ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 40653—2021

信息安全技术
安全处理器技术要求

Information security technology—
Technical requirements for security processor

2021-10-11 发布　　2022-05-01 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：北京多思科技工业园股份有限公司、中国信息安全测评中心、国家密码管理局商用密码检测中心、华北电力大学、公安部第三研究所、网神信息技术(北京)股份有限公司、中国电子信息产业发展研究院、杭州华澜微电子股份有限公司、杭州安恒信息技术股份有限公司、中国人民解放军战略支援部队信息工程大学、珠海复旦创新研究院、北京多思安全芯片科技有限公司。

本文件主要起草人：刘大力、李大为、罗鹏、张翀斌、王州府、高金萍、石竑松、杨永生、曹春春、夏宏、王闯、韦安垒、杨元原、柳会鹏、李虹阳、魏晓伟、王辉、宋克、王俊宇、高艳芳、周斌。

信息安全技术
安全处理器技术要求

1 范围

本文件规定了安全处理器的安全功能要求和安全保障要求。

本文件适用于安全处理器设计、生产和应用。

2 规范性引用文件

下列文件中的内容通过文中规范性引用而构成本文件中必不可少的条款。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 25069 信息安全技术 术语

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

安全处理器 security processor

由固件和硬件实体组成，具备物理防护、逻辑防护、应用防护能力，能够达到一定安全强度和安全等级的处理器。

注：安全处理器实现技术包括密码技术、物理防护技术、数据编码技术、可重组逻辑技术等。

3.2

物理防护 physical protection

采用攻击防护的设计、攻击检测的方法、利用检测与处理功能，监测处理器工作环境，并能支持异常行为应答审计处理，阻止物理威胁的安全能力。

注：攻击防护包括掩膜、封装、物理接口的安全保护设计等；攻击检测包括光，电磁，逻辑断路、短路、旁路检测等；工作环境包括温度、频率、电压测试等；应答审计处理包括通知、标记、应答处理、审计处理等措施。

3.3

应用防护 application protection

链接物理防护的功能，具有对程序和数据的保护能力、运行态检测和监控能力、资源调度和配置控制能力、安全通信能力，并能支持异常行为应答审计处理，阻止应用威胁的安全能力。

注：保护能力包括利用同态计算、密码技术应用对程序和数据处理能力，资源调度和配置控制包括安全存储、控制管理、安全配置等措施，安全通信包括加密传输、可信根传递的运用、身份认证等措施。

3.4

逻辑防护 logic protection

依据物理防护和应用防护的安全功能，通过资源配置、操作配置、运行态控制等方式，调整安全策略，使逻辑结构和控制具备对未知攻击更强的安全强度和弹性，阻止逻辑威胁的安全能力。

3.5

运行态 running state

安全处理器运行状态。