ICS 35.180
CCS L 63

团　体　标　准

T/WAPIA 052.4—2023

无线局域网设备技术规范
第 4 部分：鉴别服务器

Technical specification for WLAN equipment Part 4: Authentication servers

2023-12-28 发布　　2023-12-28 实施

中关村无线网络安全产业联盟　发布

版权声明

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件是 T/WAPIA 052《无线局域网设备技术规范》的第 2 部分。T/WAPIA 052 已经发布了以下部分：

— 第 2 部分：终端；
— 第 3 部分：接入点和接入控制器；
— 第 4 部分：鉴别服务器；
— 第 5 部分：证书签发服务器。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中关村无线网络安全产业联盟与信息化部宽带无线IP标准工作组联合提出。

本文件由无线网络安全标准化委员会归口。

本文件起草单位：中关村无线网络安全产业联盟、北京数字认证股份有限公司、无线网络安全技术国家工程研究中心、西安芯语慧联信息科技有限公司、江苏省电子信息产品质量监督检验研究院、西安西电捷通无线网络通信股份有限公司、锐捷网络股份有限公司、国家无线电监测中心检测中心、深圳市国电科技通信有限公司、北京智芯微电子科技有限公司、北京兴汉网际股份有限公司、山东华辰泰尔信息科技股份有限公司、工业和信息化部宽带无线 IP 标准工作组。

本文件主要起草人：王立华、葛珊、于双双、张璐璐、侯鹏亮、简练、黄振海、刘婷、童伟刚、翁祖勇、潘琪、张国强、徐梓郡、卢杰、祝张睿、郑骊、周园、刘剑昕、尹玉昂、陈晓龙、李晓华、徐书明、胡霄亮、范小伟、耿震雷、李政远、胡敬财。

本文件为首次制定。

引　言

随着无线局域网应用领域的扩展，无线局域网产品类型也逐渐丰富，从无线终端、无线接入点、鉴别服务器等典型产品发展到包括接入控制器、证书签发服务器等在内的系列产品，从独立的无线局域网设备逐步发展到集成或内置了无线局域网设备的产品。因此，亟需在GB 15629.11（所有部分）的基础上，制定针对无线局域网设备的扩展子项规范，规定无线局域网设备的功能、性能以及空中接口物理层等的技术要求与测试方法。

T/WAPIA 052拟由五个部分构成。

— 第1部分：总则。目的在于确立无线局域网设备的分类和基本要求等内容。

— 第2部分：终端。目的在于确立终端的功能、性能以及空中接口物理层等的技术要求与测试方法。

— 第3部分：接入点和接入控制器。目的在于确立接入点和接入控制器的功能、性能、操作管理维护等的技术要求和测试方法。

— 第4部分：鉴别服务器。目的在于确立鉴别服务器的功能、性能、操作管理维护等的技术要求和测试方法。

— 第5部分：证书签发服务器。目的在于确立证书签发服务器的功能、性能、操作管理维护等的技术要求和测试方法。

无线局域网设备技术规范 第4部分：鉴别服务器

1 范围

本文件规定了无线局域网设备鉴别服务器的功能、性能、操作管理维护等技术要求和测试方法。

本文件适用于无线局域网设备鉴别服务器的设计、研发和测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

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

GB 15629.11—2003/XG1 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第1号修改单GB 19286 电信网络设备的电磁兼容性要求及测量方法

GB/T 9813.2—2016 计算机通用规范 第2部分：便携式微型计算机

T/WAPIA 010.2 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：无线局域网证书鉴别漫游规范

3 定义和术语

本文件没有需要界定的术语和定义。

4 缩略语

下列缩略语适用于本文件。

AP	接入点（access point）
AS	鉴别服务器（authentication server）
CIS	证书签发服务器（certificate issue service）
CRL	证书吊销列表（certificate revocation list）
UDP	用户数据报协议（user datagram protocol）
IP	互联网协议（internet protocol）
MAC	媒体访问控制（medium access control）
MTBF	平均故障间隔时间（mean time between failures）
SSID	服务集标识（service set identifier）
STA	站点（station）
WAPI	无线局域网鉴别与保密基础结构（WLAN authentication and privacy infrastructure）
EUT	被测设备（equipment under test）

5 技术要求

5.1 基本要求

AS与AP之间的空中接口物理层应符合GB 15629.11、GB 15629.11—2003/XG1、T/WAPIA 010.2的规定。

5.2 物理接口要求

物理接口要求包括：

a) 以太网接口：应至少具备1个10/100/1000 Base-T以太网接口，应符合GB/T 15629.3的规定，

应能使用直连网线进行连接，应能自动校验连接网线，应具备 1 个或多个千兆光口；

b) 串口：应至少具备 1 个 RJ45 串口；

c) USB 接口：应至少具备 1 个 USB 接口，符合 USB2.0 或 USB3.0 要求；

d) 显示接口：宜具备 1 个显示接口，如：VGA、DVI、HDMI 等。

5.3 功能要求

5.3.1 设备信息管理

应具备设备信息管理功能，管理员可通过管理端的设备信息管理页面实现对STA和AP的管理，STA和AP设备属性包括但不限于：基础信息（如：设备名称）、MAC地址信息、设备证书信息等，能实现设备的增加、删除、更改、查询等管理操作。

5.3.2 证书管理

应具备证书管理功能，管理员可通过管理端的业务管理页面实现对STA和AP的证书管理，具体功能包括：证书申请、审核、下载等管理操作。

5.3.3 授权管理

授权管理要求包括：

a) 应能为单个STA或AP设备进行授权；

b) 应能以设备分组的方式创建授权策略，实现批量授权。

5.3.4 证书鉴别

应具备证书鉴别功能，当终端用户使用证书访问WAPI无线局域网时，AP和STA通过AS对对方证书进行双向鉴别，鉴别通过后终端设备才可接入无线网络。

5.3.5 CIS 证书同步

应具备与CIS的数据同步功能，可接收CIS下发的密钥、证书和CRL，并安全存储。

5.3.6 与 CIS 安全通信功能

AS与CIS之间涉及证书、密钥等数据的跨网络通信，应基于密码技术进行安全保护，如：GM/T 0014规定的相关协议。

5.3.7 CRL 验证

应具备CRL验证功能，对于证书在CRL中的设备，禁止该设备通过验证。

5.3.8 漫游功能

应具备漫游服务器信息配置功能和WAPI无线漫游认证功能，AS能根据证书持有者身份信息在本地AS和信任AS之间执行证书漫游鉴别，漫游鉴别应符合T/WAPIA 010.2的规定。

5.3.9 数据备份和恢复

应具备数据备份和恢复功能，能实现数据的备份与恢复。

5.3.10 MAC 地址校验

应具备MAC地址校验功能，对STA和AP对应的MAC地址与其证书绑定的MAC地址进行校验，当STA或AP的MAC地址与其证书所绑定的MAC地址不一致时校验不通过。

5.3.11 端口号

AS处理WAPI鉴别数据报文的UDP端口号应符合GB 15629.11-2003/XG1的规定。

5.3.12 热备要求

应能1:1热备份或N+1备份，故障切换时不影响业务正常运行，切换时间应小于500 ms。

5.4 信息安全要求

5.4.1 系统要求

AS所使用的操作系统应进行安全加固，仅开放UDP 3810及其他所需端口。

5.4.2 密码算法

AS应使用国家密码管理主管部门批准的用于无线局域网的算法。

5.4.3 证书及密钥管理

AS应对自身密钥和证书安全存储和管理，防止密钥被窃取、复制；应对签发过的AP和STA证书做好存储和管理，防止信息泄露。

5.4.4 安全管理

AS应遵循三权分立原则，设置管理员权限，具有管理权限的管理员可进行管理操作，管理操作应具备日志审计功能。

5.5 物理安全要求

物理安全要求包括:

a) AS 在设计、硬件配置等方面要采取相应的保护措施，实现设备基本的物理安全防护功能;

b) 宜具备双电源备份功能，电源故障时及时切换供电，实现 AS 设备供电不间断。

5.6 管理和维护要求

5.6.1 管理员管理

管理员管理要求包括：

a) 应提供出厂设备管理员凭证，可在管理界面增加或删除管理员；

b) 管理员凭证宜具备多因素身份认证方式。

5.6.2 日志要求

日志要求包括：

a) 日志应记录事件发生的时间、事件的操作者、操作类型及操作结果等信息；

b) 应能按时间、操作者、操作类型等对日志进行分类或综合查询。

5.6.3 安全审计

应提供审计管理的接口或界面，能够对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计。

5.7 性能要求

5.7.1 鉴别性能

应具备多用户鉴别功能，每秒鉴别数量不低于500张有效证书。

5.7.2 可靠性

使用平均失效间隔工作时间（MTFB）衡量终端的可靠性水平。

终端的m1值（MTBF的不可接受值）不低于10000 h。

5.8 环境适应性要求

鉴别服务器的环境条件应符合表1的要求，具体如下：

表1 环境适应性要求

环境条件参数	类型	
	工作环境	存储环境
温度	0 ℃～40 ℃	-40 ℃～55 ℃
相对湿度	10%～90%（非凝结）	
大气压	86 kPa～106 kPa	

5.9 电磁兼容性要求

证书签发服务器的电磁兼容性应符合 GB 19286 的规定。

5.10 电气安全要求

证书签发服务器的电气安全应符合 GB/T 9813.2 中 4.5 的规定。

6 测试方法

AS功能与性能测试基本连接见图1。

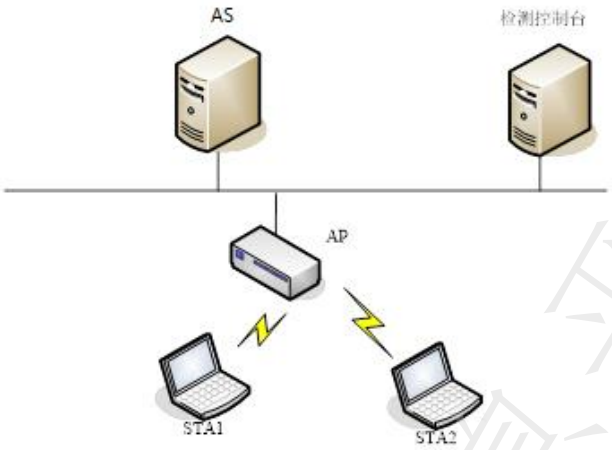

图1　AS 功能与性能测试基本连接图

6.1　测试条件

本文件中除环境试验外，其他测试均应在下述环境条件下进行：

温度：15 ℃～35 ℃。

相对湿度：25%～75%。

大气压：86 kPa～106 kPa。

6.2　功能测试

6.2.1　设备信息管理

测试步骤和判定准则如下：

a)　测试步骤：

1)　在AS上验证是否可以删除、修改、增加STA设备信息；

2)　在AS上验证是否可以删除、修改、增加AP设备信息。

b)　判定准则：

1)　在AS上可以删除、修改、增加STA设备信息；

2)　在AS上可以删除、修改、增加AP设备信息。

6.2.2　证书管理

测试步骤和判定准则如下：

a)　测试步骤：

1)　在AS上为STA1生成一个X.509 v3证书，验证证书能否审核、下载；

2)　在AS上为AP生成一个X.509 v3证书，验证证书能否审核、下载。

b)　判定准则：

1)　步骤1)：AS能够生成X.509 v3证书，能实现证书审核、下载；

2)　步骤2)：AS能够生成X.509 v3证书，能实现证书审核、下载。

6.2.3　授权管理

测试步骤和判定准则如下：

a)　测试步骤：在AS上验证是否可以实现为STA或AP设备进行批量绑定授权。

b)　判定准则：在AS上可以实现为STA或AP设备进行批量绑定授权。

6.2.4　证书鉴别

测试步骤和判定准则如下：

a)　测试步骤：

1)　检测控制台向AS发送包含有效的AP X.509 v3证书和有效的STA1 X.509 v3证书的证书鉴别请求，判断AS能否识别并正确鉴别正常和已吊销证书；

2) 检测控制台向AS发送包含有效的AP X.509 v3证书和有效的STA1 X.509 v3证书的证书鉴别请求，判断AS能否识别并正确鉴别在有效期内和不在有效期范围内的证书。

b) 判定准则：

1) 步骤1)：AS的证书鉴别响应中的证书验证结果字段能够验证AP的证书有效，STA1的证书有效；

2) 步骤2)：AS的证书鉴别响应中的证书验证结果能够识别AP/STA证书是否在有效期内。

6.2.5 CIS 证书同步

测试步骤和判定准则如下：

a) 测试步骤：

1) 在CIS上为STA1生成一个X.509 v3证书；

2) 在CIS上为AP生成一个X.509 v3证书；

3) 对AP与STA1进行授权绑定；

4) STA1请求接入AP，验证AS是否可以认证成功；

5) 将STA1证书吊销后，再次请求接入AP，验证AS是否可以认证成功。

b) 判定准则：

1) 步骤4)：认证成功；

2) 步骤5)：认证失败。

6.2.6 CRL 功能

测试步骤和判定准则如下：

a) 测试步骤；

1) 检测控制台向AS发送包含有效的AP X.509 v3证书和已吊销的STA1 X.509 v3证书的证书鉴别请求，判断AS能否识别并正确鉴别正常和已吊销证书；

2) 检测控制台向AS发送包含已吊销的AP X.509 v3证书和有效的STA1 X.509 v3证书的证书鉴别请求，判断AS能否识别并正确鉴别正常和已吊销证书；

3) 检测控制台向AS发送包含已吊销的AP X.509 v3证书和已吊销的STA1 X.509 v3证书的证书鉴别请求，判断AS能否识别并正确鉴别正常和已吊销证书。

b) 判定准则：

1) 步骤1)：AS的证书鉴别响应中的证书验证结果字段能够验证AP的证书有效，STA1的证书已吊销；

2) 步骤2)：AS的证书鉴别响应中的证书验证结果字段能够验证AP的证书已吊销，STA1的证书有效；

3) 步骤3)：AS的证书鉴别响应中的证书验证结果字段能够验证AP的证书已吊销，STA1的证书已吊销。

6.2.7 漫游功能

测试步骤和判定准则如下：

a) 测试步骤：

1) 配置AS1为AP1和STA1颁发证书，配置AS2为AP2和STA2颁发证书；

2) 验证STA1请求接入AP1是否可以认证成功，STA2请求接入AP2是否可以认证成功；

3) AS1与AS2配置漫游模式；

4) 验证STA2请求接入AP1是否可以认证成功；

5) 验证STA1请求接入AP2是否可以认证成功。

b) 判定准则：

1) 步骤2)：中STA1请求接入AP1认证成功，STA2请求接入AP2认证成功；

2) 步骤4)：中STA2请求接入AP1认证成功；

3) 步骤5)：中STA1请求接入AP2认证成功。

6.2.8 数据备份和恢复

测试步骤和判定准则如下：

a) 测试步骤：

1) 通过命令行或 WEB 方式登录AS进行管理和维护；
2) 进行数据备份处理；
3) 修改目前的数据，并用步骤b备份的数据文件进行数据恢复，查看数据情况。

b) 判定准则：

1) 步骤2)：能够完成备份；
2) 步骤3)：能够恢复数据。

6.2.9 MAC 地址校验功能

测试步骤和判定准则如下：

a) 测试步骤：

1) 设置AP的SSID（如WAPItest1），工作信道为6，安全方式为WAPI；
2) 在AS上生成一个证书，STA1下载该证书并安装；
3) AS将步骤c中生成的证书与STA1的MAC地址绑定，配置STA1关联AP，验证STA1能否接入AP；
4) STA2下载并安装步骤c中生成的证书，配置STA2关联AP，验证STA2能否接入AP。

b) 判定准则：

1) 步骤3)：STA1能够接入AP；
2) 步骤4)：STA2不能接入AP。

6.2.10 端口测试

测试步骤和判定准则如下：

a) 测试步骤：

1) 设置AP SSID为WAPItest，工作信道6，安全方式为WAPI；
2) 配置STA1接入AP，通过检测控制台观察证书鉴别请求报文与证书鉴别响应报文的UDP端口号。

b) 判定准则：

1) 步骤2)：测控制台观察到监听证书鉴别请求报文的UDP端口号为3810。

6.2.11 热备测试

测试步骤和判定准则如下：

a) 测试步骤：

1) 配置主用AS和备用AS；
2) 配置STA接入AP；
3) 断开主用AS的网络连接；
4) STA重新尝试接入AP。

b) 判定准则：

1) 步骤2)：STA应接入AP；
2) 步骤3)：备用AS转为主用AS；
3) 步骤4)：STA重新接入AP。

6.3 信息安全测试

6.3.1 密码检测

测试步骤和判定准则如下：

a) 测试步骤：

1) AS使用给定的密钥对待签名消息调用密码算法签名后，检测平台对签名结果进行验签；
2) AS使用给定的密钥对待签名消息调用密码算法签名后，调用密码算法进行验签运算。

[1] 本文件中将 SSID 设置为“WAPItest”，仅为样例。

b) 判定准则：

1) 步骤1)：检测平台对签名结果验签通过；

2) 步骤2)：AS调用密码算法进行验签运算，验签通过。

6.4 管理和维护测试

6.4.1 管理员管理

测试步骤和判定准则如下：

a) 测试步骤：

1) 操作人员通过命令或者WEB页面方式登录；

2) 验证是否可以在管理界面增加或删除管理员；

3) 验证管理员是否可以使用多因素方式登录；

4) 验证是否可以对管理员设置角色以及访问权限。

b) 判定准则：

1) 步骤2)：可以增加或删除管理员；

2) 步骤3)：管理员可以使用多因素方式登录；

3) 步骤4)：可以对管理员设置角色以及访问权限。

6.4.2 日志与审计管理

测试步骤和判定准则如下：

a) 测试步骤：

1) 操作人员通过命令行或 WEB 方式登录AS进行管理和维护；

2) 操作人员查看AS的日志审计记录信息。

b) 判定准则：

1) 步骤2)：能够查看审计日志，能够记入设备编号认证时间以及结果。

6.4.3 安全性测试

测试步骤和判定准则如下：

a) 测试步骤：

1) 操作人员通过命令或者WEB方式登录到AS进行管理和维护，观察登录的端口；

2) 操作人员通过端口扫描工具（比如:nmap）测试AS的端口开启情况并记录。

b) 判定准则：

1) 步骤1)：应能登录完成AS的管理和维护；

2) 步骤2)：AS开启的端口应符合技术规范的要求。

6.5 性能测试

6.5.1 鉴别性能测试

测试步骤和判定准则如下：

a) 测试步骤：使用性能测试工具，对数字证书认证接口进行负载测试，并记录测试结果。

b) 判定准则：测试结果的有效鉴别并发数应大于500 次/秒。

6.5.2 可靠性测试

可靠性测试步骤和判断准则应符合GB/T 9813.2的规定。

6.6 环境适应性测试

6.6.1 低温试验

测试步骤和判定准则如下：

a) 测试步骤：

1) 将EUT在室温条件(15 ℃～35 ℃)下，放入试验箱，接通电源；

2) 测试EUT的有效鉴别并发数，具体测试方法参见本文件的**错误!未找到引用源。**节；

3) 关闭EUT的电源，启动试验箱，使箱内温度逐渐降低至极限低温（温度变化速率在5 min内的平均值不大于1 ℃/min），保持此温度直至EUT达到温度稳定。接通EUT电源，保持恒温2 h后，重复步骤2）；
4) 关闭EUT的电源，将试验箱的温度逐渐升至室温（温度变化速率在5 min内的平均值不大于1℃/min），待EUT达到温度稳定后，重复步骤2）。

b) 判定准则：
1) 步骤2)：鉴别性能的测试结果符合6.5.1的要求；
2) 步骤3)：鉴别性能的测试结果符合6.5.1的要求；
3) 步骤4)：鉴别性能的测试结果符合6.5.1的要求。

6.6.2 高温试验

测试步骤和判定准则如下：

a) 测试步骤：
1) 将EUT在室温条件(15 ℃～35 ℃)下，放入试验箱，接通电源；
2) 测试EUT有效鉴别并发数，具体测试方法参见本文件的**错误!未找到引用源。**节；
3) 关闭EUT的电源，启动试验箱，使箱内温度逐渐升高至极限高温（温度变化速率在5 min内的平均值不大于1 ℃/min），保持此温度直至EUT达到温度稳定，接通EUT电源，保持恒温2 h后，重复测试步骤2）；
4) 关闭EUT的电源，将试验箱的温度逐渐降至室温（温度变化速率在5 min内的平均值不大于1 ℃/min），待EUT达到温度稳定后，重复测试步骤2）。

b) 判定准则：
1) 步骤2)：鉴别性能的测试结果符合6.5.1的要求；
2) 步骤3)：鉴别性能的测试结果符合6.5.1的要求；
3) 步骤4)：鉴别性能的测试结果符合6.5.1的要求。

6.6.3 恒定湿热试验

测试步骤和判定准则如下：

a) 测试步骤：
1) 将EUT在室温条件(15 ℃～35 ℃)下，放入试验箱，接通电源；
2) 测试EUT有效鉴别并发数，具体测试方法参见本文件的**错误!未找到引用源。**节；
3) 关闭EUT的电源，启动试验箱，使箱内温度逐渐升高至40 ℃（温度变化速率在5 min内的平均值不大于1 ℃/min），保持此温度直至EUT达到温度稳定；
4) 开始加湿，在2 h内将湿度调到90%；
5) 在湿度达到90%后，停止加湿，接通EUT电源，保持2 h后，重复测试步骤2）；
6) 关闭EUT的电源，将试验箱的湿度逐渐降至73%，然后再将试验箱的温度逐渐降至室温（温度变化速率在5 min内的平均值不大于1 ℃/min），待EUT达到温度稳定后，重复测试步骤2）。

b) 测试结果：
1) 步骤2)：鉴别性能的测试结果符合6.5.1的要求；
2) 步骤5)：鉴别性能的测试结果符合6.5.1的要求；
3) 步骤6)：鉴别性能的测试结果符合6.5.1的要求。

6.7 电磁兼容性测试

电磁兼容性测试步骤和判断准则应符合 GB 19286 的规定。

6.8 电气安全测试

电气安全测试步骤和判断准则应符合GB/T 9813.2中5.5的规定。