SSCC Engineering Technical Document

Technical White Paper

SSCC-FDEP Technical White Paper of Message Transmission System

Document No.	**FDEP-WB-PUM001**
Confidentiality	**Public**

深圳证券通信有限公司
SHENZHEN SECURITIES COMMUNICATION CO.,LTD.

April 2020

Document Information

Document Name	SSCC-FDEP Technical White Paper of Message Transmission System
Description	
Project	Financial Data Exchange Platform (FDEP)

Change History			
Date	**Version**	**Changed By**	**Change Description**
2020-04	2.0	R&D Center	Completed the revision

Contents

List of Figures

List of Tables

1 Preface

This document is a white paper for the FDEP Message Transmission System. It describes the functions and technical realization of the system.

The Financial Data Exchange Platform (FDEP) is designed to reduce the costs of the financial industry, improve standardization of data exchanges among industries, and promot innovation and development of the financial industry.

Other abbreviations are listed as follows:

FDSH：FDEP Data Switching Hub;

FDSU：FDEP Data Switching Unit (a component of FDEP);

FDAP：FDEP Data Access Point;

FDMR：Financial Data Message Router (a component of FDAP);

FDEAPI：Financial Data Exchange Application Programming Interface;

FDXP： Financial Data Exchange Protocol (This term generally refers to protocols for the exchange of all standard business data).

FMP：Foundamental Maintenance Platform.

SSCC：Shenzhen Securities Communication Co., Ltd.

2 Overview

2.1 Components

The FDEP is a data exchange system used for banks, securities companies and related financial institutions. It consists of the communications network, switching hub software & hardware, access point (FDAP), software development interfaces, standard business protocols, etc.

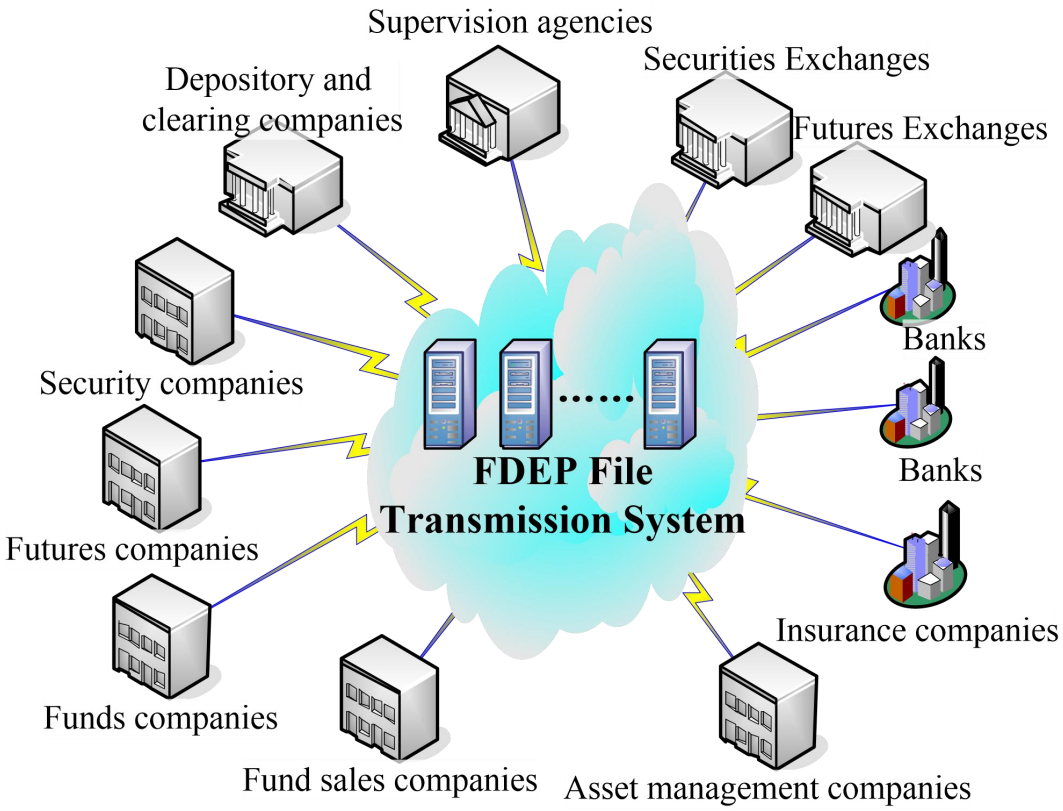

Figure 1 Diagram of FDEP

FDEP uses SSCC's communications network as the main bottom-layer network facilities. Other access methods such as dedicated line connections, and Internet VPN can also be used. These access methods allow the FDEP put the banks, security companies, funds companies, futures companies, securities exchanges, futures exchanges, depository and clearing companies, fund sales companies, asset management companies and supervision agencies link together.

The FDEP Data Switching Hub (FDSH) consists of multiple high-performance Linux servers. It is a mutually redundant, load-sharing and highly scalable cluster.

The core software of the FDEP is a message-oriented middleware (MOM) used for specific application, including Message Transmission System and File Transmission System. It is used for safe and efficient message exchange among users that have accessed the system. Such communication includes the sending and receiving of messages, load balance, the publishing and subscribing to topic message, file transmission, etc.

The platform provides the FDEP Data Access Point (FDAP) and the simple financial data exchange application programming interface (FDEAPI). The

programming interface allows you to perform programming. The FDAP allows for data exchange through the platform.

Industrial standards, national standards and international standards are used for the exchange platform as the standard protocol (FDXP) for internal data transmission.

2.2 Design Principles

- **Standard-compliant Data Exchange Interfaces**

Unified standards for data exchange enable higher efficiency of data processing and exchange for transactions among banks, security companies, funds companies and futures companies. Other advantages include less transaction costs, controlled technical risks and promote business innovation and development. They are regarded as a key factor of platform construction. Therefore, the exchange interfaces must meet industrial, national or international standards.

- **One-point Accessing**

In terms of communication lines, a unified network platform and the open access method allow one-point accessing. On the business layer, data transmission services provided by the platform allow “full network accessing”.

Unlike the interconnection between banks and securities, a message router for data exchange is used at the application layer. When data are sent to the platform, the switching hub forwards data to the outlet. The platform ensures efficient, reliable message forwarding among various communication parties.

- **High Expandability**

The amount of data to be transmitted in the platform is predicted to grow due to expanded business type and increased accessed users. Therefore, the core of FDEP is planned to be an expandable exchange cluster. These switching nodes share application requests from the user in average based on a balanced-load strategy. For increased amount of file data to be exchanged, the processing capability can be extended by increasing the number of core exchange parts of the FDEP File Transmission System and improving the data storage performance.

The access point of FDEP should also be able to balance load and provide

redundancy. The user can configure multiple access clients, which can be used at the same time.

- **High Reliability and Error Tolerance Capability**

Error tolerance shall be considered at the network and application software & hardware level. Hot standby shall be used for key components of the network. Core exchange nodes shall be mutually redundant. Access clients may also be redundant. The client connection can be automatically switched.

- **Ensuring Security**

All network accesses must be filtered using a firewall. The router control, port control, access control list and intrusion detection mechanism must be provided. The users can only access permissible paths in the network. All unnecessary protocols are banned in the network to reduce security risks.

On the application layer, the platform certificates the identity of user to ensure that the information comes from a valid user and also the destination user is valid. High-intensity encrypted algorithms are used to ensure data security during data exchange.

3 Technical Architecture

3.1 Overall Architecture

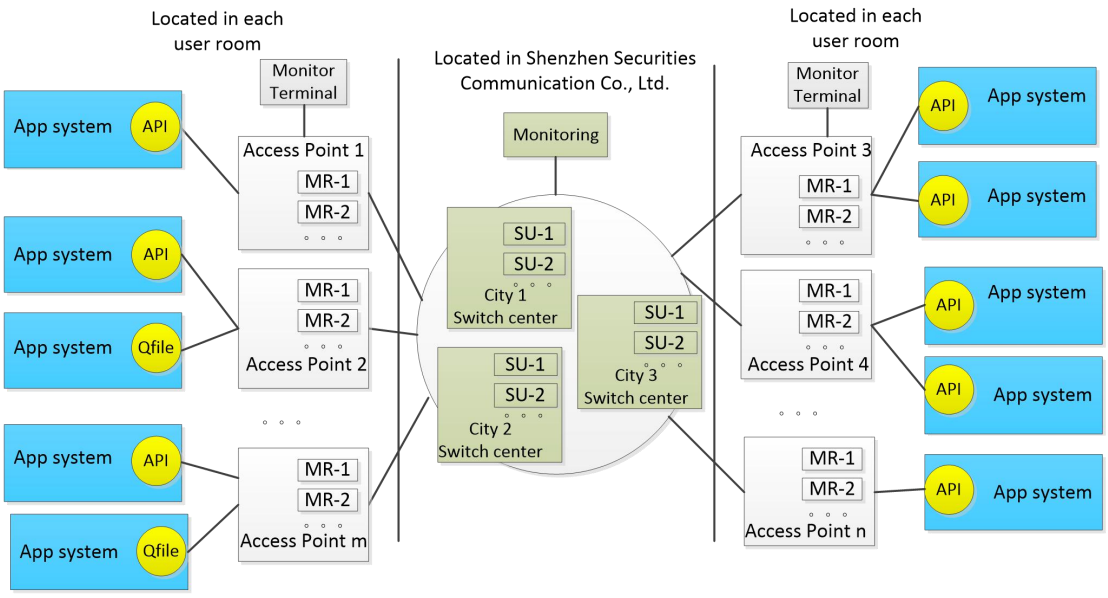

Figure 2 Overall architecture of FDEP Message Transmission System

In terms of application, FDEP Message Transmission System consists of the following parts:

FDSH: The switching hubs at the SSCC end consist of exchange centers of multiple cities. Nodes of multiple cities work together simultaneously and are mutually redundant. The switching hub of each city consists of multiple switching units (FDSH). Each switching unit can forward and handle data. These switching units form node clusters of many cities, which share the application requests in average using a balanced load strategy. In case of a fault of any server, it is replaced by another server. It provides fault tolerance, which ensures the stability and reliability of switching units of the same city. Distributed deployment in multiple cities allows other cities to replace the city where a disaster occurs. This ensures higher reliability of the system.

FDAP: A dedicated access client is placed at the user end. The access client maintains the safe long connection between the user and switching hub. The access point (FDAP) is typically deployed on two or more computers to allow redundancy backup and load sharing.

Client API (FDEAPI): The access point provides a group of user-friendly interfaces for application development. It allows the service system to communicate with the access point. Currently, if the polling is performed on FDAP by API, the exchange performance of a single API shall not be less than 500 packets/s. If FDAP sends packets to API based on the reception conditions, the exchange performance of API shall not be less than 7,000 packets/s (assume that the size of each packet is 1kb).

Monitoring terminal(FMP): designed to carry out centralized monitoring and maintain configurations of FDEP.

3.2 Network Access

3.2.1 Shenzhen securities communication network

Shenzhen securities communication network is a professional Securities communication network, which is responsible for various securities communication tasks such as securities issuing, trading, account opening, settlement, information release, multimedia information transmission among the national small and

medium-sized stock transfer system, Central government bond registration and settlement Co.,Ltd, securities company, fund management company, commercial bank, asset management company and fund sales company . It is characterized by high security, perfect function, strong authority and wide coverage.

Shenzhen Securities communication network consists of Shenzhen Securities satellite communication network, Shenzhen Securities ground communication network and VPN access network. This paper only introduces Shenzhen Securities ground communication network.

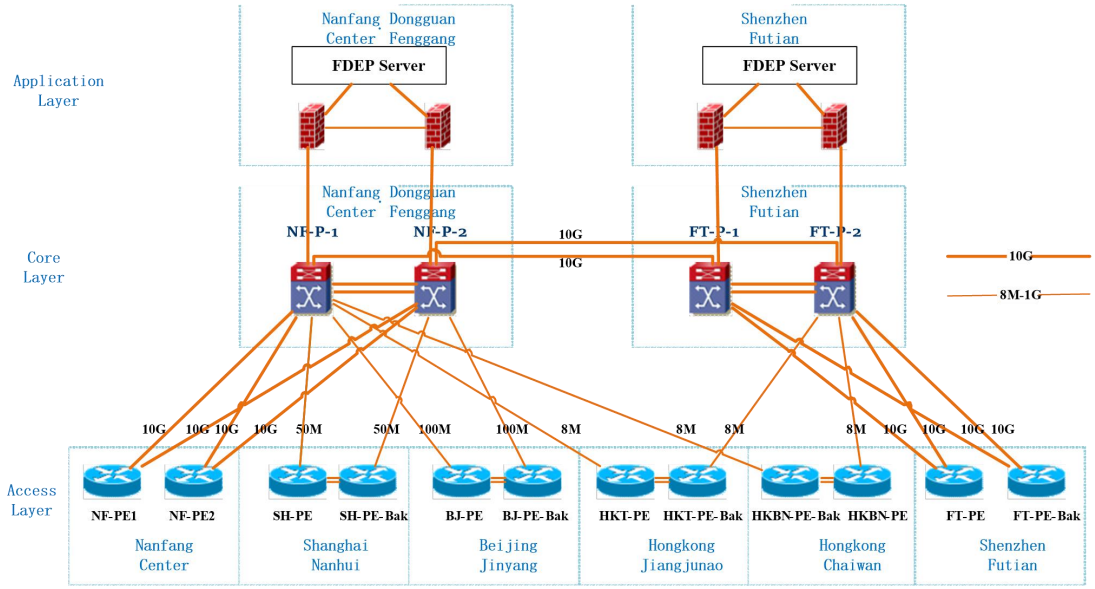

Figure 3 Diagram of Shenzhen Securities ground network

The ground communication network of Shenzhen Securities communication company (abbreviated as the ground network) is a nationwide, powerful, safe and efficient securities communication network, which has the characteristics of high availability, high security, high capacity and low delay. In terms of network physical structure, the ground network consists of application layer, core layer and access layer:

（1）The application layer has two main nodes, which are located in Dongguan and Shenzhen. The application layer mainly undertakes the access function of the application system. The application system in each node consists of firewall, load balancing and high performance server.

（2）The core layer has two main nodes, which are located in Dongguan and Shenzhen. The core layer mainly undertakes the functions of cross data center

interconnection and application system access. 10G line interconnection is used within and between each node.

（3）The access layer has six nodes, which are respectively located in five cities, including Dongguan, Shenzhen, Shanghai, Beijing and Hongkong. The access layer mainly undertakes the function of user's private line access. Apart from two access points in Hongkong, all other cities have one access point, which supports MSTP line access of Telecom, Unicom and Mobile. At present, there are in total about 2000 access lines in the ground network. The access bandwidth and network structure of different nodes are slightly different. The main equipment of the access layer is the PE router for the user's private line access, undertaking access control, routing control, etc.

In recent years, the network performance, reliability and efficiency of Shenzhen Securities communication network have been greatly improved, and the management ability has reached a new level.

（1）The processing capacity has been greatly enhanced. In 2020, the bandwidth capacity of the core layer of the ground network of Shenzhen communication system will reach the 10G level, in which the Futian access node and the South Center access node can provide the private line and large bandwidth access capacity.

（2）The system reliability is greatly improved. Redundant design of any link supports any single point of failure, and the availability of communication system is greater than 99.999%. Users only need to ensure that the two-wire redundant access, and the access line meets the specification requirements, and participate in the regular drill test, so as to realize the 30 second switching in case of single point failure.

（3）The function of communication service system is constantly improved. It provides securities trading, settlement and market communication services, as well as business communication services such as third-party depository, data depository and bank-securities-future interconnection, which effectively improves network utilization.

（4）The ability of information management is increasing day by day. It has implemented management systems such as ISO27001, ISO20000, level protection, CMMI, and its R&D management and IT service management capabilities have well supported the development of securities business.

3.2.2 FDEP private line access

The financial data exchange platform uses the mature Shenzhen Securities communication network as the main underlying network facilities. Only two lines between securities companies, commercial banks, fund companies and futures companies are needed to connected to the ground network to engage in various financial cooperation businesses, so as to achieve "one point access, full network access" in communication and business.

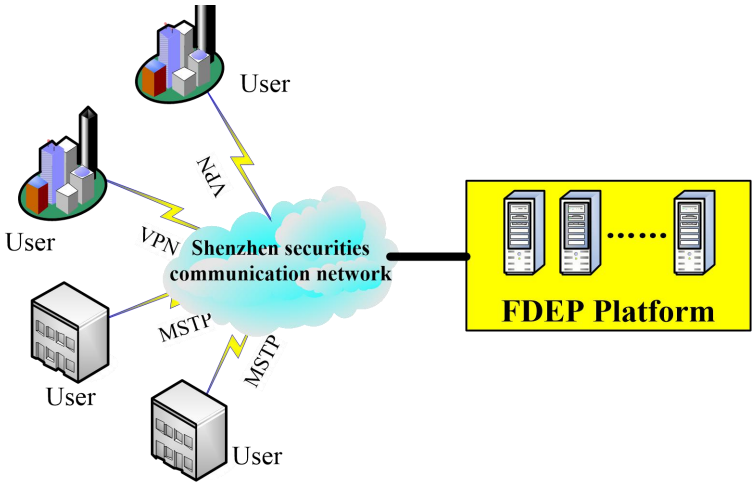

Figure 4 Diagram of FDEP access

The quantity of private line access and the technical proposal must meet the specification, which requires that, there must be at least double lines provided by two different ISP between the user and the double Data Exchange center; meanwhile, the lines must have different local area IP addresses. Based on this requirements, user can choose appropriate access point, access type and the quantity of access line to accomplish mutually redundant access. Each line has the same safe policy to carry out the FDEP businesses.

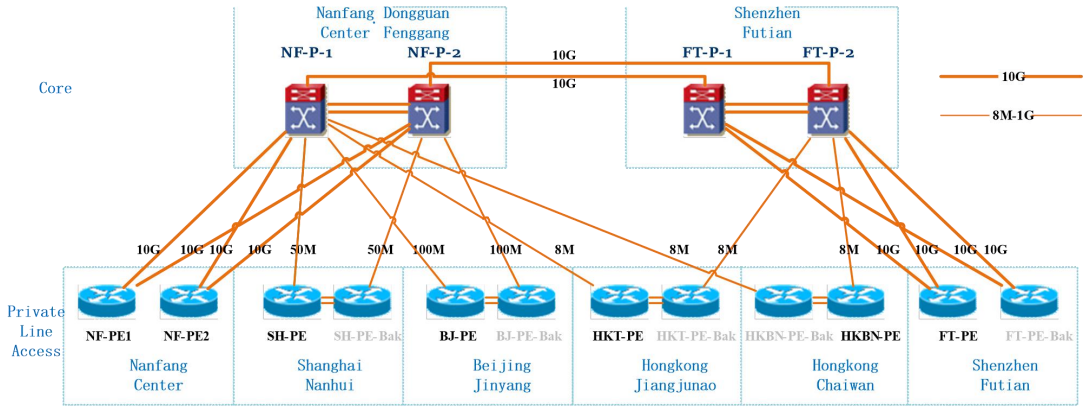

Figure 5 Diagram of private line access point

of Shenzhen Securities ground network

Please use the unified business zone to submit the special line access application. The zone address is https://biz.sscc.com.

3.3 FDSH

The switching hub of the FDEP Message Transmission System is a user-oriented message forwarding middleware. It provides a flexible platform for information exchange among participants of the FDEP, such as securities, banks, funds companies and futures companies. The switching hub acts as a message dispatcher in the FDEP message transmission system. It is designed to enable secure, efficient message communications among users of the access system. The communications include message sending and receiving, load balancing, the publishing and subscribing to topic message, file transmission, etc.

3.3.1 Running Environment

The FDEP switching hub (FDSH) is composed of multiple switching units deployed in multiple cities. Each switching unit runs in the following software & hardware environments:

Hardware: High-performance servers.

Operating system: RedHat Enterprise Linux

To ensure high redundancy, the switching hub for each city must have a minimum of two switching units.

3.3.2 Connections Among Switching Units

Each switching unit in the switching hub connects to another switching unit. This means that each switching unit connects to other switching units in TCP protocol.

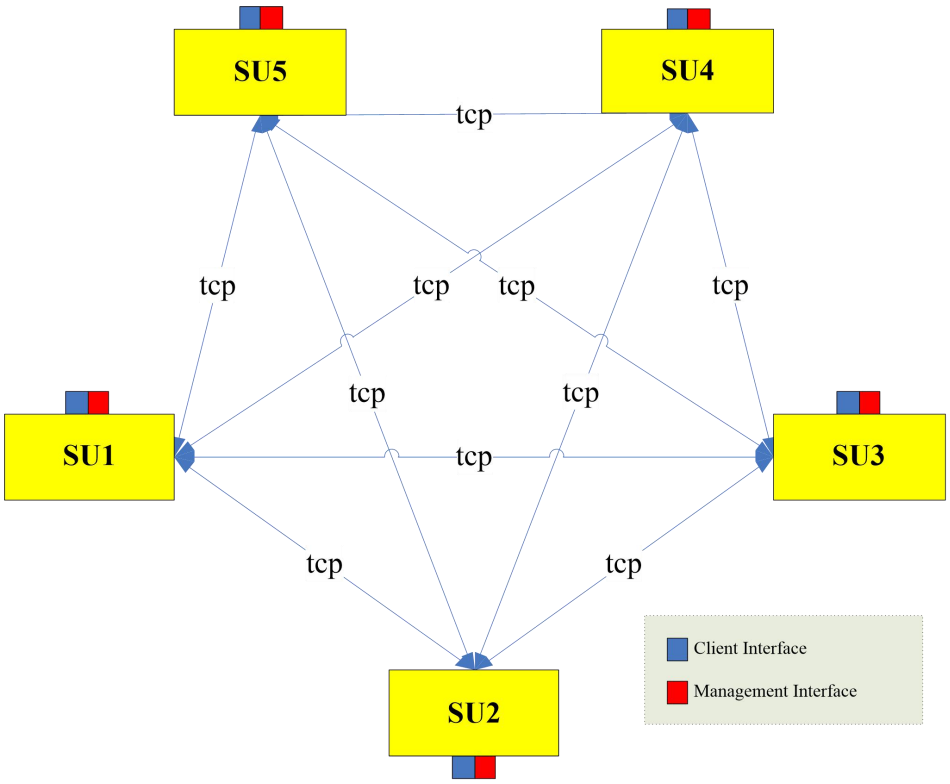

Figure 6 Connection between switching units

FDSUs are physically connected using individual networks to ensure higher communication efficiency. Switching units are connected using high-speed back-plates.

3.3.3 Load Balancing

- **Hardware Load Balancing**

The switching hub supports hardware load balancing deployment. If the access mode of hardware is chosen by the user, the client configuration of IP addresses will be greatly simplified, and the deployment of the hub is transparent to users.

- **Software Load Balancing**

The access point connects with the idlest switching unit when it connects with the switching hub. The process is shown in the following client registration flowchart.

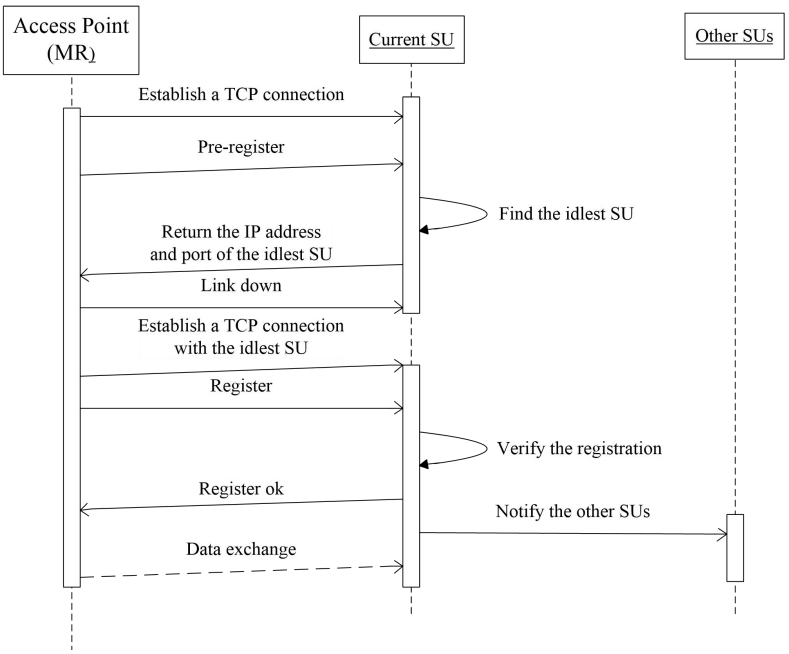

Figure 7 Registration flow of access point

The busyness of the switching unit depends on the idle memory, CUP busyness and the number of connected clients. The system can calculate the value for the busyness of the switching unit via an algorithm based on these factors. The idlest switching unit can be identified by calculating the busyness of each switching unit and comparing them.

Switching units periodically exchange their busyness information. Such information is exchanged immediately when the number of connected clients changes.

Connection between the access point and switching unit does not break during normal exchange of data packets. In case of accidental disconnection, the access point re-connects the switching unit by initiating a new registration process.

3.3.4 Client Authentication

The switching hub adopts two ways to authenticate clients. On security design of application software data, it adopts the standard of “Basic requirments for information security technology and security level protection of information system” issued by the

ministry of public security and China securities regulatory comission, in accordance with the fourth level; abbreviated as “Security Level Four”.

- **Hard Encryption**

When user attempts to log in, the certificate of hard EKey which issued by Shenzhen Securities Communication company must be used. The client uses hard EKey to verify digital signature for SSL channel. The private key is protected within hard EKey in period of negotiation, and the process of safe operation completes internally. This is called Hard Encryption.

- **Soft Encryption**

When user attempts to log in, there is no need to use of hard EKey. The application uses its own certificate to authenticate the validity of client for SSL channel, then verifies the password of the user. This is called Soft Encryption.

3.4 Monitoring System

The monitoring platform can monitor the operation of FDEP in real time and provide outputtable monitoring data. It enables the operator to configure, manage the system, output the reports and manage nodes via the menu or an interactive interface. Meanwhile, the terminal also provides a centralized management mechanism.

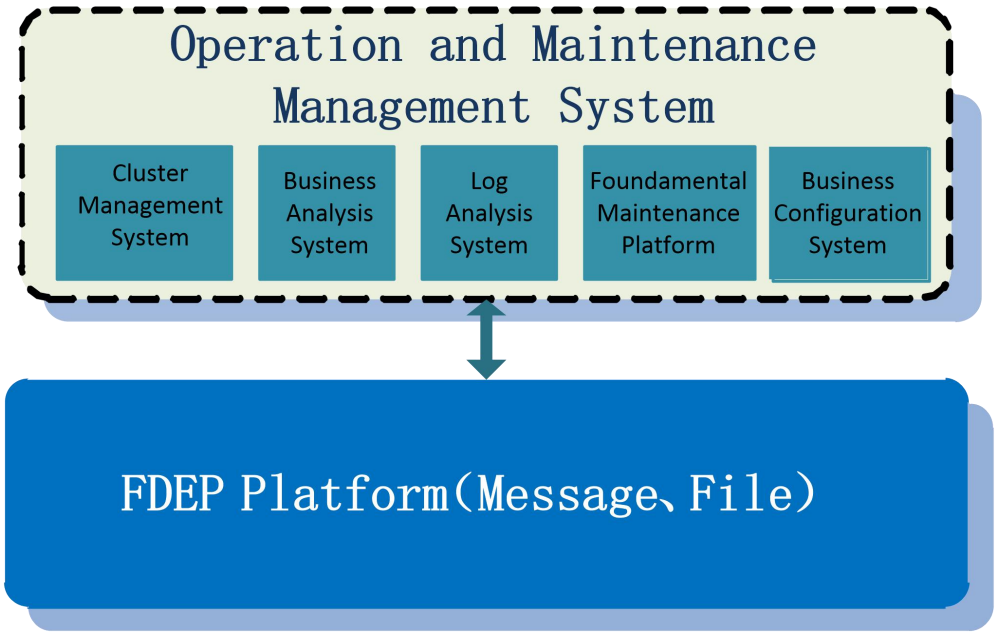

Figure 8 Diagram of monitoring and management platform

The monitoring system connects to all switching units, and monitors the information of all switching units. The monitoring system operates in SSCC.

3.5 FDAP

Each FDAP consists two or more FDMRs. The FDMR reliably exchanges messages with the switching hub. Each FDMR can perform all functions required by the FDAP. Multiple FDMRs is used for redundancy and load sharing.

The FDMR runs in the following software & hardware environments:

Hardware: ordinary PC,CUP frequency: above 2.0GHz; memory: above 4G.

Operation system: Microsoft Windows Server 2008、Microsoft Windows Server 2012、Microsoft Windows 10、Microsoft Windows Server 2016、Redhat Enterprise Linux6.8、Redhat Enterprise Linux7.5.

It is recommended to deploy at least two FDMRs to provide mutual hot backup and load balancing.

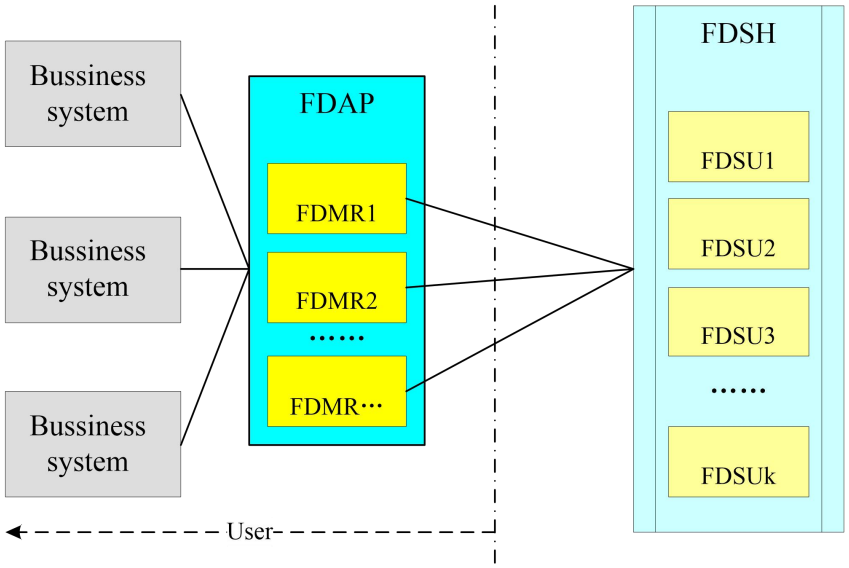

Figure 9 Composition and connections of access point

The load sharing and balancing principles of the FDMR are similar to that of the FDSU.

FDMR can run in agent mode of TCP or HTTP.

3.6 FDEAPI

FDEAPI is a set of callable application program interfaces used for C、Java programming language. Users can call this API to exchange data with the FDEP. Functions of FDEAPI include auto connection of communication, data packet sending and receiving, the publishing and subscribing to topic message, file transmission, encrypted compression, etc. The application program can communicate with the MR by FDEAPI.

Figure 10 Application modes of FDEAPI

FDEAPI is a concise and easy-to-use programming interface. The following 20 functions are provided for operations:

Table 1 Functions of the main interfaces of FDEAPI

No.	Function name	Functional features
1	Mr3Init	Initialize, get the relevant resources, and try to establish a connection with the access client FDAP.
2	Mr3IsLinkOK	Check and judge whether the current connection with the access client FDAP is normal.
3	Mr3CreatePkgID	Generate a message packet ID.
4	Mr3Send	Send message individually to the message hub via FDAP, request forwarding.
5	Mr3MultiDestSend	The message is sent in a group to the message hub through the FDAP, and split into multiple independent messages in the hub for processing and forwarding.
6	Mr3Receive1	The message forwarded by the message hub is received in the mode 1 condition.
7	Mr3Receive1_FreeBuf	Release the memory allocated in the Mr3Receive1 function call.
8	Mr3Receive2	The message forwarded by the message hub is received in the mode 2 condition.

No.	Function name	Functional features
9	Mr3Receive3	The message forwarded by the message hub is received in the mode 3 condition.
10	Mr3SendTopicMsg	Send message individually to the message hub via FDAP, request forwarding.
11	Mr3ReceiveTopicMsg	Receive the topic message forwarded by the hub.
12	Mr3SendFile	Send message individually to the message hub via FDAP, request forwarding.
13	Mr3ReceiveFile	Receive the file message forwarded by the hub.
14	Mr3Destroy	Disconnect from the FDAP and release relevant resources.
15	Mr3GetVersion	Get the version number of the API.
16	Mr3RegRecvCondition	Registration package push-down conditions, push all conditions at once.
17	Mr3GetPeerUserStat	Get the status of the communication peer user.
18	Mr3CancelSendFile	Cancel sending files.
19	Mr3GetSendFileStatus	Get the status and progress of the file sent.
20	Mr3GetAppStatus	Get app status information

Note: The MRAPI dynamic link library also contains the functions beginning with MR/MR2, which are reserved for compatibility with the old version of the interface; the function beginning with MR3 is a new interface. Old interface function cannot not be mixed with new one.

Functions in FDEAPI are thread-safe (note that **Handle**, which is generated by **Mr3Init**, cannot be used after fork progress). You can generate multiple threads related to FDAP, and allow data exchange with FDEP at the same time to improve the exchange performance. For details on the application methods of these functions and parameter descriptions, see the *FDEAPI User Manual*.

Running environments and provision methods of the FDEAPI:

Windows platform: Windows Server 2008、Windows Server 2012、Windows 10、Windows Server 2016, dynamic link library (DLL)

Linux platform: Redhat Enterprise Linux6.8 、 Redhat Enterprise Linux7.5, dynamic link library(so)

Other platforms: customizable

3.7 Financial Data Exchange Protocol(FDXP)

Fdxp refers to financial business data exchange protocol used in FDEP. In order to have a wide range of adaptability and good scalability, business data exchange in FDEP must adopt industry, national or international standard protocols.

When applied to escrow day-end liquidataion and electronic bank statement, Fdxp adopts the standard of "The information structure and design rules for data exchange between securities and futures industry and banks" issued by the people's Bank of China. This protocol mainly refers to ISO15022(ISO15022 2nd) and ISO20022. It uses the XML format popular in the market as the data representation. XML uses tags to express content and transmit information with good readability. Users can define the complex structure of tasks themselves with XML. In particular, it can be extended as needed, and the extension mechanism is standard. XML is an ideal solution for cross platform data exchange and storage.

Users can use FDXP through FDEP to achieve the existing business, such as banks and securities business, fund consignment sale, electronic bank statements, etc. It can be predicted that there will be more and more businesses in the financial industry. The unified business protocols and basic platform will play a productive role in promoting the rapid development of business in the future.

3.8 Performance Index

The FDEP platform is a high redundant, safe and reliable data exchange system with excellent performance. It has the horizontal and vertical expansion capability. Table 2 below shows the performance index of production deployment of the Message Transmission System(the size of datagram is about 1 KByte):

Table 2 Performance index of the Message Transmission System

Index Item	Index Value
Throughout capacity of common message(per second)	300,000
Throughout capacity of topic message(per second)	700,000
End-to-end delay in local area network(millisecond)	<1
Maximum bandwith of user access(Mb)	200

Throughout capacity of one BSMR(per second)	10,000
Throughout capacity of one Api client(per second)	7,000
Maximum number of relationship pairs for each user	unlimited

3.9 Security Support

3.9.1 Network Security

To access the switching hub, the user must be strictly monitored by a firewall, no matter which access method is used, which may be via Shenzhen securities communications network, the directly-linked lines or Internet VPN. All network connections must be controlled by the strictly designed router control, port control and must be subject to checks for access control list and intrusion testing mechanism. Users are only accessible to designated servers and ports. All unnecessary network protocols are prohibited for all connected networks.

3.9.2 Security of the Application System

Standard PKI security certification systems are used for the exchange platform. Point-to-point, end-to-end encrypted certification mechanisms are used. The CA of Shenzhen Stock Exchange is standard CA for the financial data exchange platform. It offers RSA 2048 bit certificates for access users of the platform, which are stored in a hard EKey. The certificates are used for verifying identity if the user attempts to connect to the switching hub. During message transmission and forwarding, it supports the SSL protocol with the maximum version of TLS1.3; RSA key of 2048 bits is used by key negotiating algorithm, and AES key of 256 bits is used by symmetric encryption algorithm. All of the above is used to ensure security and timeliness.

CA systems have been established by major banks. Certificates are issued to users via their CA servers. To improve the efficiency of certification, FDEP also recognizes certificates issued by other CA systems under the agreement.

The security system of FDEP's applications is shown below:

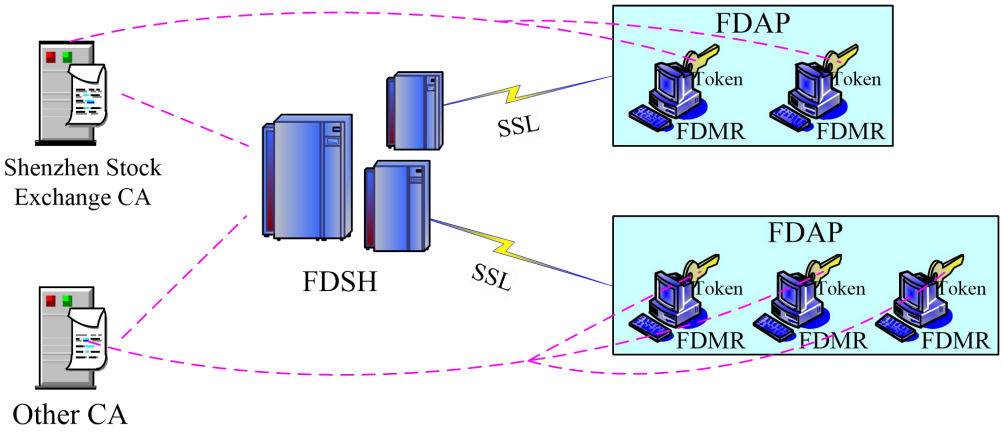

Figure 11 Security of FDEP Application Systems

4 Operation & Maintenance of the Platform

The main switching hub of the exchange platform is located at the center of SSCC. Another switching hub for disaster tolerance (in another region) shall be provided. SSCC guarantees that the operation and maintenance level for the transaction & settlement system will be the same as that for the Financial Data Exchange Platform.

Network construction and operation maintenance have been the tasks of SSCC since its founding. SSCC builds a matured and all-round service system with a decade of experience. Our professional talents have a mastery of all required technologies. A series of advanced communication software have been developed on our own. They provide safe, efficient, real-time and reliable technical supports for our customers, including the securities market, funds companies and futures companies etc. Advantages of the company in safe operation and maintenance are described as follows:

- **Safe Operation Environment**

Advanced hosts and a telecommunications room for network communication are provided for Shenzhen Securities Communication Center. The Shenzhen Securities Communications Network and its application systems are very professional in risk-control. These measures include:

- Firewalls and various backup methods;
- Large screen monitoring system in the telecommunications room, ensuring real-time monitoring of the system;
- A security and confidentiality system for the telecommunications room;
- Higher security level of the servers (C2); and
- Grade management for operations in the telecommunications room to prevent human-factor incorrect operations, and ensure security of the application system and communication data.

➢ **Real-Time System Monitoring**

Real-time monitoring is provided for the communications network and application system. “One-point monitoring and multi-point maintenance” mode is applied. 24/7 network monitoring is carried out by high-performance and professional ground/satellite communications network management system. Any fault at any node on the client or within the network can be found in 30s and cleared promptly. The advanced monitoring system can monitor the utilization of resources such as the CPU and memory of any server and the running of the application system. In case of any fault of the application system or host, an alarm is generated at the monitor screen and each monitoring terminal.

➢ **Quick Troubleshooting**

SSCC has set up a nationwide maintenance and guarantee system that covers fault acceptance, troubleshooting, periodic inspection and return visits. SSCC offers prompt, high-quality guarantee services together with many agencies across China. China Telecom, China Mobile, CNC and China Unicom, which are the partners of SSCC, assure the highest level of guarantee for line maintenance. In addition, we also actively team up with multiple telecom service providers.

➢ **Prompt Communications and Contact**

Shenzhen Securities Communication Center provides 7 (days) x 24 hours services to ensure high-quality services around the clock. Calls from multiple lines can be received by the central telecommunications room.

5 Examples of Typical Applications

The FDEP File Transmission System can be used for various services, such as fund consignment sale, escrow day-end liquidation, fund direct selling and electronic bank statements etc. More importantly, service modes will not be limited. This means that a FDEP File Transmission System is applicable to all service modes, regardless of the differences.

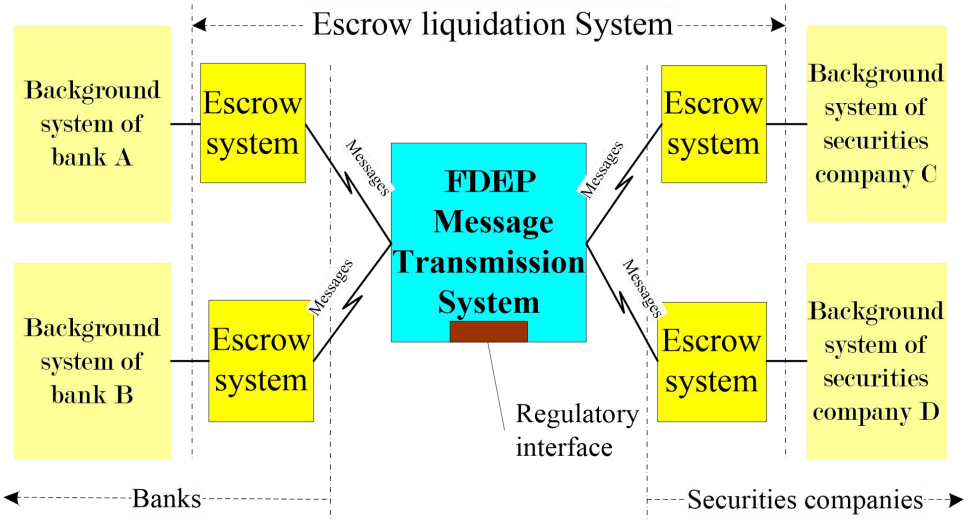

Figure 12 Application of FDEP in Escrow

Application of the system in the escrow day-end liquidation is shown in Figure 10. Protocol FDXP is used to access FDEP for both securities companies and banks. The communication modes and service interfaces are unified, regardless of the bank mode (single/multiple). Different service systems are used (i.e. the escrow system of the securities company and the escrow system of the bank). However, the common part required for services has been concluded by the transmission system and standardized. A common system is provided to improve usability of the technical system and reduce costs.

R&D Center

2020-04