ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 45230—2025

数据安全技术　机密计算通用框架

Data security technology—General framework for confidential computing

2025-01-24 发布　　2025-08-01 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。

本文件由全国网络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：华为技术有限公司、中国移动通信集团有限公司、中国电子技术标准化研究院、中国科学院软件研究所、蚂蚁科技集团股份有限公司、北京百度网迅科技有限公司、北京火山引擎科技有限公司、腾讯云计算(北京)有限责任公司、阿里云计算有限公司、北京冲量在线科技有限公司、中国移动通信集团设计院有限公司、中国工商银行股份有限公司、四川大学、中国民生银行股份有限公司、北京国家金融科技认证中心有限公司、北京数字认证股份有限公司、杭州安恒信息技术股份有限公司、南湖实验室、北京大学、华控清交信息科技(北京)有限公司、中国联合网络通信集团有限公司、超聚变数字技术有限公司、上海交通大学、神州网信技术有限公司、中国科学院信息工程研究所、长扬科技(北京)股份有限公司、郑州信大捷安信息技术股份有限公司、杭州锘崴信息科技有限公司、上海富数科技有限公司、中电云计算技术有限公司、英特尔(中国)股份有限公司北京分公司、昆仑太科(北京)技术股份有限公司、联想(北京)有限公司、超威半导体产品(中国)有限公司、深圳市洞见智慧科技有限公司、大唐高鸿信安(浙江)信息科技有限公司、浙江大华技术股份有限公司、海光信息技术股份有限公司、北京天融信网络安全技术有限公司、北京数牍科技有限公司、飞腾信息技术有限公司、浪潮电子信息产业股份有限公司、中电长城网际系统应用有限公司、奇安信科技集团股份有限公司、绿盟科技集团股份有限公司、天翼云科技有限公司、山东浪潮科学研究院有限公司、山东制创数字技术有限公司、国家工业信息安全发展研究中心、深圳大学、中国信息通信研究院、西安电子科技大学、武汉大学、北京海泰方圆科技股份有限公司、新华三技术有限公司、电子科技大学、山东大学、曙光网络科技有限公司、杭州职业技术学院、北京银联金卡科技有限公司、北京数安行科技有限公司、北京信安世纪科技股份有限公司、国网区块链科技(北京)有限公司、陕西省信息化工程研究院、国网新疆电力有限公司电力科学研究院、国网智能电网研究院、深圳微言科技有限责任公司、上海燧原科技有限公司。

本文件主要起草人：葛小宇、邱勤、王惠莅、冯登国、庞婷、苏丹、徐天妮、秦宇、张立武、胡科开、肖俊贤、张晓蒙、昌文婷、于欢、周吉文、季石磊、李克鹏、王新宇、李世奇、金意儿、陈浩栋、宋雨筱、刘尧、张高山、朱华、夏知渊、陈凌潇、侯明永、陈兴蜀、王启旭、杨苗苗、罗武、虞刚、牛博强、华佳烽、张尧、刘敬彬、李振、黄江、李向锋、张永强、王琼霄、王吾冰、张振永、张磊、严志超、陈钟、关志、杨祖艳、靳晨、傅瑜、王莹、徐雷、涂长茂、惠静、夏虞斌、杜冬冬、王强、田野、王蕊、荆丽桦、沈志淳、赵华、梁松涛、刘为华、李帜、孙琪、杨天雅、卞阳、裴超、张凡、王立刚、陈小春、孙亮、黄建东、李汝鑫、张大江、冯新宇、马博文、郑驰、刘海洁、张剑青、杨朋霖、应志伟、冯浩、晋钢、王龑、金银玉、孙一品、谭琳、麻付强、徐峥、闵京华、安锦程、刘文懋、董炳佑、张亮、孙晓宁、刘娟娟、李锐、罗清彩、余果、王冲华、刘伟丽、孔松、裴庆祺、赵博文、王鹃、严飞、陈晶、赵波、王学进、万晓兰、张小松、牛伟纳、王美琴、王薇、刘立、梅颖、王琳、郑峥、刘玉红、张宇、杨珂、王栋、赵晓荣、张勇、邹振婉、于鹏飞、石聪聪、梅敬青、王思善、马利、强锋。

引　言

机密计算是一种用于保护使用过程中数据安全的计算模式。该模式在受信任的硬件基础上，通过硬件隔离使得环境内的代码和数据在计算时无法被同一设备上运行的其他软件（包括特权软件）监视与篡改。具体而言，机密计算通过隔离机制，将普通计算环境与机密计算环境隔离开来，非授权的实体不能访问机密计算环境；通过证明机制对机密计算环境及运行在其中的应用程序进行验证，保证机密计算环境和应用程序的完整性和真实性；通过加密机制保证运行时的数据处于密文状态。机密计算技术可以单独用于保护使用状态中的数据，也可以结合其他密码学技术（如多方安全计算、同态加密等）共同保护运行时的数据和代码，尤其对于机器学习、联邦学习、区块链、云计算、大数据等应用场景，可以有效应对数据在使用过程中面临的安全保护难题。

本文件旨在提出一种通用的机密计算框架，通过定义机密计算框架的必要组件、具备的基础功能以及组件之间交互形成的机密计算服务，提高机密计算相关产品的易用性、安全性和兼容性，为机密计算的技术发展和产业应用提供指导。为了满足各个行业云化需求，本文件还提出了机密计算虚拟化部署模式。

数据安全技术　机密计算通用框架

1　范围

本文件确立了机密计算通用框架，描述了框架的核心组件和基础功能，并提供了机密计算服务及实现机制。

本文件适用于机密计算相关方设计、开发、使用和部署机密计算相关产品或解决方案时参考，也可为开展机密计算能力评估活动提供参考。

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 25069—2022　信息安全技术　术语

GB/T 32915—2016　信息安全技术　二元序列随机性检测方法

3　术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

组件　component

在系统中，实现其部分功能的可识别区分的部分。

[来源：GB/T 25069—2022，3.815]

3.2

安全信道　secure channel

为所交换消息提供机密性及真实性的通信信道。

[来源：GB/T 25069—2022，3.32，有修改]

3.3

机密计算　confidential computing

在可信的硬件基础上，通过隔离、加密、证明等机制，保护使用中数据安全的计算模式。

3.4

机密计算平台　confidential computing platform

执行机密计算任务的基础软硬件集合。

3.5

机密计算应用程序　confidential computing application program

运行在机密计算环境中，用于实现机密计算能力的程序。

3.6

机密计算环境　confidential computing environment

基于机密计算平台，为支撑机密计算应用程序运行所构建的计算环境。