

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 皮 布 国 国 家 标 准 化 管 理 委 员 会

目 次

1 范围	亰	有言 ・・		\prod
2 規範性引用文件 1 3 木语和定义 1 4.1 安全目标 3 4.2 安全级别 3 4.3 密销管理目标 3 5 密钥管理原则 3 6 光高系统 4 6.1 概要 4 6.2 密码系统 4 6.4 非对称密码系统 4 6.5 其他密码系统 5 7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全图设备 5 7.3 物理安全环境 5 8 安全性考虑 5 8.1 秘密密閉/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥学理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7	弓			
3 术语和定义 1 4 密钥管理 3 4.1 安全目标 3 4.2 安全级别 3 4.3 密钥管理目标 3 6 密码系统 4 6.1 概要 4 6.2 密码系统 4 6.3 对称密码系统 4 6.4 非对称密码系统 4 6.5 其他密码系统 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全对境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的证例环境 6 8.3 防止假冒设备 6 8.3 防止假冒设备 6 9 密码系统的密制管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7	1	范围	<u> </u>	1
4 密钥管理 4.1 安全目标 3.1 安全目标 3.2 安全级别 3.3 密钥管理目标 3.3 密钥管理原则 3.3 密钥管理原则 3.3 密钥管理原则 3.4 多种 医两系统 4.6 是 密码系统 4.6 是 密码系统 4.6 是 密码系统 4.6 是 非他密码系统 4.6 是 实全密码设备 5.7 常码环境的物理安全 5.1 物理安全性考虑 5.2 安全密码设备 5.3 物理安全性考虑 5.8 安全性考虑 5.8 安全性考虑 6.8 次 分的密码环境 6.9 密码系统的密码环境 6.9 密码系统的密码可用性 6.6 完整性 6.7 机概性 6.9 是 密钥少离 6.8 泄露检测 6.9 完整性	2			
4.1 安全目标 3 4.2 安全级别 3 4.3 密钥管理目标 3 5 密钥管理原则 3 6 密码系统 4 6.1 概要 4 6.2 密码系统 4 6.3 对称密码系统 4 6.4 非对称密码系统 5 7 密码环境的数理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 5 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止假 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7	3			
4.2 安全级别 3 4.3 密钥管理目标 3 5 密钥管理原则 3 6 密码系统 4 6.1 概要 4 6.2 密码系统 4 6.3 对称密码系统 4 6.4 非对称密码系统 4 6.5 其他密码系统 5 7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7	4	密钥	月管理	3
4.3 密钥管理目标 3 5 密钥管理原则 3 6 密码系统 4 6.1 概要 4 6.2 密码系统 4 6.3 对称密码系统 4 6.5 其他密码系统 5 7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 6 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		4.1	安全目标	3
5 密钥管理原则 3 6 密码系统 4 6.1 概要 4 6.2 密码系统 4 6.3 对称密码系统 4 6.4 非对称密码系统 4 6.5 其他密码系统 5 7 密码环境的物理安全 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10.1 概要 7 10.2 密钥生命周期 7 10.2 密钥生命周期的一般要求 7		4.2	安全级别	3
6 密码系统 4 6.1 概要 4 6.2 密码系统 4 6.3 对称密码系统 4 6.4 非对称密码系统 4 6.5 其他密码系统 5 7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10.1 概要 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		4.3	密钥管理目标	3
6.1 概要 6.2 密码系统 6.3 对称密码系统 6.4 非对称密码系统 6.5 其他密码系统 6.5 其他密码系统 6.5 其他密码系统 7 密码环境的物理安全 7.1 物理安全性考虑 7.2 安全密码设备 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 9.3 防止替换 9.1 概述 6 9.2 密钥分离 9.3 防止替换 9.6 完整性 9.7 机密性 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.1 概要 7	5			
6.2 密码系统 4 6.3 对称密码系统 4 6.4 非对称密码系统 4 6.5 其他密码系统 5 7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 9 9.7 机密性 7 9.8 泄露检测 7 10. 密钥生命周期 7 10.1 概要 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7	6	密码	马系统	4
6.3 对称密码系统 4 6.4 非对称密码系统 4 6.5 其他密码系统 5 7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.2 公钥的密码环境 6 9.2 密钥介离 6 9.1 概述 6 9.2 密钥介离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		6.1		
6.4 非对称密码系统 4 6.5 其他密码系统 5 7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 6 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		6.2		
6.5 其他密码系统 5 7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		6.3		
7 密码环境的物理安全 5 7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		6.4	非对称密码系统	4
7.1 物理安全性考虑 5 7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期・ 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		6.5	其他密码系统	5
7.2 安全密码设备 5 7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7	7	密码	马环境的物理安全	5
7.3 物理安全环境 5 8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		7.1	物理安全性考虑	5
8 安全性考虑 6 8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		7.2	安全密码设备	5
8.1 秘密密钥/私钥的密码环境 6 8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		7.3	物理安全环境	5
8.2 公钥的密码环境 6 8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7	8	安全	全性考虑	6
8.3 防止假冒设备 6 9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		8.1	秘密密钥/私钥的密码环境	6
9 密码系统的密钥管理服务 6 9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		8.2	公钥的密码环境	6
9.1 概述 6 9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		8.3	防止假冒设备	6
9.2 密钥分离 6 9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7	9	密码	马系统的密钥管理服务	6
9.3 防止替换 6 9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		9.1	概述	6
9.4 识别 6 9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		9.2	密钥分离	6
9.5 同步(可用性) 6 9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		9.3	防止替换	6
9.6 完整性 6 9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		9.4	识别	6
9.7 机密性 7 9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		9.5	同步(可用性)	6
9.8 泄露检测 7 10 密钥生命周期 7 10.1 概要 7 10.2 密钥生命周期的一般要求 7		9.6	完整性	6
9.8 泄露检测 ····· 7 10 密钥生命周期····· 7 10.1 概要····· 7 10.2 密钥生命周期的一般要求···· 7		9.7	机密性	7
10.1 概要······ 7 10.2 密钥生命周期的一般要求····· 7		9.8	泄露检测	7
10.1 概要······ 7 10.2 密钥生命周期的一般要求····· 7	1	0 密	钥生命周期	7
10.2 密钥生命周期的一般要求 ······ 7				
				•

GB/T 27909.1—2011

10.3	非对称密码系	统的附加要求	8
附录 A	(资料性附录)	零售金融服务环境的实例	9
附录B	(资料性附录)	零售金融服务环境中的威胁实例	10
参考文	献		12

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。| 密码的使用除了进及密钥处 通常还进及控制信息 侧加 知始化向景 密钥标识符 这此信息答称

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。