



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	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	1
5 标识的格式和编码	2
6 密码服务类标识	2
6.1 概述	2
6.2 算法标识	2
6.3 数据标识	5
6.4 协议标识	9
7 安全管理类标识.....	10
7.1 概述	10
7.2 角色管理标识	10
7.3 密钥管理标识	11
7.4 系统管理标识	12
7.5 设备管理标识	13
附录 A (规范性附录) 商用密码领域中的相关 OID 定义	17
参考文献	19

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)