信安世纪
Infosec
Stock Code 688201 (Shanghai)

Outreach Business of the People's Bank of China

Outreach business primarily involves business systems between banks and relevant regulatory bodies, partner institutions, and industry peers. Given the stringent requirements for system stability and security in outreach business, dedicated lines (or financial metropolitan area networks) are typically employed for interconnection. All outreach business operations must comply with security standards established by the business planning and guidance authorities.

Infosec, as a leading domestic application security vendor, has seen its products extensively deployed in critical external systems such as the People's Bank of China's Second-Generation Payment System, UnionPay Clearing System, Cross-Border Interbank Payment System (CISP), Treasury Information Processing System (TIPS),Central Bank Accounting Data Centralization System(ACS), same-city clearing and sorting, and the Treasury Electronic Payment System.

Secure Signature System for the Second-Generation Payment System of the People's Bank of China

Demand Analysis

The central bank payment clearing system serves as the nerve center of the payment system and is one of the most critical infrastructures for ensuring the normal functioning of the economy and financial sector.

Since 2002, the People's Bank of China has successively established systems including the Large-value Payment System, the Small-value Payment System, and the Cheque Image Exchange System.

Since 2009, the central bank has been advancing the development of a new generation of modern payment systems. Compared to the first-generation payment system, the new system is referred to as the second-generation payment system. Following the development principles of inheritance and smooth transition, the second-generation payment system underwent structural adjustments based on a thorough review of the first-generation system's application architecture. It established a core clearing account management system, supported by business application systems including the large-value payment system, retail payment system, cheque image exchange system, and online payment interbank clearing system. Additionally, it incorporates auxiliary support systems such as the payment management information system and public management control system.

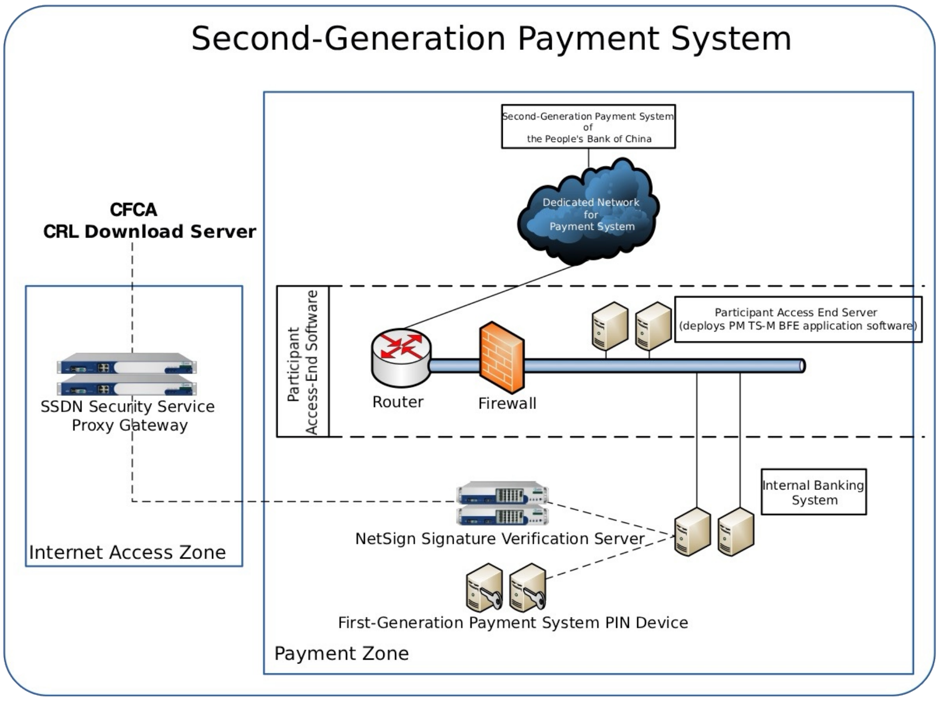
As a powerful payment system, without robust security mechanisms and architecture to ensure its safety and reliability, the impact would extend beyond the operations of the individual bank. It would compromise the security and reliability of all participating banks connected to the second-generation payment system, as well as the entire second-generation payment system of the People's Bank of China. Therefore, in the second-generation payment system, the security of business systems is uniformly consistent, whether for the People's Bank of China or any connected institution.

The People's Bank of China's security requirements for the second-generation payment system can be summarized into three characteristics: ensuring the authenticity of all participating parties, the integrity of transmitted data, and the non-repudiation of transactions.

To meet the requirements for building the second-generation payment system, both the central bank's clearing center and participating institutions need to establish their own signature systems. These signature systems must primarily fulfill five functional requirements:

- Signature and verification functions required for second-generation payment systems
- Secure storage of participants' own private key certificates and management of other parties' public key certificates
- Must support both the RSA algorithm and the national cryptographic SM algorithm.
- Requires support for validating two sets o f CA certificate revocation list (CRL) files.
- Audit Function

▪ System Architecture


Second-Generation Payment System
Second-Generation Payment System of the People's Bank of China
Dedicated Network for Payment System
CFCA CRL Download Server
Participant Access-End Software
Participant Access End Server (deploys PM TS-M BFE application software)
Router
Firewall
SSDN Security Service Proxy Gateway
Internal Banking System
NetSign Signature Verification Server
Internet Access Zone
First-Generation Payment System PIN Device
Payment Zone

▪ Solution Description

Based on this requirement, the People's Bank of China adopted digital certificates and digital signature technology within the PKI framework as the technical foundation for its security solution. The solution is as follows:

Each second-generation payment system access institution must apply to CFCA for a digital certificate representing its identity. This certificate will be used to verify the authenticity of all participating parties' identities through digital certificate validation, and must be securely stored on the signature verification server.

After obtaining digital certificates, each second-generation payment access institution must bind its identity to the digital certificate within the central bank's second-generation payment system. Upon successful binding, the central bank system will issue the public key certificate information for the bound access institution. The access institution then uploads the public key certificate issued by the central bank to the signature verification server.

Business messages exchanged between second-generation payment access institutions employ digital signatures to ensure data integrity and non-repudiation of business actions. When initiating a transaction, the originating institution invokes the signature service to digitally sign the transaction request message. The receiving institution then calls the signature verification server to validate the originating institution's transaction request. Upon successful verification, it issues a transaction response and invokes the signature verification service to digitally sign the transaction response. Simultaneously, both parties must invoke the signature verification server to validate the digital signature results of the Bank of China system's netting receipt.

Verify CRL files. Security proxy gateways deployed in bypass mode within internet access zones automatically download national cryptographic and RSA CRLs from the CFCA CRL server at scheduled intervals and validate the CRL files. Signature verification servers automatically download both CRL lists from the security proxy gateways for validation.

Solution Advantages

- **Technical Advantages**

  NetSign is the signature server brand utilized by the People's Bank of China Clearing Center's Super Online Banking and second-generation payment systems. Infosec conducted customized development for these systems, participated in designing and establishing relevant management, operation, and maintenance standards along with interface standards, and simultaneously supports both domestic cryptographic standards and RSA algorithms, enabling the concurrent download of two sets of CRL files.

- **Signature Verification Server Deployment Methods Supported**

  Dual-machine HA deployment, load balancing deployment, off-site disaster recovery deployment.

  Among the three deployment methods above, NetSign's signature verification server supports certificate synchronization requirements for services like Super Online Banking and second-generation payments. This simplifies system deployment and operational management while enabling load-balancing deployment through the device itself.

- **Product Performance Advantages**

  NetSign signature verification servers utilize the Infosec OS system and incorporate hardware acceleration cards, delivering the best performance in their class and outperforming other comparable products overall.

- **Security Advantages**

  Digital certificates utilize dedicated hardware storage to ensure that participating institutions' private key information remains secure from tampering and theft, while also preventing easy copying or replication. Furthermore, all encryption and decryption operations involving private keys must be completed entirely within the hardware, effectively preventing certificates from being stolen, copied, or replaced during use. This approach guarantees the uniqueness and non-substitutability of participating institutions' identities at the source, significantly enhancing the security level of the entire second-generation payment system.

- **Product Compatibility And Scalability**

  Infosec has partnered with over a dozen application developers in China's second-generation payment system, including Hengsheng, Shencode, Huaten, Jindian, Zantong, Changliang, Advanced Digital Communications, Yanlian, and Chipo, among others, with established collaboration cases.

  In terms of scalability, should the People's Bank of China's second-generation payment signature system undergo interface changes or introduce new requirements, Infosec can directly provide banks with the corresponding version. This eliminates the need for banks to redevelop and retest related signature interfaces.

Product Cases Advantages

NetSign signature verification servers from Infosec are widely deployed across the Big Five banks, numerous joint-stock banks, foreign banks, and other regional commercial banks. With over 200 banking clients and nearly 200 non-bank financial institutions and large corporate groups, the company boasts the most extensive customer base in the financial industry.

Product Feature Advantages

Infosec fully understands the requirements of the People's Bank of China's second-generation payment system. Through extensive preliminary requirements and functional analysis conducted jointly with the People's Bank of China, we are uniquely positioned to meet the demands of this second-generation payment system. For users, the application requires minimal development work related to signature system interfaces. All certificate-related tasks - including certificate issuance, certificate classification management, certificate renewal, certificate validity verification, and certificate synchronization - as well as data signing and verification are handled by the NetSign Signature Verification Server.

NetSign Signature Verification Server provides mature and stable APIs for Java, C, and .NET interfaces, with extensive adoption across numerous banks.

The Product Possesses Comprehensive And Complete Qualifications

Since digital certificates and signature products are classified as confidential products, national regulations stipulate that all confidential products used within the financial system must possess relevant qualifications issued by the State Cryptography Administration.

Selected Success Cases

People's Bank of China
Agricultural Development Bank of China
China Exim Bank
Agricultural Bank of China
Postal Savings Bank of China
China Everbright Bank
China CITIC Bank
China Minsheng Bank
Hengfeng Bank
Ping An Bank

China Merchants Bank
China Guangfa Bank
Bohai Bank
Industrial Bank
Shenzhen Qianhai WeBank
Bank of Beijing
Bank of Tianjin
Hebei Bank
Inner Mongolia Bank
Bank of Suzhou

Bank of Ningxia
Qilu Bank
Bank of Ningbo
Bank of Dalian
Bank of Xi'an
Jinshang Bank
Bank of Qinghai
Baoshang Bank
Bank of Xiamen
Bank of Jiangxi

Bank of Chongqing

Bank of Hangzhou

Bank of Lanzhou

Bank of Urumqi

Bank of Harbin

Bank of Jilin

Bank of Guangzhou

Beijing Rural Commercial Bank

Tianjin Rural Commercial Bank

Chongqing Rural Commercial Bank

Shenzhen Rural Commercial Bank

Shanxi Rural Credit Cooperative Union

Shaanxi Rural Credit Cooperative Union

Qinghai Rural Credit Cooperative Union

Gansu Rural Credit Cooperative Union

Henan Rural Credit Cooperative Union

Jilin Rural Credit Cooperative Union

Hunan Rural Credit Cooperative Union

Hubei Rural Credit Cooperative

Guizhou Rural Credit Cooperative Union

Fujian Rural Credit Cooperative Union

Jiangsu Rural Credit Cooperative Union

Anhui Rural Credit Cooperative Union

Yunnan Rural Credit Cooperative Union

Sichuan Rural Credit Cooperative Union

Jiangxi Rural Credit Cooperative

Hana Bank (China)

UBS (China)

ANZ China

Deutsche Bank (China)

Dahua Bank China

DBS Bank China

Citibank China

The Bank of East Asia

Mizuho Bank China

HSBC China

Standard Chartered Bank

China UnionPay Co., Ltd.

Rural Credit Funds Clearing Center

Interbank Clearing Co., Ltd.

Hangzhou People's Bank Clearing Center

Tianjin Check Clearing Center

Shanxi Check Clearing Center

Guangdong Rural Credit Cooperative Union

Heilongjiang Rural Credit Cooperative Union

Shanghai City Commercial Banks Funds Clearing Center

Shanghai Urban Commercial Banks Clearing Center

Inner Mongolia Autonomous Region Rural Credit Cooperative Union

Central Government Bond Registration & Settlement Co., Ltd (Open Market Operations Office of the People's Bank of China)

infohksec

INFO HK SECURITY LIMITED
409 Kinetic Industrial Centre
7 Wang Kwong Road, Kowloon Bay
Hong Kong
www.infohksec.com.hk
info@infohksec.com

www.infosec.com.cn

www.infohksec.com