Design and Implementation of Enterprise-oriented Quantum Key Injection Service Platform

Yan Zhuang, Ning Lü, Peizu Chen, Xuebing Gong, Hao Zheng, Pengcong Chen
China Mobile Internet Co., Ltd., Super SIM Business Unit, Guangzhou 510640, Tianhe, China
Corresponding author: Yan Zhuang (e-mail: cmicsupersimzy@163.com).

ABSTRACT This paper focuses on the application requirements of enterprise-level quantum key injection services in the field of quantum secure communication. The article first introduces the development status of quantum key injection technology and its demand characteristics in enterprise application scenarios, points out the shortcomings of traditional individual user service models in enterprise-level applications such as low management efficiency, coarse permission control, and difficulties in multi-organization collaboration, and then proposes an architecture design and implementation method for enterprise-oriented quantum key injection service platform. The platform adopts multi-tenant architecture and three-terminal service mode to realize hierarchical management of enterprise customers, provincial company operators, and platform operators. Through mechanisms such as injection device authentication, refined permission control, and organizational structure linkage, it can effectively support the large-scale operation of enterprise-level quantum key injection business, providing reliable platform support for the promotion of quantum secure communication technology in enterprise-level application scenarios.

INDEX TERMS Quantum Key Injection; Enterprise Service Platform; Multi-tenant Architecture; Injection Device Authentication; Permission Managemention and noise

I. INTRODUCTION

In recent years, quantum secure communication technology has evolved from laboratory research to industrial application, with a series of demonstration projects implemented in sectors such as government affairs, finance, and power utilities. As the infrastructure for quantum key distribution (QKD) networks continues to improve, ensuring efficient and secure delivery of quantum keys to end users has become pivotal to scaling up quantum secure communication applications.

As a critical security component in mobile communications, the super SIM card offers comprehensive capabilities including secure storage, cryptographic computation, and identity authentication, providing an ideal secure environment for storing quantum keys. The initially established quantum key storage platform has successfully delivered decentralized storage services for individual users, demonstrating the feasibility of securely distributing quantum keys to SIM cards. However, as quantum secure communication applications expand into enterprise environments, traditional user service models exhibit significant shortcomings in organizational management, permission control, and multi-tenant isolation, making it imperative to develop a dedicated enterprise-oriented quantum key storage service platform.

The initial quantum key distribution platform primarily provided fragmented distribution services to individual users, enabling secure issuance of quantum keys based on the BIP protocol. However, with the continuous expansion of quantum secure communication applications, an increasing number of enterprise customers have demanded organized, large-scale quantum key distribution solutions. The traditional service model for individual users presents several challenges in enterprise environments: first, it lacks organizational structure management capabilities, making it impossible to batch-associate personnel with cards; second, permission control granularity is too coarse to meet enterprises' needs for refined management; third, there is a lack of multi-organization collaboration mechanisms, resulting in low operational efficiency in business cooperation between provincial companies and enterprises.

Therefore, this paper proposes a design and implementation approach for an enterprise-oriented quantum key storage service platform. The platform adopts a multi-tenant architecture and a three-tier service model, establishing a three-level service framework comprising an enterprise service management layer, a provincial company operation management layer, and a platform operation management layer. Through mechanisms such as enterprise organizational structure management, authentication of storage devices, and fine-grained permission control, it provides com-

prehensive platform support for enterprise-level quantum key storage operations.

II. RESEARCH BACKGROUND

A. CURRENT STATUS OF QUANTUM KEY DISTRIBUTION TECHNOLOGY DEVELOPMENT

Quantum key distribution technology leverages the non-clonability of quantum states and measurement interference properties, enabling both parties in communication to detect any eavesdropping attempts and thereby ensuring key security. Currently, this technology has moved from laboratory research to practical applications, with a series of demonstration projects implemented in sectors such as government affairs, finance, and power utilities.

Quantum key injection refers to the secure writing of quantum keys into a super SIM card. The initially established quantum key injection platforms primarily provide decentralized injection services for individual users, establishing secure communication channels between SIM cards and servers via the BIP protocol, while employing national cryptographic algorithms to implement multi-layered security protection for quantum keys.

B. ENTERPRISE-LEVEL APPLICATION REQUIREMENTS ANALYSIS

As quantum secure communication applications continue to expand, enterprise customers have developed new demands for quantum key distribution services:

(1) Organizational management requirements: Enterprises need to establish an internal organizational structure to enable batch association management of personnel information with SIM cards.

(2) Large-scale loading requirement: Enterprises need to perform batch loading operations on a large number of SIM cards to improve efficiency.

(3) Permission control requirements: Enterprises need to assign differentiated operational permissions to personnel across various roles and departments.

(4) Multi-organizational collaboration requirements: The provincial company must provide enterprise customers within its jurisdiction with charging equipment management and offline charging service support.

(5) Operational management requirements: The platform operator must centrally manage and compile statistical data for all enterprise clients across the province as well as the operational activities of provincial subsidiaries.

The traditional personal user service model cannot meet the aforementioned enterprise-level application requirements, making it imperative to establish a quantum key distribution service platform tailored for enterprises.

III. SYSTEM ARCHITECTURE DESIGN

A. OVERALL ARCHITECTURE

The enterprise-level quantum key distribution service platform proposed in this paper adopts a layered architecture design, with its overall structure illustrated in Figure 1 and comprising the following layers:

(1) Access Layer: The API Gateway serves as the system's unified entry point, handling external request routing, authentication, rate limiting, circuit breaking, and logging. It supports HTTPS for secure access and implements load balancing by distributing requests to backend microservice instances. Key capabilities include request authentication (token verification), permission control (RBAC), API version management, traffic control, and attack prevention.

(2) Service Governance Layer: The Registration and Configuration Center (Nacos), which provides service registration and discovery mechanisms. All microservices register their information with the registry upon startup. It centrally manages all microservice configuration files, supports hot configuration updates, and enables isolation across multiple environments.

(3) Core Service Layer: A microservices cluster with independently deployed services, including user services, order services, and refueling services. Services communicate via RESTful APIs or message queues. Supports horizontal scaling and containerized deployment (Docker + Kubernetes).

(4) Data Storage Layer: Stores core business data using the relational database MySQL, supporting read-write separation and master-slave replication. Redis caches frequently accessed data to improve performance. MinIO stores unstructured data such as certificates, scripts, images, and log backups.

(5) Operations & Monitoring Layer: The ELK logging system collects logs from all microservices, supporting full-text search and visual analysis. SkyWalking enables distributed traceability, recording request paths across multiple microservices. SpringBoot Actuator provides health checks and anomaly monitoring.

(6) Infrastructure Layer: Provides underlying computing and storage resources such as encryption devices, physical machines, and virtual machines, offering hardware support for upper-layer services.

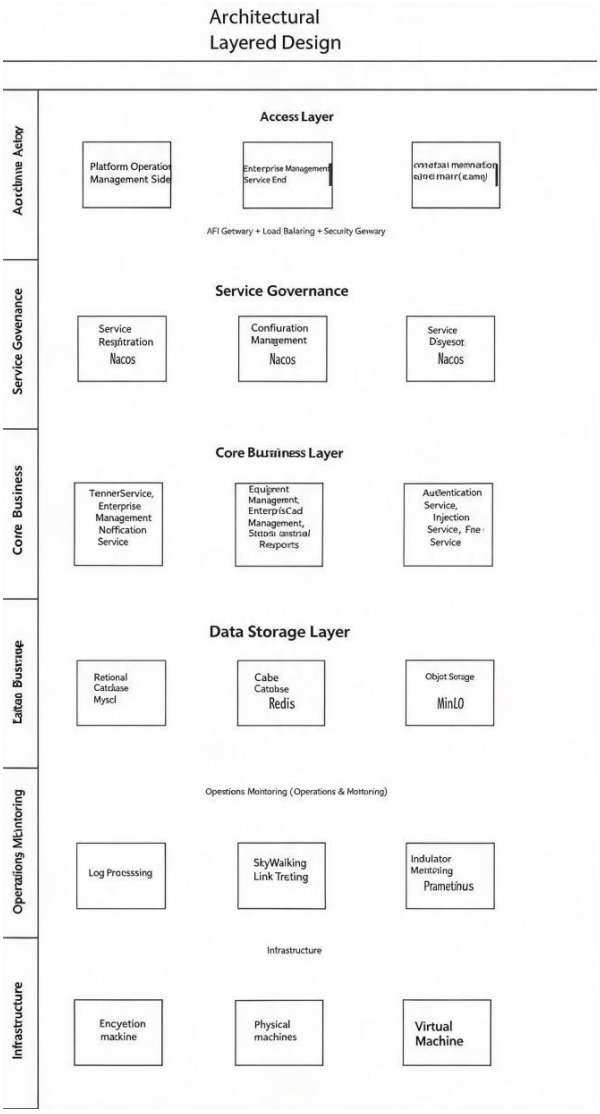

FIGURE 1. Hierarchical Design Diagram of the Enterprise-level Quantum Key Distribution Service Platform Architecture

B. MULTI-TENANT ARCHITECTURE DESIGN

The platform adopts a multi-tenant architecture design to achieve data isolation and independent management for enterprise customers, provincial companies, and platform operators. Key features of the multi-tenant architecture include:

Tenant ID: Assign a unique tenant ID to each tenant, ensuring logical isolation of all business data.

Tenant Plans: The platform offers multiple tenant plans, each with distinct feature permissions and resource quotas. Enterprises can select the appropriate plan based on their actual needs.

(3) Tenant Management: The platform operator is responsible for managing tenants throughout their entire lifecycle, including creation, configuration, activation, and deactivation.

The advantages of a multi-tenant architecture are:

Data Security: Data from different tenants is logically isolated to prevent data leakage risks.

Resource Sharing: Multiple tenants share the same platform infrastructure, reducing operational costs.

Flexible Configuration: Adjust function permissions and resource quotas flexibly based on tenant needs.

C. THREE-END SERVICE ARCHITECTURE

The platform establishes a three-tier service system comprising the enterprise service management module, provincial company operation management module, and platform operation management module, enabling hierarchical management and collaborative division of responsibilities.

1) Enterprise Service Management Portal

Provide self-service capabilities for enterprise customers, with main features including:

Account Management: Enterprise account login, information maintenance, password recovery, etc.

Personnel Management: Add, modify, delete, and batch-import personnel information; automatically link personnel to cards.

Card Management: Storage, querying, and detailed viewing of SIM card information.

Fill Management: Fill requests, fill record queries, order management.

Configuration Management: Employee account management, role management, and menu permission configuration.

2) Operations Management Department of the Provincial Company

Provide customer service and refueling support capabilities for provincial company operators, with key functions including:

Customer Management: Customer information management, document application review, and customer account management for the provincial company.

Card Management: Provincial company's card storage, querying, and binding management.

Filling Management: Authentication of filling equipment, offline filling execution, and filling record management.

Employee Management: Employee account management and role management for the provincial company.

Data Statistics: Analysis of filling data statistics.

3) Platform Operations Management Section

Provides comprehensive management capabilities for platform operators, with key features including:

Customer Management: Enterprise customer information management, provincial company management.

Security Management: Security Configuration, Security Blocking Management, Online Account Management.

Log Management: Management of access logs, command logs, and login logs.

Data Statistics: Multi-dimensional statistical analysis including total filling volume, number of fillings, and success rate.

Equipment Management: Equipment filling management, equipment check-in, and equipment flow management.
Configuration Management: System parameter configuration, interface management, scheduled task management.

IV. IMPLEMENTATION OF KEY TECHNOLOGIES

A. MANAGEMENT OF CORPORATE ORGANIZATIONAL STRUCTURE

Enterprise organizational structure management is the core capability that enables platform support for enterprise-level applications. Through this management, enterprises can establish internal organizational frameworks and batch-associate personnel with cards.

1) Establishing the Organizational Structure

Enterprises can create organizational structures and define department hierarchies on the platform. Organizational structure information includes department names, superior departments, and department heads.

2) Batch Import of Personnel

Supports batch import of personnel information using Excel templates. Required fields include name and phone number. The system automatically parses Excel files, performs data validation, and saves the data.

3) Automatic Personnel Card Binding

After importing personnel information, the system automatically queries the phone number associated with the SIM card's SEID via scheduled tasks, enabling automatic binding of personnel to their cards. Once the binding is established, personnel can request top-ups for their linked SIM cards.

The process of binding personnel to cards is shown in Figure 2:

Binding Process Instructions:
Step 1: The enterprise administrator logs in to the enterprise management platform.
Step 2: Import personnel information in bulk, including the phone number field.
Step 3: The system automatically checks whether the personnel information already exists; if not, it adds it to the personnel information table.
Step 4: The system periodically scans unlinked personnel information records.
Step 5: Send a query to the SIM card platform using your phone number to retrieve the corresponding SIM card information.
Step 6: If SIM card information is found, establish a binding relationship between the person and the card; if not found, do not proceed.
Step 7: After binding is complete, synchronize and update the associated fields between the personnel information table and the card information table.

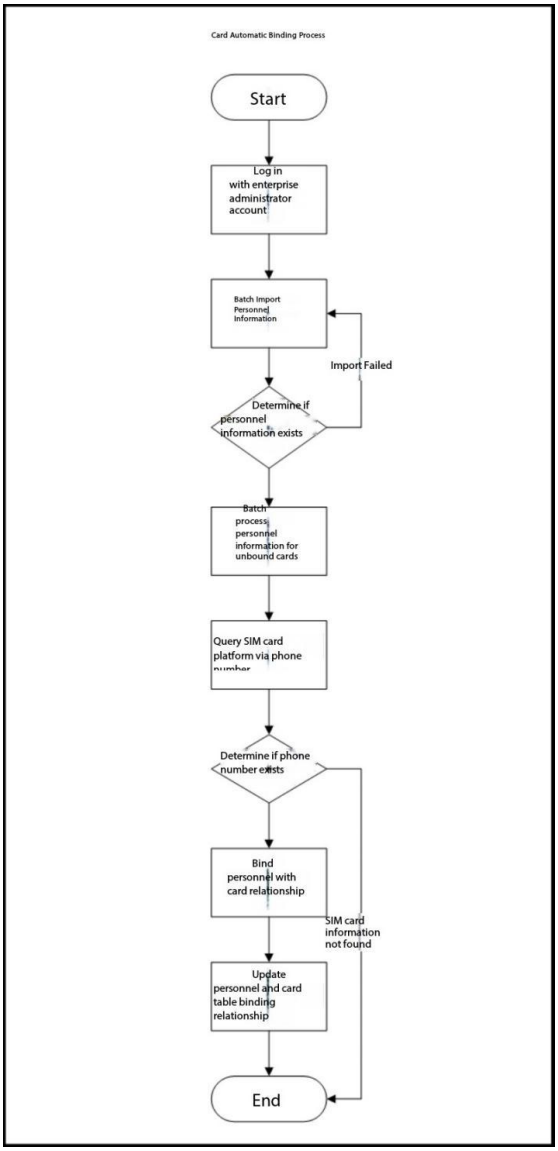

FIGURE 2. Flowchart of Automatic Personnel and Card Binding Process

B. AUTHENTICATION MECHANISM FOR FILLING EQUIPMENT

The provincial company's offline filling mode requires a physical card-writing device. To ensure operational safety, the platform has implemented an authentication mechanism for the filling equipment.

1) Device Registration

Before first use, the filling equipment must be registered on the platform with information such as device number, device type, affiliated provincial company, and customer. Upon registration, a unique device identifier is generated.

2) Equipment Authentication Process

Before the charging operation, the system performs identity and permission authentication on the card writing device. The device authentication process is shown in Figure 3:

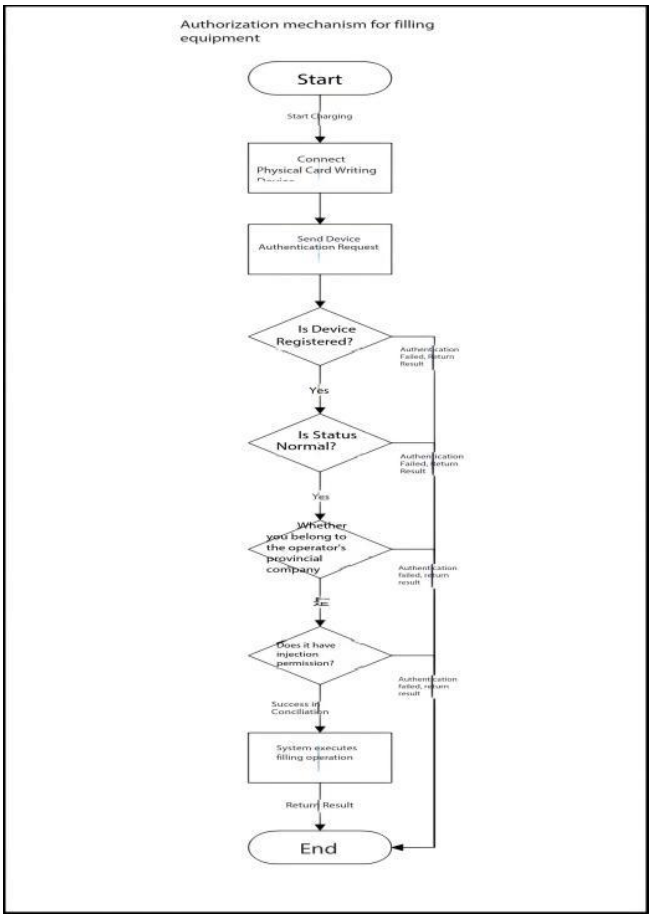

FIGURE 3. Authentication Flowchart for Filling Equipment

Authentication Process Description:
Step 1: The operator connects the physical card writer.
Step 2: The system reads the device identification information.
Step 3: Send a device authentication request to the platform.
Step 4: The platform verifies whether the device is registered.
Step 5: The platform verifies whether the device status is normal.
Step 6: The platform verifies whether the device belongs to the provincial company of the current operator.
Step 7: The platform verifies whether the device has filling permissions.
Step 8: Authentication successful. Allow the filling operation to proceed.
Step 9: Authentication failed. Return the failure reason and terminate the operation.

3) Equipment Production Flow Record

All device operations are recorded in a log, including operation time, operator, action details, and results, facilitating issue tracing and auditing.

C. REFINED PERMISSION CONTROL

The platform employs a role-based access control (RBAC) model to enable refined permission management.

1) Role Definition

The platform comes preconfigured with multiple roles, such as Enterprise Administrator, Regular Enterprise User, Provincial Company Administrator, Provincial Company Operator, and Platform Administrator. Each role has a distinct set of functional permissions.

2) Permission Configuration

Supports configuring menu permissions for roles to control accessible function modules. The permission configuration uses a tree structure with three levels: module-level, function-level, and operation-level.

3) Permission Inheritance

Supports permission inheritance, where child roles automatically inherit permissions from parent roles. Enterprises can configure different permissions for departments at various levels based on their organizational structure.

4) Permission Verification

When a user accesses system functions, the system verifies their role permissions and denies access if unauthorized. Permission verification is uniformly implemented at the gateway layer to ensure consistent permission control.

D. OFFLINE FILLING PROCESS OF THE PROVINCIAL COMPANY

Provincial company offline charging refers to the operational mode where provincial company operators use physical card writers to charge SIM cards. The offline charging process is shown in Figure 4:

Offline Filling Process Description:
Step 1: The provincial company operator logs in to the system.
Step 2: Connect the physical card writer.
Step 3: The system authenticates the card writing device.
Step 4: If authentication fails, terminate the operation.
Step 5: After successful authentication, enter the target user's recharge phone number.
Step 6: The system queries card information and available credit balance.
Step 7: Submit a refilling request and specify the refilling amount.
Step 8: The system performs the encryption operation by writing the quantum key to the SIM card using a card writer.
Step 9: Update the system to reflect the refilling order status and record the refilling log.
Step 10: Return the injection result notification.

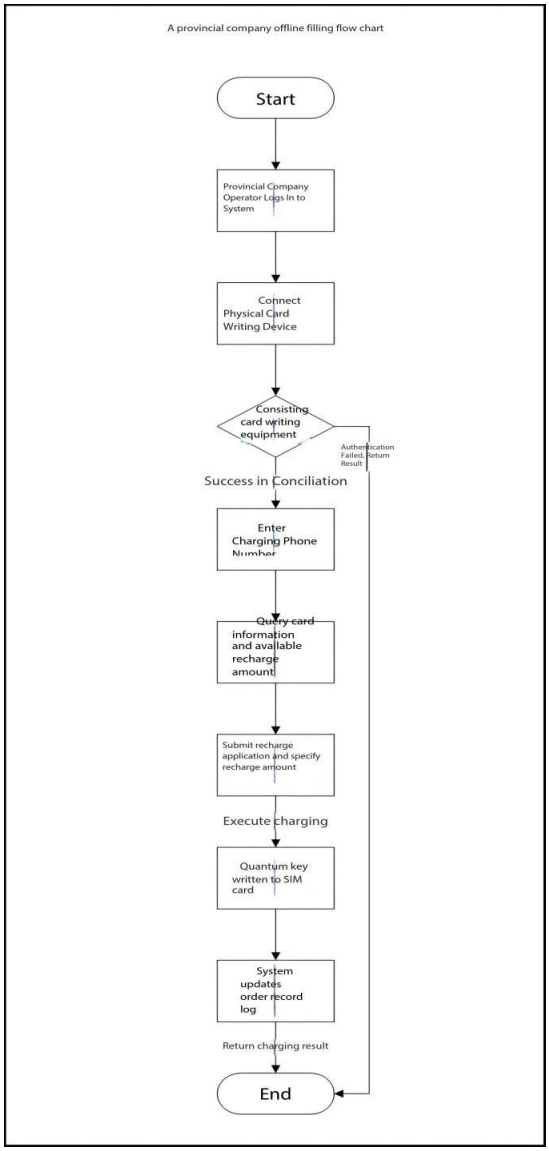

FIGURE 4. Offline Filling Process Flowchart for Provincial Companies

V. DESIGN OF SECURITY MECHANISMS

A. LOGIN SECURITY MANAGEMENT

The platform features a comprehensive login security mechanism:

(1) Password complexity verification: Forces users to set passwords that comply with security policies, including minimum length, uppercase and lowercase letters, numbers, special characters, and other requirements.

(2) Login Failure Lock: When a user fails to log in consecutively for a specified number of attempts, the account is automatically locked to prevent brute-force attacks.

(3) Session Management: Records user login sessions, supports online user queries, and enables forced log-out operations.

B. ACCESS SECURITY CONTROLS

(1) IP Access Restrictions: Supports configuring an IP whitelist to restrict access from specific IP addresses.

(2) Interface frequency limits: Implement access frequency restrictions for sensitive interfaces to prevent malicious attacks.

(3) Security interception: Intercepts and logs abnormal access behaviors, including unauthorized access, suspicious operations, and risky activities.

C. DATA SECURITY PROTECTION

(1) Encryption of sensitive data: Store sensitive data such as passwords and keys in encrypted form.

(2) Encryption: All data transmissions use the HTTPS protocol to ensure security throughout the process.

(3) Operation Log: Records all user operations, supporting operation auditing and issue tracing.

VI. SYSTEM IMPLEMENTATION AND APPLICATIONS

A. SYSTEM IMPLEMENTATION

This platform has been implemented in the Phase II project of the Quantum Key Distribution Platform, with the following key technical components:

Backend Framework: Spring Boot 2.x, Spring Cloud Alibaba

Front-end framework: Vue 3.x, Element Plus

Database: MySQL 8.0

Cache: Redis 6.x

File Storage: MinIO

Containerization: Docker, Kubernetes

Implementation of Functional Modules: The platform implements the following core functional modules:

(1) Enterprise Service Management Portal: Includes modules for account login, personnel management, card management, recharge management, and configuration management.

(2) Provincial Company Operations Management Module: including customer management, card management, refilling management, employee management, and data statistics modules.

(3) Platform Operations Management Module: including customer management, provincial company management, security management, log management, data statistics, equipment management, and configuration management modules.

(4) H5 Mobile Version: Modules include Card Management, Card Recharge, and Recharge History.

B. PERFORMANCE METRICS

After the system goes live, it meets the following performance metrics:

TABLE 1. System Performance Metrics

Indicator Item	desired value
Interface Response Time	< 1 second
Average Login Time	< 3 seconds
Data Refresh Display	< 2 seconds
Concurrency Processing Capability	100 TPS
system availability	$> 99.9\%$

C. APPLICATION SCENARIOS

This platform is suitable for the following enterprise-level use cases:

(1) Enterprise Secure Communication: Provides quantum key protection for internal corporate communications, enabling end-to-end encrypted transmission.

(2) Government confidential communications: Provides quantum-level secure communication protection for government agencies.

(3) Secure Financial Data Transmission: Provides quantum key protection for data transfers among financial institutions.

(4) Secure IoT Access: Provides quantum security authentication and key management for IoT devices.

VII. CONCLUSION

This paper proposes an architectural design and implementation approach for a quantum key distribution service platform tailored for enterprises. The platform employs a multi-tenant architecture and a three-tier service model, establishing a three-level service framework comprising an enterprise service management layer, a provincial company operation management layer, and a platform operation management layer. Through mechanisms such as enterprise organizational structure management, authentication of distribution devices, and granular permission control, the platform effectively supports the large-scale deployment of enterprise-level quantum key distribution operations.

Compared with the previous quantum key distribution service designed for individual users, this platform features the following innovations: first, it enables enterprise organizational structure management and supports batch association of personnel with keys; second, it incorporates an authentication mechanism for key distribution devices to ensure security during offline key distribution by provincial companies; third, it adopts a three-tier service architecture that facilitates hierarchical collaborative management among corporate clients, provincial company operators, and platform operators.

In the future, as quantum secure communication technology continues to expand into enterprise-level applications, the platform will further enhance its capabilities in three key areas: first, improving batch data loading capacity to meet larger-scale corporate needs; second, optimizing the loading process to boost success rates and efficiency; third, expanding open interfaces to facilitate integration with existing enterprise systems. The design and implementation of this platform provide robust support for promoting quantum secure communication technology in enterprise environments.

REFERENCES

[1] GB/T 42829–2023, *Basic Requirements for Quantum Secure Communication Applications*. State Administration for Market Regulation, 2023.

[2] GB/T 32918–2016, *Information Security Technology—SM2 Elliptic Curve Public Key Cryptographic Algorithm*. General Administration of Quality Supervision, Inspection and Quarantine, 2016.

[3] GB/T 32905–2016, *Information Security Technology—SM3 Cryptographic Hash Algorithm*. General Administration of Quality Supervision, Inspection and Quarantine, 2016.

[4] GB/T 32907–2016, *Information Security Technology—SM4 Block Cipher Algorithm*. General Administration of Quality Supervision, Inspection and Quarantine, 2016.

[5] GM/T 0028–2014, *Technical Requirements for Security of Cryptographic Modules*. National Cryptography Administration, 2014.

[6] GlobalPlatform, *Card Specification Version 2.3.1*. GlobalPlatform Inc., 2018.

[7] ETSI TS 102 225, *Smart Cards; Secured Packet Structure for UICC Based Applications*. ETSI, 2018.

[8] China Mobile Communications Research Institute, *Overall Technical Requirements for the Quantum Communication Application Service System*. China Mobile Communications Group Co., Ltd., 2024.

[9] ITU-T Y.3800, *Framework for Quantum Key Distribution Networks*. International Telecommunication Union, 2020.

[10] GSMA, *Post-Quantum Telco Network Impact Assessment Whitepaper*. GSM Association, 2024.

[11] C. Jiang, L. X. Hu, W. Z. Yu, et al., "Side-channel-secure quantum key distribution with state-dependent correlated errors and Trojan-horse attack," *Opt. Express*, vol. 33, no. 25, pp. 51715–51729, 2025, doi: 10.1364/OE.576910.

[12] H. Hajji, E. M. Baz, and O. W. Krawec, "Optimal eavesdropping in semi-quantum key distribution," *Phys. Lett. A*, vol. 567, pp. 131174–131174, 2026, doi: 10.1016/J.PHYSLETA.2025.131174.

[13] M. Kumar and B. Mondal, "Three party quantum key distribution using bilocality," *Opt. Quantum Electron.*, vol. 58, no. 1, pp. 19–19, 2025, doi: 10.1007/S11082-025-08612-3.

[14] Y. P. Vatskov, M. E. Mavrin, G. V. Potapov, et al., "Quantum key distribution in mobile networks: Modern approaches and prospects," *J. Commun. Technol. Electron.*, vol. 70, no. 4, pp. 135–141, 2025, doi: 10.1134/S1064226925700287.

[15] R. L. Gilyazov, S. K. Melnik, E. M. Sibgatullin, et al., "Investigating a quantum key distribution scheme with independent detection and sideband encoding," *Bull. Russ. Acad. Sci.: Phys.*, vol. 89, no. 12, pp. 2285–2290, 2025, doi: 10.1134/S1062873825713546.