ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38644—2020

信息安全技术　可信计算
可信连接测试方法

Information security technology—Trusted computing—Testing method of trusted connect

2020-04-28 发布　　2020-11-01 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。

本标准起草单位:西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、中关村无线网络安全产业联盟(WAPI 产业联盟)、北京工业大学、国家密码管理局商用密码检测中心、国家信息技术安全研究中心、北京计算机技术及应用研究所、中国通用技术研究院、天津市电子机电产品检测中心、国家无线电监测中心检测中心、中国电子科技集团公司第十五研究所、西安邮电大学、工业和信息化部宽带无线 IP 标准工作组。

本标准主要起草人:曹军、李琴、杜志强、芦亮、潘琪、赖英旭、黄振海、颜湘、王冠、李冬、吕春梅、铁满霞、刘科伟、刘景莉、王月辉、张国强、张变玲、井经涛、熊克琦、赵晓荣、罗鹏、吴冬宇、林德欣、彭潇、方华、于光明、朱正美、郑东、赵慧、吴冬宇、郑骊、黄奎刚。

引　言

GB/T 29828—2013 规范了基于三元对等架构的可信连接架构(Trusted Connect Architecture，TCA)，本标准针对基于 TCA 的可信网络连接协议提出一套测试要求及方法。

本文件的发布机构提请注意，声明符合本文件时，可能涉及第 6 章、第 7 章、第 8 章与 ZL201410255349.X、US15/309，861、JP2016-567036、EP15807391.6、KR10-2016-7034816 等相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件发布机构备案。相关信息可通过以下联系方式获得：

专利持有人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：冯玉晨

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

信息安全技术　可信计算
可信连接测试方法

1　范围

本标准依据 GB/T 29828—2013，规定了可信网络连接协议以及所涉及的密码算法的测试要求及方法，包括如下内容：

a)　可信网络连接协议涉及的协议交互机制符合性测试要求及方法；

b)　可信网络连接协议涉及的密码算法实现的正确性测试要求及方法。

本标准适用于符合 GB/T 29828—2013 的可信连接设备的测试，用于检测其密码算法及基于可信连接架构 TCA 的可信网络连接协议的实现是否符合要求。

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 15843.3　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 20518　信息安全技术　公钥基础设施　数字证书格式

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 29828—2013　信息安全技术　可信计算规范　可信连接架构

GB/T 32905　信息安全技术　SM3 密码杂凑算法

GB/T 32907　信息安全技术　SM4 分组密码算法

GB/T 32915　信息安全技术　二元序列随机性检测方法

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

GB/T 35276　信息安全技术　SM2 密码算法使用规范

GM/T 0042—2015　三元对等密码安全协议测试规范

GM/T 0062—2018　密码产品随机数检测要求

3　术语和定义

GB/T 29828—2013 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 29828—2013 中的一些术语和定义。

3.1

被测设备　tested equipment

实现了可信网络连接协议的测试对象。

3.2

测试平台　test platform

对可信网络连接协议进行测试，具有可信网络连接协议以及所涉及的密码算法的测试能力，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。