ICS 03.060
A 11

中华人民共和国国家标准

GB/T 21080—2007/ISO 11131:1992

银行业务和相关金融服务 基于对称算法的签名鉴别

**Banking and related financial services—
Sign-on authentication based on symmetric algorithm**

(ISO 11131:1992,Banking and related financial services—
Sign-on authentication,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 ISO 11131:1992《银行业务和相关金融服务　签名鉴别》(英文版)。

为便于使用,本标准做了下列编辑性修改:

a) 删除 ISO 前言;

b) “本国际标准”一词改为“本标准”;

c) 根据目前计算机行业实际发展情况,增加了资料性附录 B。

附录 A 和附录 B 均为资料性附录。

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、中国银行、中国建设银行、中国光大银行、中国银联股份有限公司、北京启明星辰公司。

本标准主要起草人:谭国安、杨竑、陆书春、李曙光、刘运、杜宁、刘志军、张艳、张德栋、戴宏、张晓东、马云、李红建、王威、王沁、孙卫东、李春欢。

本标准为首次制定。

引　言

金融机构正在逐渐通过使用电子通讯技术来为其客户提供更及时无误的服务，以满足个人客户的需求。该技术不断加强客户直接访问（或登录）金融机构里计算机应用程序的能力。具体例子包括资金转移和现金管理服务。

从历史上看，金融业普遍采用用户（用户识别名）个人标识符与秘密口令结合使用作为提供用户直接访问服务供应商系统的标准方法。

然而，该口令系统的有效性存在着局限性。鉴别用户的口令能用多种方法破解，例如，它能被猜测出，被窃听或公开地显示出来。假冒和重放也是两种可能的威胁：

——假冒是通过显示盗取的口令对实体进行模仿，假冒通常伴有其他攻击，例如数据篡改；

——重放是对近期已记录的有效交换的再次展现，用来产生非授权效果。

双方共享通用密钥的安全签名鉴别程序需要实现大量的条件，包括以下内容：

a) 保持鉴别系统中结点的硬件和软件的完整；

b) 保持请求者和授权人之间鉴别信息的完整，如：用户标识符的分配（用户名）、口令的选择、口令的变更、中断访问的方法、对失败的签名尝试的审计；

c) 保持成功登录后整个会话期内鉴别的连续性；

d) 保持对失败登录尝试的审计能力；

e) 确保抵抗破解和误用的密钥管理系统的完整性；

f) 确保已传输的鉴别信息的保密性；

g) 通过对鉴别信息的验证提供检测重放的方法。

银行业务和相关金融服务
基于对称算法的签名鉴别

1 范围

本标准实现了引言中的条件 f)和条件 g)。它规定了请求访问实体和授权允许访问实体之间的三种签名鉴别方式：

a) 通过诸如口令的个人鉴别信息(PAI)对用户进行鉴别；

b) 通过用户唯一密钥对用户进行鉴别；

c) 通过节点唯一密钥对节点进行鉴别。

本标准使用对称(密钥)算法，在对称算法中请求方和授权方使用相同密钥。

第 6 章给出了一个满足本标准要求的协议实例，可在实例中获得互操作性。附录 A 描述了本标准存在的一些局限性。附录 B 描述了本标准技术指标的一些局限性。

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 15277—1994 信息处理 64 bit 分组密码算法的工作方式(eqv ISO 8372:1987)

ISO 8730:1990 银行业务 报文鉴别要求(批发)

ISO 8732:1988 银行业务 密钥管理(批发)

ISO 10126-1:1991 银行业务 报文加密程序(批发) 第 1 部分：一般原则

ISO 10126-2:1991 银行业务 报文加密程序(批发) 第 2 部分：DEA 算法

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

鉴别密钥 authentication key

用于鉴别的密钥。

3.1.2

密文 ciphertext

被加密的信息。

3.1.3

密码有效期 cryptoperiod

某一密钥被授权可用的时间周期，或给定系统中密钥保持有效的一段特定时间。

3.1.4

解密 decipherment

将密文(不可读)转换为明文(可读)的过程。