ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 38638—2020

# 信息安全技术　可信计算
# 可信计算体系结构

**Information security technology—Trusted computing—Architecture of trusted computing**

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。

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。

本标准起草单位:全球能源互联网研究院有限公司、北京可信华泰信息技术有限公司、北京工业大学、北京新云东方系统科技有限责任公司、中国电子技术标准化研究院、中标软件有限公司、中电科技(北京)有限公司、北京旋极信息技术股份有限公司、国民技术股份有限公司、华大半导体有限公司、北京华胜天成信息技术发展有限公司、上海兆芯集成电路有限公司、浪潮(北京)电子信息产业有限公司、南京百敖软件有限公司、中国船舶重工集团公司第七〇九研究所、北京得安信息技术有限公司等。

本标准主要起草人:高昆仑、赵保华、安宁钰、杨建军、孙炜、张建标、于昇、宁振虎、董军平、胡俊、王惠莅、梁潇、王冠、韩兆刚、刘鑫、孙瑜、刘贤刚、陈小春、王志皓、孙亮、王薪达、施光源、吴保锡、赵江、赵勇、黄坚会、王树才、任春卉、徐宁、肖思莹、李强、徐明迪、李凯、沈昀、吕昇亮、谢立华、沈楚楚、孔凡玉。

# 信息安全技术　可信计算
# 可信计算体系结构

## 1　范围

本标准规定了可信计算的体系结构、可信部件及完整性度量模式以及可信计算节点类型。

本标准适用于可信计算体系的设计、开发和应用。

## 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 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 29828—2013　信息安全技术　可信计算规范　可信连接架构

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

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

GB/T 37935—2019　信息安全技术　可信计算规范　可信软件基

ISO/IEC 11889:2015　信息技术　可信平台模块库(Information technology—Trusted platform module library)

## 3　术语和定义

GB/T 29827—2013、GB/T 29828—2013、GB/T 29829—2013、GB/T 36639—2018 和 GB/T 37935—2019 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 29827—2013、GB/T 29829—2013、GB/T 37935—2019 中的某些术语和定义。

3.1

**可信计算节点　trusted computingnode**

由可信部件和计算部件共同构成、具备计算和防护并行特征的计算节点。

3.2

**可信密码模块　trusted cryptographymodule**

可信计算平台的硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。

[GB/T 29829—2013，定义 3.1.7]

3.3

**可信平台控制模块　trusted platform control module**

一种集成在可信计算中，用于建立和保障信任源点的硬件核心模块，为可信计算提供完整性度量、安全存储、可信报告及密码服务等功能。

[GB/T 29827—2013，定义 3.20]

3.4

**可信平台主板　trusted main board**

由可信平台控制模块和其他通用部件组成，可实现从开机到操作系统内核加载前的平台可信