ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 46798-2025

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

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

Issued on: December 2, 2025 **Implemented on: July 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1.Structure and Drafting Rules of Standardization Documents". Drafting. Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents. This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: Beijing Guomai Xin'an Technology Co., Ltd., Shenzhen Aolian Information Security Technology Co., Ltd., and Gels Software Co., Ltd. Limited Company, Xingtang Communication Technology Co., Ltd., China Electronics Technology Standardization Institute, Beijing Haitai Fangyuan Technology Co., Ltd., Guangdong Province E-commerce Certification Co., Ltd., Sanwei Xin'an Technology Co., Ltd., Zhixun Password (Shanghai) Testing Technology Co., Ltd., and Jindun Testing Technology Co., Ltd. Technology Co., Ltd., China Electronics Technology Network Security Technology Co., Ltd., Xiamen Civil Aviation Kaiya Co., Ltd., Changchun Jida Zhengyuan Information Technology Co., Ltd. Joint-stock company, Jinan Sanze Information Security

Assessment Co., Ltd., Beijing Shidai Yixin Technology Co., Ltd., Huawei Technologies Co., Ltd. Zhejiang Guoli Xin'an Technology Co., Ltd., China Southern Power Grid Digital Grid Group (Guangdong) Co., Ltd., State Grid Xinjiang Electric Power Co., Ltd., Xinjiang Hua Dianweihu Liang New Energy Co., Ltd., Beijing Zhongke Zhuoxin Software Testing Technology Center, Shanghai Shiyan Information Technology Co., Ltd., Beijing Jianhengxin An Technology Co., Ltd., Beijing Digital Certification Co., Ltd., China Academy of Cyberspace Studies, Qizhidao Technology Co., Ltd., Zhengzhou Xindajie An Information Technology Co., Ltd., Data Security Era Technology Co., Ltd., Cybersecurity Industry Development Center of the Ministry of Industry and Information Technology, CICC Data (Wuhan) Supercomputing Technology Co., Ltd., Gongxintong (Beijing) Information Technology Co., Ltd., State Grid Blockchain Technology (Beijing) Co., Ltd. Zhongke Information Security Common Technology National Engineering Research Center Co., Ltd., National University of Defense Technology of the Chinese People's Liberation Army, Qi An Xin Wang Shen Information Technology Co., Ltd. Technology (Beijing) Co., Ltd., the Sixth Research Institute of China Electronics Information Industry Group Co., Ltd., and Shaanxi Provincial Information Engineering Research Institute. The main drafters of this document are. Yuan Feng, Feng Weiduan, Cai Xianyong, Zheng Qiang, Sun Huanglong, Dan Bo, Wang Lixin, Li Xiaoqian, Zheng Lijuan, and Huang Jingjing. Luo Ying, Zhang Liyuan, Yao Le, Chen Shule, Li Xueyan, Wang Xianfang, Zeng Guang, Kuang Yun, Yin Wenji, Wang Ying, Ding Zhaowei, Zhang Rongze, Liu Weifeng, Chen Jie Xing Wei, Huang Fufei, Ai Wei, Zhang Yuzhu, Lin Peigui, Yang Yandong, Liu Haiming, Yang Wei, Zhang Lei, Wang Bing, Qiao Mengyu, Wang Zhen, Liu Zhong, Liang Songtao Lin Hao, Zhou Weilin, Wang Jin, Wang Bin, Shi Zhuyu, Hu Jianxun, Xing Qianqian, An Jincheng, Wang Long, Zhao Xiaorong. Network security technology identification password authentication system Cryptography and related security technical requirements

1 Scope

GB/T 46798-2025 is the Chinese national standard covering identity-based cryptography - where a public key is derived from the identity itself, so no certificate is needed, at the cost of a key generation centre that can compute every private key and therefore must be protected accordingly. At 26,000 words, first edition, with the public key framework GB/T 46795-2025. Issued on 2 December 2025, it has been in force since 1 July 2026.

This document specifies the security and technical requirements for services such as key generation, management, and public parameter querying in the identification cryptographic authentication system. This document applies to the design, development, use, and testing of identification and password authentication systems.

2 Normative references

The contents of the following documents, through normative references within the text,

constitute essential provisions of this document. Dated citations are not included. For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies. This document.

GB/T 22239-2019 Information Security Technology - Basic Requirements for Network Security Level Protection

GB/T 25069 Information Security Technical Terminology

GB/T 32905 Information Security Technology - SM

3 Terms and Definitions

The terms and definitions defined in GB/T 38635-2020 (all parts) and GB/T 25069, as well as the following terms and definitions, apply to this document.

3.1 Authentication The process of verifying the identity or attributes claimed by an entity.

3.2 Identity Information that can uniquely identify an entity and is undeniable. Note

1.Data in this document is identified as conforming to the Identifier definition in GM/T 0090-2020. Note

2.In GM/T 0090-2020, the identityData of the Identifier is the entity's identifiable name, email address, ID card number, telephone number, and device code. Number, street address, etc. [Source: GB/T 38635.1-2020, 3.1, with modifications]

4 Block Cipher Algorithm

GB/T 32918 (all parts) Information Security Technology SM