ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20276—2016
代替 GB/T 20276—2006

信息安全技术 具有中央处理器的 IC 卡嵌入式软件安全技术要求

**Information security technology—
Security requirements for embedded software in IC card with CPU**

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20276—2006《信息安全技术　智能卡嵌入式软件安全技术要求(EAL4 增强级)》。本标准与 GB/T 20276—2006 相比,主要变化如下:

——将标准名称变更为《信息安全技术　具有中央处理器的 IC 卡嵌入式软件安全技术要求》;

——第 3 章对术语进行了更新描述;

——第 4 章重新描述了 IC 卡嵌入式软件的结构和应用环境,并进行了更清晰的 TOE 范围定义;

——第 5 章对安全问题定义进行了整合和精简,共定义了 6 个威胁,3 项组织安全策略和 5 个假设;

——第 6 章根据新的安全问题定义更新了对 TOE 安全目的的描述;

——第 7 章对安全功能要求进行了调整,以细化新的安全目的描述,明确指出了 EAL4＋和 EAL5＋分别应满足的安全功能要求;并对安全保障要求进行了调整,增加了 EAL5＋要求的保障组件;

——第 8 章对新的安全问题定义与安全目的、安全目的与安全要求之间的对应关系基本原理重新进行了梳理,还分析了组件之间的依赖关系。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国信息安全测评中心、北京多思科技工业园股份有限公司、天地融科技股份有限公司、北京邮电大学、吉林信息安全测评中心。

本标准主要起草人:张翀斌、石竑松、高金萍、杨永生、王宇航、饶华一、王亚楠、陈佳哲、李东声、李明、曹春春、沈敏锋、崔宝江、赵晶玲、唐喜庆、刘占丰、刘丽、邹兆亮。

本标准所代替标准的历次版本发布情况为:

——GB/T 20276—2006。

引　言

IC卡应用范围的扩大和应用环境复杂性的增加，要求IC卡嵌入式软件具有更强的安全保护能力。

本标准的EAL4＋是在EAL4的基础上将AVA_VAN.3增强为AVA_VAN.4；EAL5＋是在EAL5的基础上将AVA_VAN.4增强为AVA_VAN.5，并将ALC_DVS.1增强为ALC_DVS.2。

信息安全技术
具有中央处理器的IC卡嵌入式软件
安全技术要求

1 范围

本标准规定了对EAL4增强级和EAL5增强级的具有中央处理器的IC卡嵌入式软件进行安全保护所需要的安全技术要求，涵盖了安全问题定义、安全目的、安全要求、基本原理等内容。

本标准适用于具有中央处理器的IC卡嵌入式软件产品的测试、评估和采购，也可用于指导该类产品的研制和开发。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2010 信息安全技术 术语

3 术语和定义、缩略语

3.1 术语和定义

GB/T 25069—2010和GB/T 18336.1中界定的以及下列术语和定义适用于本文件。

3.1.1

个人化数据 Personalization data

在IC卡嵌入式软件的个人化过程中写入的数据，用于配置与特定应用或用户相关的参数。

3.2 缩略语

下列缩略语适用于本文件。

CM：配置管理(Configuration Management)

EAL：评估保障级(Evaluation Assurance Level)

EEPROM：电可擦除可编程只读存储器(Electrically-Erasable Programmable Read-only Memory)

IC：集成电路(Integrated Circuit)

I/O：输入/输出(Input/Output)

RAM：随机存取存储器(Random-Access Memory)

ROM：只读存储器(Read-Only Memory)

ST：安全目标(Security Target)

TOE：评估对象(Target of Evaluation)

TSF：TOE安全功能(TOE Security Functionality)