ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35286—2017

信息安全技术　低速无线个域网空口安全测试规范

Information security technology—Air-interface security test specification for low-rate wireless personal area networks

2017-12-29 发布　　2018-07-01 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 …… 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　概述 …… 2
6　测试环境要求 …… 3
6.1　概述 …… 3
6.2　测试拓扑 …… 3
6.2.1　LR-WPAN 设备测试拓扑 …… 3
6.2.2　LR-WPAN 协调器测试拓扑 …… 4
6.2.3　可信第三方测试拓扑 …… 4
7　LR-WPAN 设备测试 …… 4
7.1　鉴别能力协商 …… 4
7.1.1　鉴别能力协商——不支持鉴别 …… 4
7.1.2　鉴别能力协商——支持鉴别 …… 5
7.2　鉴别套件 …… 5
7.2.1　基于共享密钥的 WPAN 鉴别协议 SPAP …… 5
7.2.2　基于 ID 的 WPAN 鉴别协议 IPAP …… 6
7.2.3　基于传输加密数据的 WPAN 鉴别协议 PAPTED …… 7
8　LR-WPAN 协调器测试 …… 8
8.1　鉴别能力协商 …… 8
8.1.1　鉴别能力协商——不支持鉴别 …… 8
8.1.2　鉴别能力协商——支持鉴别 …… 8
8.2　鉴别套件 …… 8
8.2.1　基于预共享密钥方式 SPAP …… 8
8.2.2　基于 ID 的 WPAN 鉴别协议 IPAP …… 9
8.2.3　基于传输加密数据的 WPAN 鉴别协议 PAPTED …… 10
8.2.4　帧安全 …… 11
9　可信第三方测试 …… 12

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:无线网络安全技术国家工程实验室、西安西电捷通无线网络通信股份有限公司、国家无线电监测中心检测中心、中国信息安全认证中心、天津市无线电监测站。

本标准主要起草人:杜志强、李明、李琴、王俊峰、布宁、姜廷学、黄振海、曹军、彭潇、颜湘、潘琪、铁满霞、张变玲、王月辉、吴迪、李楠、李华圣、张国强、童伟刚。

信息安全技术　低速无线个域网空口安全测试规范

1　范围

本标准规定了符合 GB/T 15629.15—2010 中安全机制 WSAI(WPAN 安全接入设施)的设备、协调器和可信第三方的安全协议的符合性检测方法。

本标准适用于符合 GB/T 15629.15—2010 的设备中的 WSAI 安全机制的符合性测试。

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/T 15629.15—2010　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15部分:低速无线个域网(WPAN)媒体访问控制和物理层规范

GB/T 15843.3—2016　信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制

GB/T 28455—2012　信息安全技术　引入可信第三方的实体鉴别及接入架构规范

GB/T 32905—2016　信息安全技术　SM3 密码杂凑算法

GB/T 32907—2016　信息安全技术　SM4 分组密码算法

GB/T 32918(所有部分)　信息安全技术　SM2 椭圆曲线公钥密码算法

GM/T 0009　SM2 密码算法使用规范

GM/T 0015　基于 SM2 密码算法的数字证书格式规范

ISO/IEC 9798-3:1998/Amd.1:2010　信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制　补篇1(Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques—Amendment 1)

3　术语和定义

下列术语和定义适用于本文件。

3.1

被测设备　tested equipment

被测的实现 WSAI 安全协议的设备,即被测试对象。

3.2

测试平台　test platform

提供 WSAI 安全机制测试的平台,用于收集和分析处理测试数据,按照测试规范的要求对测试数据进行判断,并且对判断结果进行呈现并记录的平台。

3.3

辅助设备　auxiliary equipment

一种特殊的基准设备,除进行 WSAI 安全机制交互外,还需要主动提供用于辅助测试的数据给测试平台。