ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 33560—2026
代替 GB/T 33560—2017

网络安全技术　密码应用标识

Cybersecurity technology—Cryptographic application identifier

2026-05-25 发布　　2026-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 33560—2017《信息安全技术　密码应用标识规范》，与GB/T 33560—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了术语“公钥证书”（见2017年版的3.2）、“网络字节顺序”（见2017年版的3.3）和“标签”（见2017年版的3.4）；

b) 在“缩略语”引入了部分新的缩略语，更新了部分原条目，删除了一些不常用条目（见第4章，2017年版的第4章）；

c) 删除了SSF33分组密码算法标识（见2017年版的6.2.1）；

d) 增加了部分SM4、SM7分组密码算法模式标识（见6.2.1），增加了ZUC-GXM、ZUC-MUR鉴别式加密机制标识（见6.2.1），增加了SM3_HMAC、SHA256_HMAC密码杂凑算法标识（见6.2.3）；

e) 在“对称密码算法标识”中增加了SM4算法基于密钥流序列的FPE加密模式、SM4算法基于Feistel结构的FPE加密模式两种算法标识（见6.2.1）；

f) 删除了“协议标识”（见2017年版的6.4）；

g) 在“数据标识”中增加了部分证书解析项标识（见6.3.4），在“角色管理标识”中增加了部分角色操作标识（见7.2.2），在“密钥管理标识”中增加了部分密钥操作标识（见7.3.2）；

h) 删除了“设备类别标识”（见2017年版的7.5.2），删除了“设备操作标识”（见2017年版的7.5.3）；

i) 删除了“产品编号”中产品编号格式的具体定义（见2017年版的7.5.5）；

j) 更改了商用密码领域中的相关OID定义（见附录A，2017年版的附录A）。

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专利的责任。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：山东得安信息技术有限公司、颢安检测技术（西安）有限责任公司、格尔软件股份有限公司、北京信安世纪科技股份有限公司、北京国脉信安科技有限公司、山东大学、中电科网络安全科技股份有限公司、北京数字认证股份有限公司、兴唐通信科技有限公司、长春吉大正元信息技术股份有限公司、北京海泰方圆科技股份有限公司、鼎铉商用密码测评技术（深圳）有限公司、上海市数字证书认证中心有限公司、北京中科卓信软件测评技术中心、安徽信科共创信息安全测评有限公司、国家工业信息安全发展研究中心、国网经济技术研究院有限公司、北京交通大学、中国电子科技集团公司第十五研究所、天翼云科技有限公司、天翼安全科技有限公司、云南电网有限责任公司、联通数字科技有限公司、麒麟软件有限公司、江苏意源科技有限公司、中国信息通信研究院、北京信长城科技发展有限公司、中科信息安全共性技术国家工程研究中心有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、中国电子信息产业集团有限公司第六研究所、深圳市永达电子信息股份有限公司、中国电力科学研究院有限公司。

本文件主要起草人：马洪富、刘平、王志达、党伟、郑强、汪宗斌、袁峰、孔凡玉、王泉景、袁中林、王中武、李向锋、肖鹏、安学刚、赵丽丽、肖飞、王玉林、程超、刘晶、邹静、艾渤、杜杰伟、刘健、辛晨、刘懿、康和、

王影新、赵勇智、曹然、韩浩、张大朋、姜建功、王娟娟、刘鹏、胡建勋、白利芳、田朝阳、王龙、戚建淮、范晶、王子涛。

本文件及其所代替文件的历次版本发布情况为：

——2017 年首次发布为 GB/T 33560—2017；

——本次为第一次修订。

引　言

在密码应用中，通常使用某一字段或短语来标识所使用的密码算法或数据实体信息。为达成密码协议、密码接口间的互联互通，需要对这些标识进行统一规范的定义。

本文件的目标是规范密码协议接口和管理方面使用的标识，以实现密码基础设施各组件间的兼容和统一，也能有效地指导、帮助密码产品的研制和协议的实现，有利于管理部门实施有效的管理。

网络安全技术　密码应用标识

1　范围

本文件规定了密码应用中所使用的密码服务类标识、安全管理类标识，以及商用密码领域中的相关OID定义。

本文件适用于密码产品、密码系统的研制和使用，也适用于相关标准、协议的编制。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 25069　信息安全技术　术语

3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

标识符　identifier

用于标识在密码应用中涉及的密码算法、运算数据、角色管理、密钥管理、系统管理和产品管理的一个整数。

4　缩略语

下列缩略语适用于本文件。

BC：分组链接（Block Chaining）

CBC：密码分组链接模式（Cipher Block Chaining）

CCM：CBC计数器模式（Counter with CBC-MAC）

CFB：密文反馈模式（Ciphertext Feedback）

CRL：证书撤销列表（Certificate Revocation List）

CTR：计数器模式（Counter）

DER：可辨别编码规则（Distinguished Encoding Rules）

ECB：电码本模式（Electronic Code Book）

FPE：保留格式加密（Format-preserving encryption）

GCM：伽罗瓦/计数器工作模式（Galois/Counter Mode）

HCTR：带泛杂凑函数的计数器（universal Hash function based CTR）

HMAC：采用杂凑算法计算的消息验证码（Hash-based Message Authentication Code）

IBC：基于标识的密码技术（Identity-Based Cryptography）

MAC：消息鉴别码（Message Authentication Code）