ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36639—2018

信息安全技术　可信计算规范
服务器可信支撑平台

Information security technology—Trusted computing specification—Trusted support platform for server

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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:浪潮电子信息产业股份有限公司、曙光信息产业(北京)有限公司、中电科技(北京)有限公司、联想(北京)有限公司、中国船舶重工集团公司第七〇九研究所、华为技术有限公司、北京工业大学、阿里云计算有限公司、上海兆芯集成电路有限公司、南京百敖软件有限公司、武汉大学、大唐高鸿信安(浙江)信息科技有限公司、北京新云东方系统科技有限责任公司、北京可信华泰信息技术有限公司、华大半导体有限公司、中国电子技术标准化研究院、全球能源互联网研究院有限公司。

本标准主要起草人:刘刚、吴保锡、黄家明、张考华、肖思莹、杜克宏、徐明迪、申峰、付颖芳、李凯、赵江、张东、公维锋、孙永博、王冠、石源、于昇、宁振虎、沈楚楚、王惠莅、赵保华、刘冰、曹永超、陈小春、高瞻、张建标、胡俊、孙瑜、徐瑞雪、赵波、余发江、黄坚会、王志皓、安宁钰、薛刚汝、李业旺、赵祯龙、刘广庆、郝庄严、王涛、孙亮、肖鹏、周斌奇。

信息安全技术　可信计算规范
服务器可信支撑平台

1　范围

本标准规定了服务器可信支撑平台的功能和安全性要求，并描述了服务器可信支撑平台的组成结构。

本标准适用于可信计算体系下服务器可信支撑平台的设计、生产、集成、管理和测试。

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 29827—2013　信息安全技术　可信计算规范　可信平台主板功能接口

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

3　术语和定义、缩略语

3.1　术语和定义

GB/T 29827—2013、GB/T 29829—2013 界定的以及下列术语和定义适用于本文件。

3.1.1

服务器可信支撑平台　trusted support platform for server

构建在服务器硬件系统或者服务器硬件系统和操作系统的组合中，用于实现可信计算功能的支撑系统。

注：在虚拟化环境中，操作系统中还应包含虚拟机监控器。

3.1.2

物理可信根　physical root of trust

用于为服务器可信支撑平台提供完整性度量、安全存储、可信报告以及密码服务等功能的模块，通常由硬件或硬件和固件组成。

3.1.3

虚拟可信根　virtual root of trust

服务器可信支撑平台中为虚拟机提供的符合物理可信根功能要求、并具备迁移特性的组件。

3.1.4

虚拟可信组件　virtual trusted component

操作系统中为虚拟机提供可信功能支撑的所有程序和数据的集合，包括虚拟可信根、虚拟可信根管理器和可信迁移组件等。

3.1.5

可信基础组件　trusted basic component

为虚拟可信组件及服务器可信支撑平台外部实体提供访问和管理物理可信根能力的软件模块统称。

注：例如，TCM 服务模块等。