ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 21079.1—2007

银行业务　安全加密设备(零售)
第1部分:概念、要求和评估方法

Banking—Secure cryptographic devices(retail)—
Part 1:Concepts,requirements and evaluation methods

(ISO 13491-1:1998,MOD)

2007-09-05 发布　　2007-12-01 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

GB/T 21079《银行业务　安全加密设备(零售)》分为两个部分：

——第1部分：概念、要求和评估方法；

——第2部分：金融交易中设备安全符合性检测清单。

本部分是GB/T 21079的第1部分。

本部分修改采用国际标准ISO 13491-1：1998《银行业务　安全加密设备(零售)第1部分：概念、要求和评估方法》(英文版)。

考虑到我国国情，在采用ISO 13491-1：1998时做了下列修改：

因为ISO 13491-1：1998原文7.5的第二段讲述全球国家和行业安全评估标准与ISO 13491-1的符合情况，在采用为国标时予以删除。

为便于使用，对于ISO 13491-1：1998，本部分还做了下列编辑性修改：

a)　规范性引用文件中所引用的国际标准，有相应国家标准的，改为引用国家标准；

b)　删除国际标准的前言。

本部分的附录A为资料性附录。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会归口。

本部分负责起草单位：中国金融电子化公司。

本部分参加起草单位：中国人民银行、中国工商银行、中国农业银行、招商银行、中国银联股份有限公司、华北计算技术研究所、启明星辰有限公司。

本部分主要起草人：谭国安、杨竑、陆书春、李曙光、王林立、周亦鹏、林中、张启瑞、史永恒、赵宏鑫、李红新、徐伟、张艳、董永乐、熊少军、黄发国、李建云。

本部分为首次制定。

引　言

本部分规定了银行零售业务中用于保护报文、密钥及其他敏感信息的安全加密设备(SCD)的物理特性、逻辑特性和管理要求。

电子银行零售业务的安全性在很大程度上依赖于加密设备的安全性。加密设备的安全性要求基于这样一些假设:计算机文件可能被非法访问和处理,通讯线路可能被“窃听”,合法的数据和控制指令可能被非法操作所取代。尽管某些加密设备(如主机安全模块)放置在安全性相对较高的处理中心,但大部分应用于零售银行业务的加密设备(如密码键盘等)都处在并不安全的环境中。因此,在这些加密设备上处理 PIN(个人标识码)、MAC(报文鉴别码)、密钥和其他机密数据时,就存在设备受到入侵、数据泄漏或被篡改的风险。通过合理使用、正确管理具有特定物理和逻辑安全特性的安全加密设备,可确保降低金融风险。

银行业务　安全加密设备(零售)
第1部分:概念、要求和评估方法

1　范围

GB/T 21079的本部分规定了安全加密设备(以下简称SCD)的要求,这些设备要求包含了ISO 9564、ISO 9807:1991和ISO 11568中定义的密码过程。

本部分有以下两个主要目的:

a)　规定SCD的操作特性和SCD整个生命周期管理方面的要求;

b)　对这些要求的一致性检查方法进行标准化。

加密设备应具有合适的特性以保证其具有适当的可操作性并能为内部数据提供足够保护。为确保设备的合法性,即设备不能被未授权的方法更改(如安装"侦听装置"等),并且设备中的敏感数据不会泄漏或篡改,适当的设备管理是非常必要的。

绝对的安全性实际上是无法达到的。加密安全性依赖于安全加密设备生命周期的每个阶段,以及适当的设备管理程序和安全加密特性两者的有效结合。管理程序可以通过防范措施来降低设备安全防护被攻破的可能性。这些防护措施是为了在设备本身特性不能阻止或检测安全攻击的情况下,提高发现非法访问敏感数据或机密数据的可能性。

附录A提供了本部分描述的安全等级在应用于安全加密设备时的说明。

本部分没有涉及SCD拒绝服务引发的问题。

在零售银行业务中使用具体类型的SCD,对其特性和管理的要求在ISO 11568-2中说明。

2　规范性引用文件

下列文件中的条款通过GB/T 21079的本部分的引用而成为本部分的条款。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部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 9387.2—1995 信息处理系统　开放系统互连基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)

ISO 8908:1993　银行业务及相关金融服务　词汇和数据元

ISO 9564-1　银行业务　个人识别码的管理与安全　第1部分:PIN保护策略和技术

ISO 9807:1991　银行业及相关金融服务　报文鉴别需求(零售)

ISO 10202(所有部分)　使用集成电路卡的金融交易系统安全结构

ISO 11568(所有部分)　银行业务　密钥管理(零售)

ISO 13491-2:2000　银行业务　安全加密设备(零售)　第2部分:金融交易中设备安全符合性检测清单

3　术语和定义

ISO 8908:1993中确立的以及下列术语和定义适用于本部分。

3.1

授权机构　accreditation authority

负责对评估机构授权并且监督其工作以确保评估结果可再现的权威机构。