ICS 35.030
CCS L 80

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

本文件按照GB/T1.1—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、深圳市信锐网科技术有限公司、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 1 1 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

GB15629.11、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。

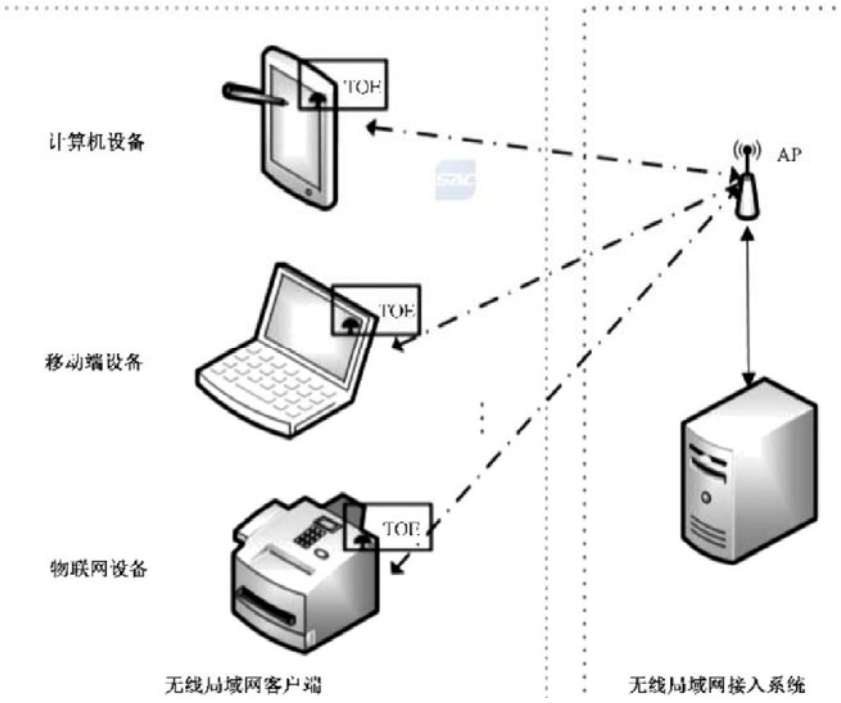

图 1 无线局域网客户端示意图

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。

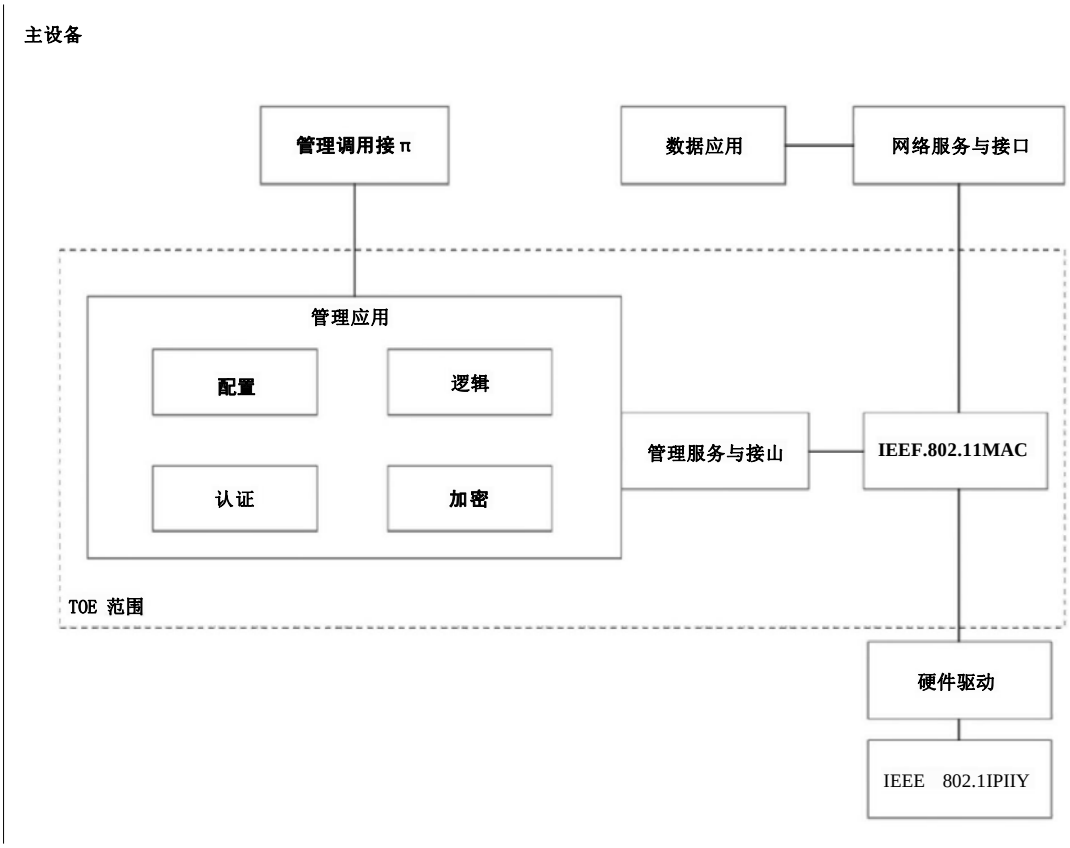

图 2 TOE 评估范围

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 TOF 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/T18336.2—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	EAL2十	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+	EAL3	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