ICS 35.240.40
A 11

中华人民共和国国家标准

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

Banking—Key management(retail)—Part 2:Symmetric ciphers—Key management and life cycle

(ISO 11568-2:2005,MOD)

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 27909《银行业务　密钥管理(零售)》分为以下3个部分：

——第1部分：一般原则；

——第2部分：对称密码及其密钥管理和生命周期；

——第3部分：非对称密码系统及其密钥管理和生命周期。

本部分是GB/T 27909的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分修改采用国际标准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》(英文版)。

在采用ISO 11568-2时做了以下修改：

删除了“ISO 11568-2附录B对称密钥管理的核准算法”，在第1章中说明本部分描述的技术中所涉及到的算法应符合国家密码管理部门的有关规定。

本部分还做了下列编辑性修改：

a)　对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ISO前言。

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、中国农业银行、中国银行、交通银行、中国光大银行、中国银联股份有限公司。

本部分主要起草人：王平娃、陆书春、李曙光、赵志兰、周亦鹏、赵宏鑫、程贯中、刘瑶、喻国栋、杨增宇、黄发国。

引　言

GB/T 27909 描述了在零售金融服务环境下密钥的安全管理过程，这些密钥用于保护诸如收单方和受理方之间，收单方和发卡方之间的报文。

本部分描述了在零售金融服务领域内适用的密钥管理要求，典型的服务类型有销售点/服务点(POS)借贷记授权和自动柜员机(ATM)交易。

当 GB/T 27909 各部分描述的密钥管理技术结合使用时，可提供 GB/T 27909.1 中描述的密钥管理服务。

这些服务包括：

——密钥分离；

——防止密钥替换；

——密钥鉴别；

——密钥同步；

——密钥完整性；

——密钥机密性；

——密钥泄露的检测。

密钥管理服务和相应的密钥管理技术的对照参考见第 7 章。

本部分描述了使用对称密码机制时，密钥安全管理中涉及的密钥生命周期。依据 GB/T 27909.1 和本部分描述的密钥管理原则、服务和技术，本部分也规定了密钥生命期内各个阶段的要求和实现方法。本部分不涉及非对称密码机制的密钥管理或生命周期，该方面的内容见 GB/T 27909.3。

本部分制定时，充分考虑了 ISO/IEC 11770 标准的要求。

本部分采用和描述的技术满足了金融服务行业的需求。

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

1　范围

本部分描述了在零售金融服务环境中,当使用对称密码机制时对称和非对称密钥的保护技术,也描述了与对称密钥相关的生命周期管理。本部分描述的技术符合GB/T 27909.1中描述的原则。

本部分描述的技术适用于任何对称密钥管理操作。

本部分所使用的符号见附录A。

本部分描述的技术中所涉及到的算法应符合国家密码管理部门的有关规定。

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。

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)

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(ISO 13491-2:2005,MOD)

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)

GB/T 21079.1　银行业务　安全加密设备(零售)　第1部分:概念、需求和评估方法(GB/T 21079.1—2007,ISO 13491-1:1998,MOD)

ISO/IEC 10116　信息技术　安全技术　n位分组密码的操作方式

ISO 16609:2004　银行业务　使用对称技术的报文鉴别要求

ISO/IEC 18033-1　信息技术　安全技术　加密算法　第1部分:概要

ISO/TR 19038:2005　银行业务和相关金融服务　三重DEA操作模式　实施指南

ANSI X9.24 Part 1-2004　零售金融服务对称密钥管理　第1部分:使用对称技术

ANSI X9.65　三重数据加密算法(3-DEA),实施标准

3　术语和定义

下列术语和定义适用于本文件。

3.1

密码　cipher

在称为密钥的参数控制下,实现密文和明文间转换的一对操作。

注:加密操作将数据(明文)转换成不可读的密文形式;解密操作将密文恢复成明文。