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。