GB

国家标准汇编

2006年 修订-22

中 国 国 家 标 准 汇 编

2006 年修订-22

中国标准出版社　编

中 国 标 准 出 版 社
北　京

图书在版编目（CIP）数据

中国国家标准汇编：2006年修订．22/中国标准出版社编．—北京：中国标准出版社，2007

ISBN 978-7-5066-4597-3

Ⅰ．中… Ⅱ．中… Ⅲ．国家标准-汇编-中国-2006

Ⅳ．T-652.1

中国版本图书馆CIP数据核字（2007）第105014号

中国标准出版社出版发行

北京复兴门外三里河北街16号

邮政编码：100045

网址 www.spc.net.cn

电话：68523946 68517548

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 38.5 字数 1 149 千字

2007年8月第一版 2007年8月第一次印刷

*

定价 180.00 元

ISBN 978-7-5066-4597-3

9 787506 645973 >

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集，自1983年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。《汇编》在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2. 由于标准的动态性，每年有相当数量的国家标准被修订，这些国家标准的修订信息无法在已出版的《汇编》中得到反映。为此，自1995年起，新增出版在上一年度被修订的国家标准的汇编本。

3. 修订的国家标准汇编本的正书名、版本形式、装帧形式与《中国国家标准汇编》相同，视篇幅分设若干册，但不占总的分册号，仅在封面和书脊上注明“2006年修订-1，-2，-3……”等字样，作为对《中国国家标准汇编》的补充。读者配套购买则可收齐前一年新制定和修订的全部国家标准。

4. 修订的国家标准汇编本的各分册中的标准，仍按顺序号由小到大排列(不连续)；如有遗漏的，均在当年最后一分册中补齐。

5. 2006年度发布的修订国家标准分27册出版。本分册为“2006年修订-22”，收入新修订的国家标准34项。

中国标准出版社

2007年6月

目　　录

ICS 35.240.15
A 11

中华人民共和国国家标准

GB/T 16790.5—2006/ISO 10202-5:1998

金融交易卡 使用集成电路卡的金融交易系统的安全体系 第5部分:算法应用

Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards—Part 5:Use of algorithms

(ISO 10202-5:1998,IDT)

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

前　言

GB/T 16790《金融交易卡　使用集成电路卡的金融交易系统的安全体系》分成以下 8 个部分：

——第 1 部分：卡生命周期

——第 2 部分：交易过程

——第 3 部分：密钥关系

——第 4 部分：安全应用模块

——第 5 部分：算法应用

——第 6 部分：持卡人身份验证

——第 7 部分：密钥管理

——第 8 部分：通用原则及概要

本部分为 GB/T 16790 的第 5 部分。

本部分等同采用 ISO 10202-5:1998《金融交易卡　使用集成电路卡的金融交易系统的安全体系　第 5 部分：算法应用》(英文版)。

为便于使用，本部分删除了 ISO 前言；

本部分的附录 A 到附录 H 均为资料性附录。

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。

本部分主要起草人：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。

本部分为首次制定。

引　言

《金融交易卡　使用集成电路卡的金融交易系统的安全体系》分成以下 8 部分：

——第 1 部分：卡生命周期

——第 2 部分：交易过程

——第 3 部分：密钥关系

——第 4 部分：安全应用模块

——第 5 部分：算法应用

——第 6 部分：持卡人身份验证

——第 7 部分：密钥管理

——第 8 部分：通用原则及概要

本部分描述了可供使用的密码过程，可用来实现第 2、4 和 6 部分定义的需要密码算法的安全功能。

GB/T 16790 可采用对称或非对称算法执行所有安全功能。GB/T 16790 未涉及零点知识技术，该技术可能在以后阶段并入。

参与给定密码过程的每一节点应能执行所要求的密码功能。

执行安全功能所必需的密码过程通过选项进行说明。在每个密码过程中，为每个算法类型规定了一单独选项。还为需要额外通信步骤的密码过程的每个变量规定了一单独选项。

第 5 章将安全功能映射到可用来实现这些安全功能的密码过程。

第 6 章规定了密码过程细节，本部分不是实施规格说明书，但它确实指出了为确保按照要求的安全程序完成密码过程双方节点所需的那些数据元素。

金融交易卡　使用集成电路卡的金融交易系统的安全体系　第5部分:算法应用

1　范围

本部分适用于密码交换,其中至少一个节点是IC卡(集成电路卡)或SAM,其他系统节点之间的交换不属于本部分的范围。

任何安全功能的规定均是可选的,其使用取决于系统要求。需要采用的功能应以本部分说明的方法实行。

2　规范性引用文件

下列文件中的条款通过GB/T 16790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 15851—1995　信息技术　安全技术　带消息恢复的数字签名方案(idt ISO/IEC 9796:1991)

GB/T 16790.1—1997　金融交易卡　使用集成电路卡的金融交易系统的安全结构　第1部分:卡的生命周期(idt ISO 10202-1:1991)

GB/T 16790.6　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第6部分:持卡人身份验证(GB/T 16790.6—2006,ISO 10202-6:1994,IDT)

GB/T 16790.7　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第7部分:密钥管理(GB/T 16790.7—2006,ISO 10202-7,1998,IDT)

ISO 4909　银行卡　第3磁道数据内容

ISO 9564-1　银行业务　个人识别码管理和安全　第1部分:PIN保护原理和技术

ISO 10202-2　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第2部分:交易过程

ISO 10202-3　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第3部分:密钥关系

ISO 10202-4　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第4部分:安全应用模块

ISO 10202-8　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第8部分:通用原则及概要

3　术语和定义

下列术语和定义适用于本部分。

3.1

非对称算法　asymmetric algorithm

一种加密密钥和解密密钥不同的算法,并且对于该算法不能由一个密钥计算推导出另一个密钥。

3.2

证书　certificate

见3.24“公钥证书”。

3.3

证书标识符 certificate identifier

能够正确验证密钥证书的证书信息。

3.4

密文 ciphertext

加密的明文。

3.5

抗冲突性 collision resistant

任何两个不同的输入值均产生不同的输出结果的功能被称为“抗冲突性”。

3.6

凭证 credentials

指定给每一实体并用于对实体进行认证的数据项集。

3.7

密码链 cryptographic link

预先同意交换数据并具有密钥关系的两个逻辑实体(节点)。

3.8

密码节点 cryptographic node

密码链中的一个逻辑实体(节点)。

3.9

解密 decipherment

将密文转换成明文的过程。

3.10

数字签名 digital signature

发起者使用非对称算法中的私钥执行密码转换的结果,提供数据源的不可否认性和签名数据的完整性。

3.11

唯一识别名称 distinguishing name

在一次过程中唯一标识一个实体的名称。

3.12

加密 encipherment

将明文转换成密文的过程。

3.13

实体鉴别 entity authentication

确认实体(节点)的身份是其所声称的身份。

3.14

显式密钥标识符 explicit key identifier

见 3.18“密钥标识符”。

3.15

散列/哈希函数 hash-function

将位串映射为定长位串的函数,它具有以下两个特性:

——对于一个给定的输出不可能推导出与之相对应的输入。

——对于一个给定的输入不可能推导出第 2 个具有同一输出的输入。

注 1:该主题的文献资料包括与哈希函数有相同或类似意义的各种术语。压缩编码和凝聚函数即为部分实例。

注 2:计算可行性取决于用户特定安全要求和环境。

3.16

发起者 initiator

开始某一过程的节点或实体。

3.17

密钥 key

与密码算法连用，执行密码转换的参数。

3.18

密钥标识符 key identifier

使接收者可以确定与某交易相关联的适当密钥的密钥信息。

3.19

报文鉴别 message authentication

提供证明报文未以非授权的方式被更改或破坏的报文密码证据过程。

3.20

报文鉴别码 MAC，message authentication code

其内容可用于验证报文或选定报文元素的完整性的数据域。

3.21

不可否认性 non-repudiation

均以不可伪造的关系对数据完整性和起源提供永久密码证据的安全服务，第三方可以随时进行验证。

3.22

单向函数 one-way function

一种数学函数，它将输入值以不可逆的方式映射为输出值。

3.23

明文 plaintext

有意义的、不经转换即可阅读或操作的可理解数据。

3.24

公钥证书 public key certificate(证书，certificate)

一组由用户凭证(包括公钥)连同可信第三方对这些凭证的数字签名组成的集合。

3.25

反射攻击 reflection attack

由假冒响应者发起的攻击，由此攻击者在一单独的对话中，用相同的随机值向发起者发起质询，该随机值与在并发的会话中发起者已经发出用来鉴别真实响应者的值相同。

3.26

响应者 respondent

对一过程的发起者作出响应的节点或实体。

3.27

对称算法 symmetric algorithm

用相同的保密密钥进行加密和解密的一种密码方法。

3.28

时效性 timeliness

一种防止有效报文在以后的时间被重放的方法，例如采用信息探针作为质询请求，要求正确和及时

的响应。

3.29

令牌 token

为一个实体向另一个实体发送的每次数据交换而形成的一组数据项。

3.30

交易认证码 transaction certification code

交易认证过程产生电子签名的结果，该结果可以是 MAC(基于对称算法)，或者是数字签名(基于非对称算法)。

3.31

交易认证 transaction certification

提供交易数据起源和完整性的密码证据的过程，该过程可由第三方进行验证。

3.32

可信第三方 trusted third party

被通信实体了解并信任的通常可访问的实体。

4 符号

本部分全文中使用了以下符号：

4.1 值和实体

值和实体采用斜体字：

A	实体 A 的唯一名。
$Cert_x$	实体 X 的证书。
CID_x	实体 X 的证书标识符(参见附录 B)。
$Cred_x$	实体 X 的凭证(参见附录 A)。
k_x	与实体 X 相关的密钥(K_x，S_x，P_x)。
K_x	与实体 X 相关的，用于对称算法的密钥。
KID_{kx}	实体 X 的密钥 k 的显式密钥标识符(参见附录 B)。
KID_{Px}	实体 X 的密钥对 S_x/P_x 的显式密钥标识符(参见附录 B)。
$PBF0$	符合 ISO 9564-1 规定的 PIN 分组格式 0。
$PBF1$	符合 ISO 9564-1 规定的 PIN 分组格式 1。
Rx	实体 X 发布的随机值。
S_x/P_x	与实体 X 相关的、用于非对称算法的公私密钥对。
TP	可信第三方的唯一名。
T_{val}	凭证有效期。
T_x	实体 X 发布的时间戳。
$Z//Z^*$	位串 Z 和 Z^* 的连接。
$<>\|<>$	域分隔。

4.2 过程

过程标识符采用大写字母：

EA	实体鉴别
KE	密钥交换
MA	报文鉴别
ME	报文加密/解密
PV	PIN 验证

TC　　交易认证

4.3 选项列表

选项标识符采用小写字母：

a　　非对称

s　　对称

m　　双向

t　　时效

4.4 函数

函数标识符采用小写字母的斜体字：

c　　比较

d　　解密

e　　加密

g　　产生随机值

h　　哈希

m　　鉴别报文

o　　应用单向函数

s　　签名

v　　验证

函数符号与密钥值和实体标记结合使用。

$c(Y,Z)$　　两个位串 Y 和 Z 的比较，结果为状态代码。

$dK(Z)$　　由对称算法使用密钥 K，对数据 Z 的解密。

$dS_x(Z)$　　由非对称算法使用保密密钥 S_x，对数据 Z 的解密。

$eK(Z)$　　由对称算法使用密钥 K，对数据 Z 的加密。

$eP_x(Z)$　　由非对称算法使用公开密钥 P_x，对数据 Z 的加密。

$R=g()$　　随机值 R 的生成。

$h(Z)$　　抗冲突的单向函数的应用，使用公开参数(哈希)将数据项 Z 映射到固定长度的输出值，哈希结果是 $h(Z)$。

$mK(Z)$　　使用作为单向函数的对称算法通过密钥 K 产生报文鉴别码(MAC-ing)；结果是报文鉴别码 MAC。

$vK(MAC)$　　使用作为单向函数的对称算法通过密钥 K 验证 MAC，结果是状态码。

$oK(Z)$　　单向函数的应用，使用算法通过保密密钥 K 将数据 Z 映射为固定长度的输出值。

$sS_x(Z)$　　使用保密密钥 S_x 将数字签名用于数据 Z(签字)，结果是签名 Sig。

$vP_x(Sig)$　　使用公开密钥 P_x 对 Sig 的验证过程，结果是状态码。

4.5 数字签名

传输未签名的 Z(待传送数据)是强制性的，除非当使用带报文恢复的数字签名方案(见 GB 15851—1995)时。这种情况下，签名的数据要组成其结构参数可被验证并且可以从中恢复出 Z 的形式。这要求 Z 足够短并且非对称算法可逆。

整个本部分中，符号 $sS_A(Z)$ 同时用于带数据恢复的签名或使用哈希函数的签名，这意味 $sS_A(Z)$ 既可代表 $sS_A(Z)$ 又可代表 $sS_A(h(Z))//Z$，其中 $h(Z)$ 可以指 Z。

4.6 安全报文格式

安全报文是标准化安全功能的逻辑命令。这些安全报文的信息可以在 8583 报文中与 IC 卡(集成电路卡)相关的域中传输，或者由 SAM 或应用程序解释，产生适合于 IC 卡的命令。

安全报文标识如下：

报文指示器：　　逻辑报文标识符;以下元素的连接：

过程:过程标识符(见 4.2)

选项列表:选项标识符列表(见 4.3)

号码:报文序列号

示例:KEss1

安全报文包括一个或多个安全报文子域。必选子域使用粗体字。在每个报文中<操作>子域至少出现一次。

报文子域:<发起者>|<响应者>|<操作>|<操作>

<发起者>:源实体的唯一名

<响应者>:目标实体的唯一名

<操作>=<Z>|<KID>|<f(Z)>

<Z>:可选的数据字段

<KID>:密钥标识符

<f(Z)>:数据 Z 进行函数 f 运算的结果(见第 4.4)

示例:$A \mid B \mid KID_K \mid KID_K^* \mid e K^*(KID_K^*) \mid eK(K^*)$

5 安全功能到过程类型的映射

ISO 10202-2、10202-4 和 GB/T 16790.6 定义的安全功能到过程类型集的映射见表 1。

表 1　安全功能对过程类型的映射

安全功能	过程类型		密　钥
IC 卡(集成电路卡)制造加工			
制造加工 嵌入和初始化	初始密钥装载 初始密钥装载		$kMprd_{M\text{-}P}$ $kEprd_{E\text{-}P}$
IC 卡个性化			
个性化	初始密钥装载		$kIctl_{I\text{-}C}$
卡会话初始化			
IC 兼容性检查	非密码过程		
CDF 参数更新			
CDF(激活/停用/再激活/终止) ADF 分配	密钥交换 密钥交换	KE KE	$kIctl_{I\text{-}C}$ $kIctl_{I\text{-}C}$
CDF 特定鉴别和验证			
持卡人验证 CDF 静态鉴别 CDF 动态鉴别 发卡行主机动态鉴别	PIN 验证 实体鉴别 实体鉴别 实体鉴别	PV EA EA EA	$kIenc_{I\text{-}C}$ [1)] $kIaut_I$ $kIaut_C$ $kIaut_{I\text{-}C}$
CDF 交易处理			
交易授权 数据保密性 交易认证	报文鉴别 报文加密 交易认证	MA ME TC	$kImac_{I\text{-}C}$ $kIenc_{I\text{-}C}$ [1)] $kIcer_{I\text{-}C}$

表 1(续)

安全功能	过程类型		密　钥
ADF 选择			
ADF 选择	非密码过程		
ADF 参数更新			
ADF $KActl_{A\text{-}C}$ 装载	密钥交换	KE	$kIkex_{I\text{-}A}$
ADF 激活/停用/再激活/终止	密钥交换	KE	$kActl_{A\text{-}C}$
ADF 特定鉴别和验证			
持卡人验证	PIN(个人身份标识号)验证	PV	$kAenc_{A\text{-}C}$ [2]
ADF 静态鉴别	实体鉴别	EA	$kAaut_{A}$
ADF 动态鉴别	实体鉴别	EA	$kAaut_{C}$
SAM 鉴别	实体鉴别	EA	$kAaut_{SC}$
应用供应商鉴别	实体鉴别	EA	$kAaut_{A\text{-}C}$
ADF 交易处理			
交易授权	报文鉴别	MA	$kAmac_{A\text{-}C}$
数据保密性	报文加密	ME	$kAenc_{A\text{-}C}$ [2]
交易认证	交易认证	TC	$kAcer_{A\text{-}C}$
卡会话终止			
卡会话终止	非密码过程		

1) 根据发卡行的判断,可以单独生成或导出这些密钥。

2) 根据提供者的判断,可以单独生成或导出这些密钥。

6 过程规范

本章规定了可用于不同安全功能的过程。每个过程可独自使用或根据需要与其他的过程结合使用。

每个过程均允许使用多个选项,它们防范不同的威胁,例如侦听、伪装、重放、篡改或否认。选项的选择应基于对来自具体环境中威胁的风险分析。有关该章的详细指南参见附录 H。

当要求保证报文是唯一的并且/或者是在特定的时间发送时,这些过程要包括提供时效性的选项。实现时效性的不同方法参见附录 E。

在实体鉴别中,时效性是固有的,与这样的过程结合则自动保证时效性。

如果密码过程建立在对称算法基础上,该过程必需的保密密钥应同时在两个参与节点建立。如果属于同一组的两个以上实体之间共享保密密钥,在这些实体之间加以区分是密码方法不可能做到的。

如果加密过程建立在非对称算法基础上,就应在每个节点生成密钥信息,保密密钥应在该节点以安全的方法存储,并且对应的公开信息应由提供证书的可信第三方进行鉴别(参见附录 A)。

目标节点上的报文的所有数据元必须被了解,以便能执行过程中的下一步骤。在过程期间,如果动态生成数据元,其传输就是强制性的。如果数据元已为目标节点所知,其传输就可以省略。

用黑体字印刷的操作和参数是强制性的。所有强制使用的元素均在图中用箭头表示。角色中描述的可选步骤并不总是与图中描述的步骤直接对应。

6.1 过程 1:密钥交换(KE)

发往或来自集成电路卡或 SAM 的密钥 K 或 S_B 的安全电子传输应依据本章说明的选项之一执行。假设发起者和响应者之间已建立密码链。