ICS 35.240.40
A 11

中华人民共和国国家标准

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

Banking—Key management(retail)—
Part 3:Asymmetric cryptosystems—Key management and life cycle

(ISO 11568-4:2007,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3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 11568-4：2005《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》(英文版)。

在采用ISO 11568-4时做了以下修改：

——删除了“ISO 11568-4附录A核准的算法”。

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。

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。

本部分描述了使用非对称密码机制时，密钥安全管理中涉及的密钥生命周期。依据标准第 1 部分和本部分描述的密钥管理原则、服务和技术，本部分还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 27909.2。

本部分是 GB/T 27909、GB/T 21078.1、GB/T 20547、ISO 9564-2、ISO 9564-3、ISO 9564-4、ISO/TR 19038 等描述金融服务领域安全要求的标准之一。

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

1　范围

本部分规定了零售金融服务环境中使用非对称密码机制时,对称和非对称密钥的保护技术,也描述了与非对称密钥相关的生命周期管理。本部分适用于技术符合GB/T 27909.1中描述的原则。

本部分的零售金融服务环境仅限于下述实体之间的接口:

——卡受理设备与收单方;

——收单方与发卡方;

——集成电路卡(ICC)与卡受理设备。

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

GB/T 27909.2　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(GB/T 27909.2—2011,ISO 11568-2:2005,MOD)

GB/T 17964—2000　信息安全技术　分组密码算法的工作模式(ISO/IEC 10116:1997,IDT)

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)

GB/T 21078.1　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(GB/T 21078.1—2007,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、要求和评估方法(GB/T 21079.1—2007,ISO 13491-1:1998,MOD)

ISO/IEC 9796-2:2002　信息技术　安全技术　实现报文恢复的数字签名方案

ISO/IEC 10118(所有部分)　信息技术　安全技术　哈希函数

ISO/IEC 11770-3　信息技术　安全技术　密钥管理　第3部分:使用非对称技术的机制

ISO/IEC 14888-3　信息技术　安全技术　带附录的签名　第3部分:基于离散对数的机制

ISO 15782-1:2003　银行业务　证书管理　第1部分:公钥证书

ISO/IEC 15946-3:2002　信息技术　安全技术　基于椭圆曲线的密码技术　第3部分:密钥的生成

ISO 16609:2004　银行业务:使用对称技术的报文认证要求

ISO/IEC 18033-2　信息技术　安全技术　加密算法　第2部分:非对称密码

ANSI X9.42-2003　金融业务的公钥密码　使用离散对数密码的对称密钥协议