ICS 35.040
CCS L 80

中华人民共和国密码行业标准

GM/T 0082—2020

可信密码模块保护轮廓

Trusted cryptography module protection profile

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。

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：中国科学院软件研究所、同方股份有限公司、国民技术股份有限公司。

本文件主要起草人：赵世军、秦宇、初晓博、冯伟、刘孜文、胡浩、常德显、张倩颖、邵健雄、郑必可、刘鑫、汪丹。

可信密码模块保护轮廓

1 范围

本文件以GB/T 29829和GB/T 18336为基础，构建可信密码模块的保护轮廓，对符合评估保障级第3级的TOE的定义、安全环境、安全目的、安全要求等进行了详细说明，并给出相应的基本原理说明。

本文件适用于可信密码模块相关产品的生产、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 18336(所有部分) 信息技术 安全技术 信息技术安全评估准则

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 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GM/T 0012 可信计算可信密码模块接口规范

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。

3.2

可信密码模块 trusted cryptography module

可信计算平台的硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。

3.3

密码模块密钥 TCM endorsement key

可信密码模块的背书密钥。

3.4

存储主密钥 storage master key

用于保护平台身份密钥和用户密钥的存储主密钥。

3.5

可迁移密钥 migratable key

可被迁移到其他特定可信密码模块的密钥。