ICS 35.040
L 80

中华人民共和国国家标准

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)

**Information security technology—
Security requirements for smartcard embedded software(EAL4+)**

2006-05-31 发布　　2006-12-01 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

本标准由全国信息安全标准化技术委员会提出并归口。

本标准主要起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：李守鹏、徐长醒、付敏、简余良、凌晨、潘莹、杨永生、祁斌、黄小鹏、杨延辉、李昊、赵子渊、李永禄。

引　言

智能卡应用范围的扩大和应用环境复杂性的增加，要求智能卡嵌入式软件具有更强的保护数据能力。

本标准在 GB/T 18336—2001 中规定的 EAL4 级安全要求组件的基础上，增加了模块化组件(ADV_INT)，并且将脆弱性分析要求由可以抵御低等攻击的组件(AVA_VLA.2)提升到可以抵御中级攻击潜力攻击的组件(AVA_VLA.3)。

本标准仅给出了智能卡嵌入式软件应满足的安全技术要求，对智能卡嵌入式软件的具体技术实现方式、方法等不做描述。

信息安全技术　智能卡嵌入式软件安全技术要求(EAL4 增强级)

1　范围

本标准规定了对 EAL4 增强级的智能卡嵌入式软件进行安全保护所需要的安全技术要求。

本标准适用于智能卡嵌入式软件的研制、开发、测试、评估和产品的采购。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡不注日期的引用文件,其最新版本适用于本标准。

GB/T 18336.1—2001　信息技术　安全技术　信息技术安全性评估准则　第 1 部分:简介和一般模型 (idt ISO/IEC 15408-1:1999)

GB/T 18336.2—2001　信息技术　安全技术　信息技术安全性评估准则　第 2 部分:安全功能要求　(idt ISO/IEC 15408-2:1999)

GB/T 18336.3—2001　信息技术　安全技术　信息技术安全性评估准则　第 3 部分:安全保证要求　(idt ISO/IEC 15408-3:1999)

3　术语和定义

GB/T 18336—2001 确立的以及下列术语和定义适用于本标准。

3.1

应用软件　application software

智能卡嵌入式软件的一部分,架构于基础软件之上,实现智能卡的应用功能。

3.2

基础软件　basic software

智能卡嵌入式软件的核心部分,实现智能卡的核心功能,如:操作系统、通用例程和解释器等。

3.3

个人化数据　personalization data

在个人化阶段写入的个性化数据。

3.4

预个人化数据　pre-personalization data

在预个人化阶段写入的非个性化数据。

4　智能卡嵌入式软件描述

4.1　概述

智能卡嵌入式软件指掩膜在智能卡存储器中并可运行的软件,一般由应用软件和基础软件组成。其主要功能是控制智能卡和外界的信息交换,管理智能卡的存储器并完成各种命令的处理。

4.2　特征

4.2.1　智能卡嵌入式软件的生命周期的特征

智能卡嵌入式软件的生命周期包含在智能卡产品的生命周期之中。智能卡产品的生命周期可分为