ICS 35.080
L 40

中华人民共和国国家标准

GB/T 29827—2013

信息安全技术 可信计算规范 可信平台主板功能接口

Information security technology—Trusted computing specification—Motherboard function and interface of trusted platform

2013-11-12 发布 2014-02-01 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:北京工业大学、中国长城计算机深圳股份有限公司、南京百敖软件股份有限公司、航天科工集团二院七〇六所、武汉大学、中国电子科技集团公司信息化工程总体研究中心、北京龙芯中科技术服务中心有限公司、江南计算技术研究所、瑞达信息安全产业股份有限公司、中安科技集团有限公司、中船重工集团 707 所、北京中科院软件研究中心、北京华大恒泰科技有限责任公司、北京超毅世纪网络技术股份有限公司、华为技术有限公司、桂林长海科技有限责任公司、中国电子技术标准化研究所。

本标准主要起草人:沈昌祥、韩永飞、张兴、王冠、林诗达、徐明迪、王正鹏、蒋志翔、赵丽娜、周艺华、石明、张斌、孔雷、张焕国、汪文杰、胡明昌、吴新军、陈林、李大东、王然、张向阳、艾方、童广胜、徐庶桓、李晨、贾兵、杜中平、杜晖、谢乾、赵波、张超、吴勇、石良军、马银生、郭景川、魏靖、宋洋、高瞻、曲新春、余发江、陈小春、蔡晔、袁爱东、庄琭、曾颖明、孙永泉、段丽娟、宋靖、朱贺新、郭灵儿、刘智君、滕志刚、靳涥、郭毅、肖祎、孙圣超、刘军,陈莹,邹娜。

信息安全技术　可信计算规范
可信平台主板功能接口

1　范围

本标准规定了可信平台主板的组成结构、信任链构建流程、功能接口。

本标准适用于基于可信平台控制模块的可信平台主板的设计、生产和使用。

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 29829—2013　信息安全技术　可信计算密码支撑平台功能与接口规范

UEFI V2.1　统一可扩展固件接口规范(Unified Extensible Firmware Interface Specification)

3　术语和定义

下列术语和定义适用于本文件。

3.1

可信根　root of trust

对应 TPCM 模块。

3.2

可信度量根　root of trust for measurement

一个能够可靠进行完整性度量的计算引擎，是信任传递链的起始点。

3.3

可信存储根　root of trust for storage

一个能够可靠进行安全存储的计算引擎。

3.4

可信报告根　root of trust for reporting

一个能够可靠报告可信存储根所保存信息的计算引擎。

3.5

通用设备　general device

在原有 PC 主板上兼容的硬件设备，包括中央处理器(CPU)、外部存储器、随机存储器、视频控制器等。

3.6

初始只读存储器　boot ROM

在计算机启动过程中提供最底层硬件设置的固件。

注：初始只读存储器在组成结构上分为 Boot Block 和 Main Block 两部分，按照类型分为传统 BIOS 和 UEFI BIOS。