



# 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 发布  
国家标准化管理委员会

## 目 次

前言 .....	III
引言 .....	IV
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 总体要求 .....	3
5.1 协议交互机制符合性和互操作性要求 .....	3
5.2 密码算法实现的正确性要求 .....	4
6 测试方法概述 .....	4
6.1 测试设备 .....	4
6.2 测试拓扑 .....	4
6.3 测试依据 .....	6
6.4 测试说明 .....	6
7 协议交互机制符合性和互操作性测试方法 .....	6
7.1 端口访问控制测试 .....	6
7.2 TAEP 协议封装测试 .....	8
7.3 TAEPoL 协议封装测试 .....	8
7.4 TCP/UDP 端口测试 .....	8
7.5 可信连接架构测试 .....	9
8 密码算法实现的正确性测试方法 .....	10
8.1 对称密码算法测试 .....	10
8.2 数字签名算法测试 .....	10
8.3 密钥交换协议测试 .....	10
8.4 公钥加密算法测试 .....	11
8.5 数字证书格式测试 .....	11
8.6 密码杂凑算法测试 .....	11
8.7 随机数测试 .....	12
8.8 算法性能测试 .....	12
附录 A (规范性附录) 可信连接架构测试涉及的新增数据元素 .....	13
附录 B (规范性附录) 密码算法性能测试方法及新增数据元素 .....	17

## 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。