ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43206-2023

Information security technology - Testing and evaluation requirements for information system cryptography application

信息安全技术 信息系统密码应用测评要求

Issued on: September 7, 2023 **Implemented on: April 1, 2024**

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 be subject to patents. The publisher of this document assumes no responsibility for identifying patents. This document is proposed and coordinated by the National Information Security Standardization Technical Committee (SAC/TC260). This document was drafted by: Commercial Cryptometry Testing Center of the State Cryptography Administration, Institute of Information Engineering, Chinese

Academy of Sciences, and the Third Research Institute of the Ministry of Public Security. Research Institute, National Information Technology Security Research Center, China Electronics Technology Group Corporation 15th Research Institute, China Electronics Technology Standardization Institute, National Information Center, Fifth Institute of Electronics of the Ministry of Industry and Information Technology, Institute of Software of the Chinese Academy of Sciences, Beijing Municipal Government Information Security Center Center (Beijing Information Security Evaluation Center), Beijing National Digital Financial Technology Testing Center Co., Ltd., Shenzhen Network Security Computer Security Testing Technology Technology Co., Ltd., Daopu Information Technology Co., Ltd., Guodian Nanjing Automation Co., Ltd., Zhejiang Dongan Testing Technology Co., Ltd., Beijing UnionPay Gold Card Technology Co., Ltd., Zhixun Password (Shanghai) Detection Technology Co., Ltd., Harbin Institute of Technology (Shenzhen), Anhui Kechai Information Technology Technology Co., Ltd., Xinjiang Quantum Communication Technology Co., Ltd. The main drafters of this document. Luo Peng, Xiao Qiulin, Ma Yuan, Zhang Lihua, Xu Changwei, Chen Tianyu, Huang Jingjing, Zheng Fangyu, Tian Minqiu, Wang Bing, Liu Jian, Yang Hongzhi, Wu Dongyu, Lu Zhen, Zhang Yuxiang, Li Sheng, Ren Jinqiang, Li Shuilin, Li Dawei, Li Hongzhuo, Zhang Wuyi, Zhang Xiaoxi, Yang Chen, Cai Yiming, Sun Xin, Gao Rui, Lu Na, Song Lingwei, Guo Shoukun, He Shuangyu, Yang Long, Li Xia, Wang Guochao, Hu Gai, Hu Yanxiong, Shen Ting, Zhang Shaobo, Han Wei. Information security technology Information system password application evaluation requirements

1 Scope

GB/T 43206-2023 sets the testing and evaluation requirements for the use of cryptography in information systems. Chinese law requires systems above a certain protection level to use approved commercial cryptography and to have that use assessed, which turns a set of good intentions into an audit: it is not enough to hold a licensed product, the algorithms must be the approved ones, the keys must be generated, stored, used and destroyed properly, and the cryptography must actually protect the things it is claimed to protect. The standard sets the general assessment requirements covering the algorithms, the techniques, the products, the services and the key management, then the technical evaluation requirements from physical and environmental security upward through network, computing and application and data security, and the management evaluation requirements covering the management system, personnel, construction and operation, and emergency response. It took effect on 1 April 2024.

This document stipulates the general evaluation requirements, technical evaluation requirements, and management evaluation requirements for information system level one to level four password applications. requirements, and provides requirements for overall assessment requirements, risk analysis and evaluation, and assessment conclusions.

Note. The information system password application levels described in this document are

consistent with the password application levels specified in GB/T 39786-2021, among which the fifth-level password application Assessment requirements are not described in this document. This document is suitable for guiding and standardizing the evaluation activities in the security assessment of information system password applications.

2 Normative reference documents

The contents of the following documents constitute essential provisions of this document through normative references in the text. Among them, the dated quotations For undated referenced documents, only the version corresponding to that date applies to this document; for undated referenced documents, the latest version (including all amendments) applies to this document.

GB/T 25069-2022 Information security technical terms

GB/T 39786-2021 Basic requirements for information security technology information system password application GM/Z4001 cryptographic terminology

3 Terms and definitions

The following terms and definitions as defined in GB/T 25069-2022, GB/T 39786-2021 and GM/Z4001 apply to this document. document.

3.1 Pass the assessment recognized by the national cryptography management department or have the professional skill level certificate of cryptography technology application technician or cryptography engineering technician Book, personnel engaged in security assessment of cryptographic applications.

Note. Referred to as "secret evaluator".

3.2 Checkexamine Secret evaluators conduct interviews, document review, on-site inspection and analysis of evaluation objects to help the secret evaluators understand, clarify or obtain evidence. the process of.

Note. Please refer to GM/T 0116-2021 for the evaluation methods that can be used during verification and the method selection instructions. [Source: GB/T 25069-2022, 3.237, with modifications]

3.3 A relatively independent and complete set of assessment content, consisting of assessment indicators, assessment objects, assessment implementation and result determination.