GB

中国国家标准汇编

456

GB 25057~25077

（2010年制定）

中国质检出版社
中国标准出版社

中 国 国 家 标 准 汇 编

456

GB 25057～25077

（2010 年制定）

中国标准出版社　编

中国质检出版社
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：2010 年制定. 456：GB 25057～25077/中国标准出版社编. —北京：中国标准出版社，2012
ISBN 978-7-5066-6473-8

Ⅰ. ①中… Ⅱ. ①中… Ⅲ. ①国家标准-汇编-中国-2010 Ⅳ. ①T-652.1

中国版本图书馆 CIP 数据核字(2011)第 187729 号

中国质检出版社
中国标准出版社 出版发行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址：www.spc.net.cn
总编室：(010)64275323 发行中心：(010)51780235
读者服务部：(010)68523946
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 字数 1 054 千字
2012 年 1 月第一版 2012 年 1 月第一次印刷
*
定价 220.00 元

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。它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.《中国国家标准汇编》收入我国每年正式发布的全部国家标准，分为“制定”卷和“修订”卷两种编辑版本。

“制定”卷收入上一年度我国发布的、新制定的国家标准，顺延前年度标准编号分成若干分册，封面和书脊上注明“20××年制定”字样及分册号，分册号一直连续。各分册中的标准是按照标准编号顺序连续排列的，如有标准顺序号缺号的，除特殊情况注明外，暂为空号。

“修订”卷收入上一年度我国发布的、修订的国家标准，视篇幅分设若干分册，但与“制定”卷分册号无关联，仅在封面和书脊上注明“20××年修订-1，-2，-3，……”字样。“修订”卷各分册中的标准，仍按标准编号顺序排列（但不连续）；如有遗漏的，均在当年最后一分册中补齐。需提请读者注意的是，个别非顺延前年度标准编号的新制定的国家标准没有收入在“制定”卷中，而是收入在“修订”卷中。

读者配套购买《中国国家标准汇编》“制定”卷和“修订”卷则可收齐上一年度我国制定和修订的全部国家标准。

3. 由于读者需求的变化，自1996年起，《中国国家标准汇编》仅出版精装本。

4. 2010年我国制修订国家标准共2846项。本分册为“2010年制定”卷第456分册，收入国家标准GB 25057～25077的最新版本。

中国标准出版社

2011年8月

目　　录

ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25057—2010

信息安全技术 公钥基础设施 电子签名卡应用接口基本要求

Information security techniques—Public key infrastructure—Specification of application interface of electronic signature card

2010-09-02 发布　　2011-02-01 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

本标准是为了配合《中华人民共和国电子签名法》的实施，在广泛征求意见的基础上，对GB/T 16649系列标准进行部分引用和扩展。

本标准的附录A为规范性附录，附录B、附录C、附录D为资料性附录。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：北京飞天诚信科技有限公司，中国电子技术标准化研究所，国家信息安全工程技术研究中心。

本标准主要起草人：于华章，周葵亮，朱鹏飞。

引　言

《中华人民共和国电子签名法》规定，电子签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。具有生成电子签名功能的安全客户端载体，简称电子签名卡。

数字签名是目前主要的电子签名形式之一。相应地，具有数字签名功能的集成电路卡是目前主要的电子签名卡类型之一。GB/T 16649 系列标准对集成电路卡进行了规定。然而，数字签名与电子签名的范畴并不相同，而电子签名卡也不仅限于集成电路卡。

为了避免技术细节对《中华人民共和国电子签名法》的实施造成干扰，规范电子签名卡的应用接口，制定本标准。旨在定义和规范一个能够完成电子签名应用的最小指令集合。

本标准在 GB/T 16649 系列标准的基础上进行部分引用和扩展。

本标准中给出的 SHA-1、RSA 等密码算法均为举例性说明，具体使用时均须采用国家密码管理部门批准的相应算法。

信息安全技术　公钥基础设施
电子签名卡应用接口基本要求

1　范围

本标准规定了电子签名卡的基本命令报文和相应的响应报文，以及电子签名卡的文件组织结构。

本标准适用于规范和指导电子签名卡的开发，规范和指导与电子签名卡进行通信，访问卡内文件，应用私钥生成电子签名的应用系统的开发。

本标准不适用于在电子签名卡内创建文件或使用公钥的应用系统的开发。

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 16649.8　识别卡　带触点的集成电路卡　第8部分：与安全相关的行业间命令(GB/T 16649.8—2002，ISO/IEC 7816-8:1999，IDT)

ISO/IEC 7816-4:2005　识别卡　带触点的集成电路卡　第4部分：行业间交换的组织结构、安全性和命令(ISO/IEC 7816-4:2005 Identification cards—Integrated circuit cards with contacts—Part 4: Organization, security and commands for interchange)

ISO/IEC 7816-15:2004　识别卡　带触点的集成电路卡　第15部分：密码信息的应用(ISO/IEC 7816-15:2004 Identification cards—Integrated circuit cards with contact—Part 15: Cryptographic information application)

3　术语和定义

下列术语和定义适用于本标准。

3.1

应用　application

为满足特定功能所需的数据结构、数据元和程序模块。

[ISO/IEC 7816-4:2005]

3.2

电子签名卡　electronic signature card

具有生成电子签名功能的安全客户端载体，简称电子签名卡。

3.2

报文　message

应用发送给电子签名卡(或反之)的字节串，不包括传输控制字符。

3.3

命令　command

应用向电子签名卡发出的一条字节串，该信息启动一个操作或请求一个应答。

3.4

响应　response

电子签名卡处理完收到的命令报文后，返回给终端的字节串。

3.5

安全环境　security environment

应用被选定后，电子签名卡所确定的逻辑条件，如密钥，密钥参数，算法标识等。

3.8

路径　path

无定界的文件标识符的链接。

[ISO/IEC 7816-4:2005]

3.9

绝对路径　absolute path

以文件标识符'3F00'开始的路径。

[ISO/IEC 7816-4:2005]

3.10

相对路径　relative path

以当前 DF 文件标识符开始的路径。

[ISO/IEC 7816-15:2004]

3.11

CLA

命令报文的第一个字节，代表该命令所属的类别。

3.12

INS

命令报文的第二个字节，代表该命令在所属类别中的索引。

3.13

P1

命令报文的第三个字节，代表该命令的第一个参数。

3.14

P2

命令报文的第四个字节，代表该命令的第二个参数。

3.15

Lc

命令报文的第五个字节(如果存在)，代表数据域的长度。

3.16

Le

命令报文的最后一个字节(如果存在)，代表期望返回的数据长度。

3.17

SW1-SW2

响应报文的前两个字节，代表命令状态码。

3.18

DER

一种数据编码方法。

3.19

RSA

一种用于电子签名和解密的非对称算法。

3.20

私钥 private key

非对称算法中不公开的密钥。

3.21

SHA-1

一种用于散列的不可逆算法。

3.22

RSAES-PKCS1-v1_5

用 RSA 算法进行解密，根据 PKCS#1v1.5 规范去除填充数据的算法。

3.23

RSASHA-PKCS1-v1_5

用 SHA-1 算法进行散列，根据 PKCS#1v1.5 规范填充数据，用 RSA 计算电子签名的算法。

4 缩略语

下列缩略语适用于本标准。

AID	应用标识符（Application ID）
AM	访问模式（Access Mode）
AODF	鉴别对象目录文件（Authentication Object Directory File）
AT	应用模板（Application Template）
CDF	证书目录文件（Certificate Directory File）
CRDO	控制引用数据对象（Control Reference Data Object）
DF	专用文件（Dedicated File）
DODF	数据对象目录文件（Data Object Directory File）
DT	解密模版（Decryption Template）
EF	基本文件（Elementary File）
EST	电子签名模版（Electronic Signature Template）
FCI	文件控制信息（File Control Information）
FCP DO	文件控制参数数据对象（File Control Parameter Data Object）
FID	文件标识符（File ID）
MF	主文件（Master File）
ODF	对象目录文件（Object Data File）
PIN	个人验证码（Personal Identification Number）
PrKDF	私钥目录文件（Private Key Directory File）
RFU	为将来使用保留（Reserved for Future Use）
SC	安全条件（Security Condition）
SFID	短文件标识符（Short File ID）
SM	安全报文传输（Secure Messaging）

5 命令接口

5.1 命令综述

本标准规定，电子签名卡支持表 1 所示的命令。

表 1　电子签名应用相关的命令

命　令	引用标准	命令功能
SELECT FILE	ISO/IEC 7816-4	选择一个文件
GET RESPONSE	ISO/IEC 7816-4	获取响应报文
READ BINARY	ISO/IEC 7816-4	读取二进制文件的内容
WRITE BINARY	ISO/IEC 7816-4	写二进制数据到文件
VERIFY PIN	ISO/IEC 7816-4	验证 PIN
MANAGE SECURITY ENVIRONMENT (MSE): **RESTORE**	GB/T 16649.8	恢复预定义的安全环境
MANAGE SECURITY ENVIRONMENT (MSE):**SET**	GB/T 16649.8	设置安全环境
PERFORM SECURITY OPERATION: **HASH**	GB/T 16649.8	散列
PERFORM SECURITY OPERATION (PSO): **COMPUTE ELECTRONIC SIGNATURE**	GB/T 16649.8	计算电子签名
PERFORM SECURITY OPERATION (PSO): **DECIPHER**	GB/T 16649.8	解密
CHANGE REFERENCE DATA	GB/T 16649.8	修改引用数据
GENERATE KEY PAIR	GB/T 16649.8	生成密钥对

响应报文中的命令状态码参见附录 C。

5.2　选择文件

选择文件(SELECT FILE)命令通过 FID、路径或 AID 来选择电子签名卡中已有的文件。命令报文和响应报文分别如表 2、表 3 所示。

表 2　SELECT File 命令报文

代　码	值
CLA	'00'
INS	'A4'
P1	'00'——根据 FID 选择文件 '04'——根据 AID 选择应用 '08'——根据绝对路径选择文件 '09'——根据相对路径选择文件
P2	'00'——返回 FCI P1='04'时,'00'为选择当前应用; '02'选择下一个应用;
Lc	数据域字节长度

表 2（续）

代　码	值
数据域	P1 = ‘00’ ——FID P1 = ‘08’ ——绝对路径 P1 = ‘09’ ——相对路径 P1 = ‘04’ ——AID
Le	期望返回的 FCI 字节长度或不存在

表 3　SELECT FILE 响应报文

数　据	值
数据域	FCI 或不存在
SW1-SW2	命令状态码

5.3　获取响应

获取响应（GET RESPONSE）命令用于在必要时强制获取响应报文（或报文的一部分）。命令报文和响应报文分别如表 4、表 5 所示。

表 4　GET RESPONSE 命令报文

代　码	值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
数据域	不存在
Le	期望的返回数据最大长度

表 5　GET RESPONSE 响应报文

数　据	值
数据域	返回的数据
SW1-SW2	命令状态码

5.4　二进制读

二进制读（READ BINARY）命令从当前所选择的文件中读取连续的二进制字节。命令报文和响应报文分别如表 6、表 8 所示。

表 6　READ BINARY 命令报文

代　码	值
CLA	'00'
INS	'B0'
P1	见表 7
P2	见表 7
Lc	不存在
数据域	不存在
Le	期望读取的字节数

表 7　P1、P2 参数

b8　b7　b6　b5	b4　b3　b2　b1	说　明
0　-　-　-	-　-　-　-	P1-P2 指定 15 位偏移量
1　-　-　-	-　-　-　-	P1 指定文件的 SFID,P2 指定偏移量
1　0　0　x	x　x　x　x	文件的 FID

表 8　READ BINARY 响应报文

数　据	值
数据域	读取的数据
SW1-SW2	命令状态码

5.5　二进制写

二进制写(WRITE BINARY)该命令把二进制数据写入当前所选择的文件。

命令报文和响应报文分别如表 9、表 10 所示。

表 9　WRITE BINARY 命令报文

代　码	值
CLA	'00'
INS	'D0'
P1	见表 7
P2	见表 7
Lc	数据域字节长度
数据域	需要写入的数据字节
Le	不存在

表 10　WRITE BINARY 响应报文

数　据	值
数据域	不存在
SW1-SW2	命令状态码

5.6 验证 PIN

验证 PIN(VERIFY PIN)命令用送入卡内的 PIN 与卡内存储的引用数据进行比较。命令报文和响应报文分别如表 11、表 13 所示。

表 11 VERIFY PIN 命令报文

代 码	值
CLA	'00'
INS	'20'
P1	'00'
P2	PIN 的属性,见表 12
Lc	不存在或数据域字节长度
数据域	不存在或者验证数据
Le	不存在

表 12 P2 的编码

P2 的编码		
b8 b7 b6 b5	b4 b3 b2 b1	含义
0		全局的 PIN
1		当前 DF 的 PIN
— x x x	X	'0000'(其他的值保留)
— — — —	— x x x	PIN 编号(引用 ISO/IEC 7816-15:2004)
— — — —	— 0 0 0	RFU

表 13 VERIFY 响应报文

数 据	值
数据域	不存在
SW1-SW2	命令状态码

5.7 安全环境:恢复

安全环境:恢复(MANAGE SECURITY ENVIRONMENT:RESTORE)命令恢复一个安全环境。命令报文和响应报文分别如表 14、表 15 所示。

表 14 MANAGE SECURITY ENVIRONMENT:RESTORE 命令报文

代 码	值
CLA	'00'
INS	'22'
P1	'F3'
P2	安全环境索引(引用 GB/T16649.8)
Lc	不存在
数据域	不存在
Le	不存在

表 15 MANAGE SECURITY ENVIRONMENT:RESTORE 响应报文

数 据	值
数据域	不存在
SW1-SW2	命令状态码

5.8 安全环境:设置

安全环境:设置(MANAGE SECURITY ENVIRONMENT:SET)在当前的安全环境中设置属性。命令报文和响应报文分别如表 16、表 17 所示。

表 16 MANAGE SECURITY ENVIRONMENT:SET 命令报文

代 码	值
CLA	'00'
INS	'22'
P1	'41'
P2	'B6'——设置电子签名安全环境 'B8'——设置解密安全环境
Lc	不存在或数据域字节长度
数据域	不存在或电子签名模版或解密模版
Le	不存在

表 17 MANAGE SECURITY ENVIRONMENT:SET 响应报文

数 据	值
数据域	不存在
SW1-SW2	命令状态码

表 18 描述了在电子签名模版(EST)和解密模版(DT)中引用的控制引用数据对象(CRDO)。表 19 描述了 P1 和 P2 的可选组合,以及各种组合的含义。

表 18 CRDO

标签(Tag)	值(Value)	DST	CT
80h	算法标识	+	+
81h	文件标识符或路径	+	+

表 19 P1-P2 的组合

支持 P1-P2 组合				
P1	P2	含义	数据域中的模版	数据字段内容
'41'	'B6'	设置电子签名安全环境	EST	'8001xx8102xxxx'
'41'	'B8'	设置解密安全环境	DT	'8001xx8102xxxx'

算法标识引用(Tag = 80h)在表 20 中指定。算法引用的高四位指定散列算法(如果散列操作是与算法相关的),低四位指定关于算法的细节部分。