ICS 35.240.40
A 11

# 中华人民共和国国家标准

GB/T 21081—2007/ISO 13492:1998

# 银行业务　密钥管理相关数据元(零售)

**Banking—Key management related data element(retail)**

(ISO 13492:1998,IDT)

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

本标准等同采用国际标准 ISO 13492:1998《密钥管理相关数据元(零售)》(英文版)。

为便于使用,对于 ISO 13492 做了下列编辑性修改:

a) 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) 删除国际标准的前言。

本标准的附录 A、附录 B 为资料性附录。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会归口。

本标准负责起草单位:中国金融电子化公司。

本标准参加起草单位:中国人民银行、中国工商银行、中国农业银行、招商银行、中国银联股份有限公司、华北计算技术研究所、启明星辰有限公司。

本标准主要起草人:谭国安、杨竑、陆书春、李曙光、王林立、周亦鹏、林中、张启瑞、史永恒、赵宏鑫、李红新、徐伟、张艳、董永乐、熊少军、黄发国、李建云。

本标准为首次制定。

# 引　言

本标准描述了密钥管理相关数据元的结构与内容，该数据元可在银行零售业务环境下，通过电子报文方式传输，以支持密钥的安全管理。其中银行零售业务环境包括卡接收装置与收单行、收单行与发卡方之间的通信。在集成电路卡中使用的密钥以及相关数据元的密钥管理不适用于本标准。

本标准兼容银行卡报文现行 ISO 标准(见 ISO 8583)。

# 银行业务　密钥管理相关数据元(零售)

## 1　范围

本标准详细说明了密钥管理相关数据元,该数据元或者在交易报文中传输(用于保护当前交易的密钥信息),或者在加密服务报文中传输(用于保护未来交易的密钥信息)。

本标准说明了在 ISO 8583:1993 范围内应用密钥管理相关数据元的要求,应使用以下两个 ISO 8583:1993数据元:安全相关控制信息(53 位元)或密钥管理数据(96 位元)。但密钥管理相关数据的传输不局限于 ISO 8583:1993 标准。

本标准适用于对称和非对称密码系统。

ISO 11568 描述了零售银行业务环境下密钥安全管理过程。ISO 9564 和 ISO 9807 分别描述了安全性相关数据,如 PIN 和 MAC。

## 2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。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标准,然而,鼓励根据本标准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标准。

GB/T 15694.1—1995　识别卡　发卡方者标识　第 1 部分:编号体系(idt ISO/IEC 7812-1:1993)

ISO/IEC 7812-2:1993　身份识别卡　发卡方身份识别　第 2 部分:申请与注册程序

ISO 8583:1993　产生报文的金融交易卡　交换报文规范

ISO 8908:1993　银行业务及相关金融服务　词汇和数据元

ISO 9564-1:1991　个人识别码的管理与安全　第 1 部分:PIN 保护原则与技术

ISO 9807:1991　银行业务和相关金融服务　报文鉴别要求(零售)

ISO 11568-1:1994　银行业务　密钥管理(零售)　第 1 部分:密钥管理介绍

ISO 11568-2:1994　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 11568-3:1994　银行业务　密钥管理(零售)　第 3 部分:对称密码的密钥生命周期

ANSI X3.92:1987　数据加密算法

## 3　术语和定义

ISO 8908:1993 给出的以及下列术语和定义适用于本标准。

3.1

**非对称密码　asymmetric cipher**

加密密钥与解密密钥不同,并且由加密密钥推导出解密密钥的计算是不可行的。

3.2

**密码　cipher**

在称之为密钥的参数控制下,实现明文、密文之间相互转换的一组运算。

注:加密运算是将数据(明文)转换为不易理解的形式(密文)。解密运算是将密文恢复为明文。

3.3

**密码算法　cryptographic algorithm**

规定实现数据加密和解密过程的一套规则。

注:设计该算法使得除非通过穷举搜索否则不可能确定控制参数(如密钥)。