ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 21079.1—2011/ISO 13491-1:2007
代替 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 13491-1:2007,IDT)

2011-12-30 发布　　2012-02-01 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)》由以下两部分构成：

——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。

本部分为GB/T 21079的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替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》，本部分与GB/T 21079.1—2007相比主要变化如下：

——在SCD的物理安全要求中增加：物理安全设备及采用“每笔交易一个密钥”管理方式设备的描述(本版的6.2.5和6.2.6)；

——在SCD的逻辑安全要求中增加：双重控制、每台设备采用惟一密钥要求(本版的6.3.1和6.3.2)；

——为保证和本标准第2部分：金融交易中设备安全符合性检测清单(已做为GB/T 20547.2—2006发布)的统一，将本部分评估方法中的“半正式评估”统一为“准正式评估”；

——对标准的结构进行了重新调整，去除了原标准中部分章节的悬置段(2007版的4、4.1、4.2、5.3、6、6.2、6.3、7、7.1、7.3、7.4；本版的5.1、5.2.1、5.3.1、7.1、7.3.1、7.4.1、8.1.1、8.3.1、8.4.1)。

本部分使用翻译法等同采用ISO 13491-1:2007《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》。

为便于使用，本部分做了下述编辑性修改：

——删除ISO前言。

与本部分规范性引用的国际标准有一致性对应关系的我国标准如下：

GB/T 20547.2　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(GB/T 20547.2—2006，ISO 13491-2:2005，MOD)

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(SAC/TC 180)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、中国银行、中国建设银行、交通银行、中信银行、北京银联金卡科技有限公司。

本部分主要起草人：王平娃、陆书春、李曙光、杨倩、赵志兰、田洁、仲志晖、刘志刚、邵冠军、李延、杨宝辉、贾静、李孟琰、贾树辉、刘运、景芸。

本部分于2007年首次发布，本次为第一次修订。

引　言

本部分规定了金融零售业务中用于保护报文、密钥及其他敏感数据的安全密码设备(SCD)的物理特性、逻辑特性和管理要求。

零售电子支付系统的安全性在很大程度上依赖于这些密码设备的安全性。安全性的提出是基于这样一些假设：

——计算机文件可能被非法访问和处理；

——通讯线路可能被“窃听”；

——输入系统的合法的数据和控制指令可能被未授权替换。

在这些密码设备上处理 PIN(个人标识码)、MAC(报文鉴别码)、密钥和其他机密数据时，存在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密码设备可降低金融风险。

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的本部分以ISO 9564、ISO 16609和ISO 11568中定义的密码方法为基础,规定了对安全密码设备(以下简称SCD)的要求。

本部分有以下两个主要目的:

a)　规定SCD的操作性要求和其在整个生命周期中的管理要求;

b)　对上述要求的符合性检查方法进行标准化。

SCD应具有合适的设备特性并进行适当的设备管理,前者保证了SCD的操作性能以及为其内部数据提供足够的保护;后者保证了SCD的合法性,即SCD不会以非授权的方式更改(如安装"侦听装置"等)且其中的任何敏感数据(如加密密钥)不会遭到泄漏或篡改。

绝对的安全性实际上是无法达到的。SCD的安全性依赖于在生命周期每个阶段中适当的管理和安全密码特性两者的有机结合。管理程序可以通过防范措施来降低SCD安全受到破坏的几率,目的是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以资料性信息的形式,描述了本部分提及的适用于SCD安全级别的概念。

本部分没有涉及由SCD拒绝服务引发的问题,也没有涉及在金融零售业务中,不同SCD在设备特性和管理方面的具体要求,该部分内容见ISO 13491-2。

本部分适用于金融零售业务中安全密码设备的安全管理。

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。

ISO 11568-1　银行业务　密钥管理(零售)　第1部分:一般原则(Banking—Key management (retail)—Part 1: Principles)

ISO 11568-2:2005　银行业务　密钥管理(零售)　第2部分:对称密码系统及其密钥管理和生命周期(Banking—Key management(retail)—Part 2:Symmetric ciphers,their key management and life cycle)

ISO 11568-4　银行业务　密钥管理(零售)　第4部分:非对称密码系统及其密钥管理和生命周期(Banking—Key management(retail)—Part 4:Asymmetric cryptosystems—Key management and life cycle)

ISO 13491-2　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(Secure cryptographic devices(retail)—Part 2:Security compliance checklists for devices used in financial transactions)

3　术语和定义

下列术语和定义适用于本文件。