ICS xx.xxx.xx
Lxx

中华人民共和国国家标准

GB/T AAAA—2008

公钥密码基础设施应用技术体系
标识规范 V1.0

Public Key Infrastructure Application Technology

Identifier Criterion V1.0

（报批稿）

2008-××-××发布　　2008-××-××实施

国家质量监督检验检疫总局 发布

目　次

前　言

本规范是《公钥密码基础设施应用技术体系 框架规范》下的系列规范之一，用于规范算法标识、密钥标识、设备标识、数据标识、协议标识、角色标识等的表示和使用。

本规范的附录 A 是规范性附录，附录 B 是资料性附录。

本规范由国家密码管理局提出并归口。

本规范主要起草单位：山东得安信息技术有限公司，成都卫士通信息产业股份公司，无锡江南信息安全工程技术中心，兴唐通信科技股份有限公司，上海格尔软件股份有限公司，北京数字证书认证中心，万达信息股份有限公司，长春吉大正元信息技术股份有限公司，海泰方圆科技有限公司，上海数字证书认证中心。

本规范主要起草人：刘晓东、商建伟、李元正、徐强、柳增寿、李述胜、谭武征、李玉峰、李伟平、崔久强、周栋。

本规范责任专家：刘平。

本规范凡涉及密码算法相关内容，按国家有关法规实施。

引　言

在密码应用中，通常使用某一字段或短语来表示所使用的密码算法或数据实体等信息数据，如果不对这些标识的定义进行统一，则很难做到密码协议、密码接口间的互联互通。

本规范的目标就是规范密码协议接口、管理等各方面使用的标识，以实现密码基础设施各组件间的兼容和统一，也能够有效的指导、帮助密码设备的研制和协议的实现，有利于管理部门实施有效管理。

本规范编制过程中得到了国家商用密码应用技术体系总体工作组的指导。

公钥密码基础设施应用技术体系 标识规范

1 范围

本规范规定了公钥密码基础设施应用技术体系中各规范所使用的标识的定义，以及对标识的管理办法。

本规范适用于指导密码设备、密码系统的研制和使用过程中，对标识进行规范化的使用和管理，也可用于指导其他相关规范或协议的编制中对标识的使用和管理。

在基于公钥密码基础设施技术应用体系框架下的系列规范开发的密码服务接口、密码应用接口、设备管理接口中，应使用本规范定义的标识。

在自定义接口、密码设备内部的模块调用或审计等接口的实现时，推荐使用本规范定义的标识。

2 规范性引用文件

下列文件中的条款通过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/T AAAA 信息技术 安全技术 密码术语

GB/T BBBB 公钥密码基础设施应用技术体系 框架规范

JR/T 0025.1-2005 中国金融集成电路（IC）卡规范

3 术语和定义

下列术语仅适用于本规范。

3.1

非对称密码算法 asymmetric cryptographic algorithm

在执行加密或与之相应的解密中，加密密钥和解密密钥不相同且不能简单的相互推导的密码算法。

3.2

属性证书 attribute certificate

一种轻量级的数字证书，一般有效期较短，用于提供用户权限信息的证明，属性证书中包含公钥证书标志，通过该标志可以找到对应的公钥证书。

3.3

密文 ciphertext

加密后的数据。

3.4

明文 clear text/plain text

待加密的数据。

3.5

分隔密钥 compartment key

用于划分系统，使不同系统之间不能互联互通的密钥。

3.6

设备密钥 device key pair

存储在设备内部的用于设备管理的非对称密钥对。

3.7

设备编号 device serial number

设备标签上的产品序号，是由生产日期、生产批次、流水号组成的一串数字编号，与设备型号组合使用可唯一标识某一密码设备。

3.8

设备型号 device type

国家密码管理机构批准使用的密码产品型号。

3.9

杂凑值 digest data

经过密码杂凑运算得到的数据。

3.10

数字信封 digital envelope

一种数据的封装方式，在该方式下使用数据加密密钥保护数据，使用接收者加密公钥保护数据加密密钥。

3.11

数字签名 digital signature

附加在数据上的签名数据，或是对数据所作的密码变换，用以确认数据来源及其完整性，防止被他人伪造或者签发者否认。

3.12

加密证书 encipherment certificate

用于协商密钥或保护数据的公钥证书。

3.13

杂凑算法 hash algorithm

将一个任意长的比特串映射到一个固定长的比特串的函数，且满足下列两个特性：

（1）为一个给定的输出找出能映射到该输出的一个输入是计算不可行的；

（2）为一个给定的输入找出能映射到同一个输出的另一个输入是计算不可行的。

3.14

标识符 identifier

一个 32 位整数，用于标识在密码服务或密码管理中涉及到的密码算法、密码协议等。

3.15

密钥部件 key component

至少两个随机或伪随机产生的、有密码密钥特点（例如，格式，随机性）的参数之一，其中密码密钥由一个或多个这样的参数组合而成。例如，通过模 2 加的方法形成一个密码密钥。

3.16

密钥分割 key division

将密钥分给多人掌管，并且必须有一定人数的掌管密钥的人同时到场才能恢复密钥。

3.17

密钥加密密钥 key encrypting key

用于对会话密钥或文件密钥进行加密时采用的密钥。又称辅助（二级）密钥(Secondary Key)或密钥传送密钥(key Transport key)。通信网中的每个节点都分配有一个这类密钥。

3.18

密钥索引 key index

在密码设备或安全系统内表示密钥位置的数值。

3.19

标签 label

用于标识在密码服务或密码管理中涉及到的密码算法、密码协议等的一个由由包含‘0’～‘9',‘A’～‘Z',和‘-’等字符串构成的短语。

3.20

口令 password

用于鉴别身份或验证访问授权的字符串。

3.21

签名私钥 private signature key

用于签名计算的私有密钥。

3.22

加密私钥 private encipherment key

用于实现数据保密性的私有密钥。

3.23

私有密钥/私钥 private key

在实体的非对称密钥对中只能由该实体使用的密钥。

3.24

私钥访问控制码 private key access password

用于获取私钥使用权限的口令字。

3.25

加密公钥 public encipherment key

用于加密数据或保护密钥的公开密钥。

3.26

公开密钥/公钥 public key

一个实体的非对称密钥对中规定能够公开的密钥。

3.27

公开密钥（公钥）证书 public key certificate

确立拥有公钥的实体的身份的数字证书（数字身份证）。该证书是由第三方可信机构签名颁发的，证明主体公钥和主体标识信息之间绑定关系的有效性。通常，证书含有与主体有关的不可伪造的公开密钥信息。

3.28

签名公钥 public signature key

用于验证签名有效性的公开密钥。

3.29

随机数 random number

理论上没有规律可循，不可计算、不可预测、不可重复的时变参数。

3.30

对称密钥/秘密密钥 secret key

在采用对称密码技术时，一组特定实体使用的密钥。

3.31

会话密钥 session key

密钥管理中的最低一层密钥，这种密钥只在一次会话和一个受限时间内使用，比如终端上的一次用户会话，完毕就销毁。

3.32

签名证书 signature certificate

用于验证签名有效性的公钥证书。

3.33

对称密码算法 symmetric cryptographic algorithm

加密和解密在算法和密钥上相同或可相互推导的密码算法。

3.34

用户密钥 user key pair

存储在设备内部的用于应用密码运算的非对称密钥对。

4 符号和缩略语

下列缩略语适用于本部分：

Base64　BASE64 编码是一种常用的将十六进制数据转换为可见字符的编码规则，在 RFC 3548 中定义

CBC　密码分组链接模式（Cipher Block Chaining）

CFB　密文反馈模式（Ciphertext Feedback）

CRL　证书撤消列表（Certificate Revocation List）

CSP　密码服务提供者（Cryptographic Service Provider），这里指密码服务接口

DER　唯一编码规则（Distinguished Encoding Rules）

ECB　电码本模式（Electronic Code Book）

IDP　身份提供者（Identity Provider）

KEK　密钥加密密钥（Key Encrypting Key）

MAC　消息鉴别码（Message Authentication Code）

OCSP　在线证书状态协议（Online Certificate Status Protocol）

OFB　输出反馈模式（Output Feedback）

OID　对象标识符（Object Identifier）

PEM　个人增强邮件（Privacy-Enhanced Mail），这里指基于 Base64 编码的一种封装格式

SP　服务提供者（Service Provider）

5 标识的格式和编码

标识符为 32 位无符号整数类型，在密码服务接口或安全管理接口的实现或调用时直接作为整数类型进行定义或处理。

在跨平台传输时，为避免不同平台字节顺序差异带来的影响或错误，应将标识符按照高位字节在前的网络字节顺序（Big-endian）进行处理。

6 密码服务类标识

6.1 概述

密码服务类标识定义了在密码服务设备或密码服务接口中涉及到的密码算法、运算数据、密码协议等项的表示短语和数据，该类数据标识在密码设备或密码服务接口的调用过程

中使用，如数据加密、数字签名、身份鉴别等应用场景。

6.2 算法标识

6.2.1 分组密码算法标识

分组密码算法标识包含密码算法的类型以及分组算法的加密模式，在调用密码服务进行密码操作或在获取密码设备的密码运算能力时使用。

分组密码算法标识的编码规则为：从低位到高位，第 0 位到第 7 位按位表示分组密码算法工作模式，第 8 位到第 31 位按位表示分组密码算法，例如：

SGD_SM1_ECB：0000 0000 0000 0000 0000 0001 0000 0001（0x 00 00 01 01）

SGD_SSF33_MAC：0000 0000 0000 0000 0000 0010 0001 0000（0x 00 00 02 10）

分组密码算法的标识如表 1 所示。

表 1

标签	标识符	描述
SGD_SM1_ECB	0x00000101	SM1 算法 ECB 加密模式
SGD_SM1_CBC	0x00000102	SM1 算法 CBC 加密模式
SGD_SM1_CFB	0x00000104	SM1 算法 CFB 加密模式
SGD_SM1_OFB	0x00000108	SM1 算法 OFB 加密模式
SGD_SM1_MAC	0x00000110	SM1 算法 MAC 运算
SGD_SSF33_ECB	0x00000201	SSF33 算法 ECB 加密模式
SGD_SSF33_CBC	0x00000202	SSF33 算法 CBC 加密模式
SGD_SSF33_CFB	0x00000204	SSF33 算法 CFB 加密模式
SGD_SSF33_OFB	0x00000208	SSF33 算法 OFB 加密模式
SGD_SSF33_MAC	0x00000210	SSF33 算法 MAC 运算
SGD_SMS4_ECB	0x00000401	SMS4 算法 ECB 加密模式
SGD_SMS4_CBC	0x00000402	SMS4 算法 CBC 加密模式
SGD_SMS4_CFB	0x00000404	SMS4 算法 CFB 加密模式
SGD_SMS4_OFB	0x00000408	SMS4 算法 OFB 加密模式
SGD_SMS4_MAC	0x00000410	SMS4 算法 MAC 运算
0x00000400—0x800000xx		为其它分组密码算法预留

6.2.2 非对称密码算法标识

非对称密码算法标识仅定义了密码算法的类型，在使用非对称算法进行数字签名运算时，可将非对称密码算法标识符与密码杂凑算法标识符进行“或”运算后使用，如“RSA with SHA1”可表示为 SGD_RSA | SGD_SHA1，即 0x00010002，“|”表示“或”运算。

非对称密码算法标识的编码规则为：从低位到高位，第 0 位到第 7 位为 0，第 8 位到第 15 位按位表示非对称密码算法的算法协议，如果所表示的非对称算法没有相应的算法协议则为 0，第 16 位到第 31 位按位表示非对称密码算法类型，例如：

SGD_SM2_1：0000 0000 0000 0010 0000 0001 0000 0000（0x 00 02 01 00）

非对称密码算法的标识如表 2 所示。

表 2

标签	标识符	描述
SGD_RSA	0x00010000	RSA 算法

SGD_SM2_1	0x00020100	椭圆曲线签名算法
SGD_SM2_2	0x00020200	椭圆曲线密钥交换协议
SGD_SM2_3	0x00020400	椭圆曲线加密算法
0x00000400～0x800000xx		为其它非对称密码算法预留

6.2.3 密码杂凑算法标识

密码杂凑算法标识符可以在进行杂凑运算或计算 MAC 时应用，也可以与非对称密码算法标识符进行“或”运算后使用，表示签名运算前对数据进行杂凑运算的算法类型。

密码杂凑算法标识的编码规则为：从低位到高位，第 0 位到第 7 位表示密码杂凑算法，第 8 位到第 31 位为 0，例如：

SGD_SM3：0000 0000 0000 0000 0000 0000 0000 0001（0x 00 00 00 01）

密码杂凑算法的标识如表 3 所示。

表 3

标签	标识符	描述
SGD_SM3	0x00000001	SM3 杂凑算法
SGD_SHA1	0x00000002	SHA1 杂凑算法
SGD_SHA256	0x00000003	SHA256 杂凑算法
0x00000010～0x000000FF		为其它密码杂凑算法预留

6.3 数据标识

6.3.1 数据类型

数据类型定义了在公钥密码基础设施技术应用体系下各规范中用到的数据类型标签。

数据类型标签的定义如表 4 所示。

表 4

标签	说明
SGD_CHAR	8 位，有符号字符
SGD_INT8	8 位，有符号字符
SGD_INT16	16 位，有符号整数
SGD_INT32	32 位，有符号整数
SGD_INT64	64 位，有符号整数
SGD_UCHAR	8 位，无符号字符
SGD_UINT8	8 位，无符号字符
SGD_UINT16	16 位，无符号整数
SGD_UINT32	32 位，无符号整数
SGD_UINT64	64 位，无符号整数
SGD_RV	32 位，无符号整数，表示函数返回值
SGD_OBJ	无符号指针类型，表示对象句柄
SGD_BOOL	32 位，有符号整数，表示布尔型

6.3.2 数据常量标识

数据常量标识定义了在公钥密码基础设施技术应用体系下各规范中用到的常量的标签及取值。

数据常量标识的定义如表 5 所示。

表 5

标签	标识符	描述
SGD_TRUE	0x00000001	布尔值为真
SGD_FALSE	0x00000000	布尔值为假

6.3.3 通用数据对象标识

在数据的存储或传输过程中，可能需要对某些数据的特殊性进行明确的标识，以保证目标系统能够对接收数据进行正确的处理。

通用数据标识的编码规则为：从低位到高位，第 0 位到第 7 位表示数据对象的属性，第 8 位为 1，第 9 位到第 31 位为 0，例如：

SGD_USER_DATA：0000 0000 0000 0000 0000 0001 0001 0111（0x 00 00 00 17）

通用数据对象标识的定义如表 6 所示。

表 6

标签	标识符	描述
SGD_KEY_INDEX	0x00000101	密钥索引
SGD_SECRET_KEY	0x00000102	对称密钥
SGD_PUBLIC_KEY_SIGN	0x00000103	签名公钥
SGD_PUBLIC_KEY_ENCRYPT	0x00000104	加密公钥
SGD_PRIVATE_KEY_SIGN	0x00000105	签名私钥
SGD_PRIVATE_KEY_ENCRYPT	0x00000106	加密私钥
SGD_KEY_COMPONENT	0x00000107	密钥部件
SGD_PASSWORD	0x00000108	口令
SGD_PUBLIC_KEY_CERT	0x00000109	公钥证书
SGD_ATTRIBUTE_CERT	0x0000010A	属性证书
SGD_SIGNATURE_DATA	0x00000111	数字签名
SGD_ENVELOPE_DATA	0x00000112	数字信封
SGD_RANDOM_DATA	0x00000113	随机数
SGD_PLAIN_DATA	0x00000114	明文数据
SGD_CIPHER_DATA	0x00000115	密文数据
SGD_DIGEST_DATA	0x00000116	摘要数据
SGD_USER_DATA	0x00000117	用户数据
0x00000118～0x000001FF		为其他数据对象预留

6.3.4 证书解析项标识

在实现身份鉴别、授权管理、访问控制等安全机制时，需要解析证书项以获取公钥证书信息，在这种情况下需要通过标识符指定证书项内容。

证书解析项标识的编码规则为：从低位到高位，第 0 位到第 7 位表示证书解析项的内容，第 8 位到第 31 位为 0，例如：

SGD_EXT_KEYUSAGE_INFO：0000 0000 0000 0000 0000 0000 0001 0011（0x 00 00 00 13）

证书解析项标识的定义如表 7 所示。

表 7

标签	标识符	描述
SGD_CERT_VERSION	0x00000001	证书版本
SGD_CERT_SERIAL	0x00000002	证书序列号
SGD_CERT_ISSUER	0x00000005	证书颁发者信息
SGD_CERT_VALID_TIME	0x00000006	证书有效期
SGD_CERT_SUBJECT	0x00000007	证书拥有者信息
SGD_CERT_DER_PUBLIC_KEY	0x00000008	证书公钥信息
SGD_CERT_DER_EXTENSIONS	0x00000009	证书扩展项信息
SGD_EXT_AUTHORITYKEYIDENTIFIER_INFO	0x00000011	颁发者密钥标示符
SGD_EXT_SUBJECTKEYIDENTIFIER_INFO	0x00000012	证书持有者密钥标示符
SGD_EXT_KEYUSAGE_INFO	0x00000013	密钥用途
SGD_EXT_PRIVATEKEYUSAGEPERIOD_INFO	0x00000014	私钥有效期
SGD_EXT_CERTIFICATEPOLICIES_INFO	0x00000015	证书策略
SGD_EXT_POLICYMAPPINGS_INFO	0x00000016	策略影射
SGD_EXT_BASICCONSTRAINTS_INFO	0x00000017	基本限制
SGD_EXT_POLICYCONSTRAINTS_INFO	0x00000018	策略限制
SGD_EXT_EXTKEYUSAGE_INFO	0x00000019	扩展密钥用途
SGD_EXT_CRLDISTRIBUTIONPOINTS_INFO	0x0000001A	CRL 发布点
SGD_EXT_NETSCAPE_CERT_TYPE_INFO	0x0000001B	Netscape 属性
SGD_EXT_SELFDEFINED_EXTENSION_INFO	0x0000001C	私有的自定义扩展项
SGD_CERT_ISSUER_CN	0x00000021	证书颁发者 CN
SGD_CERT_ISSUER_O	0x00000022	证书颁发者 O
SGD_CERT_ISSUER_OU	0x00000023	证书颁发者 OU
SGD_CERT_SUBJECT_CN	0x00000031	证书拥有者信息 CN
SGD_CERT_SUBJECT_O	0x00000032	证书拥有者信息 O
SGD_CERT_SUBJECT_OU	0x00000033	证书拥有者信息 OU
SGD_CERT_SUBJECT_EMAIL	0x00000034	证书拥有者信息 EMAIL
0x00000080～0x000000FF		为其他证书解析项预留

6.3.5 时间戳信息项标识

在时间戳系统的实现及时间戳的应用过程中，需要解析时间戳信息，在这种情况下需要通过标识符指定时间戳信息项的内容。

时间戳信息项标识的编码规则为：从低位到高位，第 0 位到第 7 位表示时间戳信息项的内容，第 8 位、第 10 位到第 31 位为 0，第 9 位为 1，例如：

SGD_SOURCE_OF_TIME：0000 0000 0000 0000 0000 0010 0000 0110（0x 00 00 02 06）

时间戳信息项标识的定义如表 8 所示。

表 8

标签	标识符	描述
SGD_TIME_OF_STAMP	0x00000201	签发时间
SGD_CN_OF_TSSIGNER	0x00000202	签发者的通用名
SGD_ORINGINAL_DATA	0x00000203	时间戳请求的原始信息
SGD_CERT_OF_TSSERVER	0x00000204	时间戳服务器的证书

SGD_CERTCHAIN_OF_TSSERVER	0x00000205	时间戳服务器的证书链
SGD_SOURCE_OF_TIME	0x00000206	时间源的来源
SGD_TIME_PRECISION	0x00000207	时间精度
SGD_RESPONSE_TYPE	0x00000208	响应方式
SGD_SUBJECT_COUNTRY_OF_TSSIGNER	0x00000209	签发者国家
SGD_SUBJECT_ORGNIZATION_OF_TSSIGNER	0x0000020A	签发者组织
SGD_SUBJECT_CITY_OF_TSSIGNER	0x0000020B	签发者城市
SGD_SUBJECT_EMAIL_OF_TSSIGNER	0x0000020C	签发者电子信箱
0x00000280～0x000002FF		为其他时间戳信息项预留

6.3.6 单点登录标识

在单点登录系统中，存在一些数据标识用于唯一的表示某一用户或某一服务提供者。

单点登录标识值的长度为 64 字节，由包含‘0’～‘9',‘A’～‘Z',和‘-’的字符串构成。

单点登录标识项的编码规则为：从低位到高位，第 0 位到第 7 位表示时间戳解析项的内容，第 8 位到第 31 位为 0，例如：

SGD_SP_ID：0000 0000 0000 0000 0000 0000 0000 0001（0x 00 00 00 01）

单点登录标识项的定义如表 9 所示。

表 9

标签	标识符	描述
SGD_SP_ID	0x00000001	服务提供者唯一标识数据
SGD_SP_USER_ID	0x00000002	SP 用户标识数据，在 SP 内唯一
SGD_IDP_ID	0x00000003	身份认证提供者唯一标识数据
SGD_IDP_USER_ID	0x00000004	IDP 用户标识数据，在 IDP 内唯一

6.3.7 数据编码格式标识

数据在存储或传输时需要按照约定的格式进行编码，以保证不同应用层或不同应用系统之间的互联互通性。编码格式标识符需要与通用数据标识符或证书解析项标识符等进行“或”运算后使用，作为数据的附加属性，表示数据对象符合指定编码格式。

数据编码格式标识的编码规则为：从低位到高位，第 0 位到第 23 位为 0，第 24 位到第 31 位表示数据编码格式，例如：

SGD_ENCODING_DER：0000 0001 0000 0000 0000 0000 0000 0000（0x 01 00 00 00）

数据编码格式标识的定义如表 10 所示。

表 10

标签	标识符	描述
SGD_ENCODING_RAW	0x00000000	无编码
SGD_ENCODING_DER	0x01000000	DER 编码
SGD_ENCODING_BASE64	0x02000000	Base64 编码
SGD_ENCODING_PEM	0x03000000	PEM 编码
SGD_ENCODING_TXT	0x04000000	由’0’～’9’、’A’～’F’等字符表示 16 进制数据的字符串
0x80000000～0xFF000000		为自定义编码格式预留

6.4 协议标识

6.4.1 接口描述标识

在安全应用系统中为区分密码服务提供者所采用的协议或规范，可以采用接口描述标识。

接口描述标识使用 32 位无符号整数表示，其定义如表 11 所示。

表 11

标签	标识符	描述
SGD_PROTOCOL_CSP	1	CSP 接口
SGD_PROTOCOL_PKCS11	2	PKCS#11 接口
SGD_PROTOCOL_SDS	3	密码设备应用接口
SGD_PROTOCOL_UKEY	4	智能 IC 卡及智能密码钥匙接口

6.4.2 证书验证模式标识

在验证证书的有效性时，除了检查证书的有效期、证书的签名是否有效外，还应通过 CRL 或 OCSP 等方式检查证书是否被注销等异常状态。

证书验证模式标识使用 32 位无符号整数表示，其定义如表 12 所示。

表 12

标签	标识符	描述
SGD_CRL_VERIFY	1	CRL 验证模式
SGD_OCSP_VERIFY	2	OCSP 验证模式

6.4.3 函数命名规范

公钥密码基础设施应用技术体系框架内各接口规范的函数命名规范如表 13 所示。

表 13

类别	命名
密码设备应用接口函数	SDF_XXXXXX
通用密码服务接口函数	SAF_XXXXXX
密码设备管理接口函数	SMF_XXXXXX
责任认定接口函数	SCF_XXXXXX
身份鉴别接口函数	SIF_XXXXXX
单点登录接口函数	SSF_XXXXXX
访问控制接口函数	SPF_XXXXXX
时间戳服务接口函数	STF_XXXXXX
智能 IC 卡及智能密码钥匙接口函数	SKF_XXXXXX

6.4.4 错误码区间定义

公钥密码基础设施应用技术体系框架内各规范接口函数分配的错误代码区间如表 14 所示。

表 14

类别	区间定义
密码设备应用接口	0x01000000～0x01FFFFFF
通用密码服务接口	0x02000000～0x02FFFFFF
密码设备管理接口	0x03000000～0x03FFFFFF
责任认定接口	0x04000000～0x04FFFFFF
身份鉴别接口	0x05000000～0x05FFFFFF

单点登录接口	0x06000000～0x06FFFFFF
访问控制接口	0x07000000～0x07FFFFFF
时间戳服务接口	0x08000000～0x08FFFFFF
智能 IC 卡及智能密码钥匙接口	0x0A000000～0x0AFFFFFF
返回代码正确为 0，非零用错误代码区间表示	

7 安全管理类标识

7.1 概述

安全管理类标识定义了在安全系统管理、设备管理中涉及到的系统角色、安全操作等项的表示短语和数据。该类数据标识在安全管理接口的调用过程中使用，或在安全系统或设备管理的日志信息采集、处理过程中使用，也可应用于其他安全管理活动中。

7.2 角色管理标识

7.2.1 角色标识

角色是在管理操作中的主体，是管理活动的实施者，在角色管理操作中也会作为被管理的对象。

角色标识的编码规则为：从低位到高位，第 0 到第 7 位表示角色，第 8 位到第 31 位为0，例如：

SGD_ROLE_OPERATOR：0000 0000 0000 0000 0000 0000 0000 0101(0x 00 00 00 05)

角色标识的定义如表 15 所示。

表 15

标签	标识符	描述
SGD_ROLE_SUPER_MANAGER	0x00000001	超级管理员
SGD_ROLE_MANAGER	0x00000002	业务管理员
SGD_ROLE_AUDIT_MANAGER	0x00000003	审计管理员
SGD_ROLE_AUDITOR	0x00000004	审计操作员
SGD_ROLE_OPERATOR	0x00000005	业务操作员
SGD_ROLE_USER	0x00000006	用户
0x00000081～0x000000FF		为自定义角色预留

7.2.2 角色操作标识

角色操作标识符包含角色自身的行为，如签入、签出、修改口令等操作，和对其他角色的管理行为，如创建角色、删除角色、修改角色、对角色授权等操作。

角色操作标识的编码规则为：从低位到高位，第 0 位到第 7 位表示角色管理操作，第 8 位到第 31 位为 0，例如：

SGD_OPERATION_SIGNIN:0000 0000 0000 0000 0000 0000 0000 0001(0x 00 00 00 01)

角色操作标识的定义如表 16 所示。

表 16

标签	标识符	描述
SGD_OPERATION_SIGNIN	0x00000001	签入
SGD_OPERATION_SIGNOUT	0x00000002	签出
SGD_OPERATION_CREATE	0x00000003	创建

SGD_OPERATION_DELETE	0x00000004	删除
SGD_OPERATION_MODIFY	0x00000005	修改
SGD_OPERATION_CHG_PWD	0x00000006	修改口令
SGD_OPERATION_AUTHORIZATION	0x00000007	授权

7.2.3 操作结果标识

操作结果标识符表示管理活动的结束状态，分别是成功和失败两种状态。

操作结果标识的定义如表 17 所示。

表 17

标签	标识符	描述
SGD_OPERATION_SUCCESS	0x00000000	成功
0x00000001～0xFFFFFFFF		失败，表示错误码

7.3 密钥管理标识

7.3.1 密钥分类标识

密钥分类标识密钥的属性信息，属于被管理的对象。

密钥分类标识的编码规则为：从低位到高位，第 0 位到第 7 位表示密钥对象，第 8 位为 1 表示为密钥管理类标识，第 9 位到第 31 位为 0，例如：

SGD_PRIKEY_PASSWD：0000 0000 0000 0000 0000 0001 0000 0110(0x 00 00 01 06)

密钥分类标识的定义如表 18 所示。

表 18

标签	标识符	描述
SGD_MAIN_KEY	0x00000101	主密钥
SGD_DEVICE_KEYS	0x00000102	设备密钥
SGD_USER_KEYS	0x00000103	用户密钥
SGD_KEK	0x00000104	密钥加密密钥
SGD_SESSION_KEY	0x00000105	会话密钥
SGD_PRIKEY_PASSWD	0x00000106	私钥访问控制码
SGD_COMPARTITION_KEY	0x00000107	分隔密钥
0x00000110～0x000001FF		为自定义密钥类型预留

7.3.2 密钥操作标识

密钥操作标识定义了对密钥的操作内容。

密钥操作标识的编码规则为：从低位到高位，第 0 位到第 7 位表示密钥管理标识，第 8 位为 1 表示为密钥管理类标识，第 9 位到第 31 位为 0，例如：

SGD_KEY_DESTROY：0000 0000 0000 0000 0000 0001 0000 1010(0x 00 00 01 0A)

密钥操作标识的定义如表 19 所示。

表 19

标签	标识符	描述
SGD_KEY_GENERATION	0x00000101	密钥生成
SGD_KEY_DISPENSE	0x00000102	密钥分发
SGD_KEY_IMPORT	0x00000103	密钥导入
SGD_KEY_EXPORT	0x00000104	密钥导出

SGD_KEY_DIVISION	0x00000105	密钥分割
SGD_KEY_COMPOSE	0x00000106	密钥合成
SGD_KEY_RENEWAL	0x00000107	密钥更新
SGD_KEY_BACKUP	0x00000108	密钥备份
SGD_KEY_RESTORE	0x00000109	密钥恢复
SGD_KEY_DESTROY	0x0000010A	密钥销毁

7.4 系统管理标识

系统管理标识定义了在对安全系统进行管理操作时的角色、操作、对象、结果等项的表示短语和数据。

角色的定义和操作结果的定义见“角色管理标识”中的“角色标识”和“操作结果标识”部分。

系统操作标识定义了对安全系统所采取的管理操作项。

系统操作标识的编码规则为：从低位到高位，第 0 位到第 7 位表示系统管理操作，第 8 位、第 10 位到第 31 位为 0，第 9 位为 1 表示为系统或设备管理类标识，例如：

SGD_SYSTEM_SHUT：0000 0000 0000 0000 0000 0010 0000 0011(0x 00 00 02 03)

系统操作标识的定义如表 20 所示。

表 20

标签	标识符	描述
SGD_SYSTEM_INIT	0x00000201	系统安装及初始化操作
SGD_SYSTEM_START	0x00000202	启动系统
SGD_SYSTEM_SHUT	0x00000203	关闭系统
SGD_SYSTEM_RESTART	0x00000204	重新启动系统
SGD_SYSTEM_QUERY	0x00000205	状态查询
SGD_SYSTEM_BACKUP	0x00000206	数据备份
SGD_SYSTEM_RESTORE	0x00000207	数据恢复

7.5 设备管理标识

7.5.1 设备基本信息标识

设备信息标识可以在从密码设备中获取设备型号、设备编号等信息时指定。

设备信息标识的编码规则为：从低位到高位，第 0 位到第 7 位表示设备信息标识，第 8 位、第 10 位到第 31 位为 0，第 9 位为 1，表示为系统或设备管理类标识，例如：

SGD_DEVICE_DESCRIPTION：0000 0000 0000 0000 0000 0010 0001 0001(0x 00 00 02 11)

设备信息标识的定义如表 21 所示。

表 21

标签	标识符	描述
SGD_DEVICE_SORT	0x00000201	设备类别，如密码机、密码卡和智能密码终端等
SGD_DEVICE_TYPE	0x00000202	设备型号
SGD_DEVICE_NAME	0x00000203	设备名称

SGD_DEVICE_MANUFACTURER	0x00000204	生产厂商
SGD_DEVICE_HARDWARE_VERSION	0x00000205	硬件版本
SGD_DEVICE_SOFTWARE_VERSION	0x00000206	软件版本
SGD_DEVICE_STANDARD_VERSION	0x00000207	符合规范版本
SGD_DEVICE_SERIAL_NUMBER	0x00000208	设备编号
SGD_DEVICE_SUPPORT_ALG	0x00000209	设备能力字段，标识密码设备支持的非对称密码算法
SGD_DEVICE_SUPPORT_ALG	0x0000020A	设备能力字段，标识密码设备支持的对称密码算法
SGD_DEVICE_SUPPORT_HASH_ALG	0x0000020B	设备能力字段，标识密码设备支持的杂凑密码算法
SGD_DEVICE_SUPPORT_STORAGE_SPACE	0x0000020C	设备能力字段，标识密码设备最大文件存储空间
SGD_DEVICE_SUPPORT_FREE_SPACE	0x0000020D	设备能力字段，标识密码设备空闲文件存储空间
SGD_DEVICE_RUNTIME	0x0000020E	已运行时间
SGD_DEVICE_USED_TIMES	0x0000020F	设备被调用次数
SGD_DEVICE_LOCATION	0x00000210	设备物理位置
SGD_DEVICE_DESCRIPTION	0x00000211	设备描述
SGD_DEVICE_MANAGER_INFO	0x00000212	设备管理者描述信息

7.5.2 设备类别标识

7.5.2.1 设备类别标识格式

设备类别标识包括设备形态和设备功能等信息，由设备形态标识和设备功能标识通过“或”运算进行组合。

7.5.2.2 设备形态标识

设备形态标识的编码规则为：从低位到高位，第 0 位到第 23 位为 0，第 24 位到第 31 位表示密码设备的形态，例如：

SGD_DEVICE_SORT_SJ： 0000 0010 0000 0000 0000 0000 0000 0000 (0x 02 00 00 00)

设备形态标识的定义如表 22 所示。

表 22

标签	标识符	描述
SGD_DEVICE_SORT_SJ	0x02000000	通过网络提供服务的密码设备
SGD_DEVICE_SORT_SK	0x03000000	不支持热拔插功能的密码设备，如 PCI 密码卡
SGD_DEVICE_SORT_SM	0x04000000	支持热拔插的 KEY 或 IC 卡类密码设备
0x05000000~0xFF000000		为其他设备形态预留

7.5.2.3 设备功能标识

设备功能标识的编码规则为：从低位到高位，第 0 位到第 7 位为 0，第 8 位到第 23 位按位表示密码设备的主要功能，第 24 位到第 31 位为 0，例如：

SGD_DEVICE_SORT_FE: 0000 0000 0000 0000 0000 0000 0001 0000 0000 (0x 00 00 01 00)

设备功能标识的定义如表 23 所示。

表 23

标签	标识符	描述
SGD_DEVICE_SORT_FE	0x00000100	加解密类密码设备
SGD_DEVICE_SORT_FA	0x00000200	数据鉴别类密码设备
SGD_DEVICE_SORT_FM	0x00000400	密钥管理类密码设备
0x00000800~0x00800000		为其他设备功能预留

7.5.3 设备操作标识

对设备内角色的管理操作见“角色管理标识”部分。

对设备内密钥的管理操作见“密钥管理标识”部分。

对设备整体的管理操作见“系统管理标识”部分。

7.5.4 设备状态标识

设备状态标识，可以标识密码设备当前的工作状态。

设备状态标识的编码规则为：从低位高位，第 0 位到第 7 位表示设备状态标识，第 8 位、第 10 位到第 31 位为 0，第 9 位为 1，表示为系统或设备管理类标识，例如：

SGD_STATUS_READY：0000 0000 0000 0000 0000 0010 0000 0010(0x 00 00 02 02)

设备状态标识的定义如表 24 所示。

表 24

标签	标识符	描述
SGD_STATUS_INIT	0x00000201	初始状态，密码设备内没有安装密钥，不能提供服务
SGD_STATUS_READY	0x00000202	就绪状态，已经安装密钥，可以提供密码服务
SGD_STATUS_EXCEPTION	0x00000203	异常状态，已安装密钥，但不能正常提供密码服务

7.5.5 设备编号格式

设备编号，与设备型号组合使用可唯一的标识某一密码设备。在设备型号相同的情况下，该设备编号具有唯一性，不可重复。

标签格式：XXXXXXXX－XXX－XXXXX（生产日期－批次号－流水号）

生产日期，8 位数字，表示改密码设备的生产日期，按从左到右的顺序，分别是年 4 位数字，月 2 位数字，日 2 位数字，如 20080229；

批次号，3 位数字，表示同型号密码设备的生产批次，不足 3 位数字，则在左边用 0 填充至 3 位，如：001；

流水号，5 位数字，某一型号某一批次产品的流水编号，不足 5 位数字，则在左边用 0 填充至 5 位，如：00123。

设备编号的编码规则为：每 4 位表示设备编号的 1 个数字，从高位到低位，第 63 位到第 32 位表示生产日期，第 33 位到第 44 位表示批次号，第 45 位到第 64 位表示流水号，例如：

20080229 – 001 – 00123 表示为：0x 20 08 02 29 00 10 01 23

附录 A
（规范性附录）
密码运算数据填充

A.1 分组密码运算数据填充

A.1.1 通用填充模式

在进行密码运算时对输入数据的长度和格式有特定的要求，在进行密码运算前需要对数据进行格式处理。数据填充标识符与密码运算标识符组合使用，用于描述在进行密码运算前是否已经进行数据填充处理及数据填充的格式。

在进行分组密码运算时，应对明文数据进行填充，填充规则如下：

设明文为 M，其长度为 L 个字节，分组长度为 B 个字节，填充数据为 PS，填充后的待加密数据为 EB，“||”表示连接，则：

EB = M || PS

填充数据 PS 由 B - (L mod B)个字节组成，每个字节的值为 B - (L mod B)，如：

EB = M || 0x01 ——如果 B - (L mod B) = 1

EB = M || 0x02 0x02 ——如果 B - (L mod B) = 2

EB = M || 0x03 0x03 0x03 ——如果 B - (L mod B) = 3

…

EB = M || B B … B ——如果 L mod B = 0，则填充一个完整的分组。

A.1.2 社保体系专用填充模式

此模式用于社保体系分组密码运算数据填充操作。

设明文为 M，其长度为 L 个字节，分组长度为 B 个字节，填充数据为 PS，填充后的待加密数据为 EB，“||”表示连接，则：

EB = M || PS

填充数据 PS 由’0x80’和 B - (L mod B)-1 个’0x00’组成，如：

EB = M || 0x80 ——如果 B - (L mod B) = 1

EB = M || 0x80 0x00 ——如果 B - (L mod B) = 2

EB = M || 0x80 0x00 0x00——如果 B - (L mod B) = 3

…

EB = M || 0x80 0x00 0x00 … 0x00 ——如果 L mod B = 0，则填充一个完整的分组。

A.2 RSA 密码运算数据填充

RSA 密码运算时应按照 PKCS#1(v1.5)中定义的格式对数据填充。

附录 B
（资料性附录）
商用密码应用领域中的相关 OID 定义

对象标识符OID	对象标识符定义	备注
通用对象标识符		
1.2	国际标准化组织成员标识	
1.2.156	中国	
1.2.156.197	国家密码管理局	
1.2.156.197.1	密码算法	
分组密码算法对象标识符		
1.2.156.197.1.100	分组密码算法	
1.2.156.197.1.101	SM6分组密码算法	
1.2.156.197.1.102	SM1分组密码算法	
1.2.156.197.1.103	SSF33密码算法	
1.2.156.197.1.104	SM4分组密码算法	
1.2.156.197.1.105	SM7分组密码算法	
1.2.156.197.1.106	SM8分组密码算法	
序列密码算法对象标识符		
1.2.156.197.1.200	序列密码算法	
1.2.156.197.1.201	SM5序列密码算法	
公钥密码算法对象标识符		
1.2.156.197.1.300	公钥密码算法	
1.2.156.197.1.301	SM2椭圆曲线密码算法	
1.2.156.197.1.301.1	SM2-1椭圆曲线数字签名算法	
1.2.156.197.1.301.2	SM2-2椭圆曲线密钥交换协议	
1.2.156.197.1.301.3	SM2-3椭圆曲线加密算法	
1.2.156.197.1.302	SM9标识密码算法	
1.2.156.197.1.302.1	SM9-1数字签名算法	
1.2.156.197.1.302.2	SM9-2密钥交换协议	
1.2.156.197.1.302.3	SM9-3密钥封装机制和公钥加密算法	
1.2.156.197.1.310	RSA密码算法*	
杂凑算法对象标识符		
1.2.156.197.1.400	杂凑算法	
1.2.156.197.1.401	SM3密码杂凑算法	
1.2.156.197.1.401.1	SM3密码杂凑算法，无密钥使用	
1.2.156.197.1.401.2	SM3密码杂凑算法，有密钥使用	
1.2.156.197.1.410	SHA-1算法*	
1.2.156.197.1.410.1	SHA-1无密钥*	
1.2.156.197.1.410.2	SHA-1有密钥*	
1.2.156.197.1.411	SHA256算法*	

1.2.156.197.1.411.1	SHA256无密钥*	
1.2.156.197.1.411.2	SHA256有密钥*	
组合运算算法对象标识符		
1.2.156.197.1.500	组合运算机制	
1.2.156.197.1.501	基于SM2算法和SM3算法的签名	
1.2.156.197.1.502	基于SM2算法和SHA-1算法的签名	
1.2.156.197.1.503	基于SM2算法和SHA256算法的签名	
1.2.156.197.1.504	基于RSA算法和SM3算法的签名	
1.2.156.197.1.505	基于RSA算法和SHA-1算法的签名*	
1.2.156.197.1.506	基于RSA算法和SHA256算法的签名*	
CA代码对象标识符		
1.2.156.197.4.3	CA代码	

注： 带* 者项表示该项有国际通用标识符。

参考文献

[1] X.208 CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.

[2] RFC 1421 - Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. 1993.

[3] PKCS #1: RSA Encryption Standard. Version 1.5, 1993.

[4] PKCS #5: Password-Based Encryption Standard. Version 1.5, 1993.

[5] PKCS #11: Cryptographic Token Interface Standard. Version 1.0, 1995.