ICS 35.040
L 80

中华人民共和国国家标准

GB/T 33565—2017

信息安全技术　无线局域网接入系统安全技术要求(评估保障级2级增强)

Information security technology—Security technology requirements for wireless local area network (wlan) access system(EAL2+)

2017-05-12 发布　　2017-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 无线局域网接入系统
安全技术要求(评估保障级2级增强)
GB/T 33565—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3 字数 85 千字
2017年5月第一版 2017年5月第一次印刷
*
书号:155066·1-55632 定价 42.00元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位:中国信息安全测评中心、湖北大学、西安西电捷通无线网络通信股份有限公司、中国人民解放军信息工程大学、国家信息中心、中国科学院研究生院信息安全国家重点实验室。

本标准主要起草人:郭涛、吕欣、贾依真、郝永乐、张普含、张龑、胡亚楠、张宝峰、毕海英、张翀斌、杨永生、刘威鹏、童伟刚、李淼、董国伟、朱龙华、张鲁国、王宪磊。

引　言

本标准依据 GB/T 18336—2015 中所规定的安全技术要求(保护轮廓)的结构形式,参考 GB/Z 20283—2006,制定了无线局域网接入系统安全技术要求(评估保障级 2 级增强)。

本标准详细描述了与无线局域网接入系统安全相关的假设、威胁和组织安全策略,定义了无线局域网接入系统及其运行环境,并由其导出安全功能要求和安全保障要求,通过基本原理论证安全要求能够追溯并覆盖安全目的,安全目的能够追溯并覆盖安全环境相关的假设、威胁和组织安全策略。

信息安全技术　无线局域网接入系统安全技术要求(评估保障级2级增强)

1　范围

本标准规定了对无线局域网接入系统的安全技术要求(评估保障级2级增强),主要包括无线局域网接入系统的假设、威胁和组织策略,以及安全目的、安全功能要求和安全保障要求。

本标准在GB/T 18336—2015中规定的评估保障级2级评估保障组件的基础上,增加了评估保障级3级中的ALC_FLR.2(缺陷报告程序)保障组件。

本标准适用于符合评估保障级2级增强的无线局域网接入系统的设计、开发、测试、评估和产品采购。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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—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

GB/T 18336.1—2015　信息技术　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—2015　信息技术　安全技术　信息技术安全性评估准则　第2部分:安全功能组件

GB/T 18336.3—2015　信息技术　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/Z 20283—2006　信息安全技术　保护轮廓和安全目标的产生指南

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 18336.1—2015、GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

审计服务器　audit server

存储审计事件/记录的设备。

3.2

保密性　confidentiality

使信息不泄露给未授权的个人、实体、进程,或不被其利用的特性。

3.3

威胁　threat

对资产或组织可能导致负面结果的一个事件的潜在源。

3.4

脆弱性 vulnerability

资产中能被威胁所利用的弱点。

3.5

无线局域网接入系统 WLAN access system;WAS

由能够实现用户接入无线局域网络的设备构成的整体。

4 缩略语

下列缩略语适用于本文件。

AE 鉴别器实体(Authenticator Entity)

ASU 鉴别服务单元(Authentication Server Unit)

BSS 基本服务组(Basic Service Set)

CM 配置管理(Configure Management)

EAL 评估保障级(Evaluation Assurance Level)

ESS 扩展服务集(Extended Service Set)

IBSS 独立基本服务组(Independent Basic Service Set)

IT 信息技术(Information Technology)

PP 保护轮廓(Protection Profile)

SFP 安全功能策略(Security Function Policy)

SFR 安全功能组件(Security Functional Requirement)

SOF 功能强度(Strength of Function)

ST 安全目标(Security Target)

STA 站(点)(Station)

TOE 评估对象(Target of Evaluation)

TSF TOE 安全功能(TOE Security Functions)

TSP TOE 安全策略(TOE Security Policy)

WAS 无线局域网接入系统(WLAN Access System)

WLAN 无线局域网(Wireless Local Area Network)

5 约定

5.1 假设

TOE 安全环境假设的命名以“A.”(Assume)开始,例如,A.ADMINISTRATION。

5.2 威胁

TOE 安全环境威胁的命名以“T.”(Threat)开始,例如,T.SIGNAL_DETECT。

5.3 策略

TOE 安全环境策略的命名以“P.”(Policy)开始,例如,P.GUIDANCE。

5.4 目的

TOE 安全目的和环境安全目的的命名分别以“O.”(Objective)和“OE.”(Objective Environment)开始,例如,O.ACCESS 和 OE.ADMIN。

5.5 扩展组件

本标准中使用的部分安全要求并未包括在 GB/T 18336—2015 中,这样的要求被称为“扩展组件”。扩展组件按照 GB/T 18336—2015 中“类/族/组件”模型进行定义和标识。在本标准中,扩展组件使用“EXP”表示。

5.6 操作

GB/T 18336—2015 允许对功能组件进行四种操作:赋值、细化、选择和反复,以执行安全功能组件。本标准按以下方式突出标识其中三种操作:

——赋值:允许指定参数。赋值部分以***粗斜体***形式表示。

——选择:允许从一个列表中选定一项或多项。选择部分将以**粗体**形式表示。

——反复:允许一个组件在不同操作时被使用超过一次以上。

6 TOE 描述

6.1 综述

本标准的评估对象(TOE)指的是基本服务组(BSS)以及扩展服务集(ESS)结构下的无线接入系统(WAS),分别如图 1 和图 2 所示。TOE 是由一个或一些能够实现站(STA)接入网络的设备所组成的整体,提供协议转换、有线网络连接、无线信号发射等功能,并提供管理、鉴别、加密/解密和审计等安全功能。典型的 TOE 安全功能结构如图 3 和图 4 所示。任何情况下 STA 与无线或有线网络间的数据交互都必须通过 TOE,TOE 通过分布式系统服务为 STA 提供对分布式系统的访问,但 TOE 不提供任何直接的网络服务。分布式系统经由泛端口与非本部分局域网进行逻辑连接。

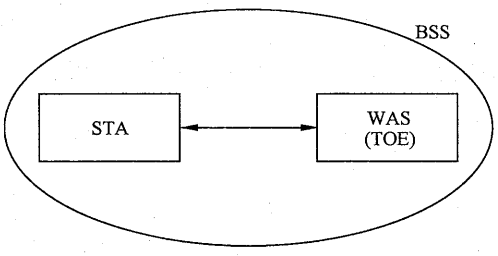

图 1 BSS 结构下的 TOE

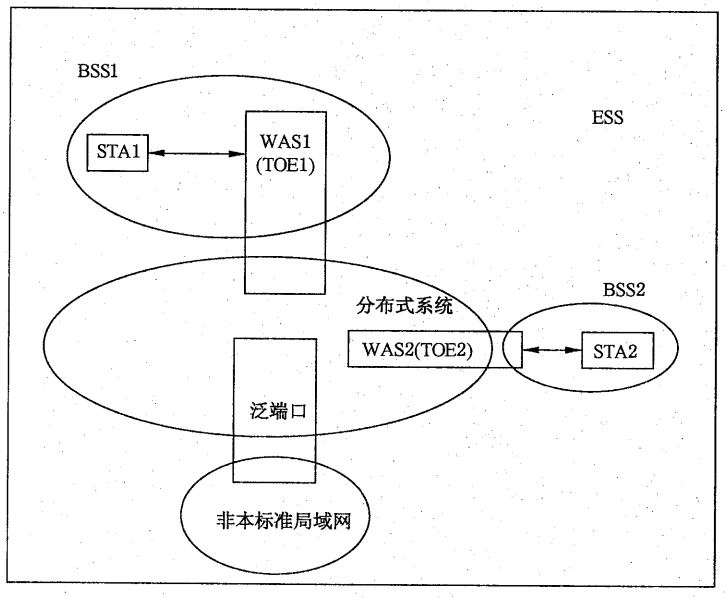

图 2　ESS 结构下的 TOE

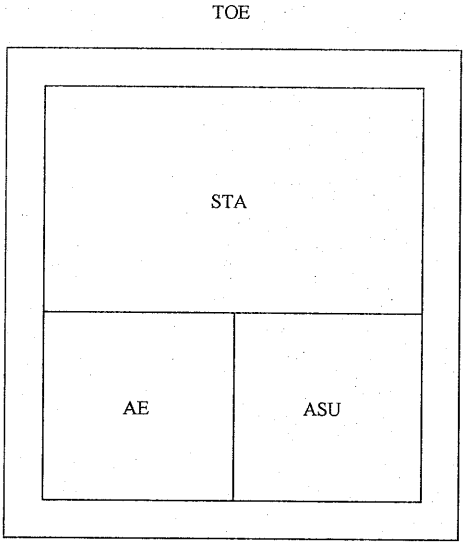

图 3　典型的 TOE 结构 1

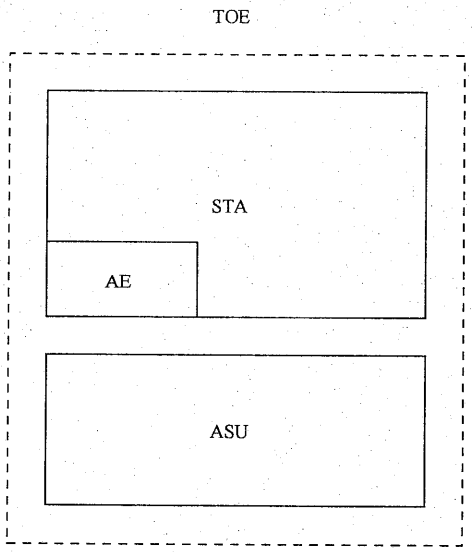

图 4　典型的 TOE 结构 2

6.2　管理

管理员负责安装、配置和维护 TOE。由于 TOE 可能是更大系统的一部分，所以负责管理 TOE 运行环境的人也应负责管理 TOE。本标准不排除多个单独管理的角色，但是要求只有一个 TOE 的管理员。

6.3　加密/解密

TOE 应提供加密/解密服务，例如对无线 MAC 帧等数据进行加密和解密操作。符合本标准的产品和系统应使用符合国家密码管理委员会办公室批准的用于无线局域网的对称密码算法的密码模块，并符合 GB 15629.11—2003 中保密机制的相关要求。

6.4 审计

TOE 在大多数情况下可以独立运行，安全审计包括产生审计事件、用户身份关联、选择性审计等。

6.5 鉴别及密钥管理

TOE 的鉴别应提供鉴别机制选择、密钥管理等功能，同时，鉴别模块应符合 GB 15629.11—2003 中鉴别机制的相关要求。

6.6 TOE 运行环境

在安全要求较高的情况下，可以借助于部署在有线局域网中的外部环境来执行更强的管理任务，例如审计服务器。但是，由于 TOE 有时是更大信息系统的一部分，因此对于 TOE 所依赖运行环境增加保护是必要的。

7 安全问题定义

7.1 假设

7.1.1 A.NO_GENERAL_PURPOSE

在 TOE 上无法获得通用的计算或存储能力(例如：编译器、编辑器或应用程序)。

7.1.2 A.TOE_NO_BYPASS

STA 与其他 STA 或有线网络上主机之间传输的数据必须通过 TOE。

7.1.3 A.PHYSICAL

环境应提供与 TOE 及其所包含数据的价值相一致的物理安全。

7.1.4 A.NO_EVIL

管理员是可信的，经过正式培训且遵循管理员指南。

7.2 威胁

7.2.1 T.ACCIDENTAL_ADMIN_ERROR

管理员可能不正确地安装或配置 TOE，从而导致安全机制失效。

7.2.2 T.ACCIDENTAL_CRYPTO_COMPROMISE

用户或进程不适当地访问(查看、修改或删除)与密码功能相关的密钥、数据或可执行代码，从而破坏了密码机制和这些机制所保护的数据。

7.2.3 T.MASQUERADE

用户可能假冒授权用户访问 TOE 资源。

7.2.4 T.POOR_DESIGN

TOE 需求规范或设计中的无意错误可能产生漏洞，可能被恶意用户或程序利用。

7.2.5 T.POOR_IMPLEMENTATION

TOE 实现中的无意错误可能引发漏洞，可能被恶意用户或程序利用。

7.2.6 T.POOR_TEST

开发或测试人员对 TOE 的测试不充分，导致不正确的 TOE 行为未被发现，恶意用户或程序可能利用这些漏洞。

7.2.7 T.RESIDUAL_DATA

用户变更或进程切换引起的 TOE 资源的重新分配导致了用户或进程对数据的非授权访问。

7.2.8 T.TSF_COMPROMISE

恶意用户或进程利用一般攻击不适当地访问(查看、修改或删除)TSF 数据或可执行代码。

7.2.9 T.UNATTENDED_SESSION

用户未授权访问了未被监管的会话。

7.2.10 T.UNAUTHORIZED_ACCESS

用户访问了未被授权访问的服务。

7.2.11 T.UNAUTH_ADMIN_ACCESS

未授权用户访问了管理员账户。

7.3 组织安全策略

7.3.1 P.ACCESS_BANNER

TOE 在管理员登录时应显示一个描述使用限制，法律规定或其他合理信息的初始旗标。

7.3.2 P.ACCOUNTABILITY

TOE 的授权用户应对自身在 TOE 内的行为负责。

7.3.3 P.CRYPTOGRAPHY

TOE 应为自身的应用提供密码功能，包括加密/解密操作。

7.3.4 P.CRYPTOGRAPHY_VALIDATED

仅有国家密码管理机构批准的密码算法(方法和实现)才能用于密钥管理(例如：密钥的产生、销毁、更新等)和密码服务(例如：加密、解密、签名等)。

7.3.5 P.ENCRYPTED_CHANNEL

应提供 TOE 与经授权接入网络的 STA 之间数据传输加/解密的功能。

8 安全目的

8.1 TOE 安全目的

8.1.1 O.AUDIT_GENERATION

TOE 应提供检查和创建与用户相关的安全事件记录的能力。

8.1.2 O.CORRECT_TSF_OPERATION

TOE 应提供验证 TSF 正确运行的能力。

8.1.3 O.CRYPTOGRAGHY

TOE 应提供密码功能以维护保密性和完整性。

8.1.4 O.CRYPTOGRAPHY_VALIDATED

TOE 应使用国家密码管理机构批准的密码模块提供密码服务。

8.1.5 O.DISPLAY_BANNER

在使用任何需要鉴别的 TOE 服务之前，TOE 应在建立管理员会话之前给出建议性警告。

8.1.6 O.MANAGE

TOE 应提供管理员管理 TOE 安全所必需的功能和设施，并防止这些功能和设施被未授权使用。

8.1.7 O.MEDIATE

TOE 必须遵循 TOE 安全策略转发 STA 的数据。

8.1.8 O.RESIDUAL_INFORMATION

TOE 应确保重新分配资源时 TOE 控制范围内受保护资源所包含的数据不被泄漏。

8.1.9 O.SELF_PROTECTION

TSF 应维护一个保护自身及其资源免受外部干预、未授权泄漏的执行域。

8.1.10 O.TIME_STAMPS

TOE 应获得可靠的时间戳。

8.1.11 O.TOE_ACCESS

TOE 应提供控制用户对 TOE 进行逻辑访问的机制。

8.1.12 O.ADMIN_GUIDANCE

TOE 应为安全管理员提供必要的安全信息。

8.1.13 O.CONFIG_IDENTIFICATION

任何实现的错误可以通过 TOE 的重新发布得到及时更正，以保证 TOE 的配置可以被确认。

8.1.14 O.DOCUMENTED_DESIGN

TOE 的开发设计应具有详细开发文档。

8.1.15 O.PARTIAL_FUNCTIONAL_TESTING

TOE 应进行安全功能测试以表明 TSF 满足 TOE 安全功能要求。

8.1.16 O.VULNERABILITY_ANALYSIS

应针对 TOE 进行脆弱性分析以表明 TOE 的设计和实现不存在明显缺陷。

8.2 运行环境安全目的

8.2.1 OE.AUDIT_PROTECTION

运行环境应提供保护审计信息和鉴别证书的能力。

8.2.2 OE.AUDIT_REVIEW

运行环境应提供选择性查看审计信息的能力。

8.2.3 OE.MANAGE

运行环境应增加管理员管理 TOE 安全所需的功能和设施，并防止这些功能和设施被未授权使用。

8.2.4 OE.NO_EVIL

使用 TOE 的组织应保证管理员是可信的，经过正式培训且遵循管理员指南。

8.2.5 OE.NO_GENERAL_PURPOSE

不存在与 TOE 运行无关的计算或存储功能(例如：编译器、编辑器或应用程序)。

8.2.6 OE.PHYSICAL

运行环境应提供与 TOE 和 TOE 所包含数据的价值相一致的物理安全。

8.2.7 OE.PROTECT_MGMT_COMMS

环境应保护审计记录到审计服务器的传输、远程网络管理以及鉴别服务器与 TOE 之间的通信。

8.2.8 OE.RESIDUAL_INFORMATION

环境应确保重新分配资源时环境控制范围内受保护资源所包含的信息不被泄漏。

8.2.9 OE.SELF_PROTECTION

环境应维护一个保护自身及其资源免受外部干扰、破坏或未授权泄漏的执行域。

8.2.10 OE.TIME_STAMPS

运行环境应提供可靠的时间戳。

8.2.11 OE.TOE_ACCESS

环境应提供有助于 TOE 控制用户对 TOE 进行逻辑访问的机制。

8.2.12 OE.TOE_NO_BYPASS

STA 与其他 STA 或有线网络上主机之间传输的数据必须通过 TOE。

9 扩展组件定义

9.1 扩展族:基准密码模块(FCS_BCM)

9.1.1 族行为

本族描述了国家密码管理机构认可的基准密码模块。

9.1.2 组件层次

FCS_BCM_EXP.1“基准密码模块”要求基准密码模块应使用国家密码管理机构认可的模块。

9.1.3 管理

无可预见的管理行为。

9.1.4 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:操作的成功和失败;

b) 基本级:除任何敏感信息(如秘密密钥或私有密钥)以外的客体属性和客体值。

9.1.5 FCS_BCM_EXP.1 基准密码模块

FCS_BCM_EXP.1.1 密码模块在执行密码功能时应采用国家密码管理机构批准的密码算法。

9.2 扩展组件

9.2.1 FCS 类:密码支持

9.2.1.1 FCS_COP_EXP.1 扩展组件:随机数产生

FCS_COP_EXP.1.1 通过在密码模块中使用[**赋值:*随机数产生器列表***],TSF 执行所有 TSF 密码功能所用到的随机数产生算法。

9.2.1.2 FCS_COP_EXP.2 扩展组件:密码运算

FCS_COP_EXP.2.1 密码模块应采用[**赋值:*密码算法***]执行加密和解密。

9.2.2 FDP 类:用户数据保护

9.2.2.1 FDP_PUD_EXP.1 用户数据保护

FDP_PUD_EXP.1.1 当管理员使用加密时,TSF 应:

a) 使用 FCS_COP_EXP.2 规定的密码算法加密从无线接入系统的无线接口传输到 STA 的已鉴

别用户的数据。

b) 使用 FCS_COP_EXP.2 规定的密码算法解密无线接入系统的无线接口接收到的来自 STA 的已鉴别用户的数据。

应用注释：本标准允许通过安全策略协商确定 TOE 使用 FCS_COP_EXP.2 规定的密码算法加密 WLAN 上传输的所有用户数据。

9.2.3 FIA 类：标识与鉴别

9.2.3.1 FIA_UAU_EXP.5(1) 扩展组件：多重鉴别机制

FIA_UAU_EXP.5.1(1)TSF 应为执行用户鉴别提供本地鉴别和远程鉴别机制。

FIA_UAU_EXP.5.2(1)TSF 应依据管理员的选择为管理员和用户调用远程鉴别机制。

应用注释：TOE 通过 ASU 对客户进行远程鉴别。另外，TSF 必须为本地管理员鉴别提供方法以免 TOE 不能与 ASU 进行通信。

9.2.3.2 FIA_UAU_EXP.5(2)远程鉴别机制

FIA_UAU_EXP.5.1(2)TOE 运行环境应为执行 TOE 远程用户鉴别提供[**赋值：*鉴别机制列表***]。

FIA_UAU_EXP.5.2(2)TOE 运行环境应依据[**赋值：*鉴别规则***]鉴别用户所声称的身份。

应用注释：对于现存 GB/T 18336—2015 是否需要特别规定 TSF 提供鉴别功能存在不同的意见，为了避免混乱，本标准包括该扩展的要求。本标准允许运行环境提供用于鉴别远程用户的鉴别服务器，ST 作者应使用该赋值以表明应用于 TOE 和运行环境的远程鉴别要求。

9.2.4 FPT 类：TSF 保护

9.2.4.1 FPT_STM_EXP.1 可靠的时间戳

FPT_STM_EXP.1.1TSF 应为自身的应用提供通过外部时间源进行同步的可靠时间戳。

应用注释：TOE 必须能够通过网络时间协议服务器获得时间戳。

9.2.4.2 FPT_TST_EXP.1TSF 检测

FPT_TST_EXP.1.1TSF 应在[***初始启动、接收到请求时***]运行一套自检程序以证实[***TSF 硬件操作***]能正确运行。

FPT_TST_EXP.1.2TSF 应能使用 TSF 提供的密码功能去验证除审计数据[**选择：*不需要验证完整性的动态 TSF 数据，无***]以外所有 TSF 数据的完整性。

FPT_TST_EXP.1.3TSF 应能通过[**TSF 提供的密码功能**]提供验证所存储的 TSF 可执行代码的完整性的能力。

应用注释：元素 1.1 中，仅有 TSF 的硬件需要自检，而软件通常不需要自检。元素 1.3 解决了 TSF 软件完整性。元素 1.2 中，ST 作者应确定不需要完整性验证的 TSF 数据。

9.2.4.3 FPT_TST_EXP.2 对密码模块进行 TSF 检测

FPT_TST_EXP.2.1TSF 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[赋值：产生自检的条件]条件时***]运行一套密码模块提供的自检程序以表明 TSF 密码组件操作的正确性。

FPT_TST_EXP.2.2TSF 在产生一个密钥后应立即运行一套密码模块提供的自检。

应用注释：如果 TOE 产生密钥，那么应提供元素 2.2 中具体的功能。

9.2.5 FTP 类:可信路径/通道

9.2.5.1 FTP_ITC_EXP.1 TSF 间可信信道

FTP_ITC_EXP.1.1TOE 应在他自己和 TOE 运行环境中的实体之间提供一条加密通信信道,此信道在逻辑上与其他通信信道不同,其端点具有保证标识,并且能保护信道中数据免遭修改或泄漏。

FTP_ITC_EXP.1.2TSF 应允许[**选择:*TOE*、*另一个可信 IT 产品***]经由可信信道发起通信。

FTP_ITC_EXP.1.3 对于[**赋值:*需要可信信道的功能列表***]],TSF 应经由可信信道发起通信。

10 TOE 安全要求

10.1 TOE 安全功能要求

10.1.1 概述

本标准 TOE 应满足表 1 列出的安全功能要求,这些要求由 GB/T 18336.2—2015 给出的和扩展的安全功能组件组成。

表 1 TOE 安全功能要求

安全功能组件类	安全功能组件	组件名称	依赖关系
FAU 类:安全审计	FAU_GEN.1	审计数据产生	FPT_STM.1
	FAU_GEN.2	用户身份关联	FAU_GEN.1 FIA_UID.1
	FAU_SEL.1	选择性审计	FAU_GEN.1 FMT_MTD.1
FCS 类:密码支持	FCS_BCM_EXP.1	基准密码模块	无
	FCS_CKM.1	密钥生成	[FCS_CKM.2,或 FCS_COP.1] FCS_CKM.4
	FCS_CKM.4	密钥销毁	[FDP_ITC.1,或 FDP_ITC.2,或 FCS_CKM.1]
	FCS_COP_EXP.1	随机数产生	[FDP_ITC.1 或 FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
	FCS_COP_EXP.2	密码运算	[FDP_ITC.1 或 FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FDP 类:用户数据保护	FDP_PUD_EXP.1	用户数据保护	无
	FDP_RIP.1	子集残余信息保护	无

表 1（续）

安全功能组件类	安全功能组件	组件名称	依赖关系
FIA 类：标识和鉴别	FIA_AFL.1	鉴别失败处理	FIA_UAU.1
	FIA_ATD.1(1)	管理员属性定义	无
	FIA_ATD.1(2)	用户属性定义	无
	FIA_UAU.1	鉴别的时机	FIA_UID.1
	FIA_UAU_EXP.5	多重鉴别机制	无
	FIA_UID.2	任何动作前的用户标识	FIA_UID.1
	FIA_USB.1	用户-主体绑定	FIA_ATD.1
FMT 类：安全管理	FMT_MOF.1(1)	安全功能行为的管理（密码功能）	FMT_SMF.1(1) FMT_SMR.1
	FMT_MOF.1(2)	安全功能行为的管理（审计记录的产生）	FMT_SMF.1(2) FMT_SMR.1
	FMT_MOF.1(3)	安全功能行为的管理（鉴别）	FMT_SMF.1 FMT_SMR.1
	FMT_MSA.2	安全的安全属性	ADV_SPM.1 [FDP_ACC.1 或 FDP_IFC.1] FMT_MSA.1 FMT_SMR.1
	FMT_MTD.1(1)	审计数据的管理	FMT_SMR.1 FMT_SMF.1
	FMT_MTD.1(2)	鉴别数据的管理（管理员）	FMT_SMR.1 FMT_SMF.1
	FMT_MTD.1(3)	鉴别数据的管理（用户）	FMT_SMR.1 FMT_SMF.1
	FMT_SMF.1(1)	管理功能规范（密码功能）	无
	FMT_SMF.1(2)	管理功能规范（TOE 审计记录产生）	无
	FMT_SMF.1(3)	管理功能规范（加密密钥数据）	无
	FMT_SMR.1	安全角色	FIA_UID.1
FPT 类：TSF 保护	FPT_STM_EXP.1	可靠的时间戳	无
	FPT_TST_EXP.1	TSF 检测	FCS_CKM.2 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2
	FPT_TST_EXP.2	对密码模块进行 TSF 检测	FCS_CKM.2 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2

表 1（续）

安全功能组件类	安全功能组件	组件名称	依赖关系
FTA 类：TOE 访问	FTA_SSL.3	TSF 原发会话终止	无
	FTA_TAB.1	缺省的 TOE 访问旗标	无
FTP 类：可信路径/通道	FTP_ITC_EXP.1	TSF 间可信信道	无
	FTP_TRP.1	可信路径	无

10.1.2 FAU 类：安全审计

10.1.2.1 FAU_GEN.1 审计数据产生

FAU_GEN.1.1 TSF 应能为下述可审计事件产生审计记录：

a) 审计功能的开启和关闭；

b) 有关[**最小级**]审计级别的所有可审计事件；

c) [***赋值：其他专门定义的可审计事件***]。

FAU_GEN.1.2 TSF 应在每个审计记录中至少记录下列信息：

a) 事件的日期和时间、事件的类型、主体身份（如果适用）、事件的结果（成功或失效）；

b) 对每种审计事件类型，基于 PP/ST 中功能组件的可审计事件定义，[表 2 第三列规定的信息]。

应用注释：表 2 第三列中，如果在产生记录的事件环境中“如果可用/适用”是有意义的，那么它用于确定应在审计记录中包含的数据。如果对于一种特别审计事件类型不要求其他的信息（FAU_GEN.1.2 除外），那么“无”也是可以接受的。

表 2 TOE 可审计事件

要求	审计事件	附加的审计记录内容
FAU_GEN.1	无	无
FAU_GEN.2	无	无
FAU_SEL.1	审计收集功能运行时修改审计配置	执行该功能的管理员身份
FCS_CKM.1	密钥生成	执行该功能的管理员身份
FCS_CKM.4	密钥销毁	如果可用，执行该功能的管理员身份
FCS_COP_EXP.1	无	无
FCS_COP_EXP.2	无	无
FDP_PUD_EXP.1	启动或关闭 TOE 对无线流量的加密	执行该功能的管理员身份
FDP_RIP.1(1)	无	无
FIA_AFL.1	到达了不成功鉴别尝试的阈值，采取行动（锁定终端）。在适当的时机，恢复正常的状态（重新激活终端）	无
FIA_ATD.1	无	无

表 2（续）

要求	审计事件	附加的审计记录内容
FIA_UAU.1	鉴别机制的使用(成功或失败)	用户身份——TOE 将不在审计日志中记录无效的密码
FIA_UAU_EXP.5	没有接收到来自远程鉴别服务器的响应	确定没有做出响应的鉴别服务器的身份
FIA_UID.2	无	无
FIA_USB.1	用户安全属性和主体之间不成功绑定	无
FMT_MOF.1(1)	变更 TOE 加密/解密算法，包括选择对通信不进行加密/解密	密码算法选择(或无)
FMT_MOF.1(2)	开始或停止产生审计记录	无
FMT_MOF.1(3)	TOE 远程鉴别环境的变更； 失败鉴别尝试的阈值变化； 会话锁定时间的变化	执行该功能的管理员身份
FMT_MSA.2	所有提供或拒绝的安全属性值；	无
FMT_MTD.1(1)	用于预先选择审计事件的规则集的变化	无
FMT_MTD.1(2) FMT_MTD.1(3)	TOE 鉴别证书的变化	如果 TOE 将不在审计日志中记录鉴别证书，那么此项为无
FMT_REV.1	安全属性撤销失败	无
FMT_SMR.1	属于同一个角色的用户组的修改	无
FPT_STM._EXP.1	时间的变化	无
FPT_TST_EXP.1	执行自检测	检测成功或失败
FPT_TST_EXP.2	执行自检测	检测成功或失败
FTA_SSL.3	TSF 原发终止	通过会话锁定机制终止一个交互式会话
FTP_ITC_EXP.1	可信信道的开启/关闭	确定尝试建立或创建信道的远程实体身份；事件的成功或失败
FTP_TRP.1	可信信道的开启	确定尝试建立或创建信道的远程实体身份；事件的成功或失败

10.1.2.2 FAU_GEN.2 用户身份关联

FAU_GEN.2.1 对于已标识身份的用户的行为所产生的审计事件，TSF 应能将每个可审计事件与引起该事件的用户身份相关联。

10.1.2.3 FAU_SEL.1 选择性审计

FAU_SEL.1.1 TSF 应能根据以下属性从审计事件集合中选择可审计事件：

a) [**选择：用户身份，事件类型**]；

b) [**赋值：*设备接口*，*STA 身份***]。

应用注释：设备接口是用户(或管理员)接收/发送数据的物理接口(如无线局域网接口、局域网接口、串口、管理局域网接口等)。

10.1.3 FCS 类:密码支持

10.1.3.1 FCS_BCM_EXP.1 扩展组件:基准密码模块

FCS_BCM_EXP.1.1 密码模块在执行密码功能时应采用国家密码管理机构批准的密码算法。

10.1.3.2 FCS_CKM.1 密钥生成

FCS_CKM.1.1 TSF 应根据符合下列标准[***国家密码管理机构批准的***]一个特定的密钥生成算法[**赋值:*密钥生成算法***]和特定的[**赋值:*密钥长度***]来产生密钥。

10.1.3.3 FCS_CKM.4 密钥销毁

FCS_CKM.4.1 TSF 应根据符合下列标准[***国家密码管理机构批准的***]的一个特定的密钥销毁方法[**赋值:*密钥销毁方法***]来销毁密钥。

10.1.3.4 FCS_COP_EXP.1 扩展组件:随机数产生

FCS_COP_EXP.1.1 通过在密码模块中使用[**赋值:随机数产生器列表**],TSF 执行所有 TSF 密码功能所用到的随机数产生算法。

10.1.3.5 FCS_COP_EXP.2 扩展组件:密码运算

FCS_COP_EXP.2.1 密码模块应采用[**赋值:国家密码管理委员会办公室批准的用于无线局域网的对称密码算法**]执行加密和解密。

10.1.4 用户数据保护(FDP)

10.1.4.1 FDP_PUD_EXP.1 用户数据保护

FDP_PUD_EXP.1.1 当管理员使用加密时,TSF 应:

a) 使用 FCS_COP_EXP.2 规定的密码算法加密从无线接入系统的无线接口传输到 STA 的已鉴别用户的数据;

b) 使用 FCS_COP_EXP.2 规定的密码算法解密无线接入系统的无线接口接收到的来自 STA 的已鉴别用户的数据。

应用注释:本标准允许通过安全策略协商确定 TOE 使用 FCS_COP_EXP.2 规定的密码算法加密 WLAN 上传输的所有用户数据。

10.1.4.2 FDP_RIP.1 子集残余信息保护

FDP_RIP.1.1 TSF 应确保一个资源的任何先前信息内容,在[**分配资源到**]下列客体[***网络数据包***]以及[**释放资源至**]客体[***网络数据包***]时不再可用。

应用注释:本标准保证 TOE 不允许先前传输的数据包数据插入到当前数据包未使用的区域或填充区。

10.1.5 标识与鉴别(FIA)

10.1.5.1 FIA_AFL.1 鉴别失败处理

FIA_AFL.1.1 TSF 应检测当[**选择:[赋值:*正整数*],*管理员可设置的***[**赋值:*可接受数值范围*]*内的一个正整数***]时,与[**赋值:*鉴别事件列表***]相关的未成功鉴别尝试。

FIA_AFL.1.2 当[**选择：达到，超过**]所定义的未成功鉴别尝试次数时，TSF 应采取的[***阻止管理员登录直到其他本地管理员采取行动***]。

应用注释：本标准没有要求 TOE 允许远程管理。可是，如果 TOE 确实允许管理员远程登录 TOE（例如：从有线接口），那么 TOE 必须提供防止对管理账户进行蛮力攻击的机制。

10.1.5.2 FIA_ATD.1(1) 管理员属性定义

FIA_ATD.1.1(1) TSF 应维护属于每个管理员的下列安全属性列表：[**选择：口令，**[**赋值：*任何附加的管理员安全属性列表*]]。

应用注释：ST 作者应指明与管理员账户相关的附加管理员安全属性。如果 TOE 没有使用附加安全属性，那么赋值应指明“无附加属性”。

10.1.5.3 FIA_ATD.1(2) 用户属性定义

FIA_ATD.1.1(2) TSF 应保存属于每个远程鉴别用户的下列安全属性列表：[**赋值：*用户安全属性列表***]。

应用注释：ST 作者应指明与远程鉴别用户相关的安全属性。

10.1.5.4 FIA_UAU.1 鉴别的时机

FIA_UAU.1.1 在用户被鉴别前，TSF 应允许执行代表用户的[**赋值：*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 TSF 促成的动作前，TSF 应要求每个用户都已被成功鉴别。

应用注释：本功能要求针对 TOE 本地鉴别的用户，并不涉及进行鉴别之前，必须在 STA 和接入系统之间传输的管理和控制数据包。

10.1.5.5 FIA_UAU_EXP.5(1) 扩展组件：多重鉴别机制

FIA_UAU_EXP.5.1(1) TSF 应为执行用户鉴别提供本地鉴别和远程鉴别机制。

FIA_UAU_EXP.5.2(1) TSF 应依据管理员的选择为管理员和用户调用远程鉴别机制。

应用注释：TOE 通过 ASU 对客户进行远程鉴别。另外，TSF 必须为本地管理员鉴别提供方法以免 TOE 不能与 ASU 进行通信。

10.1.5.6 FIA_UID.2 任何动作前的用户标识

FIA_UID.2.1 在允许执行代表该用户的任何其他 TSF 促成动作之前，TSF 应要求每个用户身份都已被识别。

应用注释：本标准不包括鉴别以前必须在 STA 和接入系统之间传输的管理和控制数据包。

10.1.5.7 FIA_USB.1 用户-主体绑定

FIA_USB.1.1 TSF 应将下列用户安全属性：[**赋值：*用户安全属性列表***] 与代表用户活动的主体相关联。

FIA_USB.1.2 TSF 应对用户安全属性与代表用户活动的主体初始关联关系执行下列规则：[**赋值：*属性初始关联规则***]。

FIA_USB.1.3 TSF 应执行下列规则管理用户安全属性与代表用户活动的主体间的关联关系的变化：[**赋值：*属性更改规则***]。

应用注释：ST 作者应指出与代表管理员和 STA 活动的主体相关联的属性。如果必要，本组件可以反复。

10.1.6 安全管理(FMT)

10.1.6.1 FMT_MOF.1(1) 密码安全功能行为的管理

FMT_MOF.1.(1) TSF 应仅限于[*管理员*]对功能[*功能列表*：

a) *密码：装入密钥*；

b) *密码：删除/销毁密钥*；

c) *密码：设置密钥生命周期*；

d) *密码：设置密码算法*；

e) *密码：设置 TOE 加密或不加密无线通信信息*；

f) *密码：对 TOE 硬件和密码功能执行自测*]具有[修改其行为]的能力。

10.1.6.2 FMT_MOF.1(2) 审计安全功能行为的管理

FMT_MOF.1.(2) TSF 应仅限于[*管理员*] 对功能[*功能列表*：

a) *审计：预先选择触发审计记录的事件*；

b) *审计：打开和关闭审计功能*]具有[激活、终止、修改其行为]的能力。

10.1.6.3 FMT_MOF.1(3) 鉴别安全功能行为的管理

FMT_MOF.1.1(3) TSF 应仅限于[*管理员*]对功能[*功能列表*：

a) *鉴别：允许或禁止鉴别服务器的使用*；

b) *鉴别：设置 TOE 采取行动禁止未登录前所发生的鉴别失败次数*；

c) *鉴别：设置会话终止前处于非活动状态的时长*]具有[修改其行为]的能力。

10.1.6.4 FMT_MSA.2 安全的安全属性

FMT_MSA.2.1 TSF 应确保安全属性[赋值：*安全属性列表*]只接受安全的值。

10.1.6.5 FMT_MTD.1(1) 预选审计数据的管理

FMT_MTD.1(1) TSF 应仅限于[*管理员*]能够对[*用于预先选择审计事件的规则集*][改变默认值、查询、修改、删除、[*创建*]]。

10.1.6.6 FMT_MTD.1(2) 鉴别数据的管理(管理员)

FMT_MTD.1(2) TSF 应仅限于给[*管理员*] 能够对[*鉴别证书、用户标识证书*] [改变默认值、查询、修改、删除、[*创建*]]。

10.1.6.7 FMT_MTD.1(3) 鉴别数据的管理(用户)

FMT_MTD.1(3) TSF 应仅限于给[*TOE 用户*] 能够对[*用户鉴别证书*][修改]。

10.1.6.8 FMT_SMF.1(1) 管理功能规范(密码功能)

FMT_SMF.1.1(1) TSF 应能够执行如下管理功能：[*依据管理员对 TOE 的配置，查询和设置对网络数据包的加密/解密(通过 FCS_COP_EXP.2)*]。

应用注释：本标准保证负责 TOE 管理的人员能选择 FCS_COP_EXP.2 规定的密码算法，对 TOE 所传输的数据进行加密/解密或选择不加密。

10.1.6.9 FMT_SMF.1(2) 管理功能规范(TOE 审计记录产生)

FMT_SMF.1.1(2) TSF 应能够执行如下管理功能:[*查询、打开或关闭安全审计*]。

应用注释:本标准保证负责 TOE 管理的人员能打开或关闭 TOE 审计记录产生功能。

10.1.6.10 FMT_SMF.1(3) 管理功能规范(密钥数据)

FMT_SMF.1.1(3) TSF 应能够执行如下管理功能:[*依据 FDP_PUD_EXP 查询、设置、修改和删除密钥,打开或关闭密钥测试验证*]。

应用注释:本标准的目的是提供配置 TOE 密钥的功能。配置密钥数据包括:设置密钥生命周期、设置密钥长度等。

10.1.6.11 FMT_SMR.1 安全角色

FMT_SMR.1.1 TSF 应维护角色[*管理员、用户*]。

FMT_SMR.1.2 TSF 应能够把用户和角色关联起来。

应用注释:只有管理员可以直接访问 TOE,用户可以通过 TOE 传输数据,但不能直接访问 TOE。本标准也假设 TOE 包含本地鉴别机制和使用远程鉴别服务器的能力。虽然用户是本地的或远程的,但是这不影响用户的角色。

10.1.7 FPT 类:TSF 保护

10.1.7.1 FPT_STM_EXP.1 可靠的时间戳

FPT_STM_EXP.1.1 TSF 应为自身的应用提供通过外部时间源进行同步的可靠时间戳。

应用注释:TOE 必须能够通过 NTP 服务器获得时间戳。

10.1.7.2 FPT_TST_EXP.1 TSF 检测

FPT_TST_EXP.1.1 TSF 应在[*初始启动、接收到请求时*]运行一套自检程序以证明[*TSF 硬件操作*]的正确性。

FPT_TST_EXP.1.2 TSF 应能使用 TSF 提供的密码功能去验证除审计数据[选择:[*不需要验证完整性的动态 TSF 数据,无*]以外所有 TSF 数据的完整性。

FPT_TST_EXP.1.3 TSF 应能通过[**TSF 提供的密码功能**]提供验证所存储的 TSF 可执行代码的完整性的能力。

应用注释:元素 1.1 中,仅有 TSF 的硬件需要自检,而软件通常不需要自检。元素 1.3 解决了 TSF 软件完整性。元素 1.2 中,ST 作者应确定不需要完整性验证的 TSF 数据。

10.1.7.3 FPT_TST_EXP.2 对密码模块进行 TSF 检测

FPT_TST_EXP.2.1 TSF 应在[*初始启动、接收到请求时*]运行一套密码模块提供的自检程序以表明 TSF 密码组件操作的正确性。

FPT_TST_EXP.2.2 TSF 在产生一个密钥后应立即运行一套密码模块提供的自检。

应用注释:如果 TOE 产生密钥,那么应提供元素 2.2 中具体的功能。

10.1.8 FTA 类:TOE 访问

10.1.8.1 FTA_SSL.3 TSF 原发终止

FTA_SSL.3.1 TSF 应在达到[*管理员配置的用户不活动的时间间隔*]之后终止一个交互式会话。

应用注释：本标准适用于本地管理会话和通过 TOE 传递数据的无线会话。

10.1.8.2 FTA_TAB.1 缺省的 TOE 访问旗标

FTA_TAB.1.1 在建立一个用户会话之前，TSF 应显示有关未授权使用 TOE 的一个劝告性警示信息。

10.1.9 FTP 类：可信路径/通道(FTP)

10.1.9.1 FTP_ITC_EXP.1 TSF 间的可信信道

FTP_ITC_EXP.1.1 TOE 应在他自己和 TOE IT 环境中的实体之间提供一条加密通信信道，此信道在逻辑上与其他通信信道不同，其端点具有保证标识，并且能保护信道中数据免遭修改或泄漏。

FTP_ITC_EXP.1.2 TSF 应允许[**TOE 或 TOEIT 环境中的实体**]经由可信信道发起通信。

FTP_ITC_EXP.1.3 对于[***所有鉴别功能、远程登录、时间***、[**选择**：[***赋值：经与 ST 作者确认的授权信息系统实体的通信***]、**无**]]，TSF 应经可信信道发起通信。

应用注释：如果 CA 服务器在鉴别用户时发挥作用，那么 CA 被认为是一个授权信息系统实体。TSF 应与该实体进行安全通信。IT 环境包括一个 NTP 服务器，审计服务器和/或鉴别服务器。

10.1.9.2 FTP_TRP.1 可信路径

FTP_TRP.1.1 TSF 应在他自己和[**STA**]之间提供一条通信路径，此路径在逻辑上与其他通信路径截然不同，并对其端点进行了有保障的标识，并能保护信道数据免遭[**修改、泄露**]。

FTP_TRP.1.2 TSF 应允许[**STA**]经由可信路径发起通信。

FTP_TRP.1.3 对于[**选择：启动 STA 鉴别**、[***赋值：其他需要可信路径服务***]]，TSF 应要求使用可信路径。

应用注释：本标准确保 STA 和接入系统之间最初的鉴别信息交换受到保护。

10.2 TOE 安全保障要求

本标准 TOE 应满足表 3 列出的安全保障要求，这些要求由 GB/T 18336.3—2015 中的评估保障级 2 级的安全保障要求组件和增强组件组成。表 3 中用粗体字突出了增强组件。这些保障要求确定了 TOE 管理和评估活动，它们对于解决本标准所确定的威胁和策略是必需的。

表 3 TOE 安全保障要求

保障类	保障组件	组件名称
ADV：开发	ADV_ARC.1	安全架构描述
	ADV_FSP.2	安全执行功能规范
	ADV_TDS.1	基础设计
AGD：指导性文档	AGD_OPE.1	操作用户指南
	AGD_PRE.1	准备程序
ALD：生命周期支持	ALC_CMC.2	CM 系统的使用
	ALC_CMS.2	部分 TOE CM 覆盖
	ALC_DEL.1	交付程序
	ALC_FLR.2	**缺陷报告程序**

表 3（续）

保障类	保障组件	组件名称
ASE:ST 评估	ASE_CCL.1	符合性声明
	ASE_ECD.1	扩展组件定义
	ASE_INT.1	ST 引言
	ASE_OBJ.2	安全目的
	ASE_REQ.2	推导出的安全要求
	ASE_TSS.1	TOE 概要规范
ATE:测试	ATE_COV.1	覆盖证据
	ATE_FUN.1	功能测试
	ATE_IND.2	独立测试-抽样
AVA:脆弱性评定	AVA_VAN.2	脆弱性分析

11 运行环境安全要求

11.1 概述

本标准 TOE 运行环境应满足表 4 列出的安全功能要求，这些要求由 GB/T 18336.2—2015 给出的和扩展的安全功能组件组成。

TOE 运行环境包括鉴别服务器、时间服务器、审计服务器等。对于审计服务器，环境提供保护审计信息和选择性查看审计数据的能力；对于鉴别服务器，环境提供管理鉴别信息和限制蛮力口令攻击的能力。如果这些实体与 TOE 不在同一个物理设备上，那么这些实体与 TOE 之间的通信应受到保护。另外，运行环境负责保护自身安全，确保它的安全机制不会被绕过。

表 4 运行环境安全要求

安全功能组件类	安全保障要求组件	组件名称	依赖关系
FAU 类:安全审计	FAU_GEN.1	审计数据产生	无
	FAU_SAR.1	审计查阅	FAU_GEN.1
	FAU_SAR.2	限制审计查阅	FAU_SAR.1
	FAU_SAR.3	可选审计查阅	FAU_SAR.1
	FAU_STG.1	受保护的审计迹存储	FAU_GEN.1
	FAU_STG.3	审计数据可能丢失情况下的行为	FAU_STG.1
FDP 类:用户数据保护	FDP_RIP.1	子集残余信息保护	无
FIA 类:标识和鉴别	FIA_AFL.1	远程用户失败处理	FIA_UAU.1
	FIA_ATD.1	用户属性定义	无
	FIA_UAU_EXP.5	远程鉴别机制	FIA_UID.1
	FIA_UID.1	适时标识	无

表 4（续）

安全功能组件类	安全保障要求组件	组件名称	依赖关系
FMT 类：安全管理	FMT_MOF.1	安全功能行为的管理	FMT_SMF.1(1)、FMT_SMF.1(2)、FMT_SMF.1(3) FMT_SMR.1
	FMT_MTD.1	时间数据的管理	FMT_SMR.1
	FMT_SMR.1	安全角色	无
FTP 类：安全功能保护	FTP_ITC_EXP.1	TSF 间可信信道	无
	FPT_STM.1	可靠的时间戳	无

应用注释：本标准要求 TOE 运行环境提供重要的功能。声明符合本标准的 ST 满足一些或所有上述运行环境要求（表 4）都是可以接受的。

11.2 FAU 类：安全审计

11.2.1 FAU_GEN.1 审计数据产生

FAU_GEN.1.1 TOE 运行环境应能为下述可审计事件产生审计记录：

a） 审计功能的启动和关闭；

b） 有关[**最小级**]审计级别的所有可审计事件；

c） [**赋值：*其他专门定义的可审计事件***]。

FAU_GEN.1.2 TOE 运行环境应在每个审计记录中至少记录如下信息：

a） 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（成功或失效）；

b） 对每种审计事件类型，基于 PP/ST 中功能组件的可审计事件定义的[***表 5 第三列规定的信息***]。

应用注释：表 5 第三列中，如果在产生记录的事件环境中“如果可用/适用”是有意义的，那么它用于确定应在审计记录中包含的数据。如果对于一种特别审计事件类型不要求其他的信息（FAU_GEN.1.2 除外），那么“无”也是可以接受的。

表 5 TOE 运行环境的审计事件

安全功能组件	审计事件	附加的审计记录内容
FAU_GEN.1.2	无	无
FAU_SAR.1	无	无
FAU_SAR.2	读取审计记录的不成功尝试	尝试执行该功能的用户身份
FAU_SAR.3	无	无
FAU_STG.1	无	无
FAU_STG.3	当审计迹超过预定的限制时所采取的任何行动	无
FDP_RIP.1	无	无
FIA_AFL.1	达到不成功鉴别尝试的阈值时，采取行动（锁定终端）。在适当的时机，恢复正常的状态（重新打开终端）	无

表 5（续）

安全功能组件	审计事件	附加的审计记录内容
FIA_ATD.1	无	无
FIA_UAU_EXP.5	鉴别机制的使用(成功或失败)	用户身份——TOE 不记录无效的口令
FIA_UID.1	无	无
FMT_MOF.1	审计服务器设置的变化 鉴别服务器设置的变化 时间服务器设置的变化	无
FMT_MTD.1	时间数据的变化	无
FMT_SMR.1	无	无
FTP_ITC_EXP.1	可信信道的开启/关闭	标识创建信道的实体身份 事件的成功或失败
FPT_STM.1	设置时间/日期	执行该行为的管理员身份

11.2.2 FAU_SAR.1 审计查阅

FAU_SAR.1.1 TOE 运行环境应为[***管理员***]提供从审计记录中读取[***所有审计数据***]的能力。

FAU_SAR.1.2 TOE 运行环境应以便于管理员理解的方式提供审计记录。

应用注释：本标准确保 TOE 运行环境为管理员提供查阅 TOE 所产生审计记录所需的功能。

11.2.3 FAU_SAR.2 限制审计查阅

FAU_SAR.2.1 除明确准许读访问的用户外，TOE 运行环境应禁止所有用户对审计记录的读访问。

应用注释：本标准确保仅有那些具有查阅信息权限的用户可以访问 TOE 产生的审计记录。

11.2.4 FAU_SAR.3 可选审计查阅

FAU_SAR.3.1 TOE 运行环境应根据[***事件类型、日期、时间和/或[赋值：其他的分类/搜索/排序标准]***]提供对审计数据进行[***搜索、分类、排序***]的能力。

11.2.5 FAU_STG.1 受保护的审计迹存储

FAU_STG.1.1 TOE 运行环境应保护审计迹中存储的审计记录，以避免未授权的删除。

FAU_STG.1.2 TOE 运行环境应能[**防止**]对审计迹中所存审计记录的未授权修改。

11.2.6 FAU_STG.3 审计数据可能丢失情况下的行为

FAU_STG.3.1 如果审计迹超过[**管理员设定的存储容量百分比**]，TOE 运行环境应采取[***通过在本地控制台上立即显示一条信息向管理员报警***，[选择：[***赋值：ST 作者采取其他行动***]，***"无"***]]。

应用注释：当审计迹超过预定的限制时，ST 作者应决定是否采取其他行动。如果采取行动，进行赋值；否则选择"无"。

11.3 FDP 类:用户数据保护

11.3.1 FDP_RIP.1 子集残余信息保护

FDP_RIP.1.1 TOE 运行环境应确保一个资源的任何先前信息内容,在[**分配资源到**]客体[***网络数据包***]时不再可用。

11.4 FIA 类:标识与鉴别

11.4.1 FIA_AFL.1 远程用户鉴别失败处理

FIA_AFL.1.1 TOE 运行环境应当检测[**选择**:[***赋值:正整数***],***管理员可设置的***[***赋值:可接受数值范围***]***内的一个正整数***]时,与[***赋值:鉴别时间列表***]相关的未成功鉴别尝试。

FIA_AFL.1.2 当[**达到,超过**]所定义的未成功鉴别尝试次数时,TOE 运行环境应采取的[***阻止管理员登录直到其他本地管理员采取行动***]。

应用注释:本标准确保 TOE 运行环境能够检测到多次鉴别尝试,并采取措施阻止进一步地鉴别尝试。

11.4.2 FIA_ATD.1 用户属性定义

FIA_ATD.1.1 TOE 运行环境应维护属于每个远程鉴别用户的下列安全属性列表:[***赋值:用户安全属性列表***]。

应用注释:ST 作者应表明运行环境所保存的、与远程鉴别用户相关的安全属性。

11.4.3 FIA_UAU_EXP.5 远程鉴别机制

FIA_UAU_EXP.5.1 TOE IT 环境应为执行 TOE 远程用户鉴别提供[**远程鉴别机制**]。

FIA_UAU_EXP.5.2 TOE IT 环境应依据[**赋值:描述远程鉴别机制如何鉴别 TOE 远程用户的规则**]鉴别用户所声称的身份。

应用注释:对于现存 GB/T 18336—2015 是否需要特别规定 TSF 提供鉴别功能存在不同的意见,为了避免混乱,本标准包括该扩展的要求。本标准允许 IT 环境提供用于鉴别远程用户的鉴别服务器,ST 作者应使用该赋值以表明应用于 TOE 和 IT 环境的远程鉴别要求。

11.4.4 FIA_UID.1 标识的时机

FIA_UID.1.1 在用户被标识之前,TOE 运行环境应允许执行代表 TOE 远程用户的[***赋值:运行环境促成的行动列表***]。

FIA_UID.1.2 在允许代表 TOE 远程用户的任何其他运行环境或 TSF 仲裁动作之前,TOE 运行环境应要求每个 TOE 远程用户身份都已被成功标识。

应用注释:本标准不包括鉴别以前必须通过 STA 和接入系统之间的管理和控制数据包。

11.5 FMT 类:安全管理

11.5.1 FMT_MOF.1 安全功能行为的管理

FMT_MOF.1. TOE 运行环境应仅限于[***管理员***]对功能[

a) ***审计;***
b) ***远程鉴别;***
c) ***时间服务***]具有[***确定其行为***]的能力。

应用注释：本标准规定同步管理 TOE 和 TOE 运行环境。

11.5.2 FMT_MTD.1 时间数据的管理

FMT_MTD.1.1 TOE 运行环境应仅限于[***安全管理员或授权信息系统实体***]能够对[***用于形成 FPT_STM.1 时间戳的时间和日期***][**设置**]。

11.5.3 FMT_SMR.1 安全角色

FMT_SMR.1.1 TOE 运行环境应维护[***管理员***]的角色。

FMT_SMR.1.2 TOE 运行环境应能够将用户与角色相关联。

应用注释：TOE 运行环境必须包括一个管理员角色，以对自身进行管理。

11.6 FTP 类：可信路径/通道

11.6.1 FTP_ITC_EXP.1 TSF 间可信信道

FTP_ITC_EXP.1.1 TOE 运行环境应在自身和 TOE 之间提供一条加密通信信道，此信道在逻辑上与其他通信信道不同，并且对其端点提供确定的标识，以及保护信道中数据免受修改或泄漏。

FTP_ITC_EXP.1.2 TOE 运行环境应允许 TSF 或 TOE 运行环境中的实体经可信信道发起通信。

FTP_ITC_EXP.1.3 对于[所有鉴别功能、远程登录、时间[ST 作者选择：[ST 作者赋值：与 ST 作者确认的授权信息系统实体通信]、无]]，TOE 运行环境应经可信信道发起通信。

应用注释：对于 FTP_ITC_EXP.1.1(2)，运行环境应提供和加密环境与 TOE 之间的信道。环境应为自身与 TOE 之间的通信提供保护。

11.7 FPT 类：TSF 保护

11.7.1 FPT_RVM.1 TSP 的不可旁路性

FPT_RVM.1.1 TOE IT 环境应确保在 IT 环境控制域内允许继续执行每一项功能前，IT 环境的执行功能都被成功激活。

11.7.2 FPT_SEP.1 TSF 域分离

FPT_SEP.1.1 TOE IT 环境应为自身执行维护一个安全域，防止不可信主体的干扰和篡改。

FPT_SEP.1.2 TOE IT 环境应分离 IT 环境控制域内各主体的安全域。

11.7.3 FPT_STM.1 可靠的时间戳

FPT_STM.1 TOE 运行环境应有能力提供可靠的时间戳。

应用注释：TOE 运行环境必须提供可靠的时间戳。

附 录 A
（资料性附录）
基本原理

A.1 概述

本附录论述了本标准所依据的原理。目的是证明本标准是一个完整的内在一致的安全要求，并且为无线局域网接入系统在安全环境中提供有效的策略集合。

本附录主要给出了安全目的和安全要求的合理性，汇总了假设、安全目的的覆盖的策略和威胁，以及安全目的覆盖的安全要求；并概述了本标准选择的适当的安全保障要求（评估保障级 2 级增强）。

A.2 安全目的基本原理

本节论述了本标准选择安全目的的基本原理。表 A.1 说明了安全目的与假设、威胁和组织安全策略之间的映射关系，即每个威胁和策略都至少有一个安全目的组件与其对应，每个安全目的都至少解决了一个威胁和策略。

表 A.1 安全目的与威胁和策略的映射关系

威胁和策略	解决威胁的安全目的	基本原理
T.ACCIDENTAL_ADMIN_ERROR 管理员可能不正确安装或配置 TOE，从而导致安全机制失效	O.ADMIN_GUIDANCE TOE 为管理员提供必要的安全管理信息。	O.ADMIN_GUIDANCE 通过保证 TOE 管理员拥有指导他们如何安全管理 TOE 的指南来缓解威胁。指南也有助于减少管理员所犯的错误，此类错误可能引起不安全地配置 TOE。
	O.MANAGE TOE 应提供管理员管理 TOE 安全所必需的功能和设施，并防止这些功能和设施被未授权的使用。	O.MANAGE 通过给管理员提供查阅和管理配置设置的能力来缓解这种威胁。比如说，如果管理员在配置已认可的用户鉴别证书时犯了错误，那么通过给安全管理员查阅鉴别证书列表的能力将使得他们查阅列表，从而发现他们所犯的错误。
	OE.NO_EVIL 使用 TOE 的组织应保证管理员是可信的，训练有素且遵循管理员指南。	OE.NO_EVIL 通过保证管理员是不敌对的、训练有素的（能够合理地管理 TOE）来缓解威胁。
	OE.NO_GENERAL_PURPOSE 在 TOE 上无法获得通用的计算或存储能力（例如：编译器、编辑器或应用程序）	OE.NO_GENERAL_PURPOSE 通过保证不会因为未授权软件或数据的引入产生意外错误；TOE 上没有通用的计算或存储库应用程序来缓解威胁

表 A.1（续）

威胁和策略	解决威胁的安全目的	基本原理
T.ACCIDENTAL_CRYPTO_COMPROMISE 用户或进程不适当地访问（查看、修改或删除）与密码功能相关联的密钥、数据或可执行代码，从而破坏了密码机制和这些机制所保护的数据	O.RESIDUAL_INFORMATION TOE 应确保重新分配资源时受保护资源所包含的信息不被泄漏。 OE.RESIDUAL_INFORMATION 环境应确保重新分配资源时环境控制范围内受保护资源所包含的信息不被泄漏。 O.SELF_PROTECTION TOE 应维护一个保护自身及其资源免受外部干预、未授权泄漏的执行域。 OE.SELF_PROTECTION 环境应维护一个保护自身及其资源免受外部干扰、破坏或通过自身接口未授权泄漏的执行域	O.RESIDUAL_INFORMATION 通过保证清除网络数据包中的任何残余数据和在加密密钥不再需要时不可访问来缓解该威胁。 OE.RESIDUAL_INFORMATION 通过保证清除网络数据包中的任何残余数据、在加密密钥不再需要时禁止访问来缓解这种威胁。 O.SELF_PROTECTION 确保 TOE 足以保护自身免受外部来源的威胁，所有 TSP 功能可以被调用。 OE.SELF_PROTECTION 保证 TOE 运行环境提供与 TOE 相似的保护
T.MASQUERADE 用户可能假冒授权用户访问 TOE 资源	O.TOE_ACCESS TOE 应提供限制用户对 TOE 进行逻辑访问的机制。 OE.TOE_ACCESS 环境应提供有助于 TOE 控制用户对 TOE 进行逻辑访问的机制。 OE.TOE_NO_BYPASS STA 与其他 STA 或有线网络上主机之间传输的数据必须通过 TOE	O.TOE_ACCESS 通过控制对 TOE 及其资源进行逻辑访问缓解这种威胁。通过限制授权用户访问 TOE 的方式和时间，通过规定鉴别机制的类型和强度，其目的是降低用户登录和假冒授权用户的可能性。另外，也为管理员提供了控制账户被锁定前用户所产生登录尝试失败次数的方法，进一步降低了用户未授权访问 TOE 的可能性。最后，TOE 包括确保受保护信道用于鉴别 STA 和与 TOE 运行环境重要组件进行通信的要求。 OE.TOE_ACCESS 通过在 TOE 运行环境中提供鉴别服务器支持 TOE 鉴别。环境也包括确保受保护信道用于与 TOE 运行环境重要组件进行通信的要求。 OE.TOE_NO_BYPASS 通过确保配置 STA 使得信息只能通过 TOE 在 STA 和其他 STA 或连接到 TOE 的主机之间进行流动来缓解威胁

表 A.1（续）

威胁和策略	解决威胁的安全目的	基本原理
T.POOR_DESIGN TOE需求规范或设计中的无意错误可能产生漏洞，可能被恶意用户或程序利用	O.CONFIG_IDENTIFICATION TOE的配置管理方式应证实设计和实施错误，并通过及时重新发布TOE更正错误。	O.CONFIG_IDENTIFICATION 通过要求开发者对TOE设计文档所做的变化进行控制和具有报告、解决安全缺陷的能力来处理这种威胁。
	O.DOCUMENTED_DESIGN TOE的设计应被充分、准确地文档化。	O.DOCUMENTED_DESIGN通过要求使用合理的工程原则开发TOE，在一定程度上处理这种威胁。高层设计和功能规范的使用确保负责开发TOE的开发者理解TOE的整体设计。这降低了设计缺陷出现的可能性，提高了发现意外设计错误的机会。ADV_RCR.1确保TOE设计与高层设计和功能规范的一致性。
	O.VULNERABILITY_ANALYSIS 应针对TOE进行脆弱性分析以表明TOE的设计和实现不存在明显的缺陷	O. VULNERABILITY _ ANALYSIS 确保已对TOE进行了脆弱性分析，任何已发现的脆弱性已经被删除或缓解
T.POOR_IMPLEMENTATION TOE实现中的无意错误可能产生漏洞，可能被恶意用户或程序利用	O.CONFIG_IDENTIFICATION TOE的配置管理方式允许证实设计和实施错误，并通过及时重新发布TOE更正错误。	O.CONFIG_IDENTIFICATION 通过要求开发者对TOE设计所做的变化进行控制来处理这种威胁。这确保TOE变化是结构化的和可跟踪的。
	O.PARTIAL_FUNCTIONAL_TESTING TOE应进行一些安全功能测试以表明TSF满足TOE安全功能要求。	O.PARTIAL_FUNCTIONAL_TESTING确保通过独立的样本测试，开发者能够说明和保证安全功能的正常运行。
	O.VULNERABILITY_ANALYSIS 应针对TOE进行脆弱性分析以表明TOE的设计和实现不存在明显的缺陷	O. VULNERABILITY _ ANALYSIS 确保通过分析和测试TOE表明它能抵抗明显的脆弱性

表 A.1（续）

威胁和策略	解决威胁的安全目的	基本原理
T.POOR_TEST 开发人员或测试人员对 TOE 的测试不充分，导致不正确的 TOE 行为未被发现，恶意用户或程序可能利用这些缺陷	O.CORRECT_TSF_OPERATION TOE 应提供测试 TSF 的能力以保证 TSF 的正确运行。 O.DOCUMENTED_DESIGN TOE 的设计应被充分、准确地文档化。 O.PARTIAL_FUNCTIONAL_TESTING TOE 应进行一些安全功能测试以表明 TSF 满足 TOE 安全功能要求。 O.VULNERABILITY_ANALYSIS 应针对 TOE 进行脆弱性分析以表明 TOE 的设计和实现不存在明显的缺陷	O.CORRECT_TSF_OPERATION 确保 TSF 持续正常的运作。 O.DOCUMENTED_DESIGN 确保文档化的 TOE 设计满足安全功能要求。为了保证实施中正确地实现了 TOE 的设计，在评估 TOE 期间必须对 TOE 的安全机制执行适当级别的功能测试。 O.PARTIAL_FUNCTIONAL_TESTING 提高了通过测试发现实施中存在错误的可能性。 O. VULNERABILITY _ ANALYSIS 要求除了功能测试以外需要执行脆弱性分析。该目的确认 TOE 没有包含功能测试未发现的安全缺陷
T.RESIDUAL_DATA 用户变更或进程切换引起的 TOE 资源的重新分配导致了用户或进程对数据的非授权访问	O.RESIDUAL_INFORMATION TOE 确保重新分配资源时 TOE 控制范围内受保护资源所包含的信息不被泄漏。 OE.RESIDUAL_INFORMATION 环境应确保重新分配资源时环境控制范围内受保护资源所包含的信息不被泄漏	O. RESIDUAL _ INFORMATION 通过保证清除网络数据包中的任何残余数据和在加密密钥不再需要时不可访问来缓解该威胁。 OE.RESIDUAL_INFORMATION 通过保证清除网络数据包中的任何残余数据、在加密密钥不再需要时禁止访问来缓解这种威胁

表 A.1（续）

威胁和策略	解决威胁的安全目的	基本原理
T.TSF_COMPROMISE 用户或进程利用一般攻击不适当地访问(查阅、修改或删除)TSF 数据或可执行代码	O.MANAGE TOE 应提供管理员管理 TOE 安全所必需的功能和设施，并防止这些功能和设施被未授权的使用。 OE.MANAGE IT 应增加管理员管理 TOE 安全所需的功能和设施，并防止这些功能和设施被未授权使用。 O.RESIDUAL_INFORMATION TOE 应确保重新分配资源时 TOE 控制范围内受保护资源所包含的信息不被泄漏。 OE.RESIDUAL_INFORMATION 环境应确保重新分配资源时环境控制范围内受保护资源所包含的信息不被泄漏。 O.SELF_PROTECTION TSF 应维护一个保护自身及其资源免受外部干预、未授权泄漏的执行域。 OE.SELF_PROTECTION 环境应维护一个保护自身及其资源免受外部干扰、破坏或未授权泄漏的执行域	O.MANAGE 仅限于管理员访问管理功能和对 TSF 数据进行管理。 OE.MANAGE 确保管理员可以查阅安全相关的审计事件。 O.RESIDUAL_INFORMATIONTION 通过保证清除网络数据包中的任何残余数据、在加密密钥不再需要时不可访问来缓解这种威胁。 OE.RESIDUAL_INFORMATION 通过保证清除网络数据包中的任何残余数据、在加密密钥不再需要时不可访问来缓解这种威胁。 O.SELF_PROTECTION 要求 TOE 环境能使自身免受威胁，TOE 的安全机制不能被绕过。只有实现该目的，才能确保用户不能查阅或修改 TSF 数据或 TSF 可执行代码。 OE.SELF_PROTECTION 保证 TOE 运行环境提供与 TOE 相似的保护
T.UNATTENDED_SESSION 用户未授权访问了未被监管的会话	O.TOE_ACCESS TOE 应提供控制用户对 TOE 进行逻辑访问的机制	本标准假定 TOE 建立的会话是可管理的会话。因此，威胁仅限于可管理的会话。运行环境应处理普通用户会话的终止。O.TOE_ACCESS 通过包含对管理员会话进行控制的机制来缓解这种威胁。在管理员定义的非活动时间后终止管理员会话。(规定的时间后)终止会话的连接降低了有人访问已建立会话的计算机(因此未授权访问会话)的风险

表 A.1（续）

威胁和策略	解决威胁的安全目的	基本原理
T.UNAUTHORIZED_ACCESS 用户访问了未被授权访问的服务	O.TOE_ACCESS TOE 应提供控制用户对 TOE 进行逻辑访问的机制。 OE.TOE_ACCESS 环境应提供有助于 TOE 控制用户对 TOE 进行逻辑访问的机制。	O.TOE_ACCESS 和 OE.TOE_ACCESS 确保 TOE 在允许访问 TOE 上或通过 TOE 转发的服务前要求进行身份鉴别。
	O.SELF_PROTECTION TSF 应维护一个保护自身及其资源免受外部干预、未授权泄漏的执行域。 OE.SELF_PROTECTION 环境应维护一个保护自身及其资源免受外部干扰、破坏或未授权泄漏的执行域。	O. SELF _ PROTECTION 和 OE. SELF_PROTECTION 确保用户访问 TOE 上或通过 TOE 转发的某种服务之前 TSF 及其环境必须调用所有已配置实施的功能（鉴别、访问控制规则等）。
	O.MANAGE TOE 应提供管理员管理 TOE 安全所必需的功能和设施，并防止这些功能和设施被未授权的使用。 OE.MANAGE 运行环境应增加管理员管理 TOE 安全所需的功能和设施，并防止这些功能和设施被未授权使用。	O.MANAGE 和 OE.MANAGE. TOE 及其环境仅限于管理员修改与 TOE 相关联的安全属性。这些目的确保没有其他用户可以修改信息流策略以绕过指定的安全策略。
	O.MEDIATE TOE 必须遵循 TOE 安全策略转发 STA 的流量。	O.MEDIATE 通过确保流经 TOE 的所有网络数据包遵守信息流策略来缓解威胁。
	OE.TOE_NO_BYPASS STA 与其他 STA 或有线网络上主机之间传输的数据必须通过 TOE	OE.TOE_NO_BYPASS 通过确保配置 STA 以使用无线接入系统转发 STA 与网络上其他主机之间的信息流来缓解威胁

表 A.1（续）

威胁和策略	解决威胁的安全目的	基本原理
T.UNAUTH_ADMIN_ACCESS 未授权用户访问了管理员账户	O.ADMIN_GUIDANCE TOE 应为管理员提供必要的安全管理信息。	O. ADMIN _ GUIDANCE 通过保证 TOE 管理员拥有指导他们如何安全管理 TOE 的指南来缓解威胁。该指南也有助于减少管理员所犯的错误，而这样的错误可能引起不安全地配置 TOE。
	O.MANAGE TOE 应提供管理员管理 TOE 安全所必需的功能和设施，并防止这些功能和设施被未授权的使用。 OE.MANAGE 运行环境应增加管理员管理 TOE 安全所需的功能和设施，并防止这些功能和设施被未授权使用。	O.MANAGE 和 OE.MANAGE 仅限于管理员访问管理功能和对 TSF 数据进行管理，这有助于缓解威胁。
	O.TOE_ACCESS TOE 应提供控制用户对 TOE 进行逻辑访问的机制。 OE.TOE_ACCESS 环境应提供有助于 TOE 控制用户对 TOE 进行逻辑访问的机制。	O.TOE_ACCESS 和 OE.TOE_ACCESS 通过包含鉴别 TOE 管理员的机制来缓解这种威胁，从而对管理员会话进行控制。
	OE.NO_EVIL 使用 TOE 的组织应保证管理员是可信的，训练有素且遵循管理员指南	OE.NO_EVIL 通过保证 TOE 管理员拥有指导他们如何安全管理 TOE 的指南来缓解威胁
P.ACCESS_BANNER TOE 在管理员登录时应显示一个描述使用限制、法律规定或其他合理信息的初始旗标	O.DISPLAY_BANNER 在使用任何需要鉴别的 TOE 服务之前，TOE 应在建立管理员会话之前给出建议性警告	O. DISPLAY _ BANNER 通过确保 TOE 显示管理员配置的旗标（向所有用户提供有关未授权使用 TOE 的警报）来满足该策略

表 A.1（续）

威胁和策略	解决威胁的安全目的	基本原理
P.ACCOUNTABILITY TOE 的授权用户应对自身在 TOE 内的行为负责	O.AUDIT_GENERATION TOE 应提供检查和创建与用户相关联的安全相关事件记录的能力。 OE.AUDIT_PROTECTION 运行环境应提供保护审计信息和鉴别证书的能力。 OE.AUDIT_REVIEW 运行环境应提供选择性查阅审计信息的能力。 O.MANAGE TOE 应提供管理员管理 TOE 安全所必需的功能和设施，并防止这些功能和设施被未授权的使用。 OE.MANAGE 运行环境应增加管理员管理 TOE 安全所需的功能和设施，并防止这些功能和设施被未授权使用。 O.TIME_STAMPS TOE 应获得可靠的时间戳。 OE.TIME_STAMPS 运行环境应提供可靠的时间戳。 O.TOE_ACCESS TOE 应提供控制用户对 TOE 进行逻辑访问的机制。 OE.TOE_ACCESS 环境应提供有助于 TOE 控制用户对 TOE 进行逻辑访问的机制	O.AUDIT_GENERATION 通过给管理员提供配置审计机制（记录特定用户的行为或基于用户的身份查阅审计迹）的能力来满足该策略。另外，当管理员对 TOE 做了任何与安全相关的变化（例如：访问控制规则的修改、审计机制的开启或关闭、可信信道的建立等）时，其 ID 都会被记录。 OE.AUDIT_PROTECTION 为 TOE 和运行环境的审计数据提供了存储保护。 OE.AUDIT_REVIEW 通过提供查阅和分类审计日志的机制进一步支持审计性。 O.MANAGE 确保仅有管理员能访问管理功能和管理 TSF 数据。 OE.MANAGE 确保管理员可以管理 TOE 运行环境中的审计功能。 O.TIME_STAMPS 通过要求 TOE 提供一个可靠的时间戳（利用外部网络时间协议服务器）支持该策略。审计机制必需在每个审计记录中包括目前的日期和时间。 OE.TIME_STAMPS 确保 TOE 运行环境应提供时间服务。 O.TOE_ACCESS 和 OE.TOE_ACCESS 通过控制对 TOE 及其资源的逻辑访问支持该策略。其目的确保通过标识和鉴别用户管理员可以跟踪用户的行为
P.CRYPTOGRAPHY TOE 为自身的应用提供密码功能，包括加密/解密操作	O.CRYPTOGRAGHY TOE 应提供密码功能以维护保密性和完整性。 O.RESIDUAL_INFORMATION TOE 确保重新分配资源时 TOE 控制范围内受保护资源所包含的信息不被泄漏	O. CRYPTOGRAGHY 通过要求 TOE 实施国家密码管理机构认可的加/解密服务来满足该策略。在 TSF 数据传输过程中，这些服务为它们提供保密性和完整性保护。 O. RESIDUAL_INFORMATION 通过确保依据国家密码管理机构标准清除加密数据来满足该策略

表 A.1（续）

威胁和策略	解决威胁的安全目的	基本原理
P.CRYPTOGRAPHY_VALIDATED 仅有国家密码管理机构认可的密码算法（方法和实现）才能用于密钥管理（例如：密钥的产生、销毁）和密码服务（例如：加密、解密、签名）	O.CRYPTOGRAGHY TOE 应提供密码功能以维护保密性和完整性。 O. CRYPTOGRAPHY _ VALIDATED TOE 应使用国家密码管理机构认可的密码模块提供密码服务	O. CRYPTOGRAGHY 通过要求 TOE 实施国家密码管理机构批准的加/解密服务来满足该策略。在 TSF 数据传输过程中，这些服务为它们提供保密性和完整性保护。 O. CRYPTOGRAPHY _ VALIDATED 通过要求提供加密服务的密码模块应是国家密码管理机构认可的来满足该策略
P.ENCRYPTED_CHANNEL 应提供 TOE 与经授权接入网络的 STA 之间数据传输加/解密的功能	O.CRYPTOGRAGHY TOE 应提供密码功能以维护保密性和完整性。 O.CRYPTOGRAPHY_VALIDATED TOE 应使用国家密码管理机构认可的密码模块提供密码服务。 O.MEDIATE TOE 必须遵循 TOE 安全策略转发 STA 的流量。 OE.PROTECT_MGMT_COMMS 环境应保护审计记录到审计服务器的传输、远程网络管理以及 TOE 与鉴别服务器的通信	O. CRYPTOGRAGHY 和 O. CRYPTOGRAPHY_VALIDATED 通过要求 TOE 实施国家密码管理机构认可的加/解密服务来满足该策略。在 TSF 数据传输过程中，这些服务为它们提供保密性和完整性保护。 O.MEDIATE 允许 TOE 管理员制定一个加密所有无线流量的策略。 OE.PROTECT_MGMT_COMMS 假设审计记录、远程网络管理信息和鉴别数据应通过环境中受保护信道加以保护

A.3 安全要求基本原理

A.3.1 TOE 安全要求的基本原理

表 A.2 说明了安全要求的充分必要性基本原理，即每个安全目的都至少有一个安全要求（包括安全功能组件和安全保障要求）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 A.2 TOE 安全要求的基本原理

TOE 安全目的	支持安全目的的要求	基本原理
O.ADMIN_GUIDANCE TOE 应为管理员提供必要的安全管理信息	ADO_DEL.1 AGD_OPE.1 AGD_PRE.1	ADO_DEL.1 确保管理员能够使用清洁版本 TOE 进行安装。这对安全管理 TOE 是必要的。 AGD_OPE.1 要求开发者应为管理员提供关于如何安全操作 TOE 的指南。该指南应描述管理员管理 TOE 所使用的接口和管理员配置的安全参数。它也应描述如何安装和使用 TOE 的审计特征。 AGD_PRE.1 面向非管理用户。如果 TOE 为这种类型的用户提供了设施/接口，该指南应描述如何安全地使用这些接口
O.AUDIT_GENERATION TOE 应提供检查和创建与用户相关联的安全相关事件记录的能力	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1 FIA_USB.1 FPT_STM_EXP.1 FTP_ITC_EXP.1	FAU_GEN.1 定义 TOE 必须记录的事件集。本标准确保管理员能够审计 TOE 发生的安全相关事件。它也定义了审计记录中每个审计事件必须包含的最小量信息。本标准规定了关于 ST 作者在本标准中增加的任何附加安全功能组件的记录细节程度。 FAU_GEN.2 确保审计记录可以关联可审计的事件和用户身份。对于授权用户，通过用户身份实现关联。其他情况下，关联依据源网络标识符。 FAU_SEL.1 允许选择审计事件。它定义了选择审计事件的标准。例如，用户身份可作为选择审计事件的标准。 FIA_USB.1 通过要求绑定与用户相关联的安全属性满足该目的。由于不能确认非鉴别用户的身份，所以本标准仅适用于授权用户。FPT_STM._EXP.1 通过确保 TOE 能够获得记录审计事件所用的时间戳来支持审计功能。 FTP_ITC_EXP.1 为 TOE 运行环境(审计服务器和时间服务器)所提供的服务建立可信信道
O.CONFIG_IDENTIFICATION 任何实现的错误可以通过 TOE 的重新发布得到及时更正，以保证 TOE 的配置可以被确认	ALC_ACM.2 ALC_CMS.1 ALC_FLR.2	ALC_ACM.2 通过要求开发者拥有描述 TOE 变化和 TOE 评估报告管理方式的配置管理计划来满足该目的。 ALC_CMS.1 要求确保 CM 系统能够跟踪实现表示、审计和测试文档(包括可执行的测试套件)、用户和管理员指南以及 CM 文档。 ALC_FLR.2 通过要求开发者具有解决产品中缺陷(通过测试发现或人为发现)的程序来满足该目的。开发者使用的缺陷修订过程应更正任何发现的缺陷和执行分析以确保修订所发现的缺陷的同时不会带来新的缺陷
O. CORRECT _ TSF _ OPERATION TOE 提供测试 TSF 的能力以保证 TSF 的正确运行	FPT_TST_EXP.1 FPT_TST_EXP.2	FPT_TST_EXP.1 对于确保 TSF 硬件的正确运行是必要的。如果 TSF 软件受到损坏，那么 TSF 可能不再实施安全策略。同理，如果 TSF 数据受到损坏，那么 TOE 可能不会正确实施安全策略。 FPT_TST_EXP.2 解决了与加密相关的 TSF 数据的关键特性和具体处理方法

表 A.2（续）

TOE安全目的	支持安全目的的要求	基本原理
O.CRYPTOGRAGHY TOE应提供密码功能以维护保密性和完整性	FCS_BCM_EXP.1 FCS_CKM.1 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2	密码支持类要求通过确保加密标准是国家密码管理机构认可的来满足该目的。 FCS_BCM_EXP.1 明确规定密码模块应遵循国家密码管理机构标准。 FCS_CKM.1 确保(在必要时)TOE能够产生密钥。 FCS_CKM.4 规定了 TOE 执行密钥销毁时必须满足的国家密码管理机构标准。 FCS_COP_EXP.1 要求使用随机数产生器。 FCS_COP_EXP.2 要求在数据加密和解密时使用国家密码管理机构批准的算法
O. CRYPTOGRAPHY _ VALIDATED TOE使用国家密码管理机构认可的密码模块提供密码服务	FCS_BCM_EXP.1 FCS_CKM.1 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2	密码支持类要求通过确保加密标准是国家密码管理机构认可的来满足该目的。 FCS_BCM_EXP.1 明确要求密码模块应遵循国家密码管理机构标准。 FCS_CKM.1 确保(在必要时)TOE能够产生 FCS_CKM.4 规定了 TOE 执行密钥销毁时必须满足的国家密码管理机构标准。 FCS_COP_EXP.1 要求使用随机数产生器。 FCS_COP_EXP.2 要求在数据加密和解密时使用国家密码管理机构批准的算法
O.DISPLAY_BANNER 在使用任何需要鉴别的TOE服务之前，TOE应在建立管理员会话之前给出建议性警告	FTA_TAB.1	FTA_TAB.1 通过要求 TOE 在用户建立可鉴别的会话之前显示管理员定义的旗标来满足该目的。该旗标由管理员完全控制。他可以规定任何有关未授权使用 TOE 的警告，删除任何产品或版本信息。建立鉴别会话的时机取决于 TOE 管理性能
O.DOCUMENTED_DESIGN TOE的设计应被充分、准确地文档化	ADV_FSP.1	ADV_FSP.1 通过要求使用合理的工程原则开发 TOE 来支持该目的。高层设计和功能规范的使用确保负责 TOE 开发的开发者理解 TOE 的整体设计。这降低了设计缺陷出现可能性，提高了发现意外设计错误的可能性
O.MANAGE TOE应提供管理员管理TOE安全所必需的功能和设施，并防止这些功能和设施被未授权的使用	FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MSA.2 FMT_MTD.1 FMT_MTD.1(2) FMT_MTD.1(3) FMT_MTD.1(4) FMT_SMR.1 FMT_SMF.1(1) FMT_SMF.1(2) FMT_SMF.1(3)	FMT 要求的基本原理集中在为管理员提供执行管理的功能，以至于管理员控制安全功能的行为。 FMT_MOF.1(1)、FMT_MOF.1 (2)、FMT_MOF.1 (3)确保管理员有能力管理加/解密、审计和鉴别功能。 FMT_MSA.2 为管理员提供了仅接受安全值和修改安全属性的能力。 FMT_MTD.1 (2)、FMT_MTD.1 (3)确保管理员能够管理 TSF 数据。本标准具体规定了审计预选、标识和鉴别数据。ST 作者可能使用附加的重复以处理其他要求没有规定的 TSF 数据。 FMT_MTD.1(4)通过确保存在对设置时间和日期(用于向 TOE 提供可靠时间戳)的安全管理员或授权 IT 实体进行管理的功能来满足该目的。 FMT_SMR.1 定义了具体的安全角色。 FMT_SMF.1(1)、FMT_SMF.1(2)、FMT_SMF.1(3)通过提供针对加密数据、审计记录和密钥数据的管理功能来支持该目的

表 A.2（续）

TOE 安全目的	支持安全目的的要求	基本原理
O.MEDIATE TOE 必须遵循 TOE 安全策略转发 STA 的流量	FIA_UAU.1 FIA_UAU_EXP.5 FIA_UID.2 FDP_PUD_EXP.1	FIA_UAU.1，FIA_UAU_EXP.5，FIA_UID.2 确保 TOE 能够依据 STA 的鉴别证书协调数据包流量。 FDP_PUD_EXP.1 允许管理员决定是否允许非加密数据通过 TOE
O. PARTIAL _ FUNCTIONAL _TESTING TOE 应进行一些安全功能测试以表明 TSF 满足 TOE 安全功能要求	ATE_COV.1 ATE_FUN.1 ATE_IND.2	ATE_COV.1 要求开发者提供测试覆盖范围分析以表明开发者的测试套件测试 TSFI 的范围。该组件也要求独立地确认测试套件的范围，这有助于确保通过测试验证 TSFI 的安全相关功能。 ATE_FUN.1 要求开发者提供必要的测试文档以允许独立地分析开发者安全功能测试的覆盖范围。另外，开发者必须提供测试套件可执行代码和源代码以便评估者可以使用这些代码独立地验证提供商的测试结果和支持测试覆盖范围分析。 ATE_IND.2 要求通过规定独立方运行测试套件的子集独立地确认开发者的测试结果。该组件也要求独立方执行附加的功能测试以解决开发者测试套件中没有证明的功能行为。一旦成功地完成这些要求，就可以证明 TOE 遵循了规定的安全功能组件
O. RESIDUAL _ INFORMATION TOE 应确保重新分配资源时 TOE 控制范围内受保护资源所包含的信息不被泄漏	FDP_RIP.1(1) FCS_CKM.4	FDP_RIP.1(1)用于确保重新分配资源时资源的内容不再可用。对于 TOE，下面的措施是重要的：清除用于构建网络数据包的存储区或者使用一些缓冲管理方案防止在以后的数据包中泄漏数据包的内容。 FCS_CKM.4 适用于 TSF 所用密钥的销毁。本标准规定了密钥销毁的方式和时间。合理销毁这些密钥对于确保重新分配资源时它们不被泄漏至关重要
O.SELF_PROTECTION TSF 应维护一个保护自身及其资源免受外部干预、未授权泄漏的执行域	ADV_ARC.1	ADV_ARC.1 提供 TSF 安全域的安全架构描述
O.TIME_STAMPS TOE 应获得可靠的时间戳	FPT_STM_EXP.1	FPT_STM_EXP.1 要求 TOE 为自身的使用能够获得可靠的时间戳（包括日期和时间），因此本标准满足了该目的。时间戳是可靠的在于 TOE 总是能够获得时间戳，且时钟是单调递增的

表 A.2（续）

TOE 安全目的	支持安全目的的要求	基本原理
O.TOE_ACCESS TOE 应提供控制用户对 TOE 进行逻辑访问的机制	FIA_AFL.1 FIA_ATD.1(1) FIA_ATD.1(2) FIA_UAU.1 FIA_UAU_EXP.5 FIA_UID.2 FTA_SSL.3 FTP_TRP.1 FTP_ITC_EXP.1	FIA_AFL.1 确保 TOE 可以保护自身及其用户免受对它们鉴别证书的蛮力攻击。 FIA_ATD.1(1)和 FIA_ATD.1(2)要求为支持鉴别要求提供了附加的控制。FIA_UAU.1 和 FIA_UAU_EXP.5 通过确保管理员和用户在访问 TOE 及其服务之前被鉴别来实现该目的。 为了控制对 TOE 的逻辑访问，需要鉴别机制。本地管理员鉴别机制确保无论网络连接状况如何，管理员能够登录 TOE(例如：鉴别服务器出现故障或鉴别服务器的网络路径不可用，导致了管理员不能登录 TOE。这种情况是不能接受的)。 FIA_UID.2 通过确保 TOE 在执行任何数据转发功能前鉴别每一个用户来满足该目的。 FTA_SSL.3 确保丢弃不活动的用户会话和管理会话。 FTP_TRP.1 确保远程用户通过可信路径进行鉴别。 FTP_ITC_EXP.1 为 TOE 运行环境(远程鉴别服务器)支持的服务提供可信信道
O. VULNERABILITY _ ANALYSIS 应针对 TOE 进行脆弱性分析以表明 TOE 的设计和实现不存在明显的缺陷	AVA_VAN.2	AVA_VLA.2 要求开发者查找 TOE 交付成果中明显的脆弱性并记录这些脆弱性的修改情况。另外，评估者在脆弱性测试期间应参考上述分析结果。该组件确保排除或缓解明显的安全缺陷

A.3.2 运行环境安全要求的基本原理

表 A.3 说明了运行环境安全要求的充分必要性基本原理，即每个运行环境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运行环境安全目的，因此安全要求对运行环境安全目的而言是充分和必要的。

表 A.3 运行环境安全要求的基本原理

运行环境安全目的	支持安全目的的安全要求	基本原理
OE.AUDIT_PROTECTION 运行环境应提供保护审计信息和鉴别证书的能力	FAU_SAR.2 FAU_STG.1 FAU_STG.3 FMT_MOF.1 FMT_SMR.1	FAU_SAR.2 仅限于管理员阅读审计记录。 FAU_STG.1 仅限于管理员删除或修改审计信息。 FAU_STG.3 确保管理员在审计迹超过预先定义的阈值时采取行动。 FMT_MOF.1 和 FMT_SMR.1 规定管理员可以控制与审计、警报产生相关的安全功能。控制这些安全功能的任务被赋予适当的管理角色

表 A.3（续）

运行环境安全目的	支持安全目的的安全要求	基本原理
OE.AUDIT_REVIEW 运行环境应提供选择性查阅审计信息的能力	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3	FAU_GEN.1 确保 TOE 运行环境产生支持 TOE 的适当审计事件。 FAU_SAR.1 确保运行环境为负责管理 TOE 的人员提供查阅 TOE 审计记录的设施。 FAU_SAR.3 为管理员提供了依据已建立的标准选择性查阅审计迹内容的能力。该能力允许管理员把审计查阅的焦点放在特定时间发生的事件上
OE.MANAGE 运行环境应增加管理员管理 TOE 安全所需的功能和设施，并防止这些功能和设施被未授权使用	FIA_USB.1 FMT_MOF.1 FMT_SMR.1	FIA_USB.1 确保 TOE 运行环境包括关联进程和角色的机制。 FMT_MOF.1 确保 TOE 运行环境仅限于管理员访问 TSF 管理功能。 FMT_SMR.1 确保 TOE 运行环境提供一个同时管理 TOE 和运行环境的管理员角色
OE.NO_EVIL 使用 TOE 的组织应保证管理员是可信的，训练有素且遵循管理员指南	AGD_OPE.1	AGD_ADM.1 要求开发者为管理员提供如何安全操作 TOE 的指南。该指南描述了管理员管理 TOE 所使用的接口和配置 TOE 所使用的安全参数。文档也提供如何安装和查阅 TOE 审计特征的描述
OE.NO_GENERAL_PURPOSE 在 TOE 上无法获得通用的计算或存储能力（例如：编译器、编辑器或应用程序）	A.NO_GENERAL_PURPOSE	假设 TOE 上没有通用的计算或存储能力，因此 SFR 是没有必要的
OE.PHYSICAL 运行环境提供与 TOE 及其所包含数据的价值相一致的物理安全	A.PHYSICAL	假设运行环境提供与 TOE 及其所包含数据的价值相称的物理安全。因此，扩展的要求是没有必要的
OE.PROTECT_MGMT_COMMS 运行环境应保护审计记录到审计服务器的传输、远程网络管理以及 TOE 与鉴别服务器的通信	FDP_ITC_EXP.1	FDP_ITC_EXP.1 应为 TOE 运行环境（远程鉴别服务器、系统日志服务器、时间服务器）所提供的服务建立可信信道
OE. RESIDUAL _ INFORMATION 环境应确保重新分配资源时环境控制范围内受保护资源所包含的信息不被泄漏	FDP_RIP.1(2)	FDP_RIP.1(2)确保 TOE 运行环境为网络数据包中的残余信息提供与 TOE 相同的保护。这确保 TOE 运行环境或 TOE 不允许先前已传输数据包的数据插入到新的数据包中

表 A.3（续）

运行环境安全目的	支持安全目的的安全要求	基本原理
OE.SELF_PROTECTION 环境应维护一个保护自身及其资源免受外部干扰、破坏或未授权泄漏的执行域	FPT_SEP.1 FPT_RVM.1	FPT_SEP.1 确保环境提供一个保护自身免受不可信用户威胁的域。如果环境不能保护自身，那么不可能指望环境实施它的安全策略。 FPT_RVM.1 确保环境对操作策略域内主体和客体的所有接口进行策略选择
OE.TOE_ACCESS 环境应提供有助于 TOE 控制用户对 TOE 进行逻辑访问的机制	FIA_AFL.1 FIA_ATD.1 FIA_UAU_EXP.5 FIA_UID.1	FIA_AFL.1 和 FIA_ATD.1 确保环境关联合适的属性与用户以及正确处理鉴别失败。 TOE 运行环境应提供远程鉴别机制以支持 TOE 对用户的鉴别。FIA_UAU_EXP.5 和 FIA_UID.1 确保用户被标识和鉴别
OE.TOE_NO_BYPASS STA 与其他 STA 或有线网络上主机之间传输的信息通过 TOE 进行转发	FIA_UAU.1 FIA_UAU_EXP.5 FIA_UID.1	FIA_UAU.1、FIA_UID.1 和 FIA_UAU_EXP.5 确保 TOE 能够依据 STA 的鉴别证书转发数据流
OE.TIME_STAMPS 运行环境应提供可靠的时间戳	FPT_STM.1 FPT_MTD.1(4)	FPT_STM.1 要求 TOE 运行环境能够为自身和 TOE 提供可靠的时间戳（包括日期和时间）。另外，时间戳也是可靠的在于 TOE 总是能够获得时间戳，且时钟是单调递增的。 FMT_MTD.1(4)通过确保存在对设置时间和日期（用于向 TOE 提供可靠时间戳）的安全管理员或授权 IT 实体进行管理的功能来满足该目的

A.3.3 TOE 安全保障要求基本原理

选择评估保障级 2 级增强可以保证用于保护安全环境下信息的安全服务的可信度。保证级的选择主要依据安全环境中定义的威胁。

通过研究 GB/T 18336—2015 中评估保障级的定义，保证包 EAL2 增强[在 EAL2 基础上增加 ALC_FLR.2(缺陷报告程序)]是实现本标准制定目的的最佳选择。

A.3.4 未满足所有依赖性的基本原理

为了证明本标准满足所有的依赖关系，本标准分析了每个功能要求（包括扩展的要求）。除了与 FMT_MSA.2 相关的依赖关系，本标准中满足所有依赖关系。

FMT_MSA.2 作为密码支持子类（FCS_COP 和 FCS_CKM）的依赖关系包括在本标准中，能够确保与密码客体（例如：密钥）相关的安全属性受到保护。另外，FMT_MSA.2 组件也被用于保护与访问控制策略（FDP_IFC 和 FDP_ACC）相关的安全属性，包括对这些安全功能组件的依赖。可是，本标准不要求 TOE 实施访问控制策略，因此这些要求没有包含在本标准中。

A.3.5 扩展族的基本原理

表 A.4 列出了本标准所包括的扩展族的基本原理。

表 A.4 扩展族的基本原理

扩展族	标识符	基本原理
FCS_BCM_EXP	基准密码模块	基准密码模块应符合国家密码管理委员会办公室批准的用于无线局域网的对称密码算法的密码模块，并符合GB 15629.11—2003 中保密机制的相关要求。 同时，由于 GB/T 18336—2015 没有提供规定密码实施基准的方式，该扩展族描述了国家密码管理机构认可的加密模块而不是整个 TSF 的要求，所以它是必要的
注：Baseline Cryptographic Module(简称 BCM)，基准密码模块。		

A.3.6 扩展要求的基本原理

表 A.5 列出了本标准所包括的扩展要求及其基本原理。

表 A.5 扩展要求的基本原理

扩展要求	标识符	基本原理
FCS_BCM_EXP.1	基准密码模块	由于 GB/T 18336—2015 没有规定基准密码模块的实现方法，所以该扩展的要求是必要的
FCS_COP_EXP.1	随机数产生	由于 GB/T 18336—2015 密码运算组件仅处理具体的算法类型和运算，所以该扩展的要求是必要的
FCS_COP_EXP.2	密码运算	由于该组件描述了密码模块的要求，所以该扩展的要求是必要的
FDP_PUD_EXP.1	用户数据保护	由于 GB/T 18336—2015 的 IFC/ACC 要求没有包含基于非客体/属性的访问控制策略，所以该扩展的要求是必要的。FDP_PUD_EXP.1 允许管理员依据设置(指明非加密数据能否通过无线局域网转发)允许或禁止访问无线局域网
FIA_UAU_EXP.5	多重鉴别机制	由于对是否明确要求 TSF 提供鉴别存在争议，所以该扩展的要求对于本地管理员来说是必要的。FIA_UAU 要求暗示 TOE 提供鉴别。当 FIA_UAU 要求包含在 TOE 中时，假定 TOE 提供鉴别。为了避免混乱，本标准包括一个扩展的鉴别要求。本标准也规定运行环境提供一个用于鉴别远程用户的鉴别服务器。TSF 必须提供鉴别本地管理员的方式以免 TOE 不能与鉴别服务器进行通信。另外，TOE 必须提供部分鉴别机制以获取和实施运行环境的鉴别选择
FPT_TST_EXP.1	TSF 测试	由于 GB/T 18336—2015 的 FPT_TST.1 存在问题，所以该扩展的要求是必要的。FPT_TST.1 的第一个问题：只有 TOE 包括硬件，FPT_TST.1.1 表达才是有意义的。第二，一些 TOE 数据是动态的(例如：审计迹中的数据、口令)，所以对 FPT_TST.1.2 的“完整性”解释是必要的。因此，本标准使用了该扩展的要求

表 A.5（续）

扩展要求	标识符	基本原理
FPT_TST_EXP.2	对密码模块进行 TSF 测试	由于基本的自测要求没有规定测试密码功能，所以该扩展的要求是必要的
FTP_ITC_EXP.1	TSF 间可信信道	由于现有的可信信道要求旨在保护分布式 TOE 各部分之间的通信而不是 TOE 与运行环境之间的通信，所以该扩展的要求是必要的

参 考 文 献

[1] GB 15629.1101—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] GB 15629.1102—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] GB 15629.1104—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] GBZ 20283—2006 信息安全技术 保护轮廓和安全目标的产生指南

[6] Common Criteria for Information Technology Security Evaluation, CCIMB-99-031, Version 2.1, August 1999.

[7] Peer-to-Peer Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments Protection Profile, Version 0.6, September 2001.

[8] Infrastructure Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments Protection Profile, Version 0.8, September 2001.

[9] US Government Wireless Local Area Network (WLAN) Client for Basic Robust Environments Protection Profile, Version 0.9, November 2003.

[10] US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robust Environments, Version 1.1, April 2004.

[11] US Government Wireless Local Area Network (WLAN) Client Protection Profile for Basic Robust Environments, Version 1.0, March 2007.

[12] US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robust Environments, Version 1.0, April 2006.

GB/T 33565-2017

版权专有 侵权必究

*

书号:155066·1-55632

定价: 42.00元

打印日期:2017年5月19日 F007