



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	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 总体描述	2
5.1 概述	2
5.2 整体架构	3
6 基础要求	4
6.1 硬件要求	4
6.1.1 硬件基本要求	4
6.1.2 可信时钟源	4
6.1.3 可信随机源	4
6.1.4 可信调试单元	4
6.1.5 可信外设	4
6.2 可信根	4
6.3 安全启动要求	5
7 可信虚拟化系统	5
8 可信操作系统	5
9 可信应用与服务管理	6
9.1 基本描述	6
9.2 技术架构	6
9.2.1 架构描述	6
9.2.2 互信过程	6
9.2.3 可信应用及服务部署	6
10 可信服务	6
10.1 可信时间服务	6
10.2 可信加解密服务	7
10.3 可信存储服务	7
10.4 可信身份鉴别服务	7
10.5 可信设备鉴证服务	7
10.6 可信人机交互服务	7
10.7 SE 管理服务	7
11 跨平台应用中间件	8
12 可信应用	9