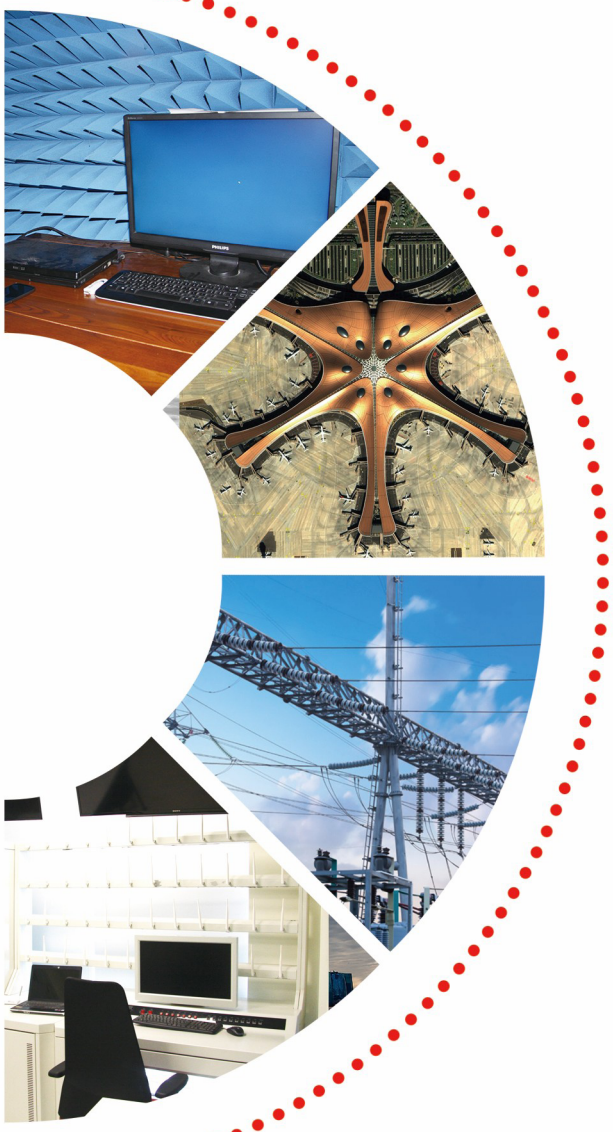
WAPI Alliance
产 | 业 | 联 | 盟



WAPI 市场应用洞察报告

WAPI产品密码算法硬件化实现的演进与应用趋势

[2026年10月版]

中关村无线网络安全产业联盟（WAPI产业联盟）
市场与产业部

编制说明

《WAPI市场应用洞察报告》是WAPI产业联盟的系列出版物，目标是指导安全无线局域网（WAPI）产业市场高质量发展。我们非常高兴地和业界分享这些重要信息，以帮助制定有关WAPI的决策，并为广大用户提供最佳体验。

《报告》每个专题均揭示了联盟在WAPI市场应用中的关键发现，所有观点均基于长期的产业市场洞察、广泛的调查、与业内专家充分的讨论以及严格的产品和系统测试。

鉴于技术标准持续演进和产业市场持续发展，每个专题都可能衍生出多个版本。详情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。

联系方式

地 址：北京市海淀区知春路27号量子芯座1608室

电 话：010-82351181

邮 箱：staff@wapia.org

网 站：www.wapia.org.cn

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

本期洞察对象与结论

当前，WAPI网络已在电力、交通、国防等关键信息基础设施，以及工业物联网和企业数字化建设场景中广泛应用。随着无线带宽提升、行业终端规模扩大和各类无线通信模组普及，WAPI产品在工程落地中同时面临两类要求：一是高并发、低时延业务、大吞吐业务对加解密提出更高性能要求；二是行业场景对私钥保护、抗物理攻击和抗侧信道攻击提出更高安全要求。

本期报告以无线接入点（AP）、行业/通用终端以及各类WAPI模组（STA）为主要观察对象，从技术必要性、合规要求和经济可行性三个方面，分析WAPI产品在密码算法实现、密钥存储和安全基础能力方面的发展趋势，形成如下判断：

1、 面向行业应用的WAPI产品，包括AP、业务终端和WAPI模组，应优先采用安全芯片或硬件安全模块（HSM）实现私钥安全存储和密码运算。对于存在物理接触风险的设备，仅依赖通用存储芯片或操作系统隔离等方式保护私钥，难以满足高安全场景下的防护要求。

2、AP和STA均应采用具备硬件WAPI协议加速能力的WLAN芯片。“密码算法硬件化”有助于从源头降低会话密钥在内存中暴露的风险，同时提升大流量场景下的加解密吞吐能力，减少因软件协议栈处

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

本期洞察对象与结论

理能力不足带来的丢包、时延和抖动问题，实现“线速”[1]网络吞吐。

3、在满足等保、密评合规要求的前提下，结合WAPI产业联盟相关高质量团体标准推动WAPI产品密码能力硬件化，是提升产业安全能力和工程可用性的重要方向。随着WLAN芯片对WAPI协议硬件加速支持能力逐步普及，安全芯片和HSM产业配套不断完善，相关技术条件和经济可行性已成熟。

1 线速（Wire Speed）指网络设备按传输介质本身的最大带宽能力，无间断、无延迟地转发数据包，即传输性能跑满或接近理论极限，不成为瓶颈。

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

引言：WAPI产品在不同硬件架构下面临的安全与性能挑战

在无线局域网（WLAN）安全体系中，密钥的产生、存储、使用和销毁是产品安全能力的核心。对于AP和STA而言，WAPI相关密钥和密码运算如果长期依赖纯软件方式实现，在面对物理接触、固件导出、调试接口提取、内存抓取和侧信道分析等攻击时，安全边界相对薄弱。

在WAPI发展早期，受限于当时WLAN芯片产业基础和产品供应情况，部分产品采用软件方式实现密码算法，在一定阶段内支撑了WAPI网络的快速部署。随着芯片产业成熟、行业安全要求提高以及高吞吐业务场景增多，传统“软算法”方案在部分典型产品中逐渐暴露出安全和性能短板。

1、AP和STA面临“线速”加解密性能挑战

AP和STA是WAPI无线通信中的核心单元，承载空口数据的实时加解密任务。

一方面，随着高速无线接入能力不断提升，AP和STA的数据吞吐能力已进入Gbps级。若对称加解密主要由主控CPU通过软件完成，密集的密码运算会占用大量CPU资源，影响设备整体处理能力。

另一方面，软件加解密难以稳定提供低时延、低抖动的实时处理能力。在工业控制、轨道交通、智能制造等场景中，这可能带来吞吐下降、时延抖动增大和丢包等问题，影响业务连续性和实时性。因此，具备WAPI协议硬件加速能力（包括但不限于配备硬件SM4密码引擎）的WLAN芯片，对于保障数据面高吞吐和低时延具有重要意义。

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

2、行业终端和WAPI模组面临更高的物理安全要求

在工业无线物联网中，终端设备形态多样，既包括运行Windows、Linux、Android等通用操作系统的复杂行业终端（如便携式工控机、高性能CPE、智能手持设备），也包括以低算力单片机（MCU）为核心的低功耗WAPI模组（如传感器、监测模组和采集终端），这类设备通常部署在现场环境中，部分设备存在被接触、拆解或复制的风险。

首先，软件保护和通用操作系统保护存在局限。用于WAPI身份鉴别的私钥如果存放在通用存储芯片或文件系统中，即使通过操作系统权限、软件加固或混淆方式进行保护，在面对固件导出（Dump）、调试接口提取、存储芯片拆取等物理攻击时，仍可能存在泄露风险。

其次，运行期密钥也需要重点保护。在AP与STA建立安全通信后，会话密钥需要参与实时数据加解密。如果WLAN芯片支持WAPI协议硬件加速，会话密钥可在芯片内部完成存储和运算，减少其暴露在主机内存中的机会。反之，若依赖软件完成保密通信过程，会话密钥通常需要加载至通用内存中，可能面临系统漏洞利用、内存抓取或侧信道分析等风险。

因此，WAPI产品的安全能力不仅取决于协议本身，也取决于密码算法和密钥管理在产品硬件架构中的实现方式。

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

WAPI产品密码算法硬件化，主要包括两类能力：一是通过安全芯片或HSM保护非对称密码算法和私钥；二是通过WLAN芯片内置硬件加速能力（SM4密码引擎）实现对称密码算法的高效处理。二者分别对应身份鉴别安全和数据传输性能，是提升WAPI产品安全性和工程可用性的关键基础。

1、非对称密码算法硬件化实现

非对称密码算法在WAPI协议中主要用于AP与STA的双向身份鉴别、证书签名/验签以及会话密钥协商。采用安全芯片或HSM实现相关能力，主要具有以下价值。

第一，提升鉴别效率，缩短接入时间。非对称密码涉及椭圆曲线点乘等复杂的数学运算。在资源受限的低功耗MCU上，纯软件实现单次签名或验签可能耗时数百毫秒甚至数秒；在高并发AP场景中，频繁鉴别也会占用CPU资源，导致设备接入、快速重连或高频漫游切换（如移动AGV小车、轨道交通车载台）产生明显卡顿。采用具备硬件协处理能力的安全芯片，有助于缩短鉴别时间，释放主系统计算资源，提升设备接入、重连和漫游切换效率。

第二，增强抗侧信道攻击能力。非对称密钥在运算过程中可能受到功耗分析（SPA/DPA）、时序攻击等侧信道攻击。安全芯片在设计时引入了常数时间执行机制、掩码技术（Masking）、随机延迟注入等防护措施，降低通过功耗、电磁或时序特征反推出密钥的风险。

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

第三，降低私钥泄露和运算流程被篡改的风险。WAPI身份鉴别依赖签名、验签等关键流程。如果相关逻辑完全运行在通用系统环境中，可能受到恶意代码注入、控制流篡改或逆向分析影响。安全芯片或HSM能将私钥和关键运算过程置于相对隔离的执行环境中，提升身份鉴别过程的完整性和可信度。

2、对称密码算法硬件化实现

对称密码算法主要用于WAPI空口数据的实时加解密，直接影响网络吞吐、时延、设备功耗等性能表现。采用硬件化实现，主要具有以下价值。

第一，提升吞吐能力，保障低时延业务。对于AP和高性能终端，硬件化SM4加速能力可在数据帧处理过程中同步完成加解密，减少主CPU参与数据面密码运算的压力。在大流量和强实时场景中，这有助于减少软件加解密带来的吞吐瓶颈、时延抖动和丢包风险。

例如：ASIC专用门电路或SoC内的硬加速核，能够在MAC层数据帧处理流水线上同步完成实时加解密。这种“边收发边加解密”的机制具备微秒级超低时延，可实现真正的“线速”网络吞吐，有效规避软件加解密带来的高延迟与丢包隐患。

此外，现代工业现场WAPI网络具有大吞吐量和低时延的要求。若采用纯软件方式在主CPU中运行SM4算法，复杂的轮函数计算将占用绝大部分CPU时钟周期，引发CPU资源竞争，导致严重的网络延

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

迟、抖动和丢包，难以满足工业实时性的要求。硬件算法模块能够实现主系统CPU的“零负担”运行，消除因CPU资源竞争导致的网络抖动，保障工业现场高频数据采集与控制指令的强实时性要求。

第二，降低终端功耗。相比通用MCU通过大量指令完成对称密码运算，专用硬件加速单元通常能以更少时钟周期完成处理，从而降低单位数据加解密能耗。对于电池供电的低功耗物联网模组，如无线监测传感器、数据采集终端等，这有助于延长设备续航时间，降低维护频次。

第三，减少会话密钥暴露。当WAPI数据加解密在WLAN芯片内部完成时，会话密钥可尽量避免进入主机通用内存，从而降低被内存抓取、系统漏洞利用或恶意程序读取的风险。这一点对于部署环境复杂、终端类型多样的行业应用尤为重要。

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

WAPI产品密码算法与密钥管理硬件化，不仅是技术层面的安全升级，也与行业合规、产品测评和长期运维成本密切相关。

1、满足等保、密评高级别合规要求

随着《网络安全法》《密码法》《网络安全等级保护基本要求》以及商用密码应用安全性评估等法律法规和标准要求持续落实，电力、交通、国防等关键信息基础设施行业对无线网络安全提出了更高要求。

在等保2.0相关要求中，GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》对重要通信过程的密码运算和密钥管理提出了明确要求。对于高安全等级场景，采用硬件密码模块更有利于满足合规测评和工程落地要求。例如，在高安全等级（四级）要求中，“9.1.2.2 通信传输”部分提出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；而在三级及以上场景中，采用硬件密码模块也是满足合规测评的最优解。

在高安全等级保护场景中，如电网关键控制区、核电控制系统、轨道交通信号控制系统等，密码技术不仅要满足算法合规要求，还需要具备更强的抗物理攻击、抗篡改和密钥保护能力。采用具备“密钥不出芯”、物理防护、防篡改等能力的安全芯片或HSM，有助于降低密钥泄露风险，并提升系统整体合规性和可信度。

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

2、顺应WAPI产业高质量建设的市场与经济需求

从产业供给侧看，WAPI密码算法硬件化的基础条件正在逐步成熟。根据联盟产业观察，目前市场超过80%的WLAN芯片支持硬件WAPI协议加速能力，为数据面高吞吐和低时延传输提供了硬件基础。同时，商用安全芯片和HSM的产品形态更加丰富，成本和集成复杂度逐步降低，为“非对称算法安全芯片/HSM保护 + 对称算法硬件加速”的产品架构提供了可行条件。

从标准引导看，WAPI产业正处于从“规模化部署”向“高质量、高可信建设”演进。WAPI产业联盟T/WAPIA 054—2025《高质量安全无线局域网 总体要求》等团体标准，对密码安全能力、设备抗物理攻击能力和抗篡改能力提出了更高要求。通过推动相关标准落地，可引导产业链逐步减少对过渡性软件方案的依赖，提升WAPI产品整体安全水平。

从全生命周期成本看，密码算法硬件化可能在产品设计和工程化实现阶段增加一定硬件物料清单（BOM）成本，但对于行业用户而言，评估其价值不能只看单台设备的初始价格，更要看其在降低长期安全风险和运维成本方面的作用。

一旦因私钥泄露或软件防护失效导致网络安全事件，可能引发设备替换、系统整改、业务中断、合规复核等多方面成本。相比之下，在产品初始设计阶段引入硬件化安全能力，有助于降低系统全生命周期风险。

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

1、洞察结论

综合以上分析，本报告形成如下结论:

第一、涉及关键信息基础设施与核心生产网的WAPI设备，包括AP、业务终端和WAPI模组，应优先采用安全芯片或HSM实现私钥物理隔离存储与密码运算，以降低物理拆解、固件导出、调试接口提取和侧信道攻击带来的密钥泄露风险。

第二、AP和STA均应采用具备硬件WAPI协议加速能力的WLAN芯片。对称算法（SM4）硬件化是提升高吞吐、低时延传输能力的重要手段，也有助于减少会话密钥在主机通用内存中的暴露。

第三、随着SM4硬件加速能力逐步普及，安全芯片、HSM等产业配套持续完善，WAPI产品推进密码能力硬件化的技术基础和经济可行性不断增强。在等保、密评以及WAPI产业联盟高质量团体标准等要求的牵引下，密码算法硬件化正成为WAPI产品向高安全、高可信方向演进的重要路径。

2、对WAPI产业链各方的行动建议

为推动安全无线局域网产业向高质量、高可信方向发展，WAPI产业联盟建议产业链各方采取以下行动:

对芯片与模组厂商，建议加快支持WAPI协议硬件加速能力的芯片和模组产品研发，提升对SM4等关键密码算法的硬件处理能力。面向

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

工业物联网、低功耗终端等场景，应同步加强私钥保护、密钥管理和抗物理攻击能力，减少对单纯软件保护方案的依赖。

对行业用户与系统集成商，建议在WAPI设备招标、采购和验收中，将产品是否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或HSM、是否采用支持WAPI协议硬件加速的WLAN芯片、是否通过联盟实验室等WAPI协议基础要素测评等内容，纳入技术评价和准入条件。

对不同类型的终端产品，建议按照应用场景、风险等级和产品形态分类推进硬件化演进。对于低功耗物联网模组、轻量终端等现场部署广、物理接触风险高、生命周期长的设备，应优先采用硬件安全架构。对于运行通用操作系统、承载多业务功能的复杂终端，可结合产品迭代周期设定明确的硬件化升级计划；在过渡期内，应重点加强软件防护、接口管控和密钥全生命周期管理，并逐步实现WAPI安全能力的整体提升。

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

Email Address **staff@wapia.org**

Phone Number **010–82351181**

Website **www.wapia.org.cn**



WAPI产业联盟公众号