

ICS 35.030
CCS L80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 43207-2023

**Information security technology - Guidelines of design for
information system cryptography application**

信息安全技术 信息系统密码应用设计指南

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

1 Scope	1
2 Normative reference documents	1
3 Terms and Definitions	1
4 Information system password application framework	1
5 Design principles for password application solutions	3
6 Password application solution design process	3
6.1 Overview	3
6.2 Analysis of password application requirements	3
6.3 Analysis of cryptographic application design	3
6.4 Security and Compliance Analysis	3
7 Password Application Solution Design Guide	4
7.1 Cryptozoological application technology framework	4
7.2 Computing platform password application solution	4
7.3 Password support platform solution	4
12 Reference	14

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: Dingxuan Commercial Cryptometry Evaluation Technology (Shenzhen) Co., Ltd., Institute of Information Engineering, Chinese Academy of Sciences, Harbin Institute of Technology University of Technology (Shenzhen), China Electronics Network Security Technology Co., Ltd., Beijing Hitech Fangyuan Technology Co., Ltd., Xingtang Communication Technology Co., Ltd. Co., Ltd., Beijing Digital Certification Co., Ltd., Third Research Institute of the Ministry of Public Security, National Information Technology Security Research Center, Beijing Xin'an Century Science and Technology Technology Co., Ltd., China National Engineering Research Center for Information Security Common Technology Co., Ltd., Beijing Product Quality Supervision and Inspection Research Institute, Ping An Insurance (Group) Co., Ltd. of China. The main

drafters of this document. Li Dawei, Chen Lei, Xiao Fei, Ma Yuan, Zheng Fangyu, Zhou Junping, Wang Xuejin, Jiang Hongyu, Yang Yuanyuan, Fu Dapeng, Liu Shangyan, Wang Yanli, Wu Dongyu, Wang Zongbin, Qin Tihong, Xu Genwei, Hu Jianxun, Li Hengyu, Li Rui, Jia Shijie, Chen Tianyu. Information security technology Information system password application design guide

1 Scope

GB/T 43207-2023 gives the design guidance for applying cryptography in information systems. Chinese law requires systems above a protection level to use approved commercial cryptography and to be assessed on it; the assessment standard says what will be checked, and this document says how to build a system that passes - which is a different problem, because retrofitting cryptography into a finished system almost never works, and the design decisions that matter are taken early. The standard sets the cryptography application framework for an information system, the design principles for a cryptography application scheme, the design process covering the analysis of requirements, the design analysis and the security and compliance analysis, and the design guidance itself for the technical framework, the computing platform, the cryptographic support platform and the business applications, with a normative annex giving the scheme template. It took effect on 1 April 2024.

This document gives information system password application design guidelines, including information system password application framework, password application solution design principles, Password application solution design process and password application solution design guide. This document is suitable for guiding the design of information system password application solutions, and can also be used as a guide for the construction of information system password protection and password application security. Security assessment and reference for the password application security assessment and filing work of the password management department.

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 22240 Information security technology network security level protection grading guide

GB/T 25069 Information Security Technical Terminology

GB/T 39786 Basic requirements for information security technology information system password application

3 Terms and definitions

The terms and definitions defined in GB/T 25069 and GB/T 39786 and the following apply to this document.

3.1 It is used to guide information system responsible entities to use cryptographic technology compliantly, correctly, and effectively, and to deploy plans for cryptographic security systems.

4 Information system password application framework

The password application framework of information systems using password protection is shown in Figure 1.