

ICS 35.240
CCS A 90

GA

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

GA/T 1574-2019

**Information security technology - Security technology
requirements for database security reinforcement products**

信息安全技术 数据库安全加固产品安全技术要求

(English Translation)

Issued on: January 1, 1970

Implemented on: July 1, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Database Security Hardening Product Description
5 General description of database security hardening products
5.1 Classification of safety technical requirements
5.2 Classification of Security Levels.
6 Safety function requirements
6.1 Dual system authentication
6.2 Data storage encryption
6.3 Application permission control
6.4 Ciphertext access control
6.5 Cipher text index
6.6 Integrity check
6.7 Separation of permissions
6.8 Database status monitoring
6.9 Other functional requirements
7 Self-safe function requirements
7.1 User Identification
7.2 Identification
7.3 Anti-unloading function (if applicable)
7.4 Security management
7.5 Audit logs
8 Security requirements
8.1 Development
8.2 Guidance documents
8.3 Life cycle support
8.4 Testing
8.5 Vulnerability assessment
9 Classification requirements
9.1 Overview

9.2 Classification of safety function requirements

9.3 Level classification of self-safety requirements

9.4 Classification of security requirements

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security, the Third Research Institute of the Ministry of Public Security, Beijing Zhongan Nebula Software Technology Co., Ltd.

1 Scope

This standard specifies the security function requirements, self-security function requirements, security guarantee requirements, and classification of database security hardening products.

Claim.

This standard applies to the design, development, and testing of database security hardening products.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336.3-2015 Information technology security technology Information technology security assessment guidelines Part 3. Security assurance components GB/T 25069-2010 Information Security Technology Terminology

3 Terms and definitions

GB/T 18336.3-2015, GB/T 25069-2010 and the following terms and definitions apply to this document.

Database security reinforcement product Based on traditional database management systems (such as Oracle, Mysql, SQLserver, DB2, etc.) A product with enhanced security functions based on technical means such as encryption, access control, and data integrity protection.

Ciphertext access control Control access to ciphertext data stored in the database.

Ciphertext index

The ciphertext retrieval is performed on the index established by the ciphertext data stored in the relational database.

Data storage encryption the important data in the database is encrypted at the storage level through an encryption algorithm.

4 Database Security Hardening Product Description

Database security hardening products generally consist of components such as a security server, security agent, and management. The security server is mainly responsible for data Management and distribution of encryption and decryption, permission verification, and security policies; security agents are installed on database servers that need to be hardened, and are mainly responsible for encryption and decryption.

The receiving and execution of solid policies; the management side is mainly a graphical tool for operation and maintenance personnel to implement system management. The product is authenticated through dual systems, Data encryption, access control, data integrity protection and other technical means, products with enhanced security functions for databases to make up for general data Defects of low library security.

Figure 1 is a typical operating environment for database security hardening products.

Figure 1 Typical operating environment of database security hardening products

5.1 Classification of safety technical requirements

This standard divides the database security hardening product security technical requirements into security function requirements, own security function requirements, and security assurance requirements Three categories. Among them, the security function requirements are specific requirements for the security functions that database security hardening products should have, including dual system authentication, Data storage encryption, application permission control, ciphertext access control, ciphertext index,

integrity check, permission separation, database status monitoring, Other functional requirements, etc .; the requirements for own security functions are requirements for the security functions that the database security hardening product should have.

Including user identification, identity authentication, anti-unloading functions, security management and audit logs, etc .; security assurance requirements for database security hardening products the content of the product development and use documents put forward specific requirements, including development, instructional documents, life cycle support and testing.

The administrator account of the database security hardening product should adopt at least three separate designs, including system administrator, security administrator, and security Auditor.

5.2 Classification of security levels

This standard divides the level of security function requirements according to the strength of the database security hardening product security function.

GB/T 18336.3-2015 divides the levels of security requirements. The security level highlights security features, and is divided into basic and enhanced levels.

Strength, weakness, and security requirements are the specific basis for the classification.

6.1 Dual system authentication

In addition to the database management system's authentication, the database management system account should also strengthen the identity of the product through database security.

Identification.

6.2 Data storage encryption

The product supports data encryption.

- a) should be able to encrypt the specified data;
- b) data encryption granularity should support table/field level;
- c) Support random number encryption technology to ensure that the same plaintext data is encrypted differently after being encrypted;
- d) Encryption algorithms specified by the National Password Administration shall be supported.