

# 中华人民共和国国家标准

GB/T 33563—2024  
代替 GB/T 33563—2017

## 网络安全技术 无线局域网客户端安全技术要求

Cybersecurity technology—  
Security technology requirements for wireless local area network client

2024-04-25发布

2024-11-01实施

国家市场监督管理总局  
国家标准化管理委员会

发布



目 次

前言 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 2

5 无线局域网客户端描述 ..... 2

6 安全问题 ..... 3

6.1 威胁 ..... 3

6.1.1 未授权访问(T.UNAUTHORIZED \_ACCESS) ..... 3

6.1.2 安全功能失效(T.SECURITY \_FUNCTIONALITY \_FAILURE) ..... 3

6.1.3 残留信息利用(T.RESIDUAL \_DATA \_EXPLOIT) ..... 4

6.1.4 逻辑接口攻击(T.LOGICAL \_INTERFACE \_ATTACK ) ..... 4

6.1.5 网络窃听(T.NETWORK \_EAVESDROP) ..... 4

6.1.6 网络攻击(T.NETWORK \_ATTACK) ..... 4

6.1.7 未检测的行为(T.UNDETECTED \_ACTIONS) ..... 4

6.2 组织安全策略 ..... 4

6.2.1 密码管理(P.CRYPTO \_MANAGEMENT) ..... 4

6.2.2 认证管理(P.AUTH \_MANAGEMENT) ..... 4

6.3 假设 ..... 4

6.3.1 可信的人员(A.TRUSTED \_PERSON) ..... 4

6.3.2 正确的连接(A.NO \_TOE \_BYPASS) ..... 4

6.3.3 可靠的平台(A.TRUSTED \_PLATFORM) ..... 4

6.3.4 正确的配置(A.SPECIFICATION CONFIGURATION) ..... 5

7 安全目的 ..... 5

7.1 无线局域网客户端安全目的 ..... 5

7.1.1 经认证的通信(O.AUTH \_COMM ) ..... 5

7.1.2 加密功能(O.CRYPTOGRAPHIC \_FUNCTIONS) ..... 5

7.1.3 自检(O.SELF \_TEST) ..... 5

7.1.4 系统监控(O.SYSTEM \_MONITORING) ..... 5

7.1.5 TOE 管理(O.TOE \_ADMINISTRATION) ..... 5

7.1.6 无线 AP 连接(O.WIRELESS \_ACCESS \_POINT \_CONNECTION) ..... 5

7.1.7 可信信道(O.TRUSTED \_CHANNEL) ..... 5

7.1.8 访问控制(O.ACCESS \_CONTROL) ..... 5

7.1.9 逻辑攻击抵抗(O.LOGICATTACK \_PREVENTION ) ..... 5

7.2 环境安全目的 ..... 6

7.2.1 可信人员(OE .TRUSTED \_PERSON) ..... 6

7.2.2 TOE 不可绕过(OE .NO \_TOE \_BYPASS) ..... 6

7.2.3 平台(OE .PLATFORM) ..... 6

7.2.4 配置(OE .CONFIG) ..... 6

8 安全要求 ..... 6

8.1 安全功能要求 ..... 6

8.1.1 安全功能要求分级 ..... 6

8.1.2 安全审计(FAU) .....7

8.1.3 密码支持(FCS) .....8

8.1.4 标识与鉴别(FIA) ..... 9

8.1.5 安全管理(FMT) .....10

8.1.6 TSF 保护(FPT) ..... 11

8.1.7 TOE 访问(FTA )和可信路径/信道(FTP) ..... 12

8.1.8 用户数据保护(FDP) ..... 13

8.2 安全保障要求 ..... 14

9 基本原理..... 14

9.1 安全目的基本原理 ..... 14

9.2 安全要求基本原理 ..... 14

9.3 组件依赖关系基本原理 ..... 16

参考文献 ..... 18

# 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。

本文件代替GB/T 33563—2017《信息安全技术 无线局域网客户端安全技术要求(评估保障级2级增强)》，与GB/T 33563—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了TOE 范围(见第5章，2017年版的第6章)；
- b) 更改了无线局域网客户端面临的威胁，包括7类威胁、2项组织安全策略和4个假设(见第6章，2017年版的第7章)；
- c) 更改了“TOE 安全目的”和“环境安全目的”，包括9项 TOE 的安全目的，4项环境安全目的(见第7章，2017年版的第8章)；
- d) 更改了无线局域网客户端安全功能要求，包括8类33项安全功能要求(见8.1, 2017年版的第9章、第10章)；
- e) 更改了无线局域网客户端安全保障要求(见8.2, 2017年版的9.2)；
- f) 增加了“基本原理”，包括安全问题与安全目的、安全目的与安全要求间的对应关系和组件间的依赖关系(见第9章)。

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息安全测评中心、中国科学院信息工程研究所、北京交通大学、中车工业研究院有限公司、西安西电捷通无线网络通信股份有限公司、公安部第一研究所、中国电子技术标准化研究院、北京天融信网络安全技术有限公司、深信服科技股份有限公司、郑州信大捷安信息技术股份有限公司、长扬科技(北京)股份有限公司、深圳市信锐网科技有限公司、北京路云天网络安全技术研究院有限公司、西安交大捷普网络科技有限公司、中孚信息股份有限公司、国网区块链科技(北京)有限公司、中国网络安全审查技术与认证中心、新华三技术有限公司、中国电力科学研究院有限公司。

本文件主要起草人：陈冬青、张亮、韩继登、郭涛、邵帅、吴润浦、李美聪、刘琦、樊玉明、王伟、刘吉强、王剑、唐海川、王俊勇、张变玲、朱振荣、张东举、寇增杰、安高峰、鲍旭华、叶润国、马红丽、韩秀德、赵华、赖国强、何建锋、朱大立、范伟、弥宝鑫、龙刚、高金萍、孙鹏科、侯梦云、杨珂、申永波、万晓兰、王海翔。

本文件及其所代替文件的历次版本发布情况为：

——2017年首次发布为 GB/T 33563—2017；

——本次为第一次修订。



# 网络安全技术

## 无线局域网客户端安全技术要求

### 1 范围

本文件规定了无线局域网客户端的安全功能要求和安全保障要求，给出了无线局域网客户端面临安全问题的说明。

本文件适用于无线局域网客户端产品的测试、评估和采购，以及指导该类产品的研制和开发。

### 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。

GB15629.11 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/T 18336.1—2024 网络安全技术 信息技术安全性评估准则 第1部分：简介和一般模型

GB/T 18336.2—2024 网络安全技术 信息技术安全性评估准则 第2部分：安全功能要求

GB/T 18336.3—2024 网络安全技术 信息技术安全性评估准则 第3部分：安全保障要求

GB/T 25069—2022 信息安全技术 术语

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

### 3 术语和定义

GB 15629.11、GB/T 18336.1—2024、GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

#### 3.1

**访问点** access point:AP

一种提供无线局域网客户端与有线网络之间的访问，在无线网络和有线网络之间转发帧的网络接口设备。

#### 3.2

**认证服务器** authentication server

无线局域网接入系统中用于身份认证的组件。

#### 3.3

**无线局域网客户端** wireless local area network client

实现远程用户使用客户端机器与被接入网络建立无线通信的执行组件。

4 缩略语

- 下列缩略语适用于本文件。
- EAL: 评估保障级(Evaluation Assurance Level)
  - TOE: 评估对象(Target of Evaluation)
  - TSF: 评估对象安全功能(TOE Security Functions)
  - WAPI: 无线局域网鉴别与保密基础结构(WLAN Authentication and Privacy Infrastructure)
  - WLAN: 无线局域网(Wireless Local Area Network)

5 无线局域网客户端描述

本文件描述的无线局域网客户端，是指基于IEEE 802.11协议族的无线局域网客户端设备(通用计算机或者无线移动终端)中用于连接无线局域网接入系统或其他设备，进行安全数据传输的组件。无线局域网客户端可通过无线局域网接入系统建立的被接入网络与用户设备之间的安全连接，与无线局域网接入系统一起保护所传输数据的完整性和机密性，实现身份验证与 WLAN 访问接入。

一个典型的无线局域网客户端的运行环境如图1所示。

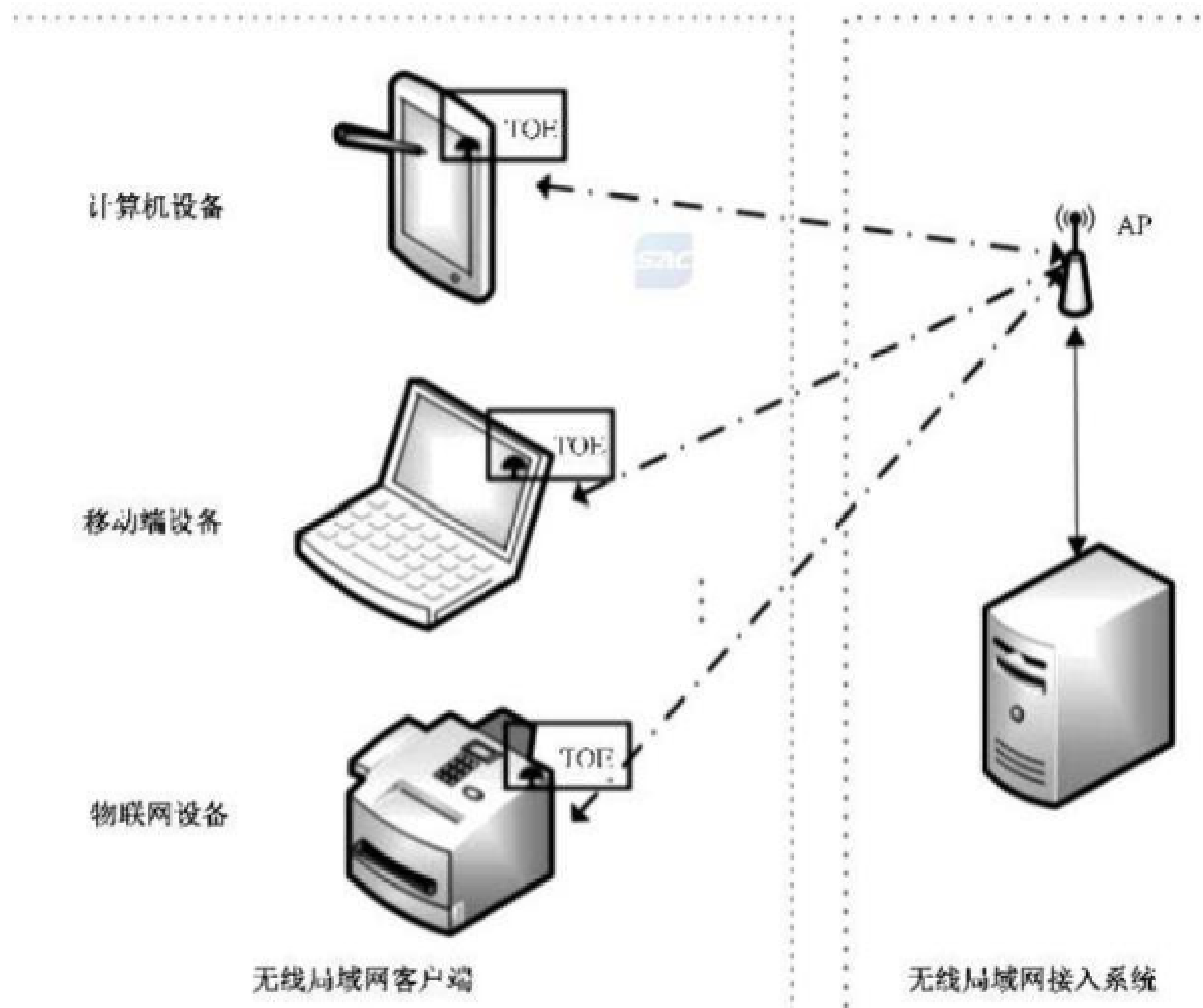


图 1 无线局域网客户端示意图

本文件的 TOE 仅包含通用操作系统或者移动设备中遵循IEEE 802.11协议规定的控制客户端设备实现 WLAN 接入流程的应用组件，其部分功能可依赖于底层设备功能实现。TOE 提供管理通道和数据通道，管理通道主要用于身份验证和访问控制，数据通道负责数据传输。TOE 提供的安全特性包括连接管理、协议合规、加密保护、审计生成。无线局域网客户端评估范围如图2所示。



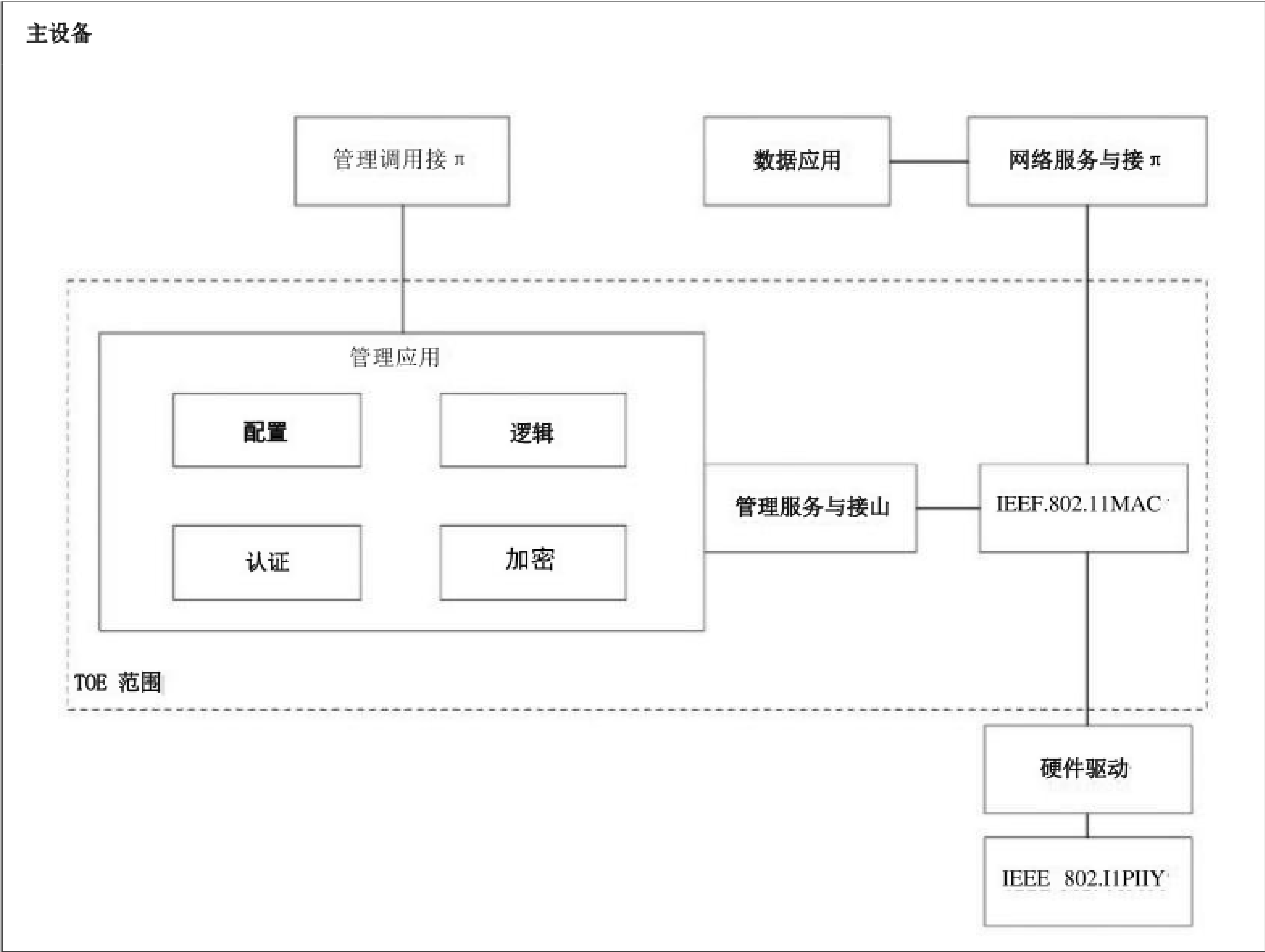


图2 TOE 评估范围

TOE 的评估通常需要与其主设备一起进行，考虑合并至其主设备进行评估。

本文件规定客户端安全技术要求分为三个等级。

- EAL2+: 同时符合 EAL2+ 级安全功能要求和 EAL2 级安全保障要求，主要应用于家庭、个人用户和有限商业应用。
- EAL3: 同时符合 EAL3 级安全功能要求和 EAL3 级安全保障要求，主要应用于组织、个人用户和一般商业。
- EAL4: 同时符合 EAL4 级安全功能要求和 EAL4 级安全保障要求，主要应用于专有的高安全等级领域。

## 6 安全问题

### 6.1 威胁

#### 6.1.1 未授权访问(T.UNAUTHORIZED\_ACCESS)

威胁主体伪装成授权实体或通过授权用户跳板以获得对无线局域网客户端数据及其驱动、应用等可执行代码的未授权访问。

#### 6.1.2 安全功能失效(T.SECURITY\_FUNCTIONALITY\_FAILURE)

威胁主体利用安全功能失效，在未认证的情况下使用或滥用安全功能，以访问和修改设备数据、关键网络流量或者安全功能配置。TOE 的安全机制通常是从受信任的初始机制构建出来的复杂机制集合，初始机制的失效影响复杂机制的运行，从而导致安全功能失效。

6.1.3 残留信息利用(T.RESIDUAL\_DATA\_EXPLOIT)

威胁主体利用无线局域网客户端残留信息的处理缺陷在执行过程中对未删除的残留信息进行利用，以获取敏感信息或滥用无线局域网客户端的安全功能。

6.1.4 逻辑接口攻击(T.LOGICAL\_INTERFACE\_ATTACK)

威胁主体通过攻击无线局域网客户端逻辑接口，非法地浏览、修改或删除 TSF 数据、配置信息、用户数据或可执行代码等，导致 TOE 的安全功能无法正常工作。

6.1.5 网络窃听(T.NETWORK\_EAVESDROP)

威胁主体对无线网络通信进行监听，获得无线局域网客户端与其他设备交互的数据，并可利用获取数据猜测 TSF 数据或用户数据。

6.1.6 网络攻击(T.NETWORK\_ATTACK)

威胁主体位于通信通道或网络基础设施的其他位置，基于设备的客户端会启动与 TOE 的通信或更改 TOE 与其他端点之间的通信，基于操作系统的客户端与运行在操作系统或操作系统的一部分上的应用程序和服务进行通信，进行攻击，更改现有的合法通信。例如威胁主体通过压制合法网络信号并模拟原接入系统，使客户端接入假冒的接入系统，从而获取 TSF 数据或用户数据。

6.1.7 未检测的行为(T.UNDETECTED\_ACTIONS)

威胁主体采取未知的攻击行为攻击TOE 网络安全，对网络的机密性、完整性、可用性造成损害。

6.2 组织安全策略

6.2.1 密码管理(P.CRYPTO\_MANAGEMENT)

密码的使用是按照相关国家标准进行的。

6.2.2 认证管理(P.AUTH\_MANAGEMENT)

认证的过程是按照相关国家标准进行的。

6.3 假设

6.3.1 可信的人员 (A. TRUSTED\_PERSON)

假设无线局域网客户端设计、开发、测试、生产等各阶段的合法操作人员遵循一套安全的流程，且遵守人员指导进行操作，且无线局域网客户端管理员可信，会以可靠的方法遵从和应用所有的管理操作指南。

6.3.2 正确的连接(A.NO\_TOE\_BYPASS)

假设运行环境在涉及范围中，无线局域网客户端用户与内部被接入网络之间的信息传递应经过无线局域网客户端。

6.3.3 可靠的平台(A.TRUSTED\_PLATFORM)

假设运行环境提供与无线局域网客户端及其传输处理的数据价值相匹配的物理安全性。通用操作系统或者无线设备平台作为无线局域网客户端运行环境部分的基本安全性是可靠的。

6.3.4 正确的配置(A.SPECIFICATION CONFIGURATION)

假设正确地配置了 TOE 的安全功能，以确保在连接的网络之间流动的所有适用的网络流量上执行TOE 安全策略。

7 安全目的

7.1 无线局域网客户端安全目的

7.1.1 经认证的通信(O.AUTH\_COMM)

TOE 将提供一种手段来确保它正在与授权接入点进行通信，而不是与其他伪装成授权接入点的实体进行通信。

7.1.2 加密功能(O.CRYPTOGRAPHIC\_FUNCTIONS)

无线局域网客户端应使用符合国家标准和国家密码管理机构规定的加解密机制并应提供符合相应的功能支持，保证无线局域网客户端能对其保护的数据采取加密措施，保证数据的机密性。

7.1.3 自检(O.SELF\_TEST)

无线局域网客户端应提供测试其安全功能及安全功能子集的相关机制，在初次启动以及系统运行过程中执行自检，以确保其安全功能的完整性，并将自检结果通知平台。

7.1.4 系统监控(O.SYSTEM\_MONITORING)

无线局域网客户端应记录安全相关的事件，应对记录的事件进行保护且只允许授权用户查看，还应提供审计相关功能。

7.1.5 TOE管理(O.TOE\_ADMINISTRATION)

无线局域网客户端应提供允许管理员配置 TOE 的机制和功能。

7.1.6 无线 AP连接(O.WIRELESS\_ACCESS\_POINT\_CONNECTION)

无线局域网客户端应提供访问控制机制，限制其能连接的无线AP。

7.1.7 可信信道(O.TRUSTED\_CHANNEL)

无线局域网客户端应提供通信信道管理选择机制，通过可信信道与外部通信并有能力识别信道异常，也可提供受保护的网络通道供用户使用。

7.1.8 访问控制(O.ACCESS\_CONTROL)

无线局域网客户端应提供访问控制机制，防止无线局域网客户端重要数据、进程及资源等在未授权情况下被访问、修改或删除。

7.1.9 逻辑攻击抵抗(O.LOGICATTACK\_PREVENTION)

无线局域网客户端应能抵抗逻辑攻击，或至少提供必要的安全措施以显著增加实施此类攻击的困难性。

7.2 环境安全目的

7.2.1 可信人员(OE.TRUSTED\_PERSON)

TOE 用户是被信任的，且遵守指导进行操作，并在符合企业应用的安全策略范围内使用该客户端。

7.2.2 TOE 不可绕过(OE.NO\_TOE\_BYPASS)

如果不通过无线局域网客户端，信息不应通过其他渠道在无线局域网客户端用户和外部网络之间流动。

7.2.3 平台(OE.PLATFORM)

运行环境可提供与无线局域网客户端及其传输处理的数据价值相匹配的物理安全性。通用操作系统或者无线设备平台作为无线局域网客户端运行环境部分的基本安全性是可靠的。

7.2.4 配置(OE.CONFIG)

管理员能正确配置 TOE 安全功能，以创建预期的安全策略。

8 安全要求

8.1 安全功能要求

8.1.1 安全功能要求分级

无线局域网客户端的安全功能要求应由GB/T 18336.2—2024 规定的功能组件构成，无线局域网客户端的安全功能要求组件见表1，8.1.2~8.1.8对各组件进行了说明。

表 1 安全功能要求组件

安全功能类	安全功能组件	EAL2+	EAL3	EAL4
安全审计 (FAU)	FAU_GEN.1审计数据产生	√	√	√
	FAU_STG.2受保护的审计数据存储	√	√	√
	FAU_STG.5防止审计数据丢失	/	√	√
密码支持 (FCS)	FCS_CKM.1密钥生成-对称密钥	/	/	√
	FCS_CKM.2密钥分发	/	/	√
	FCS_CKM.6密钥销毁的时间和事件	/	/	√
标识与鉴别 (FIA)	FIA_UAU.1鉴别的时机	√	√	√
	FIA_PAE_EXT.1端口接入实体认证	√	√	√
	FIA_X509_EXT.1X.509证书验证	√	√	√
安全管理 (FMT)	FMT_SMF.1安全功能规范	√	√	√
TSF保护 (FPT)	FPT_FLS.1失效即保持安全状态	√	√	√
	FPT_TST_.1TST自测	√	√	√
	FPT_TUD_EXT.1信任的更新	/	√	√
TOE访问 (FTA)	FTA_TSE.1TOE会话建立	√	√	√

表 1 安全功能要求组件(续)

安全功能类	安全功能组件	EAL2+	EAL?	EAL4
可信路径/信道(FTP)	FTP_ITC. 1TSF间可信信道	/	√	√
用户数据保护(FDP)	FDP_ACF. 1基于安全属性的访问控制	/	√	√
	FDP_SDC. 1存储数据的机密性	√	√	√
	FDP_SDC. 2使用专用方法的存储数据的机密性	/	√	√
	FDP_RIP. 1子集残余信息保护	/	√	√
	FDP_RIP. 1完全残余信息保护	/	√	√
注：“√”为必备满足的项，“/”为可选满足的项。				

8.1.2 安全审计(FAU)

8.1.2.1 审计数据产生(FAU\_GEN.1)

FAU\_GEN.1.1

TSF 应能[选择：调用平台的功能，实现的功能]产生以下审计事件记录：

- a) 审计功能的开启和关闭；
- b) 有关[选择：最小级，基本级，详细级，未规定]审计级别的所有可审计事件；
- c) 强制性 SFR 和可选的 SFR 的所有可审计事件，如表2所示。

表2包括 FPT\_TST.1 的可审计事件。如果 TOE 没有执行自己的自测(即在 FPT\_TST.1 中选择“TOE 平台”), 对此的审计记录事件也可能由TOE 平台生成。

FAU\_GEN.1.2

TSF 至少应记录下列信息：

- a) 可审计事件的日期和时间、事件类型、主体身份(如果适用)、事件的结果(成功或失败)；
- b) 对每种审计事件类型，基于PP、PP-模块、功能包或ST 中功能组件的可审计事件定义，附加审计记录内容如表2所示。

表2 可审计事件表

序号	功能	可审计事件	附加审计记录
1	FAU_GEN. 1	无	无
2	FCS_CKM. 1	无	无
3	FCS_CKM. 2	无	无
4	FIA_PAE_EXT. 1	无	无
5	FIA_X509_EXT. 1	验证X. 509v3证书失败	失效原因
6	FMT_SMF. 1	无	无
7	FPT_TST. 1	1) 执行TSF自检； 2) 发现违反完整性； 3) 自检结果	1) 无； 2) 导致完整性违反的TSF代码文件； 3) 若失败记录问题

表2 可审计事件表（续）

序号	功能	可审计事件	附加审计记录
8	FTA_TSE.1	所有连接接入点的尝试	每个接入点记录MAC地址关于[选择：配置MAC地址和SSID, 证书信息核对, 和不少于2个整数字节数的成功/失败状态
9	FTP_ITC.1	所有建立可信通道的尝试	非TOR节点通道识别

8.1.2.2 受保护的审计数据存储 (FAU\_STG. 2)

FAU\_STG.2.1

TSF 应保护所存储的审计记录，以避免未授权的删除。

FAU\_STG.2.2

TSF 应能[选择：防止、检测]对审计数据中所存审计记录的未授权修改。

8.1.2.3 审计数据可能丢失时的行为 (FAU\_STG. 4)

如果审计数据存储超过预定的限度，TSF 应在审计记录超过预定的限度之前发出警告，通知管理员，并[选择：删除新的审计数据，按照覆盖以前的审计记录的规则覆盖以前的审计记录]。

8.1.2.4 防止审计数据丢失 (FAU\_STG. 5)

如果审计数据存储已满，TSF 应[选择：“忽略可审计事件”“阻止可审计事件，具有特权的授权用户产生的事件除外”“覆盖所存储的最早的审计记录”], 提供关于[选择：删除，覆盖，其他信息操作]审计记录数量的信息审计存储失效时所采取的其他动作。

8.1.3 密码支持(FCS)

8.1.3.1 密钥生成(FCS\_CKM.1)

[选择：WAPI,WPA2,WAP3] 加密密钥生成，TSF 应根据符合下列标准[选择：GB 15629.11, IEEE 802.11—2020, IEEE 802.11ax—2021, 无其他标准]的一个特定的密钥生成算法[选择：PRF-128,PRF-256, PRF-384, PRF-512, PRF-704, 无其他算法]和规定的密钥长度[选择：128位、192 位、256 位、无其他密钥大小]FCS\_RNG.1 来生成对称加密密钥。

8.1.3.2 密钥分发(FCS\_CKM.2)

TSF 应根据符合下列标准[选择：GB15629.11] 的一个特定的密钥分发方法[选择：WAPI 加密密钥分发、GTK 密钥分发、PMK 密钥分发]来分发密钥。

8.1.3.3 密钥存取(FCS\_CKM.3)

TSF 应根据符合下列标准[选择：IEEE 802.11—2020, GB/T 39786—2021]的一个特定的密钥存取方法[选择：磁条卡密钥、智能卡密钥、ROM 密钥等]来执行[选择：密钥存储、密钥读取、密钥备份等]。

8.1.3.4 密钥销毁的时间和事件 (FCS\_CKM. 6)

FCS\_CKM.6.1

当操作系统[选择：不再需要，密钥或密钥材料销毁的其他情况]时，TSF 销毁所有密钥和密钥

材料。

**FCS\_CKM.6.2**

TSF 应根据以下方法来销毁 FCS\_CKM.6.1 中规定的密钥和密钥材料：[选择：对于易失性内存，销毁应由[选择：单一覆盖包括[使用TSF 的随机数产生器(RBG) 的伪随机模式、0、1、 一个新的密钥、不包含任何关键安全参数(CSP) 的静态或动态值], 销毁对密钥的引用，然后直接请求垃圾收集]。

对于非易失性存储中的明文密钥，销毁应通过调用TSF 的一部分提供的接口执行[选择：逻辑上处理密钥的存储位置，并执行[选择：单一，通过的数量-pass] 覆盖，包括[选择：使用TSF 的 RBG 的伪随机模式，0, 1, 一个新的密钥值， 一个不包含任何CSP 的静态或动态值];指示 TSF 的一部分销毁表示密钥的抽象]]。

**8.1.3.5 随机比特生成(FCS\_RBG.1)**

**FCS\_RBG.1.1**

当种子初始化之后，TSF 应根据[GB/T32915—2016] 使用[选择：Hash\_DRBG、HMAC\_DRBG 或其他算法]执行确定性随机比特生成服务。

**FCS\_RBG.1.2**

TSF 应使用[选择：TSF 噪声源[选择：基于软件的噪声源，基于平台的噪声源], TSF 用于设定种子的接口]进行种子初始化。

**FCS\_RBG.1.3**

TSF 应根据以下不同情况：[选择：从不，按需，在特定条件下，在一定时间之后]将通过[选择：重新加载种子，非实例化和重新实例化]使用一个[选择：TSF 噪声源[选择：基于软件的噪声源，基于平台的噪声源], TSF 用于设定种子的接口]更新 RBG 状态，以保持与[GB/T 32915—2016]的一致。

**8.1.3.6 随机数生成(FCS\_RNG.1)**

**FCS\_RNG.1.1**

TSF 应提供一个[选择：物理、非物理真、确定性、混合物理、混合确定性]随机数生成器，它能实现：安全能力列表。

**FCS\_RNG.1.2**

TOE 安全功能 TSF 应提供满足定义的质量指标的[选择：位、八位字节、数字或其他数字的格式]。

**8.1.4 标识与鉴别(FIA)**

**8.1.4.1 鉴别的时机(FIA\_UAU.1)**

**FIA\_UAU.1.1**

在用户被鉴别前，TSF 应执行代表用户的 TSF 促成的动作列表。

**FIA\_UAU.1.2**

在允许执行代表该用户的任何其他由TSF 促成的动作[包括且不限于：解密保护数据、数据加密密钥、密钥加密密钥，以及[选择：长期信任的信道密钥，所有的基于软件的密钥存储，没有其他密钥]]前，TSF 应要求每个用户都已被成功鉴别。

**8.1.4.2 不可伪造的鉴别(FIA\_UAU.3)**

**FIA\_UAU.3.1**

TSF 应[选择：检测、防止]由任何 TSF 用户伪造的鉴别数据的使用。

**FIA\_UAU.3.2**

TSF 应[选择：检测、防止]从任何其他的 TSF 用户处拷贝的鉴别数据的使用。

**8.1.4.3 标识的时机(FIA\_UID.1)**

**FIA\_UID.1.1**

在用户被识别之前，TSF 应执行代表用户的TSF 促成的动作列表。

**FIA\_UID.1.2**

在允许执行代表该用户的任何其他 TSF 促成的动作之前，TSF 应要求每个用户都已被成功识别。

**8.1.4.4 端口接入实体认证(FIA\_PAE\_EXT.1)**

TSF 应符合IEEE 标准802.1X中端口接入实体的“申请人”角色。

**8.1.4.5 X.509 证书验证(FIA\_X509\_EXT.1)**

**FIA\_X509\_EXT.1.1**

对于 EAP-TLS 的证书，TSF 应按照以下规则进行验证：

- a) RFC 5280 证书验证和证书路径验证；
- b) 证书路径以信任锚数据库中的证书终止；
- c) TSF 通过保证基本约束扩展的存在来验证证书路径，并为所有 CA 证书设置 CA 标志为 TRUE；
- d) TSF 按照以下规则对扩展密钥用途(KeyUsage) 字段进行验证：
  - 1) 为 TLS 提供的服务器证书在扩展密钥用途(KeyUsage) 字段中具有服务器认证目的；
  - 2) 为 TLS 提供的客户端证书在扩展密钥用途(KeyUsage) 字段中具有客户端认证目的。

**FIA\_X509\_EXT.1.2**

如果存在基本约束扩展并将CA 标志设置为 TRUE,TSF 只应将证书视为 CA 证书。

**8.1.5 安全管理(FMT)**

**8.1.5.1 安全属性管理(FMT\_MSA.1)**

TSF 应执行访问控制 SFP，信息流控制 SFP，以仅限于已标识的授权角色能对安全属性列表进行[选择：改变默认值、查询、修改、删除、其他操作]。

**8.1.5.2 安全的安全属性(FMT\_MSA.2)**

TSF 应确保安全属性列表只接受安全的值。

**8.1.5.3 静态属性初始化(FMT\_MSA.3)**

**FMT\_MSA.3.1**

TSF 应执行访问控制 SFP、信息流控制 SFP，以便为用于执行SFP 的安全属性提供[选择：受限的、许可的、其他特性]默认值。

**FMT\_MSA.3.2**

TSP 应允许已标识的授权角色在创建客体或信息时指定替换性的初始值以代替原来的默认值。

**8.1.5.4 安全角色(FMT\_SMR.1)**

**FMT\_SMR.1.1**

TSF 应维护角色已标识的授权角色。



FMT\_SMR.1.2

TSF 应能把用户和角色关联起来。

8.1.5.5 管理功能规范(FMT\_SMF.1)

TSF 应能执行如表3所示管理功能。

表 3 安全管理功能表

编号	管理功能	执行力	管理员	用户
1	配置各无线网络的安全策略： a) [选择：指定TSF接受WLAN认证服务器证书的CA(s), 指定可接受WLAN认证服务器证书的完全合格域名(FQDNs), 其他认证方式]； b) 安全类型； c) 认证协议； d) 要用于身份验证的客户端凭据。 设置无线频段为[选择：2.4GHz, 5GHz, 6GHz]	M	M	0
2	指定TSF可能链接的无线网络 (SSID)	M	M	0
3	启用/禁用[选择：预共享密钥，密码，无认证]认证的无线网络桥接能力（例如，在WLAN和蜂窝电台之间架起连接，起到热点作用）	M	M	0
4	启用/禁用证书撤销列表检查	)	M	)
5	禁用无线端到端ad hoc连接功能	)	0	)
6	禁止漫游功能	0	0	0
7	启用/禁用IEEE 802.1X预认证	0	0	0
8	将X.509证书加载到TOE	0	0	0
9	撤销加载到TOE的X.509证书	0	0	0
10	启用/禁用并配置PMK缓存： a) 设置PMK条目缓存的时间（以分钟计）； b) 设置可缓存的最大PMK条目数	0	0	0
注：M——必备；0——可选。				

8.1.6 TSF 保护(FPT)

8.1.6.1 失效即保持安全状态(FPT\_FLS.1)

TSF 在下列失效发生时应保持一种安全状态：自检失败或其他失效情况。

8.1.6.2 TSF 初始化(FPT\_INI.1)

FPT\_INI.1.1

TOE 应提供对完整性和真实性有自保护能力的初始化功能。

FPT\_INI.1.2

TOE 初始化功能应确保在安全初始状态下建立 TSF 之前，某些属性在某些元素上保持不变，如

表4所述：

表4 属性元素

序号	特性	元素
1	[属性，例如真实性、完整性、正确版本]	[TSF/用户固件、软件或数据的列表]
—	—	—

**FPT\_INI.1.3**

TOE 初始化功能应检测并响应初始化期间的错误和失败，以便TOE [选择：中止，在[选择：功能减少，发送错误状态信号，其他动作列表]情况下成功完成初始化]。

**FPT\_INI.1.4**

TOE 初始化功能只能在初始化过程中的定义的方法中与 TSF 交互。

**8.1.6.3 TST自测(FPT\_TST.1)**

**FPT\_TST.1.1**

[选择：TOE,TOE 平台]应在[选择：初始化启动期间、正常工作期间周期性地、授权用户要求时、在产生自检的条件时]运行一套自检程序以证实[选择：TSF 的组成部分、TSF] 能正确运行和演示正确的 TSF 的操作。

**FPT\_TST.1.2**

TSF 应为授权用户提供验证[选择：部分 TSF 数据、TSF 数据]完整性的能力。

**FPT\_TST.1.3**

TSF 应为授权用户提供验证[选择：部分 TSF、TSF]完整性的能力。

**8.1.6.4 可靠的时间戳(FPT\_STM.1)**

**FPT\_STM.1.1**

TSF 应能提供可靠的时间戳。

**8.1.6.5 信任的更新(FPT\_TUD\_EXT.1)**

**FPT\_TUD\_EXT.1.1**

TOE 应提供检测更新系统软件的能力。

**FPT\_TUD\_EXT.1.2**

系统应在安装之前使用数字签名验证更新。

**8.1.7 TOE访问(FTA)和可信路径/信道(FTP)**

**8.1.7.1 TOE 会话建立(FTA\_TSE.1)**

TSF 应能基于管理员配置的可信网络(此要求允许管理员限制 TOE 能连接的无线网络)拒绝会话的建立。

**8.1.7.2 TSF 间可信信道(FTP\_ITC.1)**

**FTP\_ITC.1.1**

TSF 应在自身和无线接入点之间提供一个可信的通信信道，该信道在逻辑上与其他通信信道截然不同，其端点具有保障标识，且能保护信道中数据免遭篡改或泄露。

**FTP\_ITC.1.2**

TSF 应允许[选择：TSF、另一个可信IT 产品]经由可信信道发起通信。

**FTP\_ITC.1.3**

对于需要可信信道的功能列表，TSF 应通过无线接入点连接的可信信道发起通信。

**8.1.8 用户数据保护(FDP)**

**8.1.8.1 基于安全属性的访问控制(FDP\_ACF.1)**

**FDP\_ACF.1.1**

TSF 应基于[选择：指定SFP 控制下的主体和客体列表，以及每个对应的 SFP 的相关安全属性或 SFP 相关的已命名安全属性组]对客体执行访问控制 SFP。

**FDP\_ACF.1.2**

TSF 应执行在受控主体和受控客体间，通过对受控客体采取受控操作来管理访问的一些规则，以确定在受控主体与受控客体间的一个操作是否被允许。

**FDP\_ACF.1.3**

TSF 应基于安全属性，明确授权主体访问客体的规则等附加规则，明确授权主体访问客体。

**FDP\_ACF.1.4**

TSF 应基于安全属性，明确拒绝主体访问客体的规则等附加规则，明确拒绝主体访问客体。

**8.1.8.2 存储数据的机密性(FDP\_SDC.1)**

TSF 应确保[选择：所有用户数据，指定用户数据列表]存储在[选择：临时内存，持久内存，任意内存]中的机密性。

**8.1.8.3 使用专用方法的存储数据的机密性(FDP\_SDC.2)**

**FDP\_SDC.2.1**

TSF 应确保在 TSF 控制下存储的[选择：所有用户数据，用户数据列表中用户数据]根据数据特征的机密性。

**FDP\_SDC.2.2**

TSF 应确保 FDP\_SDC.2.1 中规定的用户数据的机密性，无需用户干预。

**8.1.8.4 存储数据完整性监视(FDP\_SDI.1)**

**FDP\_SDI.1.1**

TSF 应基于用户数据属性，对所有客体，监视存储在由TSF 控制的载体内的用户数据是否存在完整性错误。

**8.1.8.5 子集残余信息保护(FDP\_RIP.1)**

TSF 应确保一个资源的任何先前信息内容，在[选择：分配资源到、释放资源自]指定客体列表时不再可用。

**8.1.8.6 完全残余信息保护(FDP\_RIP.2)**

TSF 应确保一个资源的任何先前信息内容，在[选择：分配资源到、释放资源自]所有客体时不可用。

8.2 安全保障要求

无线局域网客户端的安全保障要求按照GB/T18336.3—2024 规定的 EAL2、EAL3、EAL4 级安全保障要求执行。

9 基本原理

9.1 安全目的基本原理

无线局域网客户端安全目的能应对所有可能的威胁、组织安全策略和假设，即每一种威胁、组织安全策略和假设都至少有一个或一个以上安全目的与其对应，因此是充分的；每一个安全目的都有相应的威胁、组织安全策略和假设与之对应，这证明每个安全目的都是必要的。

表5说明了无线局域网客户端的安全目的能应对所有可能的威胁、组织安全策略和假设。

表 5 威胁、组织安全策略、假设与安全目的的对应关系

对应关系	安全功能失效	残余信息利用	未授权访问	逻辑接口攻击	网络窃听	网络攻击	未检测的行为	密码管理	认证管理	可信的人员	正确的连接	可靠的平台	正确的配置
认证的通信	/	/	√	/	/	/	/	/	√	/	√	/	/
加密功能	/	/	√	/	√	/	/	√	√	/	/	/	/
自检	√	/	/	/	/	/	/	/	/	/	/	/	/
系统监控	√	√	√	√	√	√	√	√	√	/	/	/	/
TOE管理	√	/	/	/	/	/	/	/	√	/	/	/	/
无线AP连接	/	/	/	√	/	/	/	/	/	/	/	/	/
可信信道	/	/	/	/	√	/	/	/	/	/	/	/	/
访问控制	/	/	√	√	/	/	√	/	√	/	/	/	/
逻辑接口抵抗	/	/	/	√	/	/	√	/	/	/	/	/	/
人员	/	/	/	/	/	/	/	/	√	√	/	/	/
TOE不可绕过	/	/	/	/	/	/	/	/	/	/	√	/	/
平台	/	/	/	/	/	/	/	/	/	/	/	√	/
配置	/	/	/	/	/	/	/	/	/	/	/	/	√
注：“√”为必备满足的项；“/”为可选满足的项。													

9.2 安全要求基本原理

表6说明了安全要求的充分必要性合理性，即每个安全目的都至少有一个安全要求组件与其对应，每个安全要求都至少解决了一个安全目的，因此安全要求对安全目的而言是充分和必要的。表6给出了 TOE 安全目的与安全功能要求之间的对应关系。

表 6 安全要求与安全目的的对应关系

对应关系	认证的通信	加密功能	自检	系统监控	TOE管理	无线AP连接	可信信道	访问控制	逻辑接口抵抗
审计数据产生 (FAU_GEN. 1)	/	/	/	√	/	/	/	/	/
审计数据保护 (FAU_STG. 2)	/	/	/	√	/	/	/	√	/
审计数据可能丢失时的行为 (FAU_STG. 4)	/	/	/	√	/	/	/	√	/
防止审计数据丢失 (FAU_STG. 5)	/	/	/	√	/	/	/	√	/
密钥生成-对称密钥 (FCS_CKM. 1)	/	√	/	/	√	/	√	/	/
密钥分发 (FCS_CKM. 2)	/	√	/	/	√	/	/	/	/
密钥存取 (FCS_CKM. 3)	/	√	/	/	√	/	/	/	/
密钥销毁的时间和事件 (FCS_CKM. 6)	/	√	/	/	/	/	/	/	/
随机比特生成 (FCS_RBG. 1)	/	√	/	/	/	/	/	/	/
随机数生成 (FCS_RNG. 1)	/	√	/	/	/	/	/	/	/
鉴别的时机 (FIA_UAU. 1)	√	√	/	/	/	/	/	/	/
不可伪造的鉴别 (FIA_UAU. 3)	√	/	/	/	/	/	/	/	/
标识的时机 (FIA_UID. 1)	√	/	/	/	/	/	/	√	/
端口接入实体认证 (FIA_PAE_EXT. 1)	√	√	/	/	√	/	√	√	√
X. 509证书验证 (FIA_X509_EXT. 1)	√	/	/	/	/		/	√	√
安全属性管理 (FMT_MSA. 1)	/	/	/	√	/	/	/	√	/
安全的安全属性 (FMT_MSA. 2)	/	/	/	√	/	/	/	/	/
静态属性初始化 (FMT_MSA. 3)	/	/	/	√	/	/	/	√	/
安全角色 (FMT_SMR. 1)	√	/	/	√	/	/	/	√	/
管理功能规范 (FMT_SMF. 1)	/	/	/	√	/	/	/	/	√
失效即保持安全状态 (FPT_FLS. 1)	/	/	√	/	/	/	/	/	/
TSF初始化 (FPT_INI. 1)	/	/	√	/	√	/	/	/	/
TST自测 (FPT_TST. 1)	√	√	√	/	/	/	/	/	/
可靠的时间戳 (FPT_STM. 1)	/	/	√	/	/	/	/	/	/
信任的更新 (FPT_TUD_EXT. 1)	/	/	√	/	/	/	/	/	/

表 6 安全要求与安全目的的对应关系 (续)

对应关系	认证的通信	加密功能	自检	系统监控	TOE管理	无线AP连接	可信信道	访问控制	逻辑接口抵抗
TOE会话建立 (FTA_TSE. 1)	/	/	/	/	/	/	√	√	/
TSF间可信信道 (FTP_ITC. 1)	/	/	/	/	/	/	√	/	/
基于安全属性的访问控制 (FDP_ACF. 1)	√	/	/	/	/	√	/	√	/
存储数据的机密性 (FDP_SDC. 1)	/	√	/	/	/	/	/	/	/
使用专用方法的存储数据的机密性 (FDP_SDC. 2)	/	√	/	/	/	/	/	/	/
存储数据完整性监视 (FDP_SDI. 1)	/	/	/	√	/	/	/	/	/
子集残余信息保护 (FDP_RIP. 1)	√	/	/	√	/	/	/	/	/
完全残余信息保护 (FDP_RIP. 1)	/	/	/	√	/	/	/	/	/
注：“√”为必备满足的项，“/”为可选满足的项。									

9.3 组件依赖关系基本原理

选取组件时，应符合所选组件之间的相互依赖关系。表7列出了所选安全功能组件的内部依赖关系。

表7 安全功能组件依赖关系表

序号	安全功能要求	安全功能要求依赖
1	FAU_GEN. 1审计数据产生	FPT_STM. 1可靠的时间戳
2	FAU_STG. 2受保护的审计数据存储	FAU_GEN. 1审计数据产生
3	FAU_STG. 4审计数据可能丢失时的行为	FAU_STG. 2受保护的审计数据存储
4	FAU_STG. 5防止审计数据丢失	FAU_STG. 2受保护的审计数据存储、FAU_GEN. 1审计数据产生
5	FCS_CKM. 1密钥生成	FCS_CKM. 2密钥分发、FCS_CKM. 3密钥存取、 [FCS_RBG. 1随机比特生成，或FCS_RNG. 1随机数生成]、FCS_CKM. 6密钥销毁的时间和事件
6	FCS_CKM. 2密钥分发	FCS_CKM. 1密钥生成、FCS_CKM. 3密钥存取
7	FCS_CKM. 3密钥存取	FCS_CKM. 1密钥生成
8	FCS_CKM. 6密钥销毁的时间和事件	FCS_CKM. 1密钥生成
9	FCS_RBG. 1随机比特生成	FPT_FLS. 1失效即保持安全状态、FPT_TST. 1 TSF自检

表 7 安全功能组件依赖关系表（续）

序号	安全功能要求	安全功能要求依赖
10	FCS_RNG. 1随机数生成	无依赖关系
11	FIA_UAU. 1鉴别的时机	无依赖关系
12	FIA_UAU. 3不可伪造的鉴别	无依赖关系
13	FIA_UID. 1标识的时机	无依赖关系
14	FIA_PAE_EXT. 1端口接入实体认证	FIA_X509_EXT. 1 X. 509证书验证
15	FIA_X509_EXT. 1 X. 509证书验证	无依赖关系
16	FMT_MSA. 1安全属性管理	[FDP_ACC. 1子集访问控制];FMT_SMR. 1安全角色、FMT_SMF. 1管理功能规范
17	FMT_MSA. 2安全属性管理	[FDP_ACC. 1子集访问控制];FMT_MSA. 1安全属性管理; FMT_SMR. 1安全角色
18	FMT_MSA. 3静态属性初始化	FMT_MSA. 1安全属性管理、FMT_SMR. 1安全角色
19	FMT_SMR. 1安全角色	FIA_UID. 1标识的时机
20	FMT_SMF. 1管理功能规范	无依赖关系
21	FPT_FLS. 1失效即保持安全状态	无依赖关系
22	FPT_INI. 1 TSF初始化	无依赖关系
23	FPT_TST. 1 TST自测	无依赖关系
24	FPT_STM. 1可靠的时间戳	无依赖关系
25	FPT_TUD_EXT. 1信任的更新	无依赖关系
26	FTA_TSE. 1 TOE会话建立	无依赖关系
27	FTP_ITC. 1 TSF间可信信道	无依赖关系
28	FDP_ACF. 1基于安全属性的访问控制	无依赖关系
29	FDP_SDC. 1存储数据的机密性	无依赖关系
30	FDP_SDC. 2使用专用方法的存储数据的机密性	无依赖关系
31	FDP_SDI. 1存储数据完整性监视	无依赖关系
32	FDP_RIP. 1子集残余信息保护	无依赖关系
33	FDP_RIP. 1完全残余信息保护	无依赖关系

## 参 考 文 献

- [1] GB15629.1101—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
- [2] GB15629.1102—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：2.4 GHz 频段较高速物理层扩展规范
- [3] GB/T 15629.1103—2006 信息技术 系统间远程通信和 S 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：附加管理域操作规范
- [4] GB15629.1104—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：2.4 GHz 频段更高数据速率扩展规范
- [5] GB/Z 20283—2020 信息安全技术 保护轮廓和安全目标的产生指南
- [6] GB/T 32907—2016 信息安全技术 SM4 分组密码算法
- [7] GB/T 38636—2020 信息安全技术 传输层密码协议(TLCP)
- [8] IEEE 802.11 Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11:Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specifications
- [9] IEEE 802.11ax Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11:Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specifications Amendment 1:Enhancements for High-Efficiency WLAN
- [10] IEEE 802.1X IEEE Standard for Port Based Network Access Control
- [11] X.509 Certificate Policy for the United States Department of Defense,Version 5.0,13 December 1999
- [12] Peer-to-Peer Wireless Local Area Network(WLAN)Protection Profile for Sensitive But Unclassified Environments,Version 0.1,March 2008
- [13] Draft U.S.DoD Remote Access Protection Profile for High Assurance Environments,version 0.98,24 May 2000
- [14] High-Assurance Remote Access(HARA)Architecture,Version 1.1,15 May 2000
- [15] Global Information Grid(GIG)Policy 6-8510,Information Assurance Guidance,16 June 2000
- [16] Common Methodology for Information Technology Security Evaluation,Version 1.0,CEM-99/045,August 1999
- [17] Common Methodology for Information Technology Security Evaluation,Version 2.2.CCI-MB—2004-01-004. January 2004
- [18] National Information Assurance Partnership Protection Profile for General Purpose Operating Systems,Version:4.2.1,2019-04-22
- [19]National Information Assurance Partnership Mobile Device Fundamentals Version:3.2, 2021-04-15
- [20] National Information Assurance Partnership PP-Module for WLAN Clients,Version: 1.0, 2022-03-31



[21] General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package(EP)Wireless Local Area Network(WLAN)Clients,Version: 1.0, 2016-02-08

---



