



中华人民共和国密码行业标准

GM/T 0090—2020

标识密码应用标识格式规范

Specification of identity format for identity cryptography application

2020-12-28 发布

2021-07-01 实施

国家密码管理局 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 标识结构	1

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。

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

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京国脉信安科技有限公司、深圳奥联信息技术有限公司、青岛博文广成信息技术有限公司、北京迪曼森数字标识技术有限公司、北京握奇数据股份有限公司、西安电子科技大学、西安工业大学。

本文件主要起草人：袁峰、蔡先勇、范修斌、杨恒亮、谷德富、唐璐瑶、药乐、蒋楠、汪雪林、王琨、容晓峰。

引 言

本文件的目标是给出一种标识密码技术中通用的标识信息描述,为各种标识密码技术提供具备可相互辨识性、包涵性的结构化标识数据结构。

本文件仅从标识的结构框架进行描述,不针对任何一种标识密码算法或者实现技术。

标识密码应用标识格式规范

1 范围

本文件规定了一种通用标识信息标识数据结构。

本文件适用于基于 SM2 算法和 SM9 算法的标识密码技术的应用,使不同标识密码技术体系之间标识信息能相互辨识和解析。

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 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法
GM/T 0006 密码应用标识规范
GM/T 0044(所有部分) SM9 标识密码算法
GM/Z 4001—2013 密码术语

3 术语和定义

GM/T 0044(所有部分)和 GM/Z 4001—2013 界定的以及下列术语适用于本文件。

3.1

标识 identity

可唯一确定一个实体身份的信息。

注:标识由实体无法否认的信息组成,如实体的可识别名称、电子邮箱、身份证号、电话号码、街道地址等。

3.2

SM2 算法 SM2 algorithm

由 GB/T 32918(所有部分)定义的一种算法。

3.3

SM9 算法 SM9 algorithm

由 GM/T 0044 定义的一种基于标识的密码算法。

4 标识结构

标识的 ASN.1 数据格式定义为:

```
Identifier ::= SEQUENCE{
    version(0)          EXPLICIT VERSION DEFAULT v1,
    identityType        OBJECT IDENTIFIER,
    alias               UTF8STRING,
    identityData        OCTET STRING,
```