无线局域网鉴别与保密基础结构（WAPI）

功能测试项目

（2022 年 09 月版）

WAPI 产业联盟
(中关村无线网络安全产业联盟)

编制说明

为更好地服务产业、服务各行各业 WAPI 建设，WAPI 产业联盟公布新版《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》。

目前，联盟测试实验室为产业市场提供的无线局域网鉴别与保密基础结构（WAPI）功能测试主要包括：WAPI 协议互通性测试和 WAPI 协议完整性测试（负面测试），免费面向联盟会员提供服务。

WAPI 协议互通性测试主要是测试设备实现 WAPI 协议的一致性和正确性，以及设备与其他 WAPI 设备的互联互通性；WAPI 协议完整性测试主要是检验设备所实现 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。

上述测试，依据 GB 15629.11 系列标准、GB/T 32420-2015《无线局域网测试规范》、WAPI 产业联盟有关团体标准开展。测试对象分为终端（STA）、无线接入点（AP）[1]、鉴别服务器（AS）、证书签发服务器（CIS）四大类。

[1]在无线局域网网络部署中，对于需要 AC 配合才能够完成无线接入点功能的 AP 设备，业界通常称为瘦 AP（Fit AP）；对于能够独立完成无线接入点功能的 AP 设备，业界通常称为胖 AP（Fat AP）。当采用瘦 AP 形态进行测试时，被测设备为 AC 和瘦 AP 的组合，无论 WAPI 功能实现在 AC 或者瘦 AP 上，均作为无线接入点（AP）设备开展测试，不对独立的 AC 设备接入控制器进行测试。

修订记录

日期	版本	说明	作者
2016 年 9 月 12 日	2016 年 9 月版		王立华
2018 年 10 月 16 日	2018 年 10 月版	测试项增项	王立华
2019 年 12 月 13 日	2019 年 12 月版	测试项增项	王立华
2020 年 3 月 9 日	2020 年 3 月版	测试项增项	王立华
2020 年 4 月 17 日	2020 年 4 月版	分类优化	王立华
2020 年 11 月 30 日	2020 年 11 月版	测试项增项、名称修订	王立华
2021 年 6 月 18 日	2021 年 6 月版	增加证书签发服务器（CIS）设备类型、测试项增项	王立华
2021 年 7 月 19 日	2021 年 7 月版	修订	王立华
2022 年 9 月 21 日	2022 年 9 月版	测试项增项、名称修订	王立华

测试项目

一、终端（STA）鉴别与保密基础结构功能测试项目

GB/T 32420 对应章节		测试项目
7.1.3.8.1 预共享密钥		预共享密钥鉴别和密钥管理
7.1.3.8.2 证书安装 7.1.3.8.4 证书鉴别功能		证书鉴别和密钥管理
7.1.3.8.5 加密功能		加密功能
7.1.3.8.3 证书选择功能		证书选择检测
7.1.3.8.6 密钥更新功能		预共享密钥鉴别和密钥管理方式下单播密钥更新
		预共享密钥鉴别和密钥管理方式下组播密钥更新
		证书鉴别和密钥管理方式下单播密钥更新
		证书鉴别和密钥管理方式下组播密钥更新
		证书鉴别和密钥管理方式下基密钥更新
7.1.3.8.7 WAPA 协议完整性测试	WAI 子类型	针对鉴别激活分组中 WAI 子类型字段
		针对接入鉴别响应分组中 WAI 子类型字段
		针对单播密钥协商请求分组中 WAI 子类型字段
		针对单播密钥协商确认分组中 WAI 子类型字段
		针对组播密钥通告分组中 WAI 子类型字段
	WAI 头部字	针对鉴别激活分组中 WAI 版本字段

GB/T 32420 对应章节		测试项目
7.1.3.8.7 WAPA 协议完整性测试	段	针对鉴别激活分组中 WAI 类型字段
		针对鉴别激活分组中 WAI 分组序号字段
		针对接入鉴别响应分组中 WAI 版本字段
		针对接入鉴别响应分组中 WAI 类型字段
		针对接入鉴别响应分组中 WAI 分组序号字段
		针对接入鉴别响应分组中 WAI 分片序号和标识字段
		针对单播密钥协商请求分组中 WAI 版本字段
		针对单播密钥协商请求分组中 WAI 类型字段
		针对单播密钥协商请求分组中 WAI 分组序号字段
		针对单播密钥协商确认分组中 WAI 版本字段
		针对单播密钥协商确认分组中 WAI 类型字段
		针对单播密钥协商确认分组中 WAI 分组序号字段
		针对组播密钥通告分组中 WAI 版本字段
		针对组播密钥通告分组中 WAI 类型字段
		针对组播密钥通告分组中 WAI 分组序号字段
	指定字段	针对鉴别激活分组中本地 ASU 的身份字段
		针对鉴别激活分组中鉴别标识字段
		针对鉴别激活分组中 ECDH 参数字段
		针对接入鉴别响应分组中 AE 的签名字段的类型
		针对接入鉴别响应分组中标识 FLAG 字段的 BK 更新标识

GB/T 32420 对应章节		测试项目
7.1.3.8.7 WAPA 协议完整性测试	指定字段	针对接入鉴别响应分组中标识 FLAG 字段的预鉴别标识
		针对接入鉴别响应分组中 ASUE 询问字段
		针对接入鉴别响应分组中 ASUE 密钥数据字段
		针对接入鉴别响应分组中 STAae 身份字段
		针对接入鉴别响应分组中 STAasue 身份字段
		针对接入鉴别响应分组中复合的证书验证结果字段的 ASUE 信任的服务器签名
		针对接入鉴别响应分组中复合的证书验证结果字段的 ASUE 询问
		针对接入鉴别响应分组中复合的证书验证结果字段的 AE 证书
		针对单播密钥协商请求分组中 ADDID 字段
		针对单播密钥协商请求分组中 BKID 字段
		针对单播密钥协商请求分组中 USKID 字段
		针对单播密钥协商请求分组中 AE 询问字段
		针对单播密钥协商确认分组中 ADDID 字段
		针对单播密钥协商确认分组中标识 FLAG 字段
		针对单播密钥协商确认分组中 BKID 字段
		针对单播密钥协商确认分组中 USKID 字段
		针对单播密钥协商确认分组中 ASUE 询问字段
		针对单播密钥协商确认分组中 WIEae 字段
		针对组播密钥通告分组中 ADDID 字段

GB/T 32420 对应章节		测试项目
7.1.3.8.7 WAPA 协议完整性测试	指定字段	针对组播密钥通告分组中密钥通告标识字段
	完整性校验字段	针对接入鉴别响应分组中 AE 的签名字段的签名值
		针对单播密钥协商确认分组中消息鉴别码字段
		针对组播密钥通告分组中消息鉴别码字段
	WPI 数据	针对 WPI 分组中数据分组序号 PN 字段
		针对 WPI 分组中完整性校验码 MIC 字段
	加密的组播密钥通告	针对加密的组播密钥通告分组
	证书属性字段	针对证书属性字段
7.1.4.1 扫描 AP 功能		扫描 AP 功能测试
7.1.4.2 否定非法证书功能		否定非法 AP 证书
		否定非法移动终端证书
7.1.4.3 同一 ASU 域内 AP 间切换功能		同一 ASU 域内 AP 间切换功能
7.1.4.6 证书漫游功能		证书鉴别和密钥管理（漫游方式）
7.1.4.9 无线局域网信息显示功能		无线局域网信息显示功能

终端（STA）扩展功能测试

T/WAPIA 037.2—2021 对应章节	测试项目		测试说明
A.1.8.1	管理帧保护（单播）连通性测试	STA 禁用下的接入测试	需待测 STA 具备管理帧保护功能开关
		STA 兼容模式下的接入测试	
		STA 强制启用下的接入测试	
6.4.10	终端实体证书管理（CMEE）及私钥生成方式测试		需待测 STA 同时支持 CMEE 和私钥本地生成功能
6.4.3	同一 ASU 域内 AP 间切换时延测试		

二、无线接入点（AP）鉴别与保密基础结构功能测试项目

GB/T 32420 对应章节	测试项目
7.2.3 SSID 配置	SSID 配置功能
7.2.3.8.1 预共享密钥	预共享密钥鉴别和密钥管理
7.2.3.8.2 证书安装 7.2.3.8.3 证书鉴别功能	证书鉴别和密钥管理
7.2.3.8.4 加密功能	加密功能
7.2.3.8.5 密钥更新功能	预共享密钥鉴别和密钥管理方式下单播密钥更新
	预共享密钥鉴别和密钥管理方式下组播密钥更新
	证书鉴别和密钥管理方式下单播密钥更新
	证书鉴别和密钥管理方式下组播密钥更新
	证书鉴别和密钥管理方式下基密钥更新

GB/T 32420 对应章节		测试项目
7.2.3.8.6 WAPI 协议完整性测试	WAI 子类型	针对接入鉴别请求分组中 WAI 子类型字段
		针对单播密钥协商响应分组中 WAI 子类型字段
		针对组播密钥通告响应分组中 WAI 子类型字段
		针对证书鉴别响应分组中 WAI 子类型字段
	WAI 头部字段	针对接入鉴别请求分组中 WAI 版本字段
		针对接入鉴别请求分组中 WAI 类型字段
		针对接入鉴别请求分组中 WAI 分组序号字段
		针对单播密钥协商响应分组中 WAI 版本字段
		针对单播密钥协商响应分组中 WAI 类型字段
		针对单播密钥协商响应分组中 WAI 分组序号字段
		针对组播密钥通告响应分组中 WAI 版本字段
		针对组播密钥通告响应分组中 WAI 类型字段
		针对组播密钥通告响应分组中 WAI 分组序号字段
		针对证书鉴别响应分组中 WAI 版本字段
		针对证书鉴别响应分组中 WAI 类型字段
	指定字段	针对接入鉴别请求分组中 ASUE 的签名字段
		针对接入鉴别请求分组中标识 FLAG 字段的 BK 更新标识
		针对接入鉴别请求分组中标识 FLAG 字段的预鉴别标识
		针对接入鉴别请求分组中鉴别标识字段
		针对接入鉴别请求分组中 STAae 身份字段

GB/T 32420 对应章节		测试项目
7.2.3.8.6 WAPI 协议完整性测试	指定字段	针对接入鉴别请求分组中 ECDH 参数字段
		针对单播密钥协商响应分组中 BKID 字段
		针对单播密钥协商响应分组中标识 FLAG 字段
		针对单播密钥协商响应分组中 USKID 字段
		针对单播密钥协商响应分组中 ADDID 字段
		针对单播密钥协商响应分组中 AE 询问字段
		针对单播密钥协商响应分组中 WIEasue 字段
		针对组播密钥响应分组中 ADDID 字段
		针对组播密钥响应分组中 MSKID 字段
		针对组播密钥响应分组中 USKID 字段
		针对组播密钥响应分组中密钥通告标识字段
		针对证书鉴别响应分组中 ADDID 字段
		针对证书鉴别响应分组中证书的验证结果字段的 AE 询问
		针对证书鉴别响应分组中证书的验证结果字段的 ASUE 证书
	完整性校验字段	针对接入鉴别请求分组中 ASUE 的签名字段
		针对单播密钥协商响应分组中消息鉴别码字段
		针对组播密钥响应分组中消息鉴别码字段
		针对证书鉴别响应分组中 AE 信任的服务器签名字段
	WPI 数据	针对 WPI 分组中数据分组序号 PN 字段
		针对 WPI 分组中完整性校验码 MIC 字段

GB/T 32420 对应章节	测试项目
7.2.4.6 否定非法证书功能	否定非法 AP 证书
	否定非法 STA 证书
7.2.4.11 证书漫游功能	证书鉴别和密钥管理（漫游方式）
7.2.4.13 无线局域网信息显示功能	无线局域网信息显示功能

无线接入点（AP）扩展功能测试

T/WAPIA 037.2—2021 对应章节	测试项目		测试说明
附录 A.2.6.1	管理帧保护（单播)连通性测试	AP 禁用下的接入测试	需待测 AP 具备管理帧保护功能开关
		AP 强制启用下的接入测试	
		AP 兼容模式下的接入测试	
7.4.14	终端实体证书管理（CMEE）及私钥生成方式测试		需待测 AP 同时支持 CMEE 和私钥本地生成功能

三、鉴别服务器（AS）鉴别与保密基础结构功能测试项目

GB/T 32420 对应章节	测试项目
7.3.3.1 X.509 V3 证书管理测试	X.509 v3 证书管理测试
接入地 AS 7.3.2 WAPI 端口号测试 7.3.3.2 X.509 协议流程与数据格式	证书鉴别和密钥管理（STA 与 AP 均使用正常证书）
	证书鉴别和密钥管理（STA 使用正常证书，AP 使用吊销证书）
	证书鉴别和密钥管理（STA 使用吊销证书，AP 使用正常证书）

GB/T 32420 对应章节	测试项目
	证书鉴别和密钥管理（STA 与 AP 均使用吊销证书）
7.3.3.3 证书查询功能测试	证书查询功能测试
7.3.3.4 MAC 地址绑定功能测试	MAC 地址绑定功能测试
接入地 AS 7.3.3.7 漫游功能测试	证书鉴别和密钥管理（接入地 AS 漫游方式）
中心地 AS 7.3.3.7 漫游功能测试	证书鉴别和密钥管理（中心地 AS 漫游方式）
归属地 AS 7.3.3.7 漫游功能测试	证书鉴别和密钥管理（归属地 AS 漫游方式）
7.3.4 WAPI 协议完整性测试	针对证书鉴别请求分组中 WAI 子类型字段
	针对证书鉴别请求分组中 WAI 版本字段
	针对证书鉴别请求分组中 WAI 类型字段
	针对证书鉴别请求分组中 STAasue 的证书字段
	针对证书鉴别请求分组中 STAae 的证书字段

四、证书签发服务器（CIS）基础功能测试项目

T/WAPIA 037.2—2021 对应章节	测试项目
附录 D.3.2.1	X.509 v3 证书管理测试
附录 D.3.2.2	证书查询功能测试
	通过证书申请文件（PKCS#10 格式）下载 WAPI 证书测试

证书签发服务器（CIS）扩展功能测试

T/WAPIA 037.2—2021 对应章节	测试项目	测试说明
附录 D.3.2.3	终端实体证书管理（CMEE）功能测试	需待测 CIS 同时支持 CMEE 和对端私钥本地生成功能

WAPI 产业联盟测试实验室 联系方式：

王立华：010-82351181，staff@wapia.org