ICS 35.040
L 80
备案号:36833—2012

GM

中华人民共和国密码行业标准

GM/T 0006—2012

密码应用标识规范

Cryptographic application identifier criterion specification

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　　发布

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由国家密码管理局提出并归口。

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。

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，也能够有效地指导、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。

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。

2 术语和定义

下列术语和定义适用于本文件。

2.1

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到的密码算法、密码协议等。

2.2

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 符号和缩略语

下列缩略语适用于本部分：

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)

ECB 电码本模式(Electronic Code Book)

CFB 密文反馈模式(Ciphertext Feedback)

OFB 输出反馈模式(Output Feedback)

OID 对象标识符(Object Identifier)

4 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。

5 密码服务类标识

5.1 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。

5.2 算法标识

5.2.1 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
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		为其他分组密码算法预留

5.2.2 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
SGD_SM2_3	0x00020800	SM2 椭圆曲线加密算法
0x00040000～0x80000000		为其他非对称密码算法预留

5.2.3 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		为其他密码杂凑算法预留

5.2.4 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
0x00040000～0x800000FF		为其他密码签名算法预留

5.3 数据标识

5.3.1 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

5.3.2 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

5.3.3　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		为其他数据对象预留

5.3.4　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 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

5.3.5 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。