ICS 35.240.40
CCS A 11

中华人民共和国国家标准

GB/T 21079.2—2022
代替 GB/T 20547.2—2006

金融服务　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

Financial services—Secure cryptographic devices (retail)—Part 2:Security comliance checklists for devices used in financial transactions

(ISO 13491-2:2017,MOD)

2022-12-30 发布　　2022-12-30 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 21079《金融服务　安全加密设备（零售）》的第2部分。GB/T 21079已经发布了以下部分：

——第1部分：概念、要求和评估方法。

本文件代替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》，与GB/T 20547.2—2006相比，除结构调整和编辑性改动外，主要技术变化如下：

a）　增加了术语“评估机构”（见3.4）；

b）　增加了“经授权的准正式评估”（见4.4）；

c）　增加了我国密码算法相关要求（见表A.5的A21、表B.3的B18和表E.2的E4）；

d）　增加了部分附录内容（见A.3.4、A.3.6、B.2.1.2）。

本文件修改采用ISO 13491-2：2017《金融服务　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》。

本文件与ISO 13491-2：2017相比做了下述结构调整：

——附录H中，表H.1的序号H1～H5对应ISO 13491-2：2017中表H.1的H4～H8；

——附录H中，表H.2的序号H6～H8对应ISO 13491-2：2017中表H.2的H1～H3。

本文件与ISO 13491-2：2017的技术差异及其原因如下：

——附录A中，表A.5的序号A21，关于加密算法、操作模式和密钥长度的描述修改为“设备使用的加密算法、操作模式、密钥长度应符合ISO 11568-1、ISO 11568-2、ISO 11568-4、GB/T 32918、GB/T 32905和GB/T 32907”，以符合我国密码管理部门有关要求；

——附录B中，表B.3的序号B18，关于PIN Block格式的描述修改为“PIN加密应采用ISO 9564-1规定的PIN Block格式，应采用ISO 9564-1规定的加密算法和SM4分组密码算法”，以符合我国密码管理部门有关要求；

——附录E中，表E.2的序号E4，关于密钥生成方法的描述修改为“密钥生成方法应符合ISO 11568（所有部分）、GB/T 32918、GB/T 32905和GB/T 32907”，以符合我国密码管理部门有关要求。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国金融标准化技术委员会（SAC/TC 180）提出并归口。

本文件起草单位：北京银联金卡科技有限公司、中国银联股份有限公司、中国人民银行长沙中心支行。

本文件主要起草人：杨波、张彦超、谭亦夫、佟冬、汤洋、袁思思、谭旺、杜芮。

本文件于2006年首次发布，本次为第一次修订。

引　言

零售电子支付系统的安全性在很大程度上依赖于安全加密设备的安全性。安全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，通信线路可能被“窃听”，合法的数据和控制指令可能被非法操作所取代。尽管某些安全加密设备（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安全加密设备（如密码键盘等）都处在并不安全的环境中。因此，在这些安全加密设备上处理 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、数据泄露或被篡改的风险。

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，有助于降低金融风险。国际上，ISO 13491 系列标准属于金融交易过程中各类安全加密设备的使用、管理及评估所参考和依据的通用性基础标准。按照 ISO 13491-1 中对安全加密设备（以下简称 SCD）的安全要求，ISO 13491-2：2017 基于 ISO 9564-1、ISO 9564-2、ISO 16609、ISO 11568-1、ISO 11568-2 和 ISO 11568-4 等标准，规定了评估金融服务环境中 SCD 的安全符合性检测清单。我国借鉴 ISO 13491 系列标准，并结合我国密码管理部门和金融行业主管部门有关要求，形成 GB/T 21079《金融服务　安全加密设备（零售）》，指导金融行业零售业务中安全加密设备评估，拟由两个部分组成。

——第 1 部分：概念、要求和评估方法。旨在规定金融零售业务中用于保护报文、密钥及其他敏感数据的 SCD 的物理特性、逻辑特性和管理要求，包含了对 SCD 的安全要求。

——第 2 部分：金融交易中设备安全符合性检测清单。旨在提供用于评估安全加密设备的安全符合性检测清单，内容包括设备必须具有的特性、设备操作环境的特性和设备的管理方法。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 至 3 部分和 ISO/IEC 19790，但这些已超出 GB/T 21079 本部分的范围。

中国零售金融业务正处于快速发展时期，安全加密设备对于保障零售金融业务的安全性至关重要。本文件提供了用于评估安全加密设备的安全符合性检测清单，有助于提升金融行业安全加密设备安全管理水平，并为安全加密设备相关安全评估工作的标准化和规范化提供指导。

金融服务　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

本文件规定了评估金融服务环境中安全加密设备(SCD)的安全符合性检测清单。集成电路(IC)支付卡在发卡前属于本文件范围,发卡后将被视作一种个人设备且不属于本文件范围。

本文件适用于零售金融业务中应用的SCD设备的安全符合性检测。

本文件不适用于由SCD拒绝服务所引起的问题。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 32905　信息安全技术　SM3密码杂凑算法

GB/T 32907　信息安全技术　SM4分组密码算法

GB/T 32918　信息安全技术　SM2椭圆曲线公钥密码算法

ISO 9564-1　金融服务　个人识别码管理和安全　第1部分:基于卡的系统中PIN的基本原则和要求[Financial services—Personal Identification Number (PIN) management and security—Part 1: Basic principles and requirements for PINs in card-based systems]

注:GB/T 21078.1—2007　银行业务　个人识别码的管理与安全　第1部分:ATM和POS系统中联机PIN处理的基本原则和要求(ISO 9564-1:2002,MOD)

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]

注:GB/T 27909.1—2011　银行业务　密钥管理(零售)　第1部分:一般原则(ISO 11568-1:2005,MOD)

ISO 11568-2　金融服务　密钥管理(零售)　第2部分:对称密码及其密钥管理和生命周期[Financial services—Key management (retail)—Part 2: Symmetric ciphers, their key management and life cycle]

注:GB/T 27909.2—2011　银行业务　密钥管理(零售)　第2部分:对称密码及其密钥管理和生命周期(ISO 11568-2:2005,MOD)

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]

注:GB/T 27909.3—2011　银行业务　密钥管理(零售)　第3部分:非对称密码系统及其密钥管理和生命周期(ISO 11568-4:2007,MOD)

ISO 13491-1　金融服务　安全加密设备(零售)　第1部分:概念、要求和评估方法[Financial services—Secure cryptographic devices (retail)—Part 1: Concepts, requirements and evaluation methods]