



中华人民共和国国家标准

GB/T 29829—2022

代替 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

Information security technology—Functionality and interface
specification of cryptographic support platform for trusted computing

2022-04-15 发布

2022-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

中 华 人 民 共 和 国
国 家 标 准
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 29829—2022

*

中 国 标 准 出 版 社 出 版 发 行
北 京 市 朝 阳 区 和 平 里 西 街 甲 2 号 (100029)
北 京 市 西 城 区 三 里 河 北 街 16 号 (100045)

网 址 : www.spc.org.cn

服 务 热 线 : 400-168-0010

2022 年 4 月 第 一 版

*

书 号 : 155066 · 1-70212

版 权 专 有 侵 权 必 究

目 次

前言	XV
引言	XVI
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 可信计算密码支撑平台概述	4
5.1 可信计算概述	4
5.2 可信构件	4
5.3 可信计算基	4
5.4 可信边界	5
5.5 可信传递	5
5.6 可信授权	5
6 可信计算密码支撑平台功能	5
6.1 平台体系结构	5
6.2 平台接口功能	7
7 可信密码模块接口	11
7.1 通用要求	11
7.2 启动命令	11
7.3 检测命令	13
7.4 会话命令	15
7.5 对象命令	16
7.6 复制命令	24
7.7 非对称算法命令	28
7.8 对称算法命令	32
7.9 随机数发生器命令	33
7.10 杂凑/HMAC 命令	34
7.11 证明命令	40
7.12 临时 EC 密钥命令	44
7.13 签名及签名验证命令	46
7.14 度量命令	48
7.15 增强授权命令	50
7.16 分层命令	60