》、T/WAPIA 007.1－2010/XG1－2014《无线局域网产品工程化实现指南 第1部分：WAPI与IEEE 802.11n》第1号修改单、T/WAPIA 007.1－2010/XG2－2022《无线局域网产品工程化实现指南 第1部分 WAPI与IEEE 802.11n》第2号修改单标准要求；

当产品支持11ac模式时，同时符合T/WAPIA 007.8－2016《无线局域网产品工程化实现指南 第8部分：WAPI与IEEE 802.11ac》、T/WAPIA 007.8－2016/XG1－2022《无线局域网产品工程化实现指南 第8部分 WAPI与IEEE 802.11ac》第1号修改单标准要求；

当产品支持11ax模式时，同时符合T/WAPIA 007.10－2020《无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax》、T/WAPIA 007.10－2020/XG1－2022《无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax》第1号修改单标准要求；

当鉴别服务器（AS）支持漫游时，同时符合T/WAPIA 010.2－2012 《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 补篇2：无线局域网证书漫游规范》。

以下信息更新于2024年12月11日

产品信息

序号	单位名称	产品类型	产品名称	产品型号	支持的模式	测试报告
1	深圳市信锐网科技术有限公司	AP	无线接入点	NAP3600	11a/b/g/n/ac	WAPI产业联盟测试报告
2		AP	无线接入点	NAP-3700	11a/b/g/n/ac	WAPI产业联盟测试报告
3		AP	无线接入点	NAP-8100(L)	11a/b/g/n/ac	WAPI产业联盟测试报告
4		AP	无线接入点	NAP-3600(MU)	11a/b/g/n/ac	WAPI产业联盟测试报告
5		AP	无线接入点	NAP-8100(L)-LTE	11a/b/g/n/ac	WAPI产业联盟测试报告
6		AP	无线接入点	NAP-1720-LTE	11a/b/g/n/ac	WAPI产业联盟测试报告
7		AP	室内WAPI	XHC-SW3-E12-20	11a/b/g/n/ac	WAPI产业联盟测试报告

返回目录

148. 问：是不是只有通过了 WAPI 产业联盟测试的产品，才可以做自我声明？

答：不是。

厂商声明自己的产品符合某项/某些标准，不必须提供测试报告。但附带测试报告的声明，会提升用户的信赖度。

声明时如果提供测试报告，不必须是联盟出具的。乃至厂商自身建设并具备了 WAPI 测试能力，自行出具测试报告也是可以的。但由产业公信力强的测试机构出具的报告，往往有更高市场认可度。

十多年来 WAPI 产业联盟持续为产业提供产品标准符合性测试等公共技术服务，这些都是可以公开获得的。

【第六部分 联盟与会员服务】

149. 问：WAPI 产业联盟是做什么的？

答：WAPI 产业联盟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，法人名称为“中关村无线网络安全产业联盟”。目前，联盟是北京市 5A 级社会组织、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，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。

联盟的宗旨是：整合协调产业和社会资源，提升联盟会员在无线网络和网络安全相关领域的研究、开发、制造、服务水平，促进产业健康发展；以国际领先的基础共性技术 TePA 和 WAPI，带动无线网络和网络安全健康高效发展；发挥联盟的“政、产、学、研、用”链条作用，促进产业群体协同创新、提升综合竞争力。

成立 19 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。联盟实验室等技术实体和公共服务平台，能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。

目前，联盟会员单位包括三大电信运营商、行业用户单位和 ICT 领域骨干企业。在联盟创新联合体的共同努力下，在标准化方面，已开展了 200 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。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 320 亿颗；支持 WAPI 的移动终端和网络侧设备已超过 24000 款。在服务市场应用方面，除电信运营商公共无线局域网络之外，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。

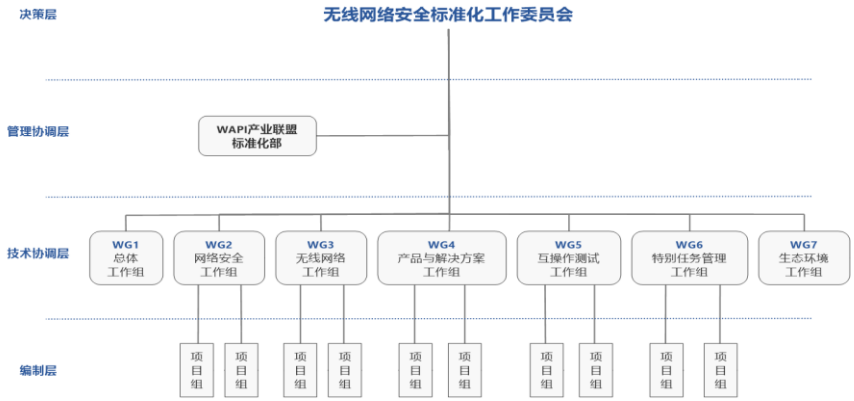
150. 问：WAPI 产业联盟和无线网络安全标准化工作委员会的关系是什么？加入联盟与加入标委会是什么关系？

答：无线网络安全标准化工作委员会秘书处工作由 WAPI 产业联盟承担。成为 WAPI 产业联盟会员后，有资格参与标委会工作，申请成为单位委员、推荐专家委员。

标委会是在无线网络和网络安全专业领域内，从事标准起草、技术审查、标准实施等标准化工作的非法人技术组织，负责 WAPI 产业联盟团体标准的制定、发布、实施，推动团体标准被国际、国外、中国、行业以及其他团体标准的采用和引用。

标委会由委员组成，委员分单位委员和专家委员两类，具广泛性和代表性，主要来自生产者、经营者、使用者、消费者、公共利益方等相关方。标委会每届任期 4 年，任期届满换届。依据《无线网络安全标准化工作委员会导则》和《WAPI 产业联盟标准化工作管理办法》开展工作。

依据 GB/T 20004.1《团体标准化 第 1 部分：良好行为指南》规范要求，标委会设置了管理协调层、技术协调层、标准编制层。具体结构见下图。



151. 问：联盟承担的无线网络安全技术国家工程研究中心产业协作中心，其主要工作和作用是什么？

答：2011 年至今，WAPI 产业联盟持续承担了无线网络安全技术国家工程研究中心（原为无线网络安全技术国家工程实验室）的产业协作中心工作，主要工作包括：关注无线网络和网络安全技术标准的创新和演进；组织产业链上下游协同创新，依标开发并推出安全的无线网络产品，满足市场需求；组织和开展公共技术研发，提供咨询、测试、整改等服务，保障产品间互联互通等。通过联盟“专职专业化人员”和“公共服务平台”，为市场和产业链利益相关方提供想做、做不了、但必须有人做的技术产业服务，持续推动科技

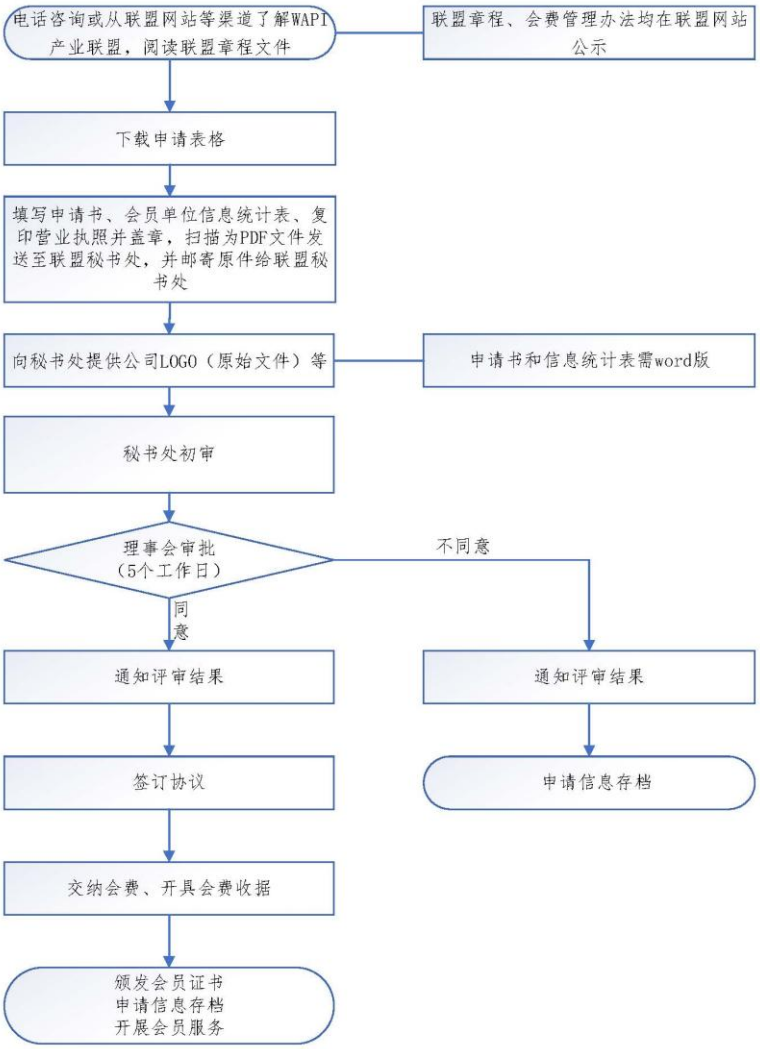
创新和成果转化。

无线网络安全技术国家工程研究中心是国家创新体系和国家战略科技力量的重要组成部分，是我国在基础性网络安全技术领域布局的唯一的产业技术创新基础设施，是我国聚焦于计算机 TCP/IP 四层网络安全协议技术研发攻关的专业机构，包括技术集成研发中心、密码工程验证中心、协议测试技术中心、产业协作中心、电子政务应用中心、智能电网研发应用中心。由西电捷通公司、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、WAPI 产业联盟、北京市政务网络管理中心、中国电力科学研究院、西安邮电大学发起共建。

152. 问：加入 WAPI 产业联盟的流程是什么？周期有多久？

答： 申请材料通过初审后，提交联盟理事会审批，时间通常为 5 个工作日。通过理事会审批并完成签订协议、缴纳会费后，可获得会员证书。具体流程见下图。

WAPI产业联盟会员加入流程



153. 问：成为 WAPI 产业联盟的会员可以享受哪些服务？

答：联盟欢迎所有希望投身 WAPI 产业的单位申请成为会员。依据联盟《章程》，所有按时履行会员义务的单位，均可享受联盟提供的标准化、市场应用、产业技术、测试验证、资源对接、信息服务六方面 20 余类服务。

154. 问：WAPI 产业联盟会员在标准化方面可以享受哪些服务？

答：（1）可以自愿加入无线网络安全标准化工作委员会，深度参与标准协同创新工作，每家会员单位拥有一个“单位委员”资格。

（2）提出标准化研究课题和立项建议。

（3）提出标准项目立项申请，牵头开展新标准项目。

（4）参与联盟在研标准项目，委派专家参与项目工作（标准起草、意见反馈、试验验证等）。

（5）参加联盟组织的标准化会议、活动、培训，参与标准推广应用等。

（6）参与标准国际化创新，参加相关国际会议、活动。

155. 问：WAPI 产业联盟会员在市场应用方面可以享受哪些服务？

答：（1）第一时间获取并掌握 WAPI 技术产业市场信息数据等，第一时间掌握 WAPI 市场建设和项目部署信息，获得更多参与机会。

（2）参与联盟组织的 WAPI 市场应用建设、重大项目等。

（3）经联盟测试通过的产品，将被纳入《WAPI 产业联盟产品名录》《WAPI 优秀产品推荐手册》《WAPI 标准产业应用及环境监测报告》等，供市场用户择优选择。高质量产品还有机会成为联盟测试基准设备。

（4）参与 WAPI 行业及市场会议活动，展示自身技术产品方案实力，获得与用户单位的直接对接机会。

156. 问：WAPI 产业联盟会员在产业技术方面可以享受哪些服务？

答：（1）在会员产业技术创新全周期中，获得安全无线局域网技术产品研发与升级优化支持。

（2）遇到市场建设中的产业技术难点，第一时间获得联盟技术研发支持、产业协作支持、方案组织支持等。

（3）根据自身需要，委托联盟开展常规化和定制化的技术、标准、产业、检测等专业培训。

（4）委托联盟组织产业技术专家研讨会/论证会/评审会等。

157. 问：WAPI 产业联盟会员在测试验证方面可以享受哪些服务？

答：联盟开创了“咨询型”产业技术服务模式，为企业提供“概念验证、功能验证、标准符合性验证、投产前实验”等公共技术服务，解决投产前的技术验证梗阻，为企业科技创新和技术研发提速。主要包括：

（1）产品测试服务：根据市场用户需求，联盟持续完善无线局域网产品鉴别与保密基础结构（WAPI）功能测试项目，并提供 WAPI 协议互通性测试、WAPI 协议完整性测试、WAPI 性能测试等。针对测试未通过项，联盟实验室会迅速进行分析定位，提供整改建议并配合会员完成整改。

（2）产品远程调试服务：在会员产品开发阶段，可通过联盟远程服务，验证该产品的 WAPI 基础功能（如互通性等），缩短会员产品的研发周期。

（3）设备短期借用服务：在会员在产品开发及测试阶段，可借用联盟测试基准设备（如：AP、AS、STA 等），用以组建安全无线局域网，并进行产品的功能与性能验证，加快研发进度。

（4）安全无线局域网系统测试服务：围绕用户单位的建设需求，事先在联盟实验室内使用将要实际参建的产品搭建仿真模拟环境，进行建设方案可行性测试、设备间互联互通测试、业务运行压力测试。

（5）WAPI 检测能力建设服务：对有需要的会员，提供 WAPI 检测系统搭建及升级、WAPI 检测系统比对、技术咨询、培训等服务。

158. 问：WAPI 产业联盟会员在资源对接方面可以享受哪些服务？

答：会员可借助联盟公共服务平台和渠道优势，获得资源对接、资金项目、宣传推广等机会。

159. 问：WAPI 产业联盟会员在信息服务方面可以享受哪些服务？

答：（1）获取联盟《在路上》期刊、微信公众号、联盟网站等

信息产品。即时掌握政策市场信息、友商动态，宣传会员单位新技术新产品研发、市场应用、荣誉奖励等方面成果。

（2）获取联盟标准技术产业市场研究报告，掌握国内外无线网络和网络安全最新情况、发展趋势和路线图、产业市场应用方案等。

（3）掌握联盟标准制定、技术研发、市场应用项目等方面工作信息。

160. 问：联盟常规开展的业务会议/活动有哪些？

答：联盟常规业务会议/活动包括：党的主题活动、理事会、监事会、全体会员大会、标准产业市场大会、标准工作和项目组会议、培训活动等。上述均依据联盟《章程》规定和市场产业需要开展。

161. 问：WAPI 产业联盟对外提供培训服务吗？培训主要包括哪些内容？

答：联盟对外提供培训服务，培训形式主要包括现场培训和网络培训。咨询请联系：staff@wapia.org

常规培训主要包括如下：

（1）无线局域网基础

（2）三元对等鉴别架构及应用

（3）密码学基础

（4）无线电通信基础

（5）WAPI 技术标准

（6）WAPI 产业、市场及应用

（7）团体标准工作及实践

（8）无线网络安全国际标准化工作及实践

常规培训范围内的，可根据需要选择。超出常规培训之外的，可商联盟进行专项定制。

162. 问：是否只有联盟会员才有资格在联盟平台发起团体标准制定？具体流程是怎样的？

答：是的。只有联盟会员才有资格在联盟平台发起团体标准制

定。且需要注意，团体标准项目应由三家或以上单位联合申请，并明确项目牵头单位。

具体流程：项目牵头单位向工作组组长提交《标准项目立项建议书》《标准项目立项申请书》和标准草案（非必须），同时向联盟标准化部报备。工作组组长组织对立项申请材料进行形式审查及技术审查，审查通过后，将立项材料报送联盟标准化部。联盟标准化部对通过工作组审查的立项申请材料进行复核，复核通过后，联盟标准化部将立项材料提交标委会全体委员进行函审。函审周期一般为 10 个工作日。标委会审查通过的项目由联盟标准化部发布立项公告，并征集项目参编单位。项目牵头单位组织参编单位组成项目组，确定项目编辑，并组织起草工作。

163. 问：有会员提出想在联盟团体标准中署名为标准起草人，但没有计划在标准编制中做出具体贡献和工作，可以吗？

答：不可以，这个想法本身就是错误的。自 2006 年成立以来，WAPI 产业联盟坚持的原则是：联盟标准工作均为免费参与；必须有实际贡献才能成为团体标准的起草人，绝不允许通过付费等形式达成标准挂名的结果。另外，2024 年国家标准化管理委员会印发《团

体标准组织综合绩效评价指标体系》，其中 1.5.2 中明确规定，“**团体标准组织不得以参编、署名、排名等为由收费，不得以标准立项为由收取管理费。**”

联盟会员单位可以申请新标准项目立项，作为项目牵头单位组织制定与自身业务密切相关的标准。在标准创制过程中，依托联盟标准化平台组织项目编制组起草并完善标准。在标准发布时，牵头单位在标准中署名，并排名第一。

如会员单位没有专门的标准化人员，对标准制定规则和标准文本的撰写尚在学习中，会员可以委派技术人员参加标准编制组工作，对标准文本的技术内容做出贡献，包括提出技术意见、文本修改建议、对标准内容进行实验验证等。上述有效贡献均可以被联盟标准平台认可。

164. 问：联盟会员如何参与国际标准化工作？

答：目前，国际上最具影响力的三大国际标准组织是国际标准化组织（International Organization for Standardization，简称 ISO）、国际电工委员会（International Electrotechnical

Commission，简称 IEC）和国际电信联盟（International Telecommunication Union，简称 ITU)。这三大国际标准组织制定的标准被称为国际标准。其成员由最有代表性的全国性的标准化机构代表其国家或地区参加，且只允许一个组织参加。

联盟会员单位、专家可通过以下方式参与 ISO、IEC 国际标准化活动：

一是确定技术领域涉及的 ISO、IEC 技术委员会（TC）或分技术委员会（SC）。登录 ISO（https：//www.iso.org）、IEC（https://www.iec.ch/）官网查找、确定要参与的 TC 或 SC。

国际标准化组织（ISO）与国际电工委员会（IEC）共同设立了规模最大、产出最丰富的技术标准委员会，即 ISO/IEC 信息技术联合技术委员会（ISO/IEC JTC 1)。如参与信息技术领域国际标准化活动可以直接登录 ISO/IEC JTC 1

（https://www.iso.org/committee/45020.html）官网查询。

二是确定国内技术对口单位。可登录国家市场监督管理总局标准创新司官网(http://www.samr.gov.cn/bzcxs/)的通知公告栏目查询 ISO、IEC 国内技术对口单位联系信息。

三是联系国内技术对口单位获取国际标准编制等信息，可向其提出选派技术专家参加国内技术对口工作组、参与国际标准文件投票和评议意见的需求，也可提出承办国际会议、参加 ISO 和 IEC 技术机构成员身份、参加 ISO 和 IEC 国际标准化制定工作组注册专家的建议等。

目前联盟已有多位专家深度参与国际标准化组织工作，其中包括 ISO/IEC JTC 1/SC 6/WG 1 工作组（物理层和数据链路层领域）召集人、ISO/IEC JTC 1/SC 27（信息安全、网络空间安全和隐私保护领域）与 ISO/IEC JTC 1/SC 6 的双向联络员、ISO/IEC JTC 1/SC 6/AG 2（术语和定义咨询组）召集人；ISO/IEC JTC 1/SC 6 的 WG 1、WG 7、WG 10 工作组专家，覆盖所有 SC 6 工作组；联盟秘书处多位同志成为 ISO/IEC JTC 1/SC 6 工作组专家并担任联合项目编辑。