ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 27909.1—2011

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

(ISO 11568-1:2005,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)》分为以下几个部分：

——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1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 11568-1：2005《银行业务　密钥管理(零售)　第1部分：一般原则》(英文版)。

在采用ISO 11568-1时做了以下修改：

删除了“ISO 11568-1附录A密码算法的核准程序”，在第1章中说明用于密钥管理的密码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的密钥安全管理过程，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。

密钥管理是为授权通信方提供密钥，且在密钥被销毁之前，使密钥持续处于安全流程控制下的过程。

数据的安全性依赖于防止密钥的泄露以及未授权的修改、替换、插入或终止，因而，密钥管理涉及到密钥的生成、存储、分发、使用和销毁各个程序。通过对这些程序的规范化，也为制定审计追踪规范奠定了基础。

本部分没有提供区分使用同一密钥的实体的方法。密钥管理过程的最终细则需要由有关的通信方协商决定，并应就个体的身份及其职责达成协议，通信方要对此细则承担相应的职责。GB/T 27909 本身没有涉及个体职责的分配，这是密钥管理在具体实施中需要考虑的。

银行业务　密钥管理(零售)
第1部分:一般原则

1　范围

本部分规定了在零售金融服务环境中实施的密码系统应遵循的密钥管理原则。本部分的零售金融服务环境指下述实体间的接口:

——卡受理设备与收单方;

——收单方与发卡方;

——集成电路卡(ICC)与卡受理设备之间。

附录A描述了该环境的一个实例,附录B阐述了本部分在实施时所受到的相关威胁。

本部分可同时适用于对称密码系统中的密钥及非对称密码系统中的私钥和公钥。在对称密码系统中,发送方和接受方使用相同的密钥。用于密钥管理的密码算法应符合国家密码管理部门的有关规定。

密码的使用除了涉及密钥外,通常还涉及控制信息,例如,初始化向量、密钥标识符。这些信息统称为"密钥要素"。虽然本部分专门描述的是密钥的管理,但是它的原则、服务和技术也适用于密钥要素。

本部分适用于金融机构和零售金融服务领域的其他组织。在这些领域中,信息交换要求具有机密性、完整性或真实性。零售金融服务包括但并不限于诸如POS借贷记授权、自动售货机和自动柜员机(ATM)交易等服务。

在ISO 9564和ISO 16609标准中,分别描述了零售金融交易中个人识别码(PIN)的加密以及在报文鉴别时所使用的密码操作。GB/T 27909也适用于对这些标准所引入的密钥的管理。此外,密钥管理过程自身也需要引入更深一层次的密钥,例如,密钥加密密钥。密钥管理过程同样适用于这些密钥。

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 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 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(ISO 11568-2:2005,MOD)

GB/T 27909.4　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(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

非对称密钥对　asymmetric key pair

在一个公开密钥密码系统中生成及使用的公钥及其相关私钥。