ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 45230-2025

Data security technology - General framework for the confidential computing

数据安全技术 机密计算通用框架

Issued on: January 24, 2025 **Implemented on: August 1, 2025**

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

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part

1.Structure and drafting rules for standardization documents" Drafting. This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: Huawei Technologies Co., Ltd., China Mobile Communications Group Co., Ltd., China Electronics Technology Standardization Institute, Institute of Software, Chinese Academy of Sciences, Ant Group Co., Ltd., Beijing Baidu Netcom Technology Co., Ltd., Beijing Volcano Engine Technology Co., Ltd., Tencent Cloud Computing (Beijing) Co., Ltd., Alibaba Cloud Computing Co., Ltd., Beijing Chongliang Online Technology Co., Ltd., China Mobile Dongtong Communication Group Design Institute Co., Ltd., Industrial and Commercial Bank of China Co., Ltd., Sichuan University, China Minsheng Bank Co., Ltd., Beijing National Financial Technology Certification Center Co., Ltd., Beijing Digital Certification Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd., Nanhu Laboratory, Peking University, Huakong Qingjiao

Information Technology (Beijing) Co., Ltd., China Unicom Group Co., Ltd., Super Fusion Digital Technology Technology Co., Ltd., Shanghai Jiao Tong University, China Information Technology Co., Ltd., Institute of Information Engineering, Chinese Academy of Sciences, Changyang Technology (Beijing) Co., Ltd. Co., Ltd., Zhengzhou Xindajiean Information Technology Co., Ltd., Hangzhou Wei Information Technology Co., Ltd., Shanghai Fushu Technology Co., Ltd., China Electronics Cloud Computing Technology Co., Ltd., Intel (China) Co., Ltd. Beijing Branch, Kunlun Tech (Beijing) Technology Co., Ltd. Strong striker.

Confidential computing is a computing model used to protect data security during use. Hardware isolation prevents the code and data in the environment from being monitored and manipulated by other software (including privileged software) running on the same device during computing. Specifically, confidential computing uses an isolation mechanism to separate the ordinary computing environment from the confidential computing environment, so that unauthorized entities cannot Ability to access confidential computing environments; verify confidential computing environments and applications running in them through certification mechanisms to ensure confidential computing The integrity and authenticity of the environment and applications; the encryption mechanism is used to ensure that the data at runtime is in ciphertext. It can be used alone to protect data in use, or it can be combined with other cryptographic techniques (such as multi-party secure computing, homomorphic encryption, etc.) to jointly protect Protecting runtime data and code, especially for application scenarios such as machine learning, federated learning, blockchain, cloud computing, big data, etc., can be effective The security protection challenges faced when using data. This document aims to propose a general confidential computing framework by defining the necessary components of the confidential computing framework, the basic functions it has, and The confidential computing services formed by the interaction between components improve the usability, security and compatibility of confidential computing related products, and provide a To meet the cloudification needs of various industries, this document also proposes the deployment of confidential computing virtualization. model. Data security technology confidential computing general framework

1 Scope

GB/T 45230-2025 sets the Chinese general framework for confidential computing, the technology that protects data while it is being processed rather than only at rest and in transit. Its premise is that the operator of the machine should not be able to see the data running on it, which is what makes cloud processing of sensitive data possible at all, and which is achieved by hardware-enforced trusted execution environments together with remote attestation that proves to the data owner what code is actually running. The standard defines the participating roles and the relationships between them, the data owner, the workload provider, the infrastructure operator, the hardware vendor and the attestation service, and then the general framework layer by layer: the hardware layer that provides the isolation, the system software layer, the system service layer, the application

layer and the security layer that spans them, together with the attestation, key management and lifecycle requirements. For any organisation evaluating or building confidential computing in China, this is the reference architecture the market will be described in. It takes effect on 1 August 2025.

This document establishes a general framework for confidential computing, describes the core components and basic functions of the framework, and provides confidential computing services and implementations. Current mechanism. This document is intended for reference by parties involved in confidential computing when designing, developing, using and deploying confidential computing related products or solutions. Provide a reference for conducting confidential computing capability assessment activities.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document. For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document.

GB/T 25069-2022 Information Security Technical Terminology

GB/T 32915-2016 Information security technology Binary sequence randomness detection method

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and the following apply to this document.

3.1 Component In a system, an identifiable and distinguishable part that implements part of its functionality. [Source: GB/T 25069-2022, 3.815]

3.2 secure channel secure channel A communications channel that provides confidentiality and authenticity for exchanged messages. [Source: GB/T 25069-2022, 3.32, modified]

3.3 A computing model that protects the security of data in use through isolation, encryption, certification and other mechanisms based on trusted hardware.

3.4 A collection of basic hardware and software for performing confidential computing tasks.

3.5 A program that runs in a confidential computing environment and is used to implement confidential computing capabilities.

3.6 A computing environment built based on the confidential computing platform to support the operation of confidential computing applications.