ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 20547.2—2006

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

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

(ISO 13491-2:2005,MOD)

2006-09-18 发布　　2007-03-01 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

GB/T 20547《银行业务　安全加密设备(零售)》分为如下部分：

——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 20547的第2部分。

本部分修改采用国际标准ISO 13491-2：2005《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》(英文版)。

本部分对ISO 13491-2：2005所做的修改主要包括以下内容：

1. 将本部分中引用的国际标准改为国际标准和国内相关法规。

2. 删除目前国内不适用的部分规范性引用文件。

本部分的附录A、附录B、附录C、附录D、附录E、附录F、附录G和附录H为规范性附录。

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管理。

本部分起草单位：中国银联股份有限公司、中国人民银行、中国工商银行、中国银行股份有限公司、中国建设银行股份有限公司、交通银行、北京银联金卡科技有限公司。

本部分主要起草人：刘钟、孙平、黄发国、徐志忠、温永盛、陆书春、刘运、赵宏鑫、薛伟、张晓东、陈立群、钱菲、李曙光、刘志刚、任冠华、姜红、李洁。

本标准于2006年首次发布。

引　言

GB/T 20547 的本部分规定了金融零售业务中用于保护报文、密钥及其他敏感信息的安全加密设备的物理特性、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，即：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。

通过合理使用以及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。为保证安全加密设备具有恰当的物理和逻辑安全特性，应对其进行评估。

本部分依据 ISO 13491-1 中对金融服务系统中安全加密设备的要求，提供了用于评估安全加密设备的安全符合性检测清单。存在其他的评估框架，并且也适合用于正式安全评估，例如：ISO/IEC 15408 的 1～3 部分和 ISO/IEC 19790，但这些已超出 ISO 13491 本部分的范围。

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被篡改，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探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行为的可能性。

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

1　范围

GB/T 20547的本部分结合国际或国内相关法规中规定的加密设备所采用的加密算法,规定了评估金融服务系统中安全加密设备的安全符合性检测清单。IC支付卡在发卡前应符合本部分的要求,发卡后作为一种个人设备不属于本部分范围。

本部分不涉及由安全加密设备故障所产生的问题。

在附录A～附录H中,"不可行"用于表示:尽管某些特定攻击在技术上是可能的,但在经济上是不可行的,因为实现这一攻击所需的经济开销要比攻破后得到的利益大得多。当然,除了为单纯的经济利益而攻击外,针对名誉的恶意攻击也应予以考虑。

2　规范性引用文件

下列文件中的条款通过GB/T 20547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。

ISO 9564-1:2002　银行业务　个人识别码管理和安全　第一部分:在ATM和POS系统中对联机PIN的保护原理与要求

ISO 11568(所有部分)　银行业务　密钥管理(零售业务)

ISO 13491-1　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

ISO 16609　银行业务　使用对称技术的报文鉴别需求

ISO 18031　信息技术　随机数的产生

3　术语和定义

下列术语和定义适用于本部分(ISO 13491-1中定义的术语和定义在本部分中同样适用)。

3.1

审计师　auditor

代表发起者或审计机构做非正式评估的具有检查、审计和评估能力的人员。

3.2

数据完整性　data integrity

数据未被非授权方式更改或破坏的特性。

3.3

双重控制　dual control

使用两个或多个实体(常为人员)互相配合来保护敏感功能或信息,以此来保证任一单个实体不能单独存取或使用这些敏感功能或信息。

3.4

异或　exclusive or

同等长度二进制数的模2加。