ICS 35.240.40
CCS A 11

中华人民共和国国家标准

GB/T 21079.1—2022
代替 GB/T 21079.1—2011

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

(ISO 13491-1:2016,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1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 21079.1—2011《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》，与GB/T 21079.1—2011相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了“认证报告”“发起机构”(见GB/T 21079.1—2011的第3章)等术语；

b) 增加了“经认可的认证机构”(见3.3)、“审批机构”(见3.4)、“批准函”(见3.5)、“评估证书”(见3.11)、“设备管理”(见3.16)、“双重控制”(见3.17)、“金融密钥”(见3.22)、“硬件安全模块”(见3.24)、“密钥加载设备”(见3.25)、“安全方案”(见3.30)、“敏感功能”(见3.32)等术语；

c) 增加了“防攻击性要求”(见6.3)、“抗攻击性要求”(见6.4)、“反攻击性要求”(见6.5)；

d) 更改了SCD的逻辑安全要求(见6.6)；

e) 增加了“SCD应支持使用SM2椭圆曲线公钥密码算法、SM3密码杂凑算法和SM4分组密码算法，符合GB/T 32918、GB/T 32905和GB/T 32907的要求”的描述(见6.6.5)；

f) 更改了设备生命周期阶段及相应保护要求(见7.2、7.3)；

g) 删除了资料性附录A“有关系统安全级别的概念”(见GB/T 21079.1—2011的附录A)，删除了正文“8 评估方法”(见GB/T 21079.1—2011的第8章)；

h) 增加了资料性附录A“评估方法”(见附录A)。

本文件修改采用ISO 13491-1:2016《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》。

本文件与ISO 13491-1:2016相比做了下述结构调整：

——第3章中3.4～3.37对应ISO 13491-1:2016的3.3～3.36。

本文件与ISO 13491-1:2016的技术差异及其原因如下：

——第3章增加了“经认可的认证机构”(见3.3)，符合《中华人民共和国认证认可条例》相关要求；

——第6章中6.6.5增加了“SCD应支持使用SM2椭圆曲线公钥密码算法、SM3密码杂凑算法和SM4分组密码算法，符合GB/T 32918、GB/T 32905和GB/T 32907的要求”的描述，符合我国密码管理部门有关要求；

——附录A中A.1.5修改了正式评估的流程(见图A.1)，符合《中华人民共和国认证认可条例》相关要求。

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2007年首次发布，2011年第一次修订，本次为第二次修订。

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。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，存在数据泄露或被篡改的风险。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有助于降低金融风险。

为了保证安全加密设备（SCD）的评估活动有序开展，促进 SCD 的合理使用与管理，建立相应的安全加密设备评估标准成为了首要任务。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，其中 ISO 13491-1：2016 基于 ISO 9564、ISO 16609、ISO 11568 等标准，规定了金融零售服务中用于保护报文、密钥及其他敏感信息的安全加密设备的特性和管理要求。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。本文件通过对应用在金融零售业务中的 SCD 的物理特性、逻辑特性和管理要求等方面进行规范，以提高 SCD 自身安全性与管理水平，对维护金融市场秩序，加强市场金融稳定，保护金融活动安全等方面具有重要的意义。

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

1　范围

本文件规定了安全加密设备的概念,以及设备安全特性和设备管理的要求。

本文件适用于零售金融业务中应用的SCD设备的安全管理。

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 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)

3　术语和定义

下列术语和定义适用于本文件。

3.1

认可机构　accreditation authority

负责认可评估机构并监督其工作以确保评估结果可再现的机构。

3.2

经认可的评估机构　accredited evaluation agency

经认可机构(3.1)根据相应规则认可后,从事评估工作的机构。