ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 42572—2023

信息安全技术　可信执行环境服务规范

Information security technology—Trusted execution environment service specification

2023-05-23 发布　　2023-12-01 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、中国科学院大学、复旦大学、华为技术有限公司、北京银联金卡科技有限公司、深圳华大北斗科技股份有限公司、中金金融认证中心有限公司、北京谦川科技有限公司、上海摩联信息技术有限公司、北京小米移动软件有限公司、OPPO广东移动通信有限公司、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、郑州信大捷安信息技术股份有限公司、恒宝股份有限公司、云从科技集团股份有限公司、北京创原天地科技有限公司、大唐高鸿信安(浙江)信息科技有限公司、上海聚虹光电科技有限公司、同盾科技有限公司。

本文件主要起草人：柴洪峰、孙权、陈成钱、王跃武、吴杰、李晓伟、孙中亮、胡莹、邹奋、张友奖、周荃、雷灵光、叶家炜、王鑫、池海章、王思善、鲁欣、孟庆洋、许刚、周博、张忠群、王磊、李根、蒋增增、林冠辰、刘为华、赵李明、李军、肖青海、郑驰、李嘉扬、谭成。

信息安全技术　可信执行环境服务规范

1　范围

本文件确立了可信执行环境服务的技术框架体系，并规定了相关安全技术要求及测试评价的方法。

本文件适用于可信执行环境服务的设计、开发、测试等，设备制造商、系统软件提供商、检测机构和科研机构等可信执行环境服务参与方可参照使用。

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 17901.1—2020　信息技术　安全技术　密钥管理　第1部分：框架

GB/T 25069—2022　信息安全技术　术语

GB/T 41388—2022　信息安全技术　可信执行环境　基本安全规范

3　术语和定义

GB/T 25069—2022 和 GB/T 41388—2022 界定的以及下列术语和定义适用于本文件。

3.1

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。

[来源：GB/T 41388—2022，3.3]

3.2

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。

[来源：GB/T 41388—2022，3.4]

3.3

可信执行环境服务　trusted execution environment service

运行在可信执行环境下，为 REE 提供基础性、通用性、公共性功能的软件程序。

注：本文件中简称“TEE 服务”。

3.4

TEE 人机交互　trusted execution environment human-machine interaction

运行在可信执行环境下，提供信息交互界面的软件程序。