ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 20544—2006

银行业务　报文加密程序(批发)　一般原则

Banking—Procedures for message encipherment(wholesale)—General principles

(ISO 10126-1:1991,MOD)

2006-09-18 发布　　2007-03-01 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

本标准修改采用国际标准 ISO 10126-1:1991《银行业务　报文加密程序(批发)　第 1 部分:一般原则》(英文版)。

考虑到我国国情,在采用 ISO 10126-1 时做了以下修改:

a) 标准名称中删除“第 1 部分”,删除规范性引用文件“ISO 10126-2:1991”,因为 ISO 10126-2 描述的算法不符合我国密码管理部门的有关规定,不宜采为国家标准,所以第 1 部分就构成本标准的全部。

b) 删除引言中“适用于本部分的特定算法在第 2 部分中有所描述”。删除 6.7 中“(10126-2 描述的密码分组链)”,因为该算法不符合我国密码管理部门的有关规定。

c) 删除“ISO 10126-1 附录 A 密码算法的核准程序”,在第 8 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,对于 ISO 10126-1 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。

本标准的附录 A、附录 B、附录 C 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管理。

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、北京工商大学。

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、张德栋。

本标准为首次制定。

引　言

本标准以提供保密性为目的，规定了整个(或部分)金融批发报文应用层加密和解密的方法。

本标准提供的安全等级取决于以下两点：

a) 与加密算法有关的安全性和算法在本标准程序中的具体实现；

b) 安全的密钥管理系统的运行。

密钥管理的相应国际标准在 ISO 8732 中有所描述。

银行业务　报文加密程序(批发)
一般原则

1　范围

本标准所定义的程序旨在通过加密的方法保护在任何通信体系结构中交换的金融报文(整个报文或者待加密元素)。这些体系结构包括存储、转发和电报环境,以及任意数目的节点和公共或私有网络。

因为加密的文本会妨碍现有批发金融网络的通信进程,所以本标准制定了允许加密报文通过多个网络传输,而不会被误解为通信协议信息—如 STX(文本开始)、EOT(文本结束)—的方法。

金融报文数据的机密性,不管是结构化的还是非结构化的数据,都受本标准的保护。

文中描述的技术并未提供完整性保护(比如,针对修改、替代和重放的保护)。ISO 8730 和 ISO 8731中讨论了数据完整性的保护。报文格式同样也超过了本标准的讨论范围。

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 1988—1998　信息技术　信息交换用七位编码字符集(eqv ISO/IEC 646:1991)

ISO 8730:1990　银行业务　报文鉴别(批发)要求

ISO 8731-1:1987　银行业务　核准的报文鉴别算法　第 1 部分:DEA 协议

ISO 8731-2:1987　银行业务　核准的报文鉴别算法　第 2 部分:报文鉴别算法

ISO 8732:1988　银行业务　密钥管理(批发)

3　术语和定义

下列术语和定义适用于本标准。

3.1

字符编码　baudot

一种五位字符的信息编码方案(不包括可选的起始位和结束位):CCITT 字母编号 2。

3.2

块　block

特定长度的数据单元。

3.3

密文　ciphertext

加密的信息。

3.4

通信对　communicating pair

就交换数据已经达成一致的两个逻辑组。

3.5

密码密钥　cryptographic key

密钥　key