ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 40650—2021

信息安全技术　可信计算规范 可信平台控制模块

Information security technology—Trusted computing specification—Trusted platform control module

2021-10-11 发布　　2022-05-01 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 …… Ⅰ
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
5.1　可信平台控制模块定位 …… 2
5.2　可信平台控制模块与周边的交互 …… 3
5.3　其他 …… 3
6　可信平台控制模块功能组成 …… 4
6.1　功能组成框架 …… 4
6.2　硬件层 …… 4
6.3　基础软件层 …… 4
6.4　功能组件层 …… 4
6.5　互联接口 …… 5
7　可信平台控制模块的接口 …… 5
7.1　计算部件接口 …… 5
7.2　可信软件基接口 …… 5
7.3　管理接口 …… 5
7.4　可信密码模块接口 …… 6
8　安全防护 …… 6
8.1　身份鉴别 …… 6
8.2　资源访问控制 …… 6
8.3　审计 …… 6
8.4　存储空间安全要求 …… 7
8.5　数据保护 …… 7
8.6　物理防护 …… 7
9　运行维护 …… 7
9.1　自检 …… 7
9.2　状态维护 …… 7
10　证实方法 …… 8
10.1　可信计算节点的可信平台控制模块 …… 8
10.2　可信平台控制模块功能组成 …… 8
10.3　可信平台控制模块的接口 …… 8
10.4　安全防护 …… 9
10.5　运行维护 …… 10

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：华大半导体有限公司、北京工业大学、北京可信华泰信息技术有限公司、全球能源互联网研究院有限公司、上海算石科技有限公司、同济大学、阿里巴巴(中国)有限公司、浪潮(北京)电子信息产业有限公司、中国船舶重工集团公司第七〇九研究所、武汉大学、上海兆芯集成电路有限公司、广东玖章信息科技有限公司、上海工业控制安全创新科技有限公司、蓝玛卓信科技(上海)有限公司、中安科技集团有限公司、北京新云东方系统科技有限责任公司。

本文件主要起草人：黄坚会、张建标、王冠、胡俊、王昱波、公备、宁振虎、孙瑜、高昆仑、赵保华、蒋昌俊、喻剑、洪宇、王亮、杨欢、付颖芳、肖鹏、徐明迪、吴保锡、苏振宇、王鹃、薛刚汝、凌金弘、刘虹、程军、苏秋雨、刘建利、徐万山、王晓、杨勇敢。

信息安全技术　可信计算规范
可信平台控制模块

1　范围

本文件描述了可信平台控制模块在可信计算节点中的位置和作用，规定了可信平台控制模块的功能组成、功能接口、安全防护、运行维护要求和证实方法。

本文件适用于可信平台控制模块的设计、生产、运行维护和测评。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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　信息安全技术　可信计算密码支撑平台功能与接口规范

GB/T 37935　信息安全技术　可信计算规范　可信软件基

GM/T 0008　安全芯片密码检测准则

3　术语和定义

下列术语和定义适用于本文件。

3.1

可信密码模块　trusted cryptography module

具有可信计算所需要的密码运算等功能，并可提供受保护的存储空间的一种模块。

3.2

可信计算节点　trusted computing node

由可信防护部件和计算部件共同构成、具备计算和防护并行运行功能的计算节点。

3.3

可信平台控制模块　trusted platform control module

集成在可信计算节点中的防护部件组件，由硬件、软件及固件组成，与计算部件的硬件、软件及固件并行连接，是用于建立和保障信任源点的一种基础核心模块，为可信计算节点提供主动度量、主动控制、可信验证、加密保护、可信报告、密码调用等功能。

3.4

有效状态　enabled state

可信平台控制模块处于可以接收、执行所有指令的工作状态。

3.5

禁用状态　disable state

可信平台控制模块处于只能执行查询及启用指令的特殊工作状态。

3.6

主动自检　active self-checking

可信平台控制模块上电后主动对模块内部指定内容进行的检测操作。