ICS 35.040
L 80

# 中华人民共和国国家标准

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)

**Information security technology—Security technology requirements for wireless local area network (wlan) client(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

# 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、北京邮电大学、中国科学院研究生院信息安全国家重点实验室、西安西电捷通无线网络通信股份有限公司。

本标准主要起草人:郭涛、朱龙华、崔宝江、刘威鹏、胡亚楠、张宝峰、毕海英、杨永生、张翀斌、张普含、时志伟、郝永乐、王眉林、童伟刚。

# 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 制定了无线局域网客户端安全技术要求(评估保障级 2 级增强)。

本标准详细描述了与无线局域网客户端安全相关的假设、威胁和组织安全策略,定义了无线局域网客户端及其运行环境的安全目的,并由其导出安全功能要求和安全保障要求,通过基本原理论证了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　无线局域网客户端安全技术要求(评估保障级2级增强)

## 1　范围

本标准规定了无线局域网客户端的安全技术要求(评估保障级2级增强),主要包括无线局域网客户端的假设、威胁和组织安全策略,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级安全保障要求的基础上,增加了评估保障级3级ALC_FLR.2(缺陷报告过程)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客户端的设计、开发、测试、评估和产品的采购。

## 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:安全保障组件

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—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

**基本服务组　basic service set;BSS**

受单个协调功能所控制的站集合。

3.2

**扩展服务集　extended service set; ESS**

由一个或多个互联的BSS与集成的局域网(LAN)构成的集合,对与其中某个BSS站点关联的任何站的逻辑链路控制层而言,它表现为单个的BSS。

3.3

**独立基本服务组　independent basic service set; IBSS**

能够成一个自包含网络且不能访问DS的BSS。

3.4

**泛端口 portal**

逻辑点，来自非本标准的局域网的MAC服务数据单元在本逻辑点上进入ESS中的分布式系统。

3.5

**站(点) station;STA**

包含符合本标准的与无线媒体的MAC和PHY接口的任何设备。

3.6

**无线局域接入系统 WLAN access system**

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

下列略缩语适用于本文件。

BSS 基本服务组(Basic Service Set)
CM 配置管理(Configuration 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)
SF 安全功能(Security Function)
SFP 安全功能策略(Security Function Policy)
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)
TSC TSF控制范围(TSF Scope of Control)
TSF TOE安全功能(TOE Security Functions)
TSFI TSF接口(TSF Interface)
TSP TOE安全策略(TOE Security Policy)
WAS WLAN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 安全目的和运行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功能组件并未包括在 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，以执行安全功能要求。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者多项。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

典型的无线局域网系统包括 IBSS、BSS 和 ESS 三种结构，如图 1～图 3 所示。本标准的评估对象(TOE)指的是 IBSS、BSS 以及 ESS 结构下的无线局域网客户端，是 STA 的一种存在形态。目前 TOE 典型的存在形式有 PCI、PCMICA、USB 接口无线网卡以及其他嵌入式无线网卡等。TOE 是用户接入 WLAN 的最终设备，任何情况下 WLAN 客户端与无线或有线网络间的数据交互都必须通过无线局域网接入系统(WAS)。

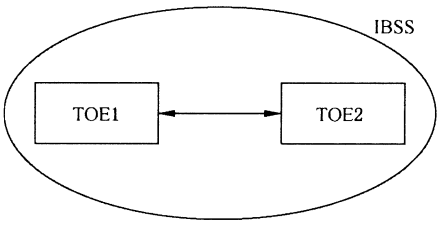


**图 1 IBSS 结构下的 TOE**

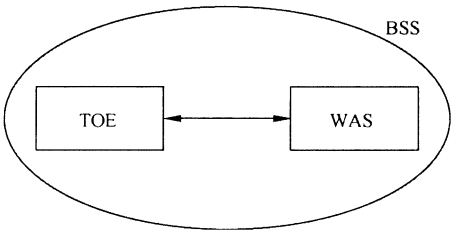


**图 2 BSS 结构下的 TOE**

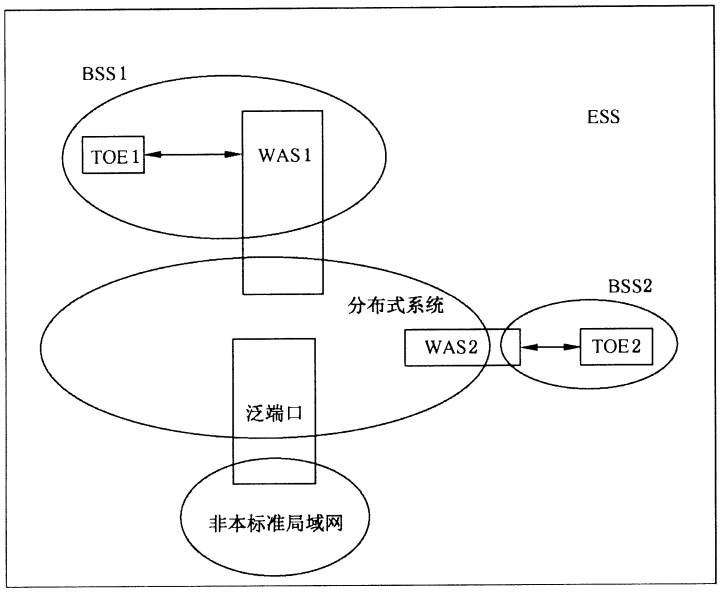


**图 3　ESS 结构下的 TOE**

TOE 在大多数情况下组件作为存在于计算机或移动设备中。因此，TOE 自身不能提供运行环境下所需要的全部安全要求。TOE 主要依靠其自身附带的计算环境来执行管理任务。因此需要对于 TOE 运行环境附加一定的安全要求。TOE 安全功能要求和运行环境安全要求能够缓解威胁和满足策略。

### 6.2　管理

管理员负责安装、配置和维护 TOE。由于 TOE 是更大系统的一部分，所以负责管理 TOE 运行环境的管理员也应负责管理 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 管理员。

### 6.3　加密

TOE 包括密码模块的要求。密码模块是提供密码服务的系统或应用的一部分。符合本标准的产品和系统应使用符合国家标准和国家密码管理机构批准的密码模块。

### 6.4　审计

TOE 是更大系统的一部分，其审计的职责仅限于产生审计事件。TOE 的运行环境可以提供审计事件存储、查阅和恢复等审计机制。

### 6.5　鉴别

TOE 在大多数情况下组件作为存在于计算机或移动设备中，因此，不需要标识和鉴别功能。但 TOE 的运行环境可以提供用户-主体绑定等鉴别机制。

### 6.6　TOE 运行环境

运行 TOE 所需的操作系统和硬件平台（例如，计算机、移动设备）一般不要求作为 TOE 的一部分。但是，由于 TOE 是更大系统的一部分，因此对于 TOE 所依赖运行环境增加保护是必要的。

# 7 TOE 安全环境

## 7.1 假设

### 7.1.1 A.PHYSICAL

TOE 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。

### 7.1.2 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

管理员可能不正确安装或配置 TOE，导致无效的安全机制。

### 7.2.2 T.CRYPTO_COMPROMISE

用户或进程可能引起与密码功能相关联的关键数据或可执行代码被不适当的访问（查看、修改或删除），从而破坏了密码机制和受该机制保护的数据。

### 7.2.3 T.POOR_DESIGN

要求规范或 TOE 设计中的无意错误可能导致可被恶意用户或进程利用的缺陷。

### 7.2.4 T.IMPLEMENTATION

TOE 设计的实施中的无意错误可能导致恶意用户或进程利用的缺陷。

### 7.2.5 T.POOR_TEST

由于缺乏或对 TOE 安全功能正确运行的测试不充分，导致不正确 TOE 的行为未被发现，从而存在潜在的安全脆弱性。

### 7.2.6 T.RESIDUAL_DATA

恶意用户或进程利用重新分配 TOE 资源来获取对于资源的未授权访问。

### 7.2.7 T.TSF_COMPROMISE

恶意用户或进程通过简易的攻击引起 TSF 数据或可执行代码被非法的访问（查看、修改或删除）。

## 7.3 组织安全策略

### 7.3.1 P.ACCOUNTABILITY

TOE 的授权用户对自身在 TOE 内的行为负责。

### 7.3.2 P.CRYPTOGRAPHY

只有符合国家标准和国家密码管理机构要求的密码（方法和实施）才能用于密钥管理（例如，密钥的产生、访问、分发、销毁、处理和储存）和密码服务（例如，加密、解密、签名、散列、密钥交换和随机数产生

服务)。

## 8 安全目的

### 8.1 TOE 安全目的

#### 8.1.1 O.ADMIN_GUIDANCE

TOE 应为安全管理员提供必要的信息以便于安全管理。

#### 8.1.2 O.AUDIT_GENERATION

TOE 应具有检查和创建与用户相关联的安全相关事件记录的能力。

#### 8.1.3 O.CORRECT_TSF_OPERATION

TOE 应提供测试 TSF 以确保 TSF 在客户站点正确运行的能力。

#### 8.1.4 O.CRYPTOGRAGHY

TOE 应使用已获国家标准和国家密码管理机构要求的密码服务。

#### 8.1.5 O.MANAGE

TOE 应提供支持管理员管理 TOE 安全所必需的功能和设施。

#### 8.1.6 O.RESIDUAL_INFORMATION

TOE 应确保资源被重新分配时 TOE 控制范围受保护资源所包含的任何信息不被泄漏。

#### 8.1.7 O.CONFIGURATION_IDENTIFICATION

由于 TOE 迅速重新分发,应采用一种方式完全标识 TOE 的配置,该方式将允许在实现时错误能够被标识和改正。

#### 8.1.8 O.DECUMENTED_DESIGN

TOE 的设计应以文档的形式充分和准确地记录。

#### 8.1.9 O.PARTIAL_FUNCTIONAL_TESTING

应对 TOE 进行安全功能测试以表明 TSF 满足它的安全功能要求。

#### 8.1.10 O.VULNERABILITY_ANALYSIS

应对 TOE 进行脆弱性分析以表明 TOE 的设计和实施不包含任何明显的缺陷。

### 8.2 运行环境安全目的

#### 8.2.1 OE.MANAGE

TOE 运行环境应增加 TOE 的功能和设施以支撑管理员对于 TOE 安全的管理,并且要防止这些功能和设施被未授权使用。

#### 8.2.2 OE.NO_EVIL

管理员是可信的，经过正式培训且遵循管理员指南。

#### 8.2.3 OE.PHYSICAL

TOE 运行环境提供与 TOE 价值和 TOE 包含的数据相称的物理安全。

#### 8.2.4 OE.RESIDUAL_INFORMATION

TOE 运行环境确保资源被重新分配时 TOE 控制范围内保护资源包含的信息不能被泄漏。

#### 8.2.5 OE.TIME_STAMPS

TOE 运行环境应提供可靠的时间戳并为管理员提供为时间戳设置时间的能力。

#### 8.2.6 OE.TOE_ACCESS

TOE 运行环境应提供对用户逻辑访问 TOE 进行控制的机制。

## 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

从属于：无其他组件。

依赖关系：无依赖关系。

FCS_BCM_EXP.1.1 密码模块在执行密码功能时应采用[**赋值**：***密钥生成算法***]。

FCS_BCM_EXP.1.2 对 TOE 密码模块进行认可的测试应该遵循[**赋值**：***标准列表***]。

### 9.2 扩展组件

#### 9.2.1 FAU_GEN_EXP.1 审计数据产生

##### 9.2.1.1 FAU_GEN_EXP.1.1

TSF 应能为下述可审计事件产生审计记录：

a) 有关[**选择，选取一个：*最小级*、*基本级*、*详细级*、*未规定***]审计级别的所有可审计事件；

b) [**赋值：*其他专门定义的可审计事件***]。

#### 9.2.1.2 FAU_GEN_EXP.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的定义，**[**赋值：*其他审计相关信息***]。

### 9.2.2 FCS_CKM_EXP.2 加密密钥建立

#### 9.2.2.1 FCS_CKM_EXP.2.1

TSF 应提供以下加密密钥建立技术[**赋值：*密钥加密技术***]。密码模块依据[**赋值：*密钥分发办法***]能在下面的环境[**赋值：*密码模块输出密钥的环境***]接受密钥输入和输出密钥。

### 9.2.3 密钥运算 FCS_COP 族：FCS_COP_EXP.1 随机数产生

#### 9.2.3.1 FCS_COP_EXP.1.1

TSF 应产生 TSF 密码功能中所使用的所有随机数。随机数产生器应符合[**赋值：*标准列表***]。

### 9.2.4 密钥运算 FCS_COP 族：FCS_COP_EXP.2 密码运行

#### 9.2.4.1 FCS_COP_EXP.2.1

TSF 应产生 TSF 密码功能中所使用的所有随机数。随机数产生器应符合[**赋值：*标准列表***]。

TSF 应遵循无线客户加密策略，通过使用[***赋值：加密算法***]运行在[***赋值：运行模式***]支持[***赋值：密钥长度***]的密码模块执行加密和解密。

### 9.2.5 TSF 自检 FPT_TST 族：FPT_TST_EXP.1 TSF 测试

#### 9.2.5.1 FPT_TST_EXP.1.1

TSF 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***]运行一套自检程序以证明[**选择：**[***赋值：TSF 的组成部分***]、***TSF*** ]运行的正确性。

#### 9.2.5.2 FPT_TST_EXP.1.2

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

#### 9.2.5.3 FPT_TST_EXP.1.3

TSF 应为授权用户提供验证所存储的 TSF 可执行代码完整性的能力。

### 9.2.6 TSF 自检 FPT_TST 族：FPT_TST_EXP.2 对密码模块进行 TSF 测试

#### 9.2.6.1 FPT_TST_EXP.2.1

TSF 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***]运行一套自检程序以证明[**选择：**[***赋值：TSF 的组成部分***]、***TSF*** ]运行的正确性。

#### 9.2.6.2 FPT_TST_EXP.2.2

TSF 应在产生密钥后立即运行一套遵循国家标准和国家密码管理机构相关标准的密码模块自测工具。

## 10 TOE 安全要求

### 10.1 TOE 安全功能要求

#### 10.1.1 概述

本标准的 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_EXP.1 | 审计数据产生 | FPT_STM.1 |
| FCS 类：密码支持 | FCS_BCM_EXP.1 | 基准密码模块 | 无 |
| | FCS_CKM_EXP.2 | 密钥建立 | [FDP_ITC.1<br>或<br>FCS_COP_EXP.1]；<br>FCS_CKM.1；<br>FCS_CKM.4；<br>FMT_MSA.2 |
| FCS 类：密码支持 | FCS_CKM.4 | 密钥销毁 | [FDP_ITC.1<br>或<br>FDP.ITC.2<br>或<br>FCS_CKM.1] |
| | FCS_COP_EXP.1 | 随机数产生 | [FDP_ITC.1<br>或<br>FCS_CKM.1]；<br>FCS_CKM.4；<br>FMT_MSA.2 |
| | FCS_COP_EXP.2 | 密码操作(数据加解密) | [FDP_ITC.1<br>或<br>FCS_CKM.1]；<br>FCS_CKM.4；<br>FMT_MSA.2 |
| FDP 类：用户数据保护 | FDP_IFC.1 | 子集信息流控制 | FDP_IFF.1 |
| | FDP_IFF.1 | 简单安全属性 | FDP_IFC.1<br>FMT_MSA.3 |
| | FDP_RIP.1 | 子集残留信息保护 | 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 |
|---|---|---|---|
| FMT 类：安全管理 | FMT_MSA.2 | 安全的安全属性 | [ADV_SPM.1 或<br>FDP_ACC.1 或<br>FDP_IFC.1]；<br>FMT_MSA.1<br>FMT_SMR.1 |
| | FMT_MSA.3 | 静态属性初始化 | FMT_MSA.1<br>FMT_SMR.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(审计记录产生) | 无 |
| | FMT_SMF.1(3) | TSF 数据管理(密码密钥数据) | 无 |
| FPT 类：TSF 保护 | FPT_TST_EXP.1 | TSF 测试 | 无 |
| | FPT_TST_EXP.2 | 对密码模块进行 TSF 测试 | 无 |

### 10.1.2 FAU 类：安全审计

#### 10.1.2.1 FAU_GEN_EXP.1 审计数据产生

**FAU_GEN_EXP.1.1 TSF** 应能为下述可审计事件产生审计记录：

a) ***所有表 2 中列出的审计事件***。

表 2 审计事件

| 安全功能组件 | 审计事件 | 附加的审计记录内容 |
|---|---|---|
| FCS_CKM_EXP.2 | 密钥传输过程中的检测到的错误 | 无 |
| FCS_CKM.4 | 密钥的销毁 | 无 |
| FDP_IFC.1 | 丢弃不满足无线客户端加密策略的数据包 | 源和目的设备的 MAC 地址 |
| FMT_SMF.1(1) | 改变 TOE 加密算法，包括选择对通信不进行加密 | 加密算法选择(或无) |
| FMT_SMF.1(3) | 改变密钥数据 | 无(TOE 不应在审计日志中记录密钥) |
| FPT_TSF_EXP.1 | 执行自检 | 自检成功或失败 |
| FPT_TSF_EXP.2 | 执行自检 | 自检成功或失败 |

FAU_GEN_EXP.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[表 2 审计事件第三列规定的信息。]

应用注释：如果在审计事件中记录的数据是有意义的，那么“如果适用”指的就是在审计记录中应包含的数据。对于某些审计事件而言，如果没有特别说明，那么“无”审计记录也是可以接受的。

### 10.1.3 FCS 类:密码支持

#### 10.1.3.1 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***国家标准和国家密码管理机构相关标准要求的密码算法***。

FCS_BCM_EXP.1.2 对 TOE 密码模块进行认可的测试应该遵循***国家标准和国家密码管理机构相关标准***。

#### 10.1.3.2 FCS_CKM_EXP.2 加密密钥建立

FCS_CKM_ EXP.2.1 TSF 应提供以下加密密钥建立技术:[***通过人工装载建立加密密钥***,[***赋值:附加的加密密钥建立技术***]]。

密码模块依据国家标准和国家密码管理机构相关标准规定的手工加密密钥分发方法能在下面的环境[***赋值:密码模块输出密钥的环境***]接受密钥输入和输出密钥。

应用注释:ST 作者使用第一个赋值以显示评估中应该包括的附加密钥生成技术。如果 TOE 不包括附加密钥生成技术,那么就赋值为"无"。

应用注释:ST 作者使用第二个赋值去详细描述密钥从密码模块输出的条件(例如,仅在某种类型的密钥产生活动期间)。

应用注释:这个要求规定 TSF 密码模块有能力执行手工密钥输入/输出,这个能力应遵循国家标准和国家密码管理机构认可的过程。这不排除 ST 作者规定额外的密钥生成技术。

#### 10.1.3.3 FCS_CKM.4 密钥销毁

FCS_CKM.4.1 TSF 应根据符合下列条件的***密钥归零方法***来销毁密钥:

a) ***符合国家标准和国家密码管理机构相关标准中的密钥安全管理的密钥归零要求;***

b) ***对所有私钥、明文加密密钥和其他重要的密码安全参数进行清零是迅速的、完备的;***

c) ***通过三次或三次以上交替地覆盖重要的密码安全参数储存区执行归零操作;***

d) ***一旦将密钥/CSP 传输到其他地方,TSF 应三次或三次以上交替地覆盖私钥、明文加密密钥和其他重要的密码安全参数的中间储存区。***

应用注释:d)适用于密钥/参数在处理过程中进行复制时涉及的位置,而 b)、c)适用于规定的存储密钥时被使用的位置。临时位置包括寄存器、物理存储器位置,甚至页文件和内存转储区。

#### 10.1.3.4 FCS_COP_EXP.1 随机数产生

FCS_COP_EXP.1.1 TSF 应产生 TSF 密码功能中所使用的所有随机数。随机数产生器应符合[***国家标准和国家密码管理机构相关标准的要求***]。

应用注释:无论何时一个参考标准要求随机数产生功能,这个要求确认了可以接受的随机数产生器的子集。虽然国家标准和国家密码管理机构认可的密码模块中要求实施随机数产生功能,但是在执行满足 FCS_COP_EXP.2 的密码运行的密码模块中没有要求实施随机数产生功能。注意,这个要求没有要求随机数产生功能是通用的(例如,通过 API 的非可信用户)。

#### 10.1.3.5 FCS_COP_EXP.2 密码运行

FCS_COP_EXP.2.1 遵循无线客户加密策略,通过使用[***国家标准和国家密码管理机构认可的算法***]运行在[***一个或多个国家标准和国家密码管理机构支持的模式***]支持[***一个或多个国家标准和国家***

*密码管理机构认可的密钥长度*]的密码模块执行加密和解密。

#### 10.1.4 FDP 类:用户数据保护

##### 10.1.4.1 FDP_IFC.1 子集信息流控制

FDP_IFC.1.1 TSF 应对[*主体:客户端,接入系统;信息:网络数据包;操作:接收数据包和传输数据包*]执行[*TOE 加密策略*]。

##### 10.1.4.2 FDP_IFF.1 简单安全属性

FDP_IFF.1.1 TSF 应基于下列类型的主体和信息安全属性:[*主体:客户端,接入系统;信息:加密/加密标志;网络接口的传播方向*]执行[*TOE 加密策略*]。

FDP_IFF.1.2 如果支持下列规则,TSF 应允许一个受控主体和受控信息之间由受控操作流动:

a) *如果加密/解密标志没有显示 TOE 应该执行加密,那么所有数据包可能不进行任何修改就通过;*

b) *如果传输的方向是从操作系统到网络接口,且加密/解密标志显示 TOE 应该执行加密,那么 TOE 必须通过 FCS_COP_EXP.2.1 加密用户数据。如果成功,通过无线接口传输数据包;*

c) *如果传输的方向是从网络接口到操作系统,且加密/解密标志显示 TOE 应该执行解密,那么 TOE 必须通过 FCS_COP_EXP.2.1 解密用户数据。如果成功,把信息交给操作系统;*

d) [*选择:*[*赋值:对于每一个 TSF 将执行的操作,主体和信息安全属性之间支持的基于安全属性的关系*],*访问点/系统策略规则没有确定附加的信息流*]。

FDP_IFF.1.3 TSF 应执行[*选择:*[*赋值:附加的信息流控制 SFP 规则*],*"没有附加的信息流控制 SFP 规则"*]

FDP_IFF.1.4 TSF 应提供下列[*选择:*[*赋值:附加的 SFP 能力列表*],*"没有附加的 SFP 能力"*]。

FDP_IFF.1.5 TSF 应根据下列规则:[*选择:*[*赋值:基于安全属性明确授权信息流的规则*],*"没有清晰的授权规则"*]明确批准一个信息流。

FDP_IFF.1.6 TSF 应根据下列规则:[*选择:*[*赋值:基于安全属性明确拒绝信息流的规则*],*"没有清晰的拒绝规则"*]明确拒绝一个信息流。

应用注释:加解密标志确定对 TOE 进行管理设置。

##### 10.1.4.3 FDP_RIP.1 子集残留信息保护

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

应用注释:这个要求保障 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。相似地,TOE 必需确保清除共享存储区内先前传输的数据包内容或用于传输 TOE 与安装 TOE 的计算机之间数据包的机制(TSC 内)。

#### 10.1.5 FMT 类:安全管理

##### 10.1.5.1 FMT_MSA.2 安全的安全属性

FMT_MSA.2.1 TSF 应确保安全属性只接受安全的值。

##### 10.1.5.2 FMT_MSA.3 静态属性初始化

FMT_MSA.3.1 TSF 应执行[*无线客户加密策略*],以便为用于执行 SFP 的安全属性提供受限的默

认值。

FMT_MSA.3.2 TSF 应允许[***管理员***]在客体或信息被创建时指定替换性的初始值以代替原来的默认值。

#### 10.1.5.3 FMT_SMF.1(1) 管理功能规范(密码功能)

FMT_SMF.1.1(1) TSF 应能执行下面的安全管理功能:[***遵照无线客户端策略(通过 FCS_COP_EXP.2)对网络数据包进行加解密***]。

应用注释:这个要求确保负责管理 TOE 的人员能够对 WLAN 客户端传输的加密/解密数据选择 FCS_COP_EXP.2 指定的加密算法或不进行加密。

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

FMT_SMF.1.1(2) TSF 应能执行下面的管理功能:[***打开或关闭安全审计(FAU_GEN_EXP.1)***]。

应用注释:这个要求确保负责管理 TOE 的人员能够打开或关闭 TOE 审计记录产生。

#### 10.1.5.5 FMT_SMF.1(3) 管理功能规范(密码密钥数据)

FMT_SMF.1.1(3) TSF 应能执行下面的安全管理功能:[***遵照无线客户端策略设置、修改和删除密码密钥和密钥数据,打开或关闭密码密钥测试验证的功能***]。

应用注释:这个要求的目的是提供配置 TOE 密钥的能力。配置密钥数据包括:设置密钥的生命周期,设置密钥长度等。

### 10.1.6 FPT 类:TSF 保护

#### 10.1.6.1 FPT_TST_EXP.1 TSF 测试

FPT_TST_EXP.1.1 TSF 应在**初始启动或接收到授权用户的请求**时将运行一套自检程序以***显示 TSF 硬件部分的正常运行***。

FPT_TST_EXP.1.2 TSF 应为授权用户提供使用 TSF 提供的加密功能去验证***除审计数据以外所有 TSF 数据***的完整性的能力。

FPT_TST_EXP.1.3 TSF 应能使用 TSF 提供的加密功能去验证存储的 TSF 可执行代码的完整性。

应用注释:FPT_TST_EXP.1.1 中,仅有 TSF 的硬件需要自检,这是因为硬件会随时间而变化(老化出现故障),所以这是有意义的;而软件通常不需要自检。FPT_TST_EXP.1.3 解决了 TSF 软件完整性。FPT_TST_EXP.1.2 中,ST 作者应确定不需要完整性验证的 TSF 数据。虽然一些 TSF 数据是动态的,因此不应该进行完整性验证,但是所有需要完整性验证的 TSF 数据被期望遵循这个要求。在元素 FPT_TST_EXP.1.1 和 FPT_TST_EXP.1.2 中,虽然典型的 MAC 和散列函数能被用于完整性验证,但是密码机制必须是 FCS_COP_EXP.2 指定的加密算法。由于本标准没有明确要求任何 MAC 或散列函数,ST 作者可能重复 FCS_COP_EXP.2。

#### 10.1.6.2 FPT_TST_EXP.2 对密码模块进行 TSF 测试

FPT_TST_EXP.2.1 TSF 应在**初始启动或接收到授权用户的请求**时将运行一套自检程序以***显示 TSF 加密组件的正常运行***。

FPT_TST_EXP.2.2 TSF 应在产生密钥后立即运行一套遵循国家标准和国家密码管理机构相关标准的密码模块自检程序。

应用注释:FPT_TST_EXP.2.2 元素并没有强制要求 TOE 产生密钥。

### 10.2 TOE 安全保障要求

本标准的 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。这些保障组件确定了 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:开发 | 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** |
| 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.1 | 陈述性的安全要求 |
| | 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

本标准的 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。

表 4 运行环境安全要求

| 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.2 | 用户身份关联 | FAU_GEN.1<br>FIA_UID.1 |
| | FAU_SAA.1 | 潜在侵害分析 | FAU_GEN.1 |
| | FAU_SAR.1 | 审计查阅 | FAU_GEN.1 |
| | FAU_SAR.2 | 限制审计查阅 | FAU_SAR.1 |
| FAU 类:安全审计 | FAU_SAR.3 | 可选审计查阅 | FAU_SAR.1 |
| | FAU_SEL.1 | 选择性审计 | FAU_GEN.1<br>FMT_MTD.1 |
| | FAU_STG.1 | 受保护的审计迹存储 | FAU_GEN.1 |
| | FAU_STG.3 | 审计数据可能丢失时的行为 | FAU_STG.1 |
| FDP 类:用户数据保护 | FDP_RIP.1 | 子集残留信息保护 | 无 |
| FIA 类:标识与鉴别 | FIA_USB.1 | 用户-主体绑定 | FIA_ATD.1 |
| FMT 类:安全管理 | FMT_MOF.1 | 安全功能行为的管理 | FMT_SMR.1<br>FMT_SMF.1 |
| FMT 类:安全管理 | FMT_MTD.1 | TSF 数据的管理 | FMT_SMR.1<br>FMT_SMF.1 |
| | FMT_SMR.1 | 安全角色 | FIA_UID.1 |
| FPT 类:TSF 保护 | FPT_STM.1 | 可信时间戳 | 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 通过包括同样的要求作为 TOE 的一部分,满足一些或全部运行环境应该实现的要求也是可以接受的。

## 11.2 FAU 类:安全审计

### 11.2.1 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,TOE 运行环境应能将每个可审计事件与引起该事件的用户身份相关联。

### 11.2.2 FAU_SAA.1 潜在侵害分析

FAU_SAA.1.1 TOE 运行环境应能使用一组规则去监测审计事件,并根据这些规则指示出实施 SFR 的潜在侵犯。

FAU_SAA.1.2 TOE 运行环境应执行下列规则监测审计事件:

a) 已知的用来指示潜在安全侵害的***可审计事件的积累或表 2 中审计事件的组合***;

b) 无附加的规则。

### 11.2.3 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 运行环境应以便于用户理解的方式提供审计记录。

应用注释:这个要求确保 TOE 运行环境为管理员提供管理员查看 TOE 产生的审计记录所必需的

功能。

#### 11.2.4 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：这个要求确保访问 TOE 产生的审计记录仅限于那些被授权查看信息的用户。

#### 11.2.5 FAU_SAR.3 可选审计查阅

FAU_SAR.3.1 TOE 运行环境应根据***逻辑关系标准***提供对审计数据进行***分类***、***搜索***、***排序***的能力。

#### 11.2.6 FAU_SEL.1 选择性审计

FAU_SEL.1.1 TOE 运行环境应能根据以下属性从审计事件集中包含或排除可审计事件：

a) [**用户身份，主体身份，主机身份**]；

b) [***赋值：附加的可选的审计属性***]。

#### 11.2.7 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。

#### 11.2.8 FAU_STG.3 审计数据可能丢失时的行为

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警告管理员***，[**选择**：[***赋值：采取其他的行动***]，“无”]。

应用注释：如果审计迹设置被超过，那么 ST 作者应该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

FDP_RIP.1 子集残留信息保护

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**[***网络数据包对象***]时不再可用。

应用注释：这个要求保障 TOE 运行环境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。既然运行环境要求的操作必须完成，因此选择“资源被分配到”。它包括两个选项（当资源被释放时资源的信息内容不可用的系统也可以声称满足资源回收之前资源的内容已被释放的要求）。

### 11.4 FIA 类：标识与鉴别

FIA_USB.1 用户-主体绑定

FIA_USB.1.1 TOE 运行环境应将用户安全属性：[***鉴别凭证***] 与代表用户活动的主体相关联。

FIA_USB.1.2 TOE 运行环境应执行[***赋值：属性初始关联规则***]将用户安全属性与代表用户活动的主体初始关联。

FIA_USB.1.3 TOE 运行环境应执行[***赋值：属性更改规则***]管理用户安全属性与代表用户活动的主体间关联关系的变化。

### 11.5 FMT 类:安全管理

#### 11.5.1 FMT_MOF.1 安全功能行为管理(加密功能)

FMT_MOF.1.1 TOE 运行环境应仅限于[***管理员***]对[***加密/解密网络数据包(FMT_SMF.1(1),FMT_SMF.1(3)),审计(FMT_SMF.1(2))***]具有确定其行为的能力。

#### 11.5.2 FMT_MTD.1 TSF 数据的管理(时间 TSF 数据)

FMT_MTD.1.1 TOE 运行环境应仅限于[***管理员***]能够对[***用于形成 FPT_STM.1 中时间戳的时间和日期***]进行设置。

应用注释:TOE 运行环境必须为管理员提供设置时间和日期的接口。

#### 11.5.3 FMT_SMR.1 安全角色

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

FMT_SMR.1.2 TOE 运行环境应能够把用户和角色关联起来。

应用注释:TOE 运行环境支持用于管理 TOE 的管理角色。在一些环境中,终端用户(例如,便携式计算机)扮演管理角色。可是,其他环境(例如,多用户系统)中,除终端用户的其他人扮演管理角色。

### 11.6 FPT 类:TSF 保护

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 TOE 使用的时间戳。

# 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，并且为无线局域网客户端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

本条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之间的映射关系

| 威胁和策略 | 解决威胁的安全目的 | 基本原理 |
| --- | --- | --- |
| T.ACCIDENTAL_ADMIN_ERROR<br>管理员可能不正确安装或配置 TOE，导致无效的安全机制 | O.ADMIN_GUIDANCE<br>TOE 应为安全管理员提供必要的信息以便于安全管理<br>OE.MANAGE<br>TOE 运行环境应增加 TOE 的功能和设施以支撑管理员对于 TOE 安全的管理，并且要防止这些功能和设施被未授权使用 | O.ADMIN_GUIDANCE 通过保障 TOE 管理员拥有一个指导他们如何安全地管理 TOE 的指南来缓解威胁。该指南也有助于减少管理员引起的不安全地配置 TOE 的错误。<br>OE.MANAGE 保障 TOE 运行环境能够支撑管理员对于 TOE 安全的管理 |
| T.CRYPTO_COMPROMISE<br>用户或进程可能引起与密码功能相关联的关键数据或可执行代码被不适当的访问（查看、修改或删除），从而破坏了密码机制和受该机制保护的数据 | O.RESIDUAL_INFORMATION<br>TOE 应确保资源被重新分配时 TOE 控制范围内受保护资源所包含的任何信息被泄漏。<br>OE.RESIDUAL_INFORMATION<br>TOE 运行环境确保资源被重新分配时 TOE 控制范围内保护资源包含的信息不能被泄漏。<br>O.CRYPTOGRAGHY<br>TOE 应使用已获国家密码管理机构批准的密码服务 | O. RESIDUAL _ INFORMATION 和 OE.RESIDUAL_INFORMATION 通过保障 TOE 或 TOE 运行环境在网络数据包中不会作为填充插入关键数据（和加解密有关）或可执行代码来缓解这个威胁。<br>O.CRYPTOGRAGHY 确保处理和销毁密钥时能够遵循国家密码管理机构相关标准中规定的程序 |

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<br>要求规范或 TOE 设计中的无意错误可能导致恶意用户或进程可利用的缺陷 | O.DECUMENTED_DESIGN<br>TOE 的设计应以文档的形式充分地和准确地记录。<br>O. CONFIGURATION _ IDENTIFICATION<br>由于 TOE 迅速重新分发，应采用一种方式完全标识 TOE 的配置，该方式将允许在实现时错误能够被标识和改正。<br>O.VULNERABILITY_ANALYSIS<br>应对 TOE 进行脆弱性分析以表明 TOE 的设计和实施不包含任何明显的缺陷 | O.DECUMENTED_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个威胁。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。这降低了设计缺陷产生的可能性，提高了发现意外设计错误的机会。<br>支持 O. DECUMENTED _ DESIGN 的 ADV_RCR.1 确保 TOE 设计与高层设计和功能规范的一致性。<br>O. CONFIGURATION _ 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个威胁。<br>O. VULNERABILITY _ ANALYSIS 确保可以发现 TOE 的明显漏洞，由于任何发现的漏洞已被删除从而能缓解漏洞的威胁。这包括分析任何声称符合本标准 TOE 中的概率的或置换的机制 |
| T.POOR_IMPLEMENTATION<br>TOE 设计的实施中的无意错误可能导致恶意用户或进程利用缺陷 | O. CONFIGURATION _ IDENTIFICATION<br>由于 TOE 迅速重新分发，应采用一种方式完全标识 TOE 的配置，该方式将允许在实现时错误能够被标识和改正。<br>O.PARTIAL_FUNCTIONAL_TESTING<br>应对 TOE 进行安全功能测试以表明 TSF 满足它的安全功能要求。<br>O.VULNERABILITY_ANALYSIS<br>应对 TOE 进行脆弱性分析以表明 TOE 的设计和实施不包含任何明显的缺陷 | O. CONFIGURATION _ IDENTIFICATION 通过要求开发者控制对 TOE 设计所做的改变来处理这个威胁。<br>O. PARTIAL _ FUNCTIONAL _ TESTING 确保开发者对 TOE 的测试能够充分满足所有的 TOE 安全功能要求。这个目的通过确保依据安全功能要求对 TOE 安全相关部分进行测试来解决这个威胁。<br>O. VULNERABILITY _ ANALYSIS 确保 TOE 的明显漏洞已被分析和 TOE 能够抵制恶意用户。这包括分析任何声称符合本标准 TOE 中的概率的或置换的机制 |

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<br>由于缺乏或对 TOE 安全功能正确运行的测试不充分，导致不正确 TOE 的行为未被发现，从而潜在的安全脆弱性 | O.CORRECT_TSF_OPERATION<br>TOE 应提供测试 TSF 的以确保 TSF 在客户站点正确运行的能力。<br>O.PARTIAL_FUNCTIONAL_TESTING<br>应对 TOE 进行安全功能测试以表明 TSF 满足它的安全功能要求。<br>O.VULNERABILITY_ANALYSIS<br>应对 TOE 进行脆弱性分析以表明 TOE 的设计和实施不包含任何明显的缺陷。<br>O.DECUMENTED_DESIGN<br>TOE 的设计应以文档的形式充分地和准确地记录 | O.CORRECT_TSF_OPERATION 确保一旦 TOE 被安装在客户端，就应该证明 TSF(硬件和软件)的完整性。这使得用户相信 TOE 的安全策略连续地被实施。<br>O. PARTIAL _ FUNCTIONAL _ TESTING 提高了通过测试发现实施(例如，功能规范，高层和低层设计)中存在的错误的可能性。<br>O. VULNERABILITY _ ANALYSIS (AVA_VLA.1)通过要求脆弱性分析和功能性测试之外的测试同时执行。这个目的确认 TOE 没有包含功能测试没有发现的安全缺陷。<br>虽然这些测试活动对于成功地完成评估是必要的，但是它们不能确保一旦 TOE 被安装，它就能持续地正确运行和实施它的安全策略。必须为终端用户提供一些层次的曾是以确保一旦 TOE 被安装，TOE 的安全机制就能持续地正确运行。<br>O.DECUMENTED_DESIGN 能帮助确保 TOE 文档化的设计满足安全功能要求。为了保障 TOE 的设计在它的实施中正确地实现，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 |
| T.RESIDUAL_DATA<br>恶意用户或进程利用重新分配 TOE 资源来获取对于资源的未授权访问 | O.RESIDUAL_INFORMATION<br>TOE 应确保资源被重新分配时 TOE 控制范围内受保护资源所包含的任何信息不被泄漏。<br>OE.RESIDUAL_INFORMATION<br>TOE 运行环境确保资源被重新分配时 TOE 控制范围内保护资源包含的信息不能被泄漏。<br>O.CRYPTOGRAGHY<br>TOE 应使用已获国家密码管理机构批准的密码服务 | O.RESIDUAL_INFORMATION 通过确保网络数据包对象在使用之前被清除来缓解这个威胁。当考虑残留信息时，TOE 控制范围内关注的资源是网络数据包。<br>O.CRYPTOGRAGHY 保护被提供给符合国家标准和国家密码管理机构相关标准的(通过 FCS_CKM_EXP.2 和 FCS_CKM.4)的密码对象以确保用于存储密钥的对象不再被使用时被覆盖。<br>OE.RESIDUAL_INFORMATION 通过确保 TOE 和 TOE 运行环境不能把重要数据(与加密有关的数据)和可执行代码插入到网络数据包对象的填充区 |

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<br>恶意用户或进程通过不高级的攻击引起 TSF 数据或可执行代码被不适当的访问（查看、修改或删除） | O.MANAGE<br>TOE 应提供支持管理员管理 TOE 安全所必需的功能和设施。<br>OE.MANAGE<br>TOE 运行环境应增加 TOE 的功能和设施以支撑管理员对于 TOE 安全的管理，并且要防止这些功能和设施被未授权使用。<br>O.RESIDUAL_INFORMATION<br>TOE 应确保资源被重新分配时 TOE 控制范围内受保护资源所包含的任何信息不被泄漏。<br>OE.RESIDUAL_INFORMATION<br>TOE 运行环境确保资源被重新分配时 TOE 控制范围内保护资源包含的信息不被泄漏。<br>O.CRYPTOGRAGHY<br>TOE 应使用已获国家密码管理机构批准的密码服务 | 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。<br>O.RESIDUAL_INFORMATION，OE.RESIDUAL _ INFORMATION 和 O.CRYPTOGRAGHY 通过保障清除网络数据包中的任何残留数据和在加密素材不再需要时禁止访问来缓解这个威胁 |
| P.ACCOUNTABILITY<br>TOE 的授权用户对自身在 TOE 内的行为负责 | O.AUDIT_GENERATION<br>TOE 应具有检查和创建与用户相关联的安全相关事件记录的能力。<br>O.MANAGE<br>TOE 应提供支持管理员管理 TOE 安全所必需的功能和设施。<br>OE.MANAGE<br>TOE 运行环境应增加 TOE 的功能和设施以支撑管理员对于 TOE 安全的管理，并且要防止这些功能和设施被未授权使用。<br>OE.TIME_STAMPS<br>TOE 运行环境应提供可靠的时间戳，并为管理员提供为时间戳设置时间的能力。<br>OE.TOE_ACCESS<br>TOE 运行环境应提供控制用户对 TOE 进行逻辑访问的机制 | O.AUDIT _ GENERATION 确保 TOE 能够产生与用户相关联的审计事件记录。<br>O.MANAGE 确保管理员能够打开或关闭审计功能。<br>OE.MANAGE 确保仅限于管理员查看审计日志信息。<br>OE.TIME_STAMPS 通过要求 TOE 运行环境提供可靠的时间戳（管理员本地配置或通过外部 NTP 服务器配置）来支持该策略。审计机制被要求在每个审计记录中包括目前的日期和时间。<br>OE.TOE_ACCESS 通过确保 TOE 运行环境提供一个管理角色及一个机制来标识一个代表管理员行为的进程 |

表 A.1（续）

| 威胁和策略 | 解决威胁的安全目的 | 基本原理 |
| --- | --- | --- |
| P.CRYPTOGRAGHY<br>仅有国家密码管理机构认可的密码系统（方法和实施）才能用于密钥管理（例如，密钥的产生、访问、分发、销毁、处理和储存）和密码服务（例如，加解密、签名、散列、密钥交换和随机数产生服务） | O.CRYPTOGRAGHY<br>TOE 应使用已获国家密码管理机构批准密码服务 | O.CRYPTOGRAGHY 通过要求 TOE 实施已获国家标准和国家密码管理机构批准的密码服务来满足该策略。当 TSF 数据在传输时，通过这些服务为它们提供保密性和完整性保护 |

## 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 TOE 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（包括安全功能要求和安全保障要求）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 | 支持安全目的的安全要求 | 基本原理 |
| --- | --- | --- |
| O.ADMIN_GUIDANCE<br>TOE 应为安全管理员提供必要的信息以便于安全管理 | ALC_DEL.1<br>AGD_OPE.1<br>AGD_PRE.1 | ALC_DEL.1 确保管理员能够使用 TOE 安全管理所必需的清洁（一旦 TOE 离开了开发者的控制，恶意代码不能被插入）版本的 TOE 开始 TOE 安装。<br>AGD_OPE.1 确保开发者应为用户提供一个关于如何安全操作 TOE 的指南。这包括描述用户管理 TOE 所使用的接口和管理员所需要配置的安全参数。这个文档也提供一个如何安装和使用 TOE 审计特征的描述。<br>AGD_PRE.1 准备程序用于保障 TOE 一开发者预期的安全方式被接收和安装 |
| O. AUDIT _ GENERATION<br>TOE 应具有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_EXP.1 | FAU_GEN_EXP.1 定义 TOE 必需记录的事件集。该要求确保管理员能够审计 TOE 中发生的任何安全相关事件。这个要求也定义了审计记录中每个审计事件必须包含的信息，同时也定义了每个审计记录中必须存在的最小量信息 |

表 A.2（续）

| TOE 安全目的 | 支持安全目的的安全要求 | 基本原理 |
| --- | --- | --- |
| O.CONFIGURATION_IDENTIFICATION<br>由于 TOE 迅速重新分发，应采用一种方式完全标识 TOE 的配置，该方式将允许在实现时错误能够被标识和改正 | ALC_CMC.2<br>ALC_CMS.2<br>ALC_FLR.2 | ACM_CAP.2 需要一个唯一的参照号，以确保 TOE 实例再被评估时不会产生歧义。<br>ALC_CMS.2 CM 系统只能控制处于 CM 下配置项的改变。将 TOE 本身、TOE 组成部分和其他安全保障要求所需的评估证据置于 CM 之下，可以确保他们的修改是在一个带正确授权的方式下进行的。<br>ALC_FLR.2TOE 为了让开发者能够对来自 TOE 用户的安全缺陷报告采取适当的动作，并且知道该向谁发送修正补丁，TOE 用户需要了解如何将安全缺陷报告提交给开发者。开发者将缺陷纠正指南提供给 TOE 用户，确保 TOE 用户知道这一重要信息 |
| O.CORRECT_TSF_OPERATION<br>TOE 应提供测试 TSF 的以确保 TSF 在客户站点正确运行的能力 | FPT_TST_EXP.1<br>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，那么也许不能正确实施安全策略。<br>FPT_TST_EXP.2 功能要求被包括以解决与加密相关的 TSF 数据的关键特性和具体处理。由于加密的 TSF 数据有具体的国家密码管理机构相关标准要求，所以确保对这些数据的完整性测试的级别应该与 FCS 功能要求所确定评估级别相同是重要的 |
| O.CRYPTOGRAGHY<br>TOE 应使用国家密码管理机构认可的密码服务 | FCS_BCM_EXP.1<br>FCS_CKM_EXP.2<br>FCS_CKM.4<br>FCS_COP_EXP.1<br>FCS_COP_EXP.2<br>FDP_IFC.1<br>FDP_IFF.1 | FCS 要求通过确保加密标准包括国家密码管理机构出版物（在必要时）和国家密码管理机构认可标准来满足这个目的。<br>FCS_BCM_EXP.1 明确规定了加密模块必须满足的国家密码管理机构相关标准的评估等级。<br>FCS_CKM_EXP.2 确保加密密钥处理和存储要求在执行密钥输入和输出时满足国家密码管理机构相关标准。<br>FCS_CKM.4 规定了 TOE 执行密钥零化时必须满足的国家密码管理机构相关标准。<br>FCS_COP_EXP.1 要求在 TOE 中实施的任何加密模块在有必要使用随机数时应该使用国家密码管理机构认可的随机数产生器（产品）。<br>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认可的算法，算法满足相关密码标准。<br>FDP_IFC.1 和 FDP_IFF.1 确定了 TOE 加密/解密用户数据时必须实施的策略 |

表 A.2（续）

| TOE 安全目的 | 支持安全目的的安全要求 | 基本原理 |
| --- | --- | --- |
| O.DECUMENTED_DESIGN<br>TOE 的设计应以文档的形式充分地和准确地记录 | ADV.ARC.1<br>ADV_FSP.2<br>ADV_TDS.1 | ADV.ARC.1 开发者应提供对 TSF 安全架构的描述。允许额外提供的其他 TSF 证据对这些信息进行分析，这些信息将确保 TSF 达到期望的属性。<br>ADV_FSP.2 要求开发者提供所有 TSFI 的目的、使用方法、参数和参数描述。另外，对已 SFR-执行 TSFI，开发者必须描述 SFR-执行行为和直接错误消息。<br>ADV_TDS.1 开发者应提供 TOE 的设计，提供从功能规范的 TSFI 到 TOE 设计中获取到的最底层分解的映射 |
| O.MANAGE<br>TOE 将提供支持管理员管理 TOE 安全所必需的功能和设施 | FMT_MSA.2<br>FMT_MSA.3<br>FMT_SMF.1(1)<br>FMT_SMF.1(2)<br>FMT_SMF.1(3) | FMT 要求被用于满足这个管理目的和其他规定了控制功能的目的。这个目的的要求的基本原理集中于管理员有能力执行管理功能以至于控制安全功能的行为。<br>FMT_MSA.2 通过防止管理员错误地为安全属性赋值来实现这个目的。<br>FMT_MSA.3 要求安全属性使用的默认值是受限制的，管理员能够覆盖这些默认值。<br>FMT_SMF.1(1)和 FMT_SMF.1(3)确保 TOE 与外部系统通信时管理员能够控制加密的使用。<br>FMT_SMF.1(2)为管理员提供了控制 TOE 审计记录产生的机制能力 |
| O. PARTIAL _ FUNCTIONAL_TESTING<br>应对 TOE 进行安全功能测试以表明 TSF 满足它的安全功能要求 | ATE_COV.1<br>ATE_FUN.1<br>ATE_IND.2 | 为了满足 O.FUNCTIONAL_TESTING，ATE 类的要求是必要的。<br>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子类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。<br>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子类覆盖 TSFI 的程度。这个组件也要求独立地确认测试族的程度，这有助于确保 TSFI 正确的安全相关功能通过测试被证明。<br>ATE_IND.2 要求通过规定一个独立方运行测试子类的子集独立地确认开发者的测试结果。这个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族中没有证明的功能行为。一旦成功地完成这些要求，可以证明 TOE 遵循了规定的安全功能要求 |

表 A.2（续）

| TOE 安全目的 | 支持安全目的的安全要求 | 基本原理 |
| --- | --- | --- |
| O. RESIDUAL _ INFORMATION<br>TOE 应确保资源被重新分配时 TOE 控制范围内受保护资源所包含的任何信息不被泄漏 | FDP_RIP.1<br>FCS_CKM.4 | FDP_RIP.1(1)被用于确保资源被重新分配时资源的内容不再可用。TOE 清除用于构建网络数据包的存储器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(例如，如果在数据包的构建中使用了填充区，那么填充区禁止包含用户的数据或 TSF 数据)。<br>FCS_CKM.4 要求使用国家密码管理机构认可的证书。并且对如何管理 TOE 内的密钥提出了要求。除了 FDP_RIP.1，这个要求提出了在于当密钥从一个位置移动到另一个位置的时候(在临时存储器计算后移动到永久位置)，存储器应立即被清除而不是等待直到存储器被重新分配给另一个主体。FCS_CKM.4 也适用于 TSF 使用的密钥的销毁。这个要求规定了密钥销毁的方式和时间。这些密钥的合理销毁对于确保资源被重新分配给用户时这些密钥不被泄漏至关重要 |
| O.VULNERABILITY_ANALYSIS<br>应对 TOE 进行脆弱性分析以表明 TOE | AVA_VAN.2 | AVA_VAN.2 评估者执行脆弱性分析以确认脆弱性的存在。评估者执行穿透性测试，以确认潜在的脆弱性在 TOE 运行环境中不能被利用。评估者在假定具有基本的供给潜力的情况下执行穿透性测试 |

### A.3.2 运行环境安全要求的基本原理

表 A.3 说明了 TOE 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。

运行环境安全目的中的“OE.PHYSICAL”和“OE.NO_EVIL”等两个安全目的应对了第 7 章“TOE 安全环境”中的“A.PHYSICAL”和“A.NO_EVIL”等两个假设。因此，这两个环境安全目的能够追溯到假设。

表 A.3 TOE 运行环境安全要求的基本原理

| TOE 运行环境安全目的 | 支持安全目的的安全要求 | 基本原理 |
| --- | --- | --- |
| OE.MANAGE<br>TOE 运行环境应增加 TOE 的功能和设施以支撑管理员对于 TOE 安全的管理，并且要防止这些功能和设施被未授权使用 | FAU_SAR.1<br>FAU_SAR.2<br>FAU_SAR.3<br>FIA_USB.1<br>FMT_MOF.1<br>FMT_MTD.1<br>FMT_SMR.1<br>FAU_SAA.1<br>FAU_STG.1 | FAU_SAR.1 确保 TOE 运行环境为负责管理 TOE 的人员提供查看 TOE 审计记录的设施(例如，如果审计了必要的事件，那么管理员能够构建事件的顺序)。<br>FAU_SAR.2 确保 TOE 运行环境能够仅限于那些有权查看 TOE 审计记录的用户进行访问。<br>FAU_SAR.3 确保 TOE 运行环境能够提供对审计数据进行分类、搜索、排序的能力。<br>FIA_USB.1 确保 TOE 运行环境包括关联进程和角色的机制。这确保 TOE 和 TOE 运行环境能够确定它的关联 |

表 A.3（续）

| TOE 运行环境安全目的 | 支持安全目的的安全要求 | 基本原理 |
| --- | --- | --- |
| OE.MANAGE<br>TOE 运行环境应增加 TOE 的功能和设施以支撑管理员对于 TOE 安全的管理，并且要防止这些功能和设施被未授权使用 | FAU_STG.3<br>FAU_GEN.2<br>FAU_SEL.1 | FMT_MOF.1 确保 TOE 运行环境仅限于管理员访问 TSF 管理功能。<br>FMT_MTD.1 确保 TOE 运行环境提供管理时间戳机制的设施。<br>FAU_SMR.1 确保 TOE 运行环境提供一个用于管理 TOE 和运行环境的角色。<br>FAU_SAA.1 确保 TOE 运行环境依据一套能够向管理员显示一个潜在威胁的规则监测审计事件。<br>FAU_STG.1 确保 TOE 运行环境防止非授权地删除和修改审计记录。<br>FAU_STG.3 确保一旦发现潜在的审计数据丢失，管理员立即被警告。<br>FAU_GEN.2 确保审计记录与促发审计事件的用户身份的关联。这允许管理员管理审计数据和监测与用户关联的事件。<br>FAU_SEL.1 允许安全管理员配置被记录的审计事件类型。这给管理员带来了灵活性，即仅记录站点策略认为是必要的事件，因此减少了审计机制消耗的资源数量 |
| OE.RESIDUAL_INFORMATION<br>TOE 运行环境确保资源被重新分配时 TOE 控制范围内保护资源包含的信息不能被泄漏 | FDP_RIP.1 | FDP_RIP.1 确保 TOE 运行环境为网络数据包中的残留信息提供与 TOE 相同的保护。这确保 TOE 运行环境或 TOE 不允许先前传输的数据包数据被插入到新的数据包中 |
| OE.TIME_STAMPS<br>TOE 运行环境应提供可靠的时间戳，并为管理员提供为时间戳设置时间的能力 | FMT_MTD.1<br>FPT_STM.1<br>FMT_SMR.1 | FPT_STM.1 确保运行环境提供一个用于同步审计事件的时间戳机制。<br>FMT_MTD.1 确保 TOE 运行环境提供管理时间戳机制的设施，仅限于管理员访问时间戳机制。<br>FMT_SMR.1 确保 TOE 运行环境提供一个用于管理 TOE 和运行环境的角色 |
| OE.TOE_ACCESS<br>TOE 运行环境应提供对用户逻辑访问 TOE 进行控制的机制 | FMT_SMR.1<br>FIA_USB.1 | FMT_SMR.1 确保 TOE 运行环境提供一个用于管理 TOE 和运行环境的角色。<br>FIA_USB.1 确保 TOE 运行环境包括关联进程和角色的机制。这确保 TOE 和 TOE 运行环境能够确定它的关联 |

### A.3.3 不被 TOE 处理的威胁的基本原理

在无线局域网环境下，TOE 是一个更大系统的一个组件。因此，TOE 不会处理运行环境下的所有威胁，表 A.4 说明了运行环境中不被 TOE 处理的威胁。

表 A.4 运行环境下不被 TOE 处理的威胁

| 威胁名称 | 威胁定义 | 运行环境下未包含威胁的基本原理 |
| --- | --- | --- |
| T.AUDIT_COMPROMISE | 用户或进程可能查看审计记录，引起审计记录的丢失或修改，或防止后续的审计信息不被记录，从而掩盖用户的行为 | TOE 是更大系统上的一个组件，TOE 依据系统管理员规定的审计策略负责产生审计记录。这些记录被期望储存在 TOE 的外面。TOE 运行环境将提供适当的机制保护这些产生的审计记录。由于 TOE 没有缓解这个威胁，所以本标准不包括此威胁 |
| T.MASQUERADE | 用户或进程可能通过冒充另一个实体来非授权地访问数据或 TOE 资源 | TOE 是更大系统上的一个组件，TOE 不给用户或进程提供认证信息，也不被期望防止非授权用户或进程的假扮行为。由于 TOE 没有缓解这个威胁，所以本标准不包括此威胁 |
| T. UNATTENDED_SESSION | 用户可能非授权地访问无人管理的会话 | TOE 是更大系统上的一个组件，在 TOE 控制范围内的惟一无人管理的会话是网络连接。本标准认为，这个威胁由安装 TOE 的操作系统处理更合适。操作系统能够统一地对无人管理的网络、串行接口和控制台会话实施一个策略。由于 TOE 没有缓解这个威胁，所以本标准不包括此威胁 |
| T.UNAUTHORIZED_ACCESS | 用户可能非授权地访问了用户数据 | TOE 作为更大系统上的一个组件，它不能访问那些用于标识授权或非授权用户的信息。由于 TOE 没有缓解这个威胁，所以本标准不包括此威胁 |
| T.UNIDENTIFIED_ACTIONS | 管理员可能无法发现潜在的安全违反，因此限制了管理员对安全违反进行标识和采取行动的能力 | TOE 是更大系统上的一个组件，TOE 依据系统管理员规定的审计策略负责产生审计记录。但是，TOE 不被期望提供储存或检查审计记录的设施。TOE 运行环境被期望提供检查、分类、选择和管理审计记录的设施。由于 TOE 没有缓解该威胁，所以本标准不包括此威胁 |

### A.3.4 运行环境下不被 TOE 处理的策略的基本原理

在无线网络环境下，TOE 作为更大系统上的一个组件不能解决所有策略。表 A.5 确定了 TOE 运行环境下不被 TOE 处理的策略。

表 A.5 运行环境下不被 TOE 处理的策略

| 策略名称 | 策略定义 | 运行环境下未包含策略的基本原理 |
| --- | --- | --- |
| P.ACCESS_BANNER | TOE 将显示一个初始旗语用于描述使用的限制，法律协定或接入系统时用户同意的任何其他合理的信息 | TOE 运行环境（操作系统）负责显示一个合适的标语信息。由于 TOE 没有实施这个策略，所以本标准不包括此策略 |

### A.3.5 未满足所有依赖关系的基本原理

表 A.6 说明了 TOE 和 TOE 运行环境中某些安全功能组件未满足所有依赖关系的基本原理。

**表 A.6 未满足依赖关系的基本原理**

| 安全功能组件 | 未满足的依赖关系 | 依赖关系的分析和基本原理 |
|---|---|---|
| FCS_CKM_EXP.2 | FCS_CKM.1 | 在 FCS_CKM_EXP.2 背景下，FCS_CKM.1 要求允许 PP/ST 作者规定 TOE 使用的密钥的产生标准。既然 WLAN 客户 TOE 不被期望产生密钥，所以该组件被忽略。注意：本标准规定了手工密钥输入 |
| FDP_IFF.1 | FMT_MSA.3 | FDP_IFF.1 规定了 WLAN 客户端策略。FMT_MSA.3 允许本标准作者规定策略的安全默认值。既然 FMT_SMF.1(1)和 FMT_SMF.1(3)提供了设置策略的能力，所以设置安全的初始默认值(例如，默认解密)是不必要的 |
| FIA_USB.1 | FIA_ATD.1 | 该依赖关系是关于一个 TOE 运行环境的要求。对 TOE 运行环境施加的要求补充了 TOE，确保 TOE 和运行环境共同满足所有的安全目的。为了限制运行环境的范围，仅有那些直接满足目的的运行环境要求包括在本标准中。仅仅满足管理指南、审计指南或依赖关系链的运行环境要求没有包括在本标准中。<br>在 FIA_USB 背景下，FIA_ATD 依赖关系被用于规定实施 TSP 的用户安全属性。由于 TOE 运行环境有必要规定 FIA_USB，则 TOE 运行环境有必要规定 FIA_ATD。由于 TOE 运行环境包括该组件没有直接满足任何 TOE 目的，所以该要求被忽略 |
| FMT_SMR.1 | FIA_UID.1 | 这个依赖关系是关于一个 TOE 运行环境的要求。对 TOE 运行环境施加的要求补充了 TOE，确保 TOE 和运行环境共同满足所有的安全目的。为了限制运行环境的范围，仅有那些直接满足目的的运行环境要求包括在本标准中。仅仅满足管理指南、审计指南或依赖关系链的运行环境要求没有包括在本标准中 |
| FMT_SMR.1 | FIA_UID.1 | 在 FMT_SMR 背景下，FIA_UID 被用于规定未被证实身份的用户可用的行动。运行环境支持的任何角色被期望需要标识和鉴别组件。可是，由于 TOE 运行环境包括该求没有直接满足任何 TOE 目的，所以该组件被忽略 |

### A.3.6 扩展族的基本原理

表 A.7 列出了本标准包括的扩展的基本原理。

**表 A.7 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 WLAN 客户端密码模块的相关要求。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.3.7 扩展组件的基本原理

表 A.8 列出了本标准包括的扩展组件的基本原理。

**表 A.8 扩展组件的基本原理**

| 扩展组件 | 标识符 | 基本原理 |
| --- | --- | --- |
| FAU_GEN_EXP.1 | 审计数据产生 | 由于 GB/T 18336—2015 要求 FAU_GEN.1 规定 TOE 应该产生表明审计日志打开和关闭的审计记录，所以该扩展组件是必要的。TOE 被期望产生审计记录，但是它不被期望控制审计记录。因此，它不被要求产生与审计日志打开和关闭相关联的事件的审计记录 |
| FCS_BCM_EXP.1 | 基准密码模块 | 由于 GB/T 18336—2015 没有提供规定密码实施基准的方式，所以该扩展组件是必要的。该扩展组件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 |
| FCS_CKM_EXP.2 | 密码密钥建立 | 该扩展组件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 |
| FCS_COP_EXP.1 | 随机数产生 | 由于 GB/T 18336—2015 密码运行组件关注于具体的算法类型、运行模式和密钥长度，所以该扩展组件是必要的 |
| FCS_COP_EXP.2 | 密码操作（数据加密/解密） | 该扩展组件描述了密码模块而不是整个 TSF，该扩展组件是必要的 |
| FPT_TST_EXP.1 | TSF 测试 | 该扩展组件对于划分 TOE 自身必要的测试要求和密码模块特定的测试要求是必要的 |
| FPT_TST_EXP.2 | 对密码模块进行 TSF 测试 | 该扩展组件对于划分 TOE 自身必要的测试要求和密码模块特定的测试要求是必要的 |

## 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] GB/Z 20283—2006 信息安全技术 保护轮廓和安全目标的产生指南

[6] X.509 Certificate Policy for the United States Department of Defense, Version 5.0, 13 December 1999.

[7] Peer-to-Peer Wireless Local Area Network (WLAN) Protection Profile for Sensitive But Unclassified Environments, Version 0.1, March 2008.

[8] Draft U.S. DoD Remote Access Protection Profile for High Assurance Environments, version 0.98, 24 May 2000.

[9] High-Assurance Remote Access (HARA) Architecture, Version 1.1, 15 May 2000.

[10] Global Information Grid (GIG) Policy 6-8510, Information Assurance Guidance, 16 June 2000.

[11] Common Methodology for Information Technology Security Evaluation, Version 1.0, CEM-99/045, August 1999.

[12] US Government Wireless Local Area Network Client for Basic Robust Environments Protection Profile, Version 1.0.

[13] Global Information Grid (GIG) Policy 6-8510, Information Assurance Guidance, 16 June 2000.

[14] Common Methodology for Information Technology Security Evaluation, Version 2.2. CCIMB-2004-01-004. January 2004.

[15] FIPS PUB 140-2:Security Requirement for Cryptographic Modules, National Institute of Standards and Technology, May 25,2008.

[16] US Government Wireless Local Area Network (WLAN) Client for Basic Robustness Environments Protection Profile (Unclassified) Version 1.0, November 2003.

[17] US Government Wireless Local Area Network (WLAN) Access System Protection Profile For Basic Robustness Environments (Unclassified) Version 1.1, April 2004.

[18] US Government Wireless Local Area Network (WLAN) Access System Protection Profile For Basic Robustness Environments Version 1.0, April 2006.