

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

JR/T 0204-2020

**Distributed Database Technology Financial Application
Specification Security Technical Requirements
(English Translation)**

Issued on: November 26, 2020

Implemented on: November 26, 2020

Issued by: People's Bank of China

Table of Contents

Foreword	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Overview	
6 Basic support guarantee	
6.1 Cybersecurity requirements	
6.2 System safety requirements	
6.3 Equipment safety requirements	
7 User Management	
7.1 Identification and authentication	
7.2 User authorization	
7.3 Role management	
8 Access control	
8.1 Object access control	
8.2 Cluster access control	
8.3 Session access control	
8.4 Node access control	
8.5 Resource control	
8.6 Read and write security policy	

Foreword

This document starts from the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules of Standardization Documents" grass.

This document was submitted by the People's Bank of China. Please note that some of the contents of this document may involve patents. The issuing agency of this document is not responsible for Don't be responsible for these patents.

This document is under the jurisdiction of the National Financial Standardization Technical Committee (SAC/TC 180).

Introduction

With the transformation and upgrading of the distributed architecture in the financial field, the application of distributed database technology in the financial field has gradually deepened. Distributed for the specification Application of database technology in the financial field, strengthen the technical support of distributed database technology for financial services, and improve the performance of distributed database technology this document is specially prepared for business continuity and information security assurance capabilities.

This document is one of the distributed database technology financial application series standards. The distributed database technology financial application series standards include.

- "Technical Framework of Distributed Database Technology Financial Application Specification";

- "Distributed Database Technology Financial Application Specification Security Technical Requirements";

- "Disaster Recovery Requirements for Distributed Database Technology Financial Application Specification".

Distributed database technology financial application specification security technical requirements

1 Scope

This document specifies the security requirements for distributed transaction database technology in the financial sector, covering basic support guarantees, user management, and access Control, data security, monitoring and early warning, key management, security management, and security auditing.

This document is suitable for the development, testing, evaluation and application of distributed transaction databases in the financial sector.

2 Normative references

The contents of the following documents constitute the indispensable clauses of this document through normative references in the text. Among them, dated reference documents, Only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document file.

GB/T 32633 Distributed relational database service interface specification JR/T 0203 Distributed database technology financial application specification technical architecture

3 Terms and definitions

The terms and definitions defined by JR/T 0203 apply to this document.

4 Abbreviations

The following abbreviations apply to this document.

DCL. Data Control Language DDL. Data Definition Language (Data Definition Language)
DML. Data Manipulation Language (Data Manipulation Language) DQL. Data Query
Language IO. Input and Output (Input Output) QPS. Queries Per Second (Queries Per
Second) SQL. Structured Query Language (Structured Query Language) TPS. Transactions
Per Second (Transactions Per Second)

5 Overview

Compared with traditional centralized databases, distributed transaction databases have horizontal server expansion, separation of computing and storage, data fragmentation, and multiple Replica technology achieves the advantages of large-capacity storage, high-concurrency processing, high data reliability, and high service availability. This document mainly guarantees from basic support, User management, access control, data security, monitoring and early warning, key management, security management and security audit According to the security requirements of database financial applications.

This document divides the specific clauses into basic requirements and enhanced requirements. The basic requirements are general and basic security requirements, distributed transaction data the library should be fully supported; enhancement requirements are recommended requirements from the development trend of security technology and the forward-looking needs of financial users.

The security system of the distributed transaction database is shown in Figure 1.

Figure 1 Distributed transaction database security system

6.1 Cybersecurity requirements

basic requirements.

a) Different network security areas should be divided, and security isolation levels should be set. Distributed transaction database clusters should be deployed in high security Level within the area.

b) The network domain deployed by the distributed transaction database cluster should be regularly tested for security penetration, and network security vulnerabilities should be repaired.

Enhancement requirements.

- a) The physical isolation of the deployed different database cluster networks should be ensured.
- b) The physical isolation between the network that provides external services and the database management network should be ensured.

6.2 System safety requirements

basic requirements.

- a) The access control strategy of the system should be determined according to business requirements and system security analysis.
- b) A system security management system should be established, and the system security strategy, security configuration, log management and daily operation procedures should be implemented.

Specify specific regulations.

- c) Malicious code static detection and behavior detection should be performed on the underlying software environment on which the distributed transaction database cluster depends on a regular basis, and timely update the security patch package, such as operating system, virtualization software.
- d) The open source components on which the distributed transaction database cluster depends should be statically detected and behaviorally detected for malicious code, and Update the security patch package from time to time.

Enhancement requirements.

6.3 Equipment safety requirements

basic requirements.

- a) The key equipment should be deployed redundantly according to high availability requirements.
- b) Data storage devices should be safely cleared when they are reused, replaced, or scrapped.
- c) The cryptographic equipment shall be safely cleared of the key when it is reused, replaced, or discarded.
- d) Respond to the safe removal of sensitive configuration information when key network equipment is reused, replaced, or scrapped.

Enhancement requirements.