ICS 35.030
CCS L 80

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

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》，与 GB/T 29829—2013 相比，除结构调整和编辑性改动外，主要技术内容变化如下：

a) 更改了“术语、定义和缩略语”，且增加和更改了术语和定义的内容（见第 3 章，2013 年版的 3.1）；
b) 增加了第 4 章“缩略语”且增加和更改了部分内容（见第 4 章，2013 年版的 3.2）；
c) 更改了“平台体系架构”和“功能原理”的内容，并将其调整为 6.1 和 6.2，对部分内容进行了更改（见 6.1 和 6.2，2013 年版的 4.1 和 4.3）；
d) 删除了“密码算法要求”的内容（见 2013 年版的 4.2）；
e) 增加了“可信计算密码支撑平台概述”的内容（见第 5 章）；
f) 删除了“可信计算密码支撑平台功能服务接口”的内容（2013 年版的第 5 章）；
g) 增加了“可信密码模块接口”的内容（见第 7 章）；
h) 增加了关于 SM2 非对称加解密的指令的实现要求（见 7.7）；
i) 增加了“证实方法”的内容（见第 8 章）；
j) 更改了附录 A（规范性）“数据结构”（见附录 A）。

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：联想（北京）有限公司、国民技术股份有限公司、中国科学院软件研究所、北京信息科技大学、中国电子技术标准化研究院、武汉大学、北京大学、北京奇虎科技有限公司、大唐高鸿信安（浙江）信息科技有限公司、中电科技（北京）股份有限公司、神州网信技术有限公司、浪潮电子信息产业股份有限公司、兴唐通信科技有限公司、阿里云计算有限公司、深圳数字电视国家工程实验室股份有限公司、国家计算机网络与信息安全管理中心、公安部第三研究所、国民认证科技（北京）有限公司、北京蚂蚁云金融信息服务有限公司、华为技术有限公司、北京卓识网安技术股份有限公司、同方股份有限公司、山谷网安科技股份有限公司、联想（北京）信息技术有限公司、全球能源互联网研究院有限公司、深圳市腾讯计算机系统有限公司、新华三技术有限公司。

本文件主要起草人：韦卫、李汝鑫、秦宇、刘鑫、宁晓魁、付月朋、柴海新、吴秋新、张屹、王惠莅、张严、孙彦、王鹃、严飞、沈晴霓、张晓磊、郑驰、张佳建、陈小春、孙亮、王强、杨尚欣、吴保锡、白欣璐、王悦、付颖芳、肖鹏、李新国、王晖、陶源、李俊、初晓博、张小虎、张梦良、许东阳、刘韧、刘锋、姚金龙、吴会军、杜克宏、卢卫疆、赵保华、刘大遒、黄超、蒋增增、万晓兰、冯伟、李为、张立强、余发江、赵波、李业旺、秦文杰、罗武。

本文件及其所代替文件的历次版本发布情况为：

——2013 年首次发布为 GB/T 29829—2013；
——本次为第一次修订。

引　言

为满足可信计算产业不断发展的新需求。本文件以商用密码算法应用为核心，以可信计算技术应用需求为基础，描述了可信计算密码支撑平台的功能；参考了我国商用密码算法、可信计算技术在ISO国际标准中采纳和应用的成果，定义了可信计算密码支撑平台接口形式。本文件符合不同应用场景下可信计算密码支撑平台设计需求，兼容各种硬件平台、宿主机软件系统、应用系统，确保产业界产品的统一性和兼容性，用于指导我国可信计算相关产品开发和应用。

信息安全技术　可信计算
密码支撑平台功能与接口规范

1　范围

本文件给出可信计算密码支撑平台的体系框架和功能原理，规定了可信密码模块的接口规范，描述了对应的证实方法。

本文件适用于可信计算密码支撑平台相关产品的研制、生产、测评与应用开发。

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 20518　信息安全技术　公钥基础设施　数字证书格式

GB/T 25069　信息安全技术　术语

GB/T 32905　信息安全技术　SM3 密码杂凑算法

GB/T 32907　信息安全技术　SM4 分组密码算法

GB/T 32915　信息安全技术　二元序列随机性检测方法

GB/T 32918.2　信息安全技术　SM2 椭圆曲线公钥密码算法　第 2 部分：数字签名算法

GB/T 32918.3　信息安全技术　SM2 椭圆曲线公钥密码算法　第 3 部分：密钥交换协议

GB/T 32918.4　信息安全技术　SM2 椭圆曲线公钥密码算法　第 4 部分：公钥加密算法

GB/T 35276　信息安全技术　SM2 密码算法使用规范

3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

存储主密钥　storage master key

用于保护操作系统密钥和用户密钥的主密钥。

3.2

可信计算平台　trusted computing platform

构建在计算系统中，用于实现可信计算功能的支撑系统。

3.3

可信计算密码支撑平台　cryptographic support platform for trusted computing

可信计算平台的重要组成部分，包括密码算法、密钥管理、证书管理、密码协议、密码服务等内容，为可信计算平台自身的完整性、身份真实性和数据保密性提供密码支持。