ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 21082.4—2007

银行业务　密钥管理(零售)
第4部分:使用公开密钥密码的密钥管理技术

Banking—Key management(retail)—
Part 4:Key management techniques using public key cryptography

(ISO 11568-4:1998,MOD)

2007-09-05 发布　　2007-12-01 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 21082《银行业务　密钥管理(零售)》分为如下6个部分：

——第1部分　密钥管理介绍；

——第2部分　对称密码的密钥管理技术；

——第3部分　对称密码的密钥生命周期；

——第4部分　使用公开密钥密码的密钥管理技术；

——第5部分　公开密钥密码系统的密钥生命周期；

——第6部分　密钥管理方案。

本部分是GB/T 21082的第4部分。

本部分修改采用国际标准ISO 11568-4:1994《银行业务　密钥管理(零售)　第4部分:使用公开密钥密码的密钥管理技术》(英文版)。

考虑到我国国情,在采用ISO 11568-4时做了以下修改：

删除了“ISO 11568-4附录A核准的算法和算法审核程序”,在第1章中说明应遵循我国密码管理部门的有关规定。

为便于使用,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。

本部分的附录A为规范性附录,附录B、附录C为资料性附录。

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归口管理。

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、招商银行、华北计算技术研究所、启明星辰有限公司。

本部分主要起草人:谭国安、杨竑、陆书春、李曙光、林中、张启瑞、史永恒、赵宏鑫、李红新、徐伟、董永乐、王林立、周亦鹏、熊少军。

本部分为首次制定。

引　言

GB/T 21082 是描述在零售银行业务环境下密钥安全管理过程的一系列标准，这些密钥用于保护诸如收单行和受卡方之间，或收单行和发卡行之间的报文。用于集成电路卡的密钥管理不包括在GB/T 21082标准中。

鉴于批发银行环境中的密钥管理是以在安全系数相对高的安全环境中的密钥交换为特征的，本标准描述了在零售银行服务涉及的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)借记支付，信用卡凭证支付和自动柜员机(ATM)交易。

GB/T 21082 的本部分主要描述适用于公开密钥密码系统的密钥管理技术。在组合使用时，这些技术将提供 ISO 11568-1 中描述的密钥管理服务。这些服务是：

——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；

——密钥泄露检测。

银行业务　密钥管理(零售)
第4部分:使用公开密钥密码的
密钥管理技术

1　范围

GB/T 21082的本部分详细描述了在零售银行业务环境下对公开密钥密码系统密钥的使用和保护技术。

它适用于任何在密钥生命周期内负责执行密钥保护程序的组织。GB/T 21082的本部分描述的技术符合ISO 11568-1描述的原则。

注:在密钥生命周期每一阶段所要求的保护公开密钥密码系统的保护细节在ISO 11568-1中有详细描述。

公开密钥密码系统包括非对称密码、数字签名系统和公开密钥分发系统。虽然本部分主要描述在密钥管理中应用这些系统的技术,但其中一些技术也同样适用于数据的安全管理。

本部分描述的技术主要针对一般的公开密钥密码系统。针对某个特定系统的具体标准见附录。

批准与本部分中描述的技术一起使用的算法和算法的审批程序应遵从国家密码管理相关机构的规定。

附录A概述了公钥证书管理的标准化。

附录B描述了属性证书,这项技术能加强公钥证书的功能。

附录C介绍了上面提到的三种公开密钥密码系统。

2　规范性引用文件

下列文件中的条款通过GB/T 21082的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 15843.3—1998　信息技术　安全技术　实体鉴别　第3部分:用非对称签名技术的机制(idt ISO/IEC 9798-3:1993)

GB/T 17964—2000　信息技术　安全技术n位块密码算法的操作方式(idt ISO/IEC 10116:1997)

ISO/IEC 8824:1990　信息技术　开放系统互连　抽象语法记数法一(ASN.1)规范

ISO/IEC 8825:1990　信息技术　开放系统互连　抽象语法记数法一(ASN.1)基本编码规则规范

ISO 8908:1993　银行业务及相关金融服务　词汇和数据元

ISO/IEC 9594-8:1990　信息技术　开放系统互连　目录　第8部分:鉴别框架

ISO 9807:1991　银行业务和相关金融服务　报文鉴别要求(零售)

ISO 11166(所有部分)　银行业务　采用非对称算法的密钥管理

ISO 11568-1　银行业务　密钥管理(零售)　第1部分:密钥管理介绍

ISO 11568-2　银行业务　密钥管理(零售)　第2部分:对称密码的密钥管理技术

ISO/IEC 11770-3:1999　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 13491-1:1999　银行业务　安全密码设备(零售)　第1部分:概念、要求和评估方法

3　术语和定义

ISO 8908:1993中给出的以及下列术语和定义适用于本部分。