



团 体 标 准

T/CIIPA 00011—2024

自主可控网络安全技术 机密计算 安全服务接口规范

Autonomous and controllable cybersecurity technology—
Interface specification of confidential computing security services

2025-06-09 发布

2025-06-11 实施

中关村华安关键信息基础设施安全保护联盟 发 布
中 国 标 准 出 版 社 出 版

目 次

前言	III
引言	IV
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 机密计算安全服务接口框架	2
6 机密计算安全服务数据结构	3
6.1 信息类型定义	3
6.2 结构体定义	6
6.3 通用错误码定义	12
7 机密计算安全服务接口	12
7.1 隔离计算类接口	12
7.2 远程证明类接口	13
7.3 安全信道类接口	14
7.4 密钥派生类接口	18
7.5 存储保护类接口	20
7.6 密码运算类接口	23
7.7 数据封装类接口	32
7.8 硬件加速类接口	34
附录 A (规范性) 通用错误码	36

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。

本文件由中关村华安关键信息基础设施安全保护联盟提出并归口。

本文件起草单位：麒麟软件有限公司、奇安信科技集团股份有限公司、飞腾信息技术有限公司、北京源堡科技有限公司、中电(海南)联合创新研究院有限公司、华北电力大学、北京江民新科技术有限公司、北京国家金融科技认证中心有限公司、中电和瑞科技有限公司、北京神州绿盟科技有限公司、成都久信信息技术股份有限公司、北京柏睿数据技术股份有限公司、浙江脑动极光医疗科技有限公司。

本文件主要起草人：于博、纪胜龙、张大朋、战茅、靳佑鼎、王震、王舒、姬一文、张帆、岳佳圆、杨诏钧、王非、吴彤、于晴晴、杨伟平、张坤、陈晓峰、常凯翔、郦文琪、廖菁菁、杨修、唐磊、黄江、刘涛、赵勇、王雪松、高翔、朱光剑、王雨翰、李阳冬、赵菁华、王晓怡。

引 言

自主可控网络安全技术,能够从根源上缓解信息技术产品存在“后门”、供应链不可控等安全风险,并通过在自主可控产品中植入安全模块、自主可控系统各安全功能协同等措施,提升网络安全防护的效率与能力。

安全模块的实现需要系统提供接口,而不同系统的安全功能协同、跨平台之间的互联互通、用户应用程序的迁移和维护都需要解决机密计算安全服务接口、参数、版本等的一致性和统一性问题,从而实现机密计算安全服务的标准化。安全服务接口是实现机密计算的入口,目的是屏蔽底层硬件架构和软件的开发接口差异,为上层应用程序提供统一的机密计算服务接口及安全服务。因此,为了更好地实现自主可控网络安全技术,制定本文件。

自主可控网络安全技术 机密计算 安全服务接口规范

1 范围

本文件依据机密计算通用框架,给出了机密计算安全服务的数据结构、安全服务接口描述。

本文件适用于指导机密计算应用开发厂商开展机密计算安全服务接口的设计、研制,也用于指导机密计算相关产品的接口测试。

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 45230—2025 数据安全技术 机密计算通用框架

GM/T 0002 SM4 分组密码算法

GM/T 0003(所有部分) SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

T/ZISIA 01—2024 自主创新型网络安全技术 框架

3 术语和定义

GB/T 25069—2022、GB/T 45230—2025、T/ZISIA 01—2024 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

安全服务 security service

根据安全策略,为用户提供某种安全功能及相关保障的服务。

[来源:GB/T 25069—2022,3.7,有修改]

3.3

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 45230—2025,3.2]

3.4

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。