ICS 35.040
L 80

中华人民共和国国家标准

GB/T 33560—2017

信息安全技术　密码应用标识规范

**Information security technology—
Cryptographic application identifier criterion specification**

2017-05-12 发布　　2017-12-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家密码管理局提出。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)归口。

本标准起草单位:山东得安信息技术有限公司、成都卫士通信息产业股份有限公司、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。

本标准主要起草人:刘平、刘晓东、孔凡玉、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、郑海森。

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。

本标准的目标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的管理。

本标准中规定的标识不适用于无线通信、金融 IC 卡应用。

本标准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。

信息安全技术　密码应用标识规范

1　范围

本标准定义了密码应用中所使用的标识，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。

本标准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，也可用于指导其他相关标准或协议的编制中对标识的使用。

本标准仅适用于 PKI 体系。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GM/Z 0001—2013　密码术语

3　术语和定义

GM/Z 0001—2013 界定的以及下列术语和定义适用于本文件。

3.1

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的密码算法、密码协议等。

3.2

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。

3.3

网络字节顺序　network byte order

采用 Big-endian 排序方式规定好的一种数据表示格式。该排序方式与具体的 CPU 类型、操作系统等无关，从而可以保证数据在不同主机之间传输时可以被正确解释。

3.4

标签　label

用于唯一指定某个标识符的名称。

4　符号和缩略语

下列符号和缩略语适用于本文件。

BASE64　将十六进制数据转换为可见字符的编码规则

CBC　密码分组链接模式(Cipher Block Chaining)

CFB　密文反馈模式(Ciphertext Feedback)
CRL　证书吊销列表(Certificate Revocation List)
DER　识别名编码规则,为每一个 ASN.1 类型制定唯一的编码方案
ECB　电码本模式(Electronic Code Book)
MAC　消息认证码(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　隐私增强邮件标准规定的证书编码格式
PKI　公钥基础设施(Public Key Infrastructure)

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存储于低地址的网络字节顺序进行处理。

商用密码领域中的对象标识符(OID)的定义见附录 A。

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)

当多个分组密码算法同时存在时,可用“或”的形式表示。

分组密码算法的标识如表 1 所示。

表 1　分组密码算法的标识

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

表 1（续）

标签	标识符	描述
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_SM4_ECB	0x00000401	SM4 算法 ECB 加密模式
SGD_SM4_CBC	0x00000402	SM4 算法 CBC 加密模式
SGD_SM4_CFB	0x00000404	SM4 算法 CFB 加密模式
SGD_SM4_OFB	0x00000408	SM4 算法 OFB 加密模式
SGD_SM4_MAC	0x00000410	SM4 算法 MAC 运算
SGD_ZUC_EEA3	0x00000801	ZUC 祖冲之机密性算法 128-EEA3 算法
SGD_ZUC_EIA3	0x00000802	ZUC 祖冲之完整性算法 128-EIA3 算法
0x00001000～0x800000FF[a]		为其他分组密码算法预留
[a] 为其他分组密码算法预留的标识符，预留的标签可自定义。		

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 SHA_1”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 0010 0000 0000（0x 00 02 02 00）

当多个非对称密码算法同时存在时，可用“或”的形式表示。

非对称密码算法的标识如表 2 所示。

表 2 非对称密码算法的标识

标签	标识符	描述
SGD_RSA	0x00010000	RSA 算法
SGD_SM2	0x00020100	SM2 椭圆曲线密码算法
SGD_SM2_1	0x00020200	SM2 椭圆曲线签名算法
SGD_SM2_2	0x00020400	SM2 椭圆曲线密钥交换协议

表 2（续）

标签	标识符	描述
SGD_SM2_3	0x00020800	SM2 椭圆曲线加密算法
SGD_SM9	0x00040100	SM9 标识密码算法
SGD_SM9_1	0x00040200	SM9 数字签名算法
SGD_SM9_2	0x00040400	SM9 密钥交换协议
SGD_SM9_3	0x00040800	SM9 密钥封装机制和公钥加密算法
0x00080000～0x80000000[a]		为其他非对称密码算法预留
[a] 为其他非对称密码算法预留的标识符，预留的标签可自定义。		

6.2.3 密码杂凑算法标识

密码杂凑算法标识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）

当多个密码杂凑算法同时存在时，可用“或”的形式表示。

密码杂凑算法的标识如表 3 所示。

表 3 密码杂凑算法的标识

标签	标识符	描述
SGD_SM3	0x00000001	SM3 杂凑算法
SGD_SHA1	0x00000002	SHA_1 杂凑算法
SGD_SHA256	0x00000004	SHA_256 杂凑算法
0x00000008～0x000000FF[a]		为其他密码杂凑算法预留
[a] 为其他密码杂凑算法预留的标识符，预留的标签可自定义。		

6.2.4 签名算法标识

签名算法标识在进行数字签名时应用。

签名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 位表示非对称密码算法，例如：

SGD_SHA1_RSA：0000 0000 0000 0001 0000 0000 0000 0010（0x 00 01 00 02）

签名算法的标识如表 4 所示。

表 4　签名算法的标识

标签	标识符	描述
SGD_SM3_RSA	0x00010001	基于 SM3 算法和 RSA 算法的签名
SGD_SHA1_RSA	0x00010002	基于 SHA_1 算法和 RSA 算法的签名
SGD_SHA256_RSA	0x00010004	基于 SHA_256 算法和 RSA 算法的签名
SGD_SM3_SM2	0x00020201	基于 SM3 算法和 SM2 算法的签名
SGD_SM3_SM9	0x00040201	基于 SM3 算法和 SM9 算法的签名
0x00080000～0x800000FF[a]		为其他密码签名算法预留
[a] 为其他密码签名算法预留的标识符，预留的标签可自定义。		

6.3　数据标识

6.3.1　数据类型

数据类型定义了在 PKI 体系下各标准中用到的数据类型标签。

数据类型标签的定义如表 5 所示。

表 5　数据类型标签

标签	说明
SGD_CHAR	8 位，有符号字符
SGD_INT8	8 位，有符号整数
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，无符号整数
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 PKI 体系下各标准中用到的常量的标签及取值。

数据常量标识的定义如表 6 所示。

表 6　数据常量标识

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 01 17）

通用数据对象标识的定义如表 7 所示。

表 7　通用数据对象标识

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[a]		为其他数据对象预留
[a] 为其他数据对象预留的标识符，预留的标签可自定义。		

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 8 所示。

表 8　证书解析项标识

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	颁发者密钥标识符
SGD_EXT_SUBJECTKEYIDENTIFIER_INFO	0x00000012	证书持有者密钥标识符
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	策略映射
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	证书颁发者通用名
SGD_CERT_ISSUER_O	0x00000022	证书颁发者组织
SGD_CERT_ISSUER_OU	0x00000023	证书颁发者组织机构
SGD_CERT_SUBJECT_CN	0x00000031	证书拥有者通用名
SGD_CERT_SUBJECT_O	0x00000032	证书拥有者组织
SGD_CERT_SUBJECT_OU	0x00000033	证书拥有者组织机构
SGD_CERT_SUBJECT_EMAIL	0x00000034	证书拥有者电子信箱
SGD_CERT_NOTBEFORE_TIME	0x00000035	证书起始日期
SGD_CERT_NOTAFTER_TIME	0x00000036	证书截至日期
0x00000080～0x000000FF[a]		为其他证书解析项预留

[a] 为其他证书解析项预留的标识符，预留的标签可自定义。

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 9 所示。

表 9 时间戳信息项标识

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[a]		为其他时间戳信息项预留
[a] 为其他时间戳信息项预留的标识符，预留的标签可自定义。		

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。

单点登录标识项的编码规则为：从低位到高位，第 0 位到第 7 位表示单点登录标识项的内容，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）

单点登录标识的定义如表 10 所示。

表 10 单点登录标识

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	服务提供者用户标识数据，在服务提供者内唯一
SGD_IDP_ID	0x00000003	身份鉴别提供者唯一标识数据
SGD_IDP_USER_ID	0x00000004	身份鉴别提供者用户标识数据，在身份鉴别提供者内唯一

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 11 所示。

表 11 数据编码格式标识

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[a]		为自定义编码格式预留
[a] 为自定义编码格式预留的标识符，预留的标签可自定义。		

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 12 所示。

表 12 接口描述标识

标签	标识符	描述
SGD_PROTOCOL_CSP	1	Cryptographic Service Provider 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
SGD_PROTOCOL_CNG	5	Cryptographic Next Generation 接口
SGD_PROTOCOL_GCS	6	通用密码服务接口

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 13 所示。

表 13　证书验证模式标识

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

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 14 所示。

表 14　角色标识

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[a]		为自定义角色预留
[a] 为自定义角色预留的标识符，预留的标签可自定义。		

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 15 所示。

表 15　角色操作标识

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 16 所示。

表 16　操作结果标识

标签	标识符	描述
SGD_OPERATION_SUCCESS	0x00000000	成功
0x00000001～0xFFFFFFFF[a]		失败，表示错误码
[a] 为错误码预留的标识符，预留的标签可自定义。		

7.3　密钥管理标识

7.3.1　密钥分类标识

密钥分类标识定义了密钥的属性信息，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 17 所示。

表 17　密钥分类标识

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

表 17（续）

标签	标识符	描述
SGD_COMPARTITION_KEY	0x00000107	分隔密钥
0x00000110～0x000001FF[a]		为自定义密钥类型预留
[a] 为自定义密钥类型预留的标识符，预留的标签可自定义。		

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 18 所示。

表 18 密钥操作标识

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。

系统管理标识的编码规则为：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）

系统管理标识的定义如表 19 所示。

表 19　系统管理标识

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

设备基本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。

设备基本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)

设备基本信息标识的定义如表 20 所示。

表 20　设备基本信息标识

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	符合标准版本
SGD_DEVICE_SERIAL_NUMBER	0x00000208	设备编号
SGD_DEVICE_SUPPORT_ASYM_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_SYMM_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

表 20（续）

标签	标识符	描述
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
SGD_DEVICE_MAX_DATA_SIZE	0x00000213	设备能力字段，一次能处理的数据容量

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 21 所示。

表 21 设备形态标识

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	支持热拔插的智能密码钥匙或智能卡类密码设备
0x05000000～0xFF000000[a]		为其他设备形态预留
[a] 为其他设备形态预留的标识符，预留的标签可自定义。		

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 0001 0000 0000（0x 00 00 01 00）

设备功能标识的定义如表 22 所示。

表 22　设备功能标识

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[a]	为其他设备功能预留	
[a] 为其他设备功能预留的标识符，预留的标签可自定义。		

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 23 所示。

表 23　设备状态标识

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
0x00000204～0x000002FF[a]		
[a] 为其他设备状态预留的标识符，预留的标签可自定义。		

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：××××××××-×××-×××××(生产日期-批次号-流水号)

生产日期，8 位数字，表示该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，从低位到高位，第 0 位到第 19 位表示流水号，第 20 位到第 31 位表示批次号，第 32 位到第 63 位表示生产日期，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）
商用密码领域中的相关 OID 定义

商用密码领域中的 OID 定义了各类对象的标识符，具体定义见表 A.1。

表 A.1 商用密码领域中的相关 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	
1.2.156.10197	国家密码行业标准化技术委员会	
1.2.156.10197.1	密码算法	
分组密码算法对象标识符		
1.2.156.10197.1.100	分组密码算法	
1.2.156.10197.1.102	SM1 分组密码算法	
1.2.156.10197.1.103	SSF33 分组密码算法	
1.2.156.10197.1.104	SM4 分组密码算法	
序列密码算法对象标识符		
1.2.156.10197.1.200	序列密码算法	
1.2.156.10197.1.201	祖冲之序列密码算法	
公钥密码算法对象标识符		
1.2.156.10197.1.300	公钥密码算法	
1.2.156.10197.1.301	SM2 椭圆曲线公钥密码算法	
1.2.156.10197.1.301.1	SM2-1 数字签名算法	
1.2.156.10197.1.301.2	SM2-2 密钥交换协议	
1.2.156.10197.1.301.3	SM2-3 公钥加密算法	
1.2.156.10197.1.302	SM9 标识密码算法	
1.2.156.10197.1.302.1	SM9-1 数字签名算法	
1.2.156.10197.1.302.2	SM9-2 密钥交换协议	
1.2.156.10197.1.302.3	SM9-3 密钥封装机制和公钥加密算法	
杂凑算法对象标识符		
1.2.156.10197.1.400	杂凑算法	
1.2.156.10197.1.401	SM3 密码杂凑算法	
1.2.156.10197.1.401.1	SM3 密码杂凑算法，无密钥使用	
1.2.156.10197.1.401.2	SM3 密码杂凑算法，有密钥使用	

表 A.1（续）

对象标识符 OID	对象标识符定义	备注
组合运算算法对象标识符		
1.2.156.10197.1.500	组合运算机制	
1.2.156.10197.1.501	基于 SM2 算法和 SM3 算法的签名	
1.2.156.10197.1.502	基于 SM9 算法和 SM3 算法的签名	
1.2.156.10197.1.504	基于 RSA 算法和 SM3 算法的签名	
CA 代码对象标识符		
1.2.156.10197.4.3	CA 代码	
标准体系对象标识符		
1.2.156.10197.6	标准体系	
1.2.156.10197.6.1	基础类	
1.2.156.10197.6.1.1	算法类	
1.2.156.10197.6.1.1.1	《祖冲之序列密码算法》	
1.2.156.10197.6.1.1.2	《SM4 分组密码算法》	
1.2.156.10197.6.1.1.3	《SM2 椭圆曲线公钥密码算法》	
1.2.156.10197.6.1.1.4	《SM3 密码杂凑算法》	
1.2.156.10197.6.1.2	标识类	
1.2.156.10197.6.1.2.1	《密码应用标识规范》	
1.2.156.10197.6.1.3	工作模式	
1.2.156.10197.6.1.4	安全机制	
1.2.156.10197.6.1.4.1	《SM2 密码使用规范》	
1.2.156.10197.6.1.4.2	《SM2 加密签名消息语法规范》	
1.2.156.10197.6.1.4.3	《SM9 密码使用规范》	
1.2.156.10197.6.1.4.4	《SM9 加密签名消息语法规范》	
1.2.156.10197.6.2	设备类	
1.2.156.10197.6.3	服务类	
1.2.156.10197.6.4	基础设施	
1.2.156.10197.6.5	检测类	
1.2.156.10197.6.5.1	《随机性检测规范》	
1.2.156.10197.6.6	管理类	

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.