ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41388—2022

信息安全技术　可信执行环境　基本安全规范

Information security technology—Trusted execution environment—Basic security specification

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

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：中国银联股份有限公司、中国电子技术标准化研究院、中国科学院大学、北京银联金卡科技有限公司、中国信息通信研究院、公安部第三研究所、华为技术有限公司、北京小米移动软件有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、中国金融认证中心、深圳市腾讯计算机系统有限公司、蚂蚁科技集团股份有限公司、北京百度网讯科技有限公司、北京谦川科技有限公司、联想(北京)有限公司、高通无线通信技术(中国)有限公司、华控清交信息科技(北京)有限公司、上海聚虹光电科技有限公司。

本文件主要起草人：柴洪峰、孙权、孙彦、王跃武、渠韶光、胡莹、曾望年、国炜、胥怡心、张炼、张友奖、王磊、李根、贾科、龚喜杰、郭铁涛、林冠辰、周吉文、郝春亮、任泽君、雷灵光、周荃、马哲、王鑫、魏凡星、孟庆洋、张强、王思善、刘渤、杜志敏、王云河、李嘉扬。

信息安全技术　可信执行环境
基本安全规范

1　范围

本文件确立了可信执行环境系统整体技术架构，描述了可信执行环境基础要求、可信虚拟化系统、可信操作系统、可信应用与服务管理、跨平台应用中间件等主要内容及其测试评价方法。

本文件适用于指导可信执行环境系统的设计、生产及测试。

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 20271—2006　信息安全技术　信息系统通用安全技术要求

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

虚拟化　virtualization

将一种或多种形式资源虚拟化成另外一种或多种形式资源的方法。

3.2

可信虚拟化　trusted virtualization

基于可信执行环境的虚拟化方法。

3.3

可信执行环境　trusted execution environment

基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

注：硬件级隔离是指基于硬件安全扩展机制，通过对计算资源的固定划分或动态共享，保证隔离资源不被富执行环境访问的一种安全机制。

3.4

富执行环境　rich execution environment

为应用程序提供基础功能和计算资源的一种软件运行环境。

注：富执行环境是相对可信执行环境独立存在的运行环境。

3.5

可信执行环境系统　trusted execution environment system

由可信执行环境及富执行环境下用以支撑客户端应用的运行环境共同构成的系统。