WAPI 技术简介

一、定义与定位

WAPI（WLAN Authentication and Privacy Infrastructure，无线局域网鉴别与保密基础结构）是我国自主研发、拥有完整知识产权的无线局域网安全接入技术标准，也是全球 WLAN 领域两大独立安全技术体系之一，核心解决无线局域网接入身份可信与数据传输保密两大基础安全问题。

该技术于 2003 年被纳入 GB 15629.11 系列国家标准，成为我国无线局域网领域的强制性安全机制。同时已获得 IEEE 注册权威机构分配的专属以太类型字段，是我国在计算机宽带无线网络通信领域首个获得国际标准化组织认可的自主安全协议。

WAPI 底层基于 ISO/IEC 8802-11 统一的 WLAN 通信物理层与 MAC 层基础协议，与 Wi-Fi 体系底层传输架构兼容，核心差异在于安全接入与加密协议栈的自主设计，可同时支持 WAPI 与 Wi-Fi 两种安全模式。

二、体系与演进

WAPI 技术形成了两代完整的标准体系，覆盖国家标准、行业规范与团体标准。

1. WAPI 1.0 标准体系

1) 核心标准

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》，2003 年正式发布，2006 年完成密码算法配套修订。

2) 技术底座

仅供博洛米网站、网上商城使用。

基于三元对等鉴别架构（TePA），替代传统 Wi-Fi 的二转三元过渡架构，从架构层面解决了接入点无独立身份、依赖后端服务器转发信任的安全缺陷。

3) 密码体系

采用国家密码管理局批准的商用密码算法，完成身份鉴别与数据加密全流程的国密适配。

2. WAPI 2.0 标准体系

1) 核心标准

GB/T 28455-2026《网络安全技术 引入可信第三方的实体鉴别及接入架构规范》、T/WAPIA 046-2021《无线局域网安全技术规范》及 2025 年第 1 号修改单，是面向后量子时代的新一代安全标准，2025 年已达到规模产业化应用成熟度。

2) 核心升级

a) 提出 AKEA（鉴别与密钥建立原子机制），将实体身份鉴别与会话密钥生成合并为不可分割的原子流程，任何一方未收到完整报文均无法完成身份验证或密钥推导，从协议设计层面规避了中间人攻击、密钥泄露风险。

b) 全面适配 SM2（非对称鉴别）、SM3（哈希校验）、SM4（对称加密）全系列国密算法，支持 WPI-SM4-OFB+CMAC、WPI-SM4-GCM 两种加密模式。

c) 支持身份保护、抗字典攻击、抗重放攻击，预留后量子密码算法演进接口，可实现与 WAPI 1.0 网络的无感共存与平滑迁移。

d) 新增管理帧保护、快速切换（WAPIFT）等功能，适配高移动性、高可靠性工业场景。

三、架构与原理

WAPI 采用三元对等安全架构，由三类核心实体构成：

- STA（Station，无线终端）：接入网络的用户侧设备

- AP（Access Point，无线接入点）：网络侧接入设备
- AS（Authentication Service，鉴别服务器）：独立第三方身份认证与密钥管理中心

该架构中 AP 与 STA 具备对等的身份地位，二者均通过 AS 完成身份核验，不存在一方主导、一方被动的信任关系，从根源上抵御伪造 AP（假基站）、非法终端接入等攻击。

WAPI 协议由两大核心子协议协同工作：WAI（鉴别基础结构）负责身份认证与密钥管理，WPI（保密基础结构）负责数据传输加密。

1. WAI：无线局域网鉴别基础结构

WAI 是 WAPI 的身份安全核心，基于公钥密码体制实现双向身份鉴别与动态密钥协商，支持两种鉴别模式。

1) 证书鉴别模式（WAPI-CERT）

基于 X.509 数字证书实现身份认证，是高安全等级场景的主流模式，核心流程如下：

a) 接入请求：STA 向 AP 发起接入请求，携带自身数字证书；

b) 证书转发：AP 将 STA 证书与自身证书一并转发至 AS；

c) 双向核验：AS 分别验证 STA 与 AP 的证书合法性、有效期与吊销状态，生成包含双方认证结果的签名报文返回 AP；

d) 结果确认：AP 将认证结果转发给 STA，双方分别验证 AS 签名，确认对方身份合法；

e) 密钥协商：身份验证通过后，双方通过非对称加密交互密钥材料，派生单播会话密钥；

f) 组播密钥通告：AP 生成组播密钥，通过已协商的单播密钥加密后分发给 STA，完成广播/组播数据的保护密钥同步。

g) 该模式下密钥由 AS 集中管理，全动态生成且基于用户维度隔离，无需人工配置共

享密钥，不存在密钥扩散风险。

2) 预共享密钥模式（WAPI-PSK）

适用于小型网络场景，STA 与 AP 预先配置相同的预共享密钥，基于该密钥派生基础密钥 BK，后续完成单播、组播密钥的协商，流程轻量化但安全等级低于证书模式。

2. WPI：无线局域网保密基础结构

WPI 工作在 MAC 层，针对 MAC 服务数据单元（MSDU）提供全链路数据安全防护，核心能力包括数据机密性、完整性校验与抗重放保护。

1) 加密算法

采用国密 SM4 分组对称密码算法，128 位密钥长度与分组长度，符合国家商用密码标准。

2) 加密模式

a) WAPI 1.0：采用 SMS4-OFB（输出反馈模式）实现数据加密，配合 SMS4-CMAC（密码分组链消息认证码）实现完整性校验；

b) WAPI 2.0：新增 SM4-GCM（伽罗瓦/计数器模式），同步实现加密与完整性校验，加密效率更高，适配高带宽无线传输场景。

c) 防护范围：覆盖单播、组播/广播全类型无线数据帧，通过逐包序列号机制抵御重放攻击，确保传输数据不可篡改、不可伪造、不可窃听。

四、特性与优势

双向对等身份鉴别区别于 Wi-Fi 体系中终端被动接受 AP 认证的单向信任模式，WAPI 实现终端与网络的双向身份核验，既防止非法终端接入内网，也避免终端接入伪造 AP，从架构上杜绝“蹭网”与“钓鱼热点”风险。

集中式密钥管理体系所有身份凭证与会话密钥由独立 AS 统一管控，密钥基于每次鉴别

仅供博洛米网站、网上商城使用。

动态生成，支持按需更新，无需在 AP 与终端间预配置共享密钥，避免了人工密钥分发带来的泄露风险，适配大规模组网与集中运维场景。

全栈国密算法适配从身份鉴别、哈希校验到数据加密全流程采用自主可控的 SM 系列商用密码算法，密码体系自主可控，符合国家信息安全与密码合规要求，不存在算法后门与供应链风险。

协议原子性与抗攻击能力 WAPI 2.0 的 AKEA 原子机制将鉴别与密钥生成绑定为不可拆分流程，规避了传统 Wi-Fi 安全协议中密钥协商与身份认证分步执行的逻辑漏洞，至今未被证明存在可被利用的安全缺陷；可有效抵御 KRACK、DragonBlood 等针对 Wi-Fi 安全协议的已知攻击手段。

平滑演进与兼容性两代 WAPI 标准向下兼容，且底层适配 802.11a/b/g/n/ac/ax 全代际 Wi-Fi 通信协议，可与现有 WLAN 硬件基础设施深度融合，支持 Wi-Fi 5/6/7 等新一代通信技术同步部署，无需独立搭建物理网络。

五、与主流 Wi-Fi 安全机制的对比

对比维度	WAPI 体系	IEEE 802.11i(WPA/WPA2/WPA3)
安全架构	三元对等架构，AP 与 STA 身份对等	二转三元架构，AP 作为认证中转节点
鉴别机制	双向对等鉴别，AS 集中管理身份	单向为主，依赖 Radius 与预共享密钥，厂商实现兼容性差异大
核心密码算法	SM2/SM3/SM4 国密算法体系	AES、RC4、SHA 系列国际算法
密钥管理	全集中动态管理，基于用户维度隔离	分布式配置，共享密钥存在扩散风险
已知安全漏洞	无公开可利用的结构性漏洞	存在 KRACK、DragonBlood 等协议级攻击面

仅供博洛米网站、网上商城使用。

对比维度	WAPI 体系	IEEE 802.11i(WPA/WPA2/WPA3)
合规属性	中国无线局域网强制性安全标准，符合等保、商密合规要求	国际行业标准，不满足国内关键领域密码合规要求

六、典型应用场景

WAPI作为高安全等级无线接入技术,主要应用于对信息安全有强合规要求的行业领域。

- 政务与涉密场景：党政机关内网无线接入、政务办公移动终端接入，满足保密合规与等保要求。
- 能源与工业领域：电力电网智能巡检、工业厂区无线工控、智慧矿山设备接入，保障工业控制数据与生产数据传输安全。
- 交通与公共服务：机场、地铁、轨道交通内部无线调度，海关、口岸查验设备无线接入，支撑关键业务可靠运行。
- 安防与应急领域：智能安全帽、布控球、AR 巡检眼镜等移动安防设备接入，实现视频与传感数据的加密传输。
- 金融与医疗领域：银行网点无线办公、医院移动医护终端接入，保护用户隐私与敏感业务数据。

仅供博洛米网站、网上商城使用。