ICS 35.040
CCS L 80

中华人民共和国密码行业标准

GM/T 0012—2020
代替 GM/T 0012—2012

可信计算　可信密码模块接口规范

Trusted computing—Trusted computing interface specification of trusted cryptography module

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　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。

本文件代替GM/T 0012—2012《可信计算　可信密码模块接口规范》。

本文件与GM/T 0012—2012相比，主要的技术变化如下：

a) 修改了前言和引言的内容；

b) 修改了原有标准第3章“术语、定义和缩略语”，按照GB/T 1.1—2020的要求修改为第3章，并修改和增加了术语和定义的内容；

c) 删除原有标准的第4章“概述”内容；

d) 增加了第4章“缩略语”，且增加和修改了部分内容；

e) 删除原有标准的第5章、第6章、第7章、第8章内容；

f) 增加了第5章“可信密码模块功能概述”内容；

g) 增加了第6章“可信密码模块功能接口”内容，该内容参照了ISO/IEC 11889-3：2015；

h) 增加了6.7，关于SM2非对称加解密的指令的实现要求；

i) 修改了规范性附录A“数据结构”，该内容参照了ISO/IEC 11889-2：2015。

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：国民技术股份有限公司、联想控股有限公司、山谷网安科技股份有限公司、同方股份有限公司、中国科学院软件所、长春吉大正元信息技术股份有限公司、中国长城计算机深圳股份有限公司、成都卫士通信息产业股份有限公司、无锡江南信息安全工程技术中心、中国人民解放军国防科学技术大学、北京信息科技大学、北京卓识网安技术股份有限公司、北京天融信网络安全技术有限公司。

本文件主要起草人：范琴、刘鑫、付月朋、秦宇、谷晶中、吴秋新、杨贤伟、邹浩、余发江、宁晓魁、王梓、郑必可、林洋、李伟平、雷晓锋、徐震、姚金龙、严飞、李丰、许勇、贾兵、王蕾、顾健、何长龙、刘韧。

本文件所代替文件的历次版本发布情况为：

——GM/T 0012—2012。

引　言

本文件描述了可信计算　可信密码模块接口规范。通过本文件的接口，向应用层提供统一的 TCM 接口，适用于可信计算应用的开发、使用及检测并提供标准依据和指导，有利于提高可信计算产业发展水平。

本文件在 GM/T 0012—2012《可信计算　可信密码模块接口规范》的基础上，参考了 TPM2.0 标准(ISO/IEC 11889:2015)相关内容进行了修订。

本文件支持中国密码 SM2、SM3、SM4 算法，在功能上与 TPM2.0 标准中使用中国算法模式的内容兼容。在密码算法使用设计上，未来密码算法如密钥长度升级，杂凑算法摘要长度升级等，相关接口的设计上兼容后续算法的更新或新增密码算法。预留国际算法模式，为中国可信计算走向国际奠定基础。

《可信计算　可信密码模块接口规范》为芯片接口规范，可信计算密码支撑平台功能与接口规范是为应用层提供服务的接口规范，是对可信密码模块接口规范的接口进行的封装，厂商或者开发者可以在可信计算密码支撑平台功能与接口规范的产品中开发兼容可信密码模块接口规范中定义的接口。

可信计算密码支撑平台功能原理相关内容，请参考 GB/T 29829 相关章节。

可信计算　可信密码模块接口规范

1　范围

本文件描述了可信密码模块的功能，详细定义了可信密码模块的命令接口。

本文件适用于可信密码模块相关产品的研制、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　数字证书格式规范

GB/T 29829　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 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(所有部分)　信息安全技术　SM2 椭圆曲线公钥密码算法

3　术语和定义

下列术语和定义适用于本文件。

3.1

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。

[GB/T 29829—2013，3.1.1]

3.2

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、身份可信性和数据安全性提供密码支持。其产品形态主要表现为可信密码模块和可信密码服务模块。

[GB/T 29829—2013，3.1.2]

3.3

完整性度量　integrity measurement

使用密码杂凑算法对被度量对象计算其杂凑值的过程。

[GB/T 29829—2013，3.1.3]

3.4

可信度量根　root of trust for measurement

一个可信的完整性度量单元，是可信计算平台内进行可信度量的基础。

[GB/T 29829—2013，3.1.4]