ICS 35.240.15
A 11

中华人民共和国国家标准

GB/T 23695—2009

银行业务　安全文件传输(零售)

Banking—Secure file transfer(retail)

(ISO 15668:1999,MOD)

2009-05-06 发布　　2009-10-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 2
3　术语和定义 …… 3
4　原则 …… 4
5　应用 …… 5
6　鉴别机制 …… 10
附录 A（资料性附录）　机制示例 …… 11
附录 B（资料性附录）　实施的例子 …… 17
附录 C（资料性附录）　保证文件传输完整性确认的示例 …… 20
附录 D（资料性附录）　安全服务的图形概要参考 …… 24

前　言

本标准修改采用 ISO 15668:1999《银行业务　安全文件传输(零售)》(英文版)。

本标准根据 ISO 15668:1999 重新起草,与 ISO 15668:1999 的技术性差异及原因为:

——删除“2　规范性引用文件”中对此文件的引用:ISO 8731-1:1987《银行业务　核准的报文鉴别算法　第1部分:DEA》,因为此标准中的算法不符合我国密码管理部门的有关规定,且该标准已于2005年被ISO废止。

——删除“2　规范性引用文件”中对此文件的引用:ISO 11568(所有部分)《银行业务　密钥管理(零售)》,因为此标准中的算法不符合我国密码管理部门的有关规定。

——删除“图1　终端软件的表示(示意图)”中的标号8,因为图1注释中未给出标号8的说明,且根据原文可知标号8是指引导程序(标号7)的运行环境或其他支持程序,而标准中提到引导程序(即层a)的安全性不在本标准的讨论范围之内,它的运行环境和支持程序被标为了灰色。在不影响理解的情况下,删除图中未给出解释的标号8。

——5.1.2.3中“密钥管理技术应符合ISO 11568的要求”,改为:“密钥管理技术应遵循我国密码管理部门的有关规定”。

——“6　鉴别机制”和“A.1　鉴别机制”中,“已核准的算法参考ISO 11568”改为:“已核准的算法应遵循国家的相关规定”。

——删去A.3中最后一句:“ISO 9807给出了已经核准的用于计算MAC的算法列表,其中在ISO 8731-1中说明的算法,以操作的密码分组链模式使用DEA,它是当 $n=64$,$m=32$,ISO/IEC 9797的一个特殊情况”。因为ISO 8731中的算法不符合我国密码管理部门的有关规定。

——删去A.2最后一句:“——ISO/IEC 10118-2,附录A,说明一种使用 $n=64$,哈希长度=56的DES方法”。

——删去A.2.3所举的例子,因为其中引用了DSA、RSA,不符合我国密码管理部门的规定。

——删去资料性附录B,因为其中引用了DEA,不符合我国密码管理部门的规定。

——C.4.3.3中“MAC密钥应遵循ISO 11568”,改为“MAC密钥应遵循我国密码管理部门的有关规定”。

为便于使用,本标准做了下列编辑性修改:

——用“本标准”代替“本国际标准”;

——删除国际标准前言;

——修改图1、图2中的印刷错误。

本标准的附录A、附录B、附录C和附录D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、泛太领时科技(北京)有限公司。

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、中国建设银行、交通银行、中国银联股份有限公司、华北计算技术研究所、北京工商大学。

本标准主要起草人:王平娃、李曙光、吕毅、杨颖莉、鲍乐群、万良君、林中、张启瑞、仲志晖、景芸、刘运、钱湘隆、赵金波、曹文中、李劲松、刘先、周亦鹏、王威。

引　言

本标准说明在零售银行业务环境下如何保护文件传输。使用该类文件传输的典型例子是在卡的接收设备和收单机构之间，或在收单机构和发卡方之间的文件传输。

银行业务　安全文件传输(零售)

1　范围

批发银行业务的文件传输是在安全性相对高的主机之间进行大量的信息交换(大宗文件传输);与此相比,零售银行业务文件传输以量少、下载设备操作环境的可信赖程度较低为特点。这类设备可以是(但不仅限于)电子销售点终端(EPOS)、自动售卖机(AVM)、自动柜员机(ATM)或与支付网关通信的商户服务器。

假设参与安全文件传输的实体之间预先建立的关系已经存在,尤其是涉及与文件传输责任相关的法律和商业等方面。

本标准适用于零售银行业务中不同类型的文件传输,但不包括 ISO 8583 中涉及的交易报文。

文件传输必须要求时效性,并且至少需要符合下列安全服务要求之一:

——报文源鉴别;

——接收方鉴别;

——完整性;

——机密性;

——信息源的不可否认性;

——接收的不可否认性;

——可审计性。

假设在传输前发起方传送的全部数据的合法性和正确性已经确认。

不同类型的传输文件可包括:

——软件;

——已经执行和注册的零售交易(上载);

——与收单机构相关的技术数据(存取参数)(下载);

——与收单机构相关的应用数据(BIN 列表、黑名单)(下载)。

该类文件传输的特点:

a)　传输的数据类型可以是:

——非保密数据(零售交易、技术类数据和应用数据的集合);

——保密数据。

b)　可以接收数据的实体数量:

——一个;

——多于一个(甚至向数千的接收者广播)。

c)　通讯通路可以包括以下一个或全部:

——电信:公用网络、专用网络。

d)　该类传输的方式是:

——直接连接、实时传输(电路交换);

——存储转发传送(报文交换)。

注:本标准考虑到了传输过程中的安全服务要求。确保文件传输完成之后不被更改的要求不在本标准的范围之内。