ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 46798—2025

网络安全技术　标识密码认证系统密码及其相关安全技术要求

Cybersecurity technology—Technical requirements for cryptography and related security of identity-based cryptographic authentication system

2025-12-02 发布　　2026-07-01 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。

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：北京国脉信安科技有限公司、深圳奥联信息安全技术有限公司、格尔软件股份有限公司、兴唐通信科技有限公司、中国电子技术标准化研究院、北京海泰方圆科技股份有限公司、广东省电子商务认证有限公司、三未信安科技股份有限公司、智巡密码(上海)检测技术有限公司、金盾检测技术股份有限公司、中电科网络安全科技股份有限公司、厦门民航凯亚有限公司、长春吉大正元信息技术股份有限公司、济南三泽信息安全测评有限公司、北京时代亿信科技股份有限公司、华为技术有限公司、浙江国利信安科技有限公司、南方电网数字电网集团(广东)有限公司、国网新疆电力有限公司、新疆华电苇湖梁新能源有限公司、北京中科卓信软件测评技术中心、上海势炎信息科技有限公司、北京建恒信安科技有限公司、北京数字认证股份有限公司、中国网络空间研究院、企知道科技有限公司、郑州信大捷安信息技术股份有限公司、数安时代科技股份有限公司、工业和信息化部网络安全产业发展中心、中金数据(武汉)超算技术有限公司、工信通(北京)信息技术有限公司、国网区块链科技(北京)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、中国人民解放军国防科技大学、奇安信网神信息技术(北京)股份有限公司、中国电子信息产业集团有限公司第六研究所、陕西省信息化工程研究院。

本文件主要起草人：袁峰、封维端、蔡先勇、郑强、孙皇龙、但波、王立欣、李晓千、郑丽娟、黄晶晶、罗影、张立圆、药乐、陈树乐、李雪雁、王现方、曾光、匡云、尹文基、王迎、丁肇伟、张荣泽、刘伟丰、陈洁、邢伟、黄福飞、艾微、张玉柱、林培桂、杨延栋、刘海明、杨伟、张磊、王兵、乔梦宇、王震、刘中、梁松涛、林浩、周蔚林、王进、王斌、石竹玉、胡建勋、邢倩倩、安锦程、王龙、赵晓荣。

网络安全技术　标识密码认证系统
密码及其相关安全技术要求

1　范围

本文件规定了标识密码认证系统密钥生成、管理以及公开参数查询等服务的安全要求和技术要求。

本文件适用于标识密码认证系统的设计、开发、使用和检测。

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 22239—2019　信息安全技术　网络安全等级保护基本要求

GB/T 25069　信息安全技术　术语

GB/T 32905　信息安全技术　SM3 密码杂凑算法

GB/T 32907　信息安全技术　SM4 分组密码算法

GB/T 32918（所有部分）　信息安全技术　SM2 椭圆曲线公钥密码算法

GB/T 37092　信息安全技术　密码模块安全要求

GB/T 38635—2020（所有部分）　信息安全技术 SM9 标识密码算法

GM/T 0016—2023　智能密码钥匙密码应用接口规范

GM/T 0018—2023　密码设备应用接口规范

GM/T 0057—2018　基于 IBC 技术的身份鉴别规范

GM/T 0081—2020　SM9 密码算法加密签名消息语法规范

GM/T 0090—2020　标识密码应用标识格式规范

3　术语和定义

GB/T 38635—2020（所有部分）和 GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

鉴别　authentication

确认一个实体所声称的身份或属性的过程。

3.2

标识　identity

可唯一确定实体身份且不可否认的信息。

注 1：本文件中标识为符合 GM/T 0090—2020 中 Identifier 定义的数据。

注 2：GM/T 0090—2020 中 Identifier 的 identityData 为实体的可识别名称、电子邮箱、身份证号、电话号码、设备编号、街道地址等。

［来源：GB/T 38635.1—2020，3.1，有修改］