信安世纪 Infosec

Stock Code 688201 (Shanghai)

4A Solution

Infosec's next-generation 4A solution for the financial industry integrates traditional 4A services, identity and behavioral big data analytics, and mobile security applications into a comprehensive, unified solution.

The products involved in the plan, including mobile security authentication apps, digital certificate systems, security gateways, signature servers, unified identity management, and single sign-on systems, are all independently developed by Infosec. The solutions offer excellent integration, ensuring user legitimacy and preventing illegal data theft, while guaranteeing secure and stable system operation.

Unified Identity Management and Single Sign-On Security Solution

▪ Demand Analysis

The bank currently operates over 150 application systems, both established and under development, with more to be added as business needs evolve and information system construction progresses. Since these systems use independent authentication mechanisms, employees must register and log in separately for each application. Consequently, users often manage multiple, sometimes dozens, of accounts and passwords simultaneously.

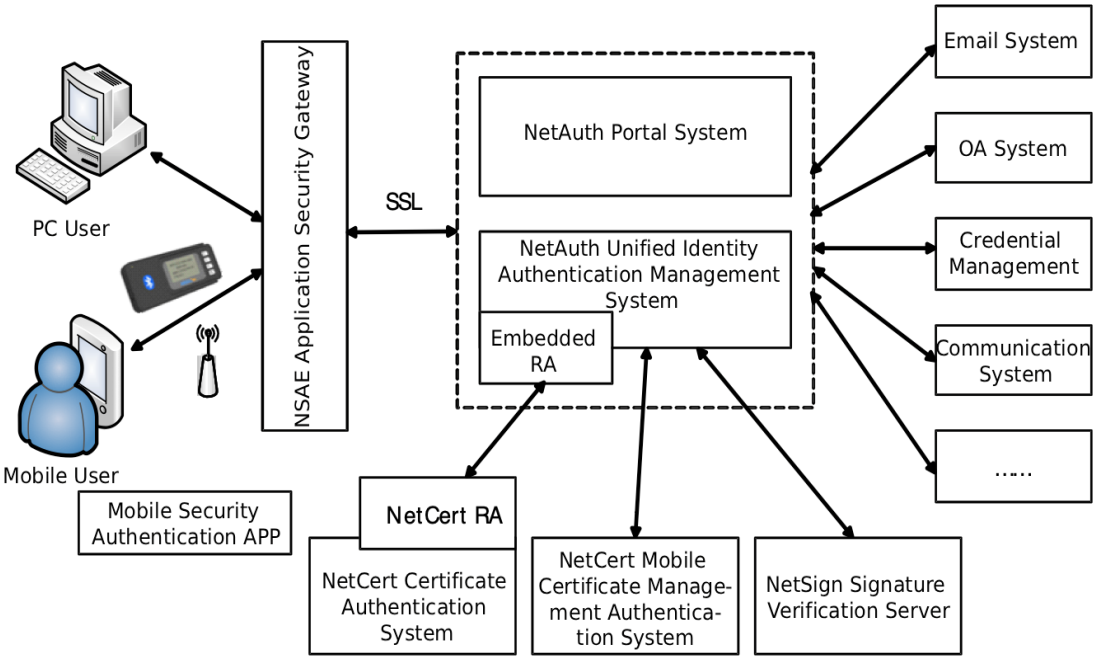
The account rules for these systems are inconsistent, with statistics revealing a total of 10 categories, such as internal employee IDs, email aliases, teller numbers, agent numbers, Chinese names, mobile phone numbers, and so on. Additionally, due to factors like differing password setting rules and periodic password changes, passwords across various application systems also vary.

This makes it difficult for users to remember all their account credentials across various application systems. Not only does this hinder convenient access to these systems, but it also increases the risk of illegal interception and tampering. The bank has now completed the implementation of a single sign-on system, which helps users bind their accounts and passwords across different application systems, thereby improving convenience to some extent. However, this transformation is not comprehensive and does not fundamentally alter the current situation where authentication remains independent across application systems. Users still need to remember their accounts and passwords for each individual system.

Additionally, employee information sources for various application systems are scattered across multiple locations, making it impossible to implement unified and effective control and management when employees log in to these systems.

Therefore, there is an urgent need to establish a unified identity authentication system that integrates with existing single sign-on systems as a subsystem. This will accelerate the consolidation of various information application systems and resource sharing, enabling "single sign-on for network-wide access." It will conveniently and securely meet business and management requirements.

Solution Architect



The unified user management and security authentication solution primarily consists of the NetCert certificate authentication system, the NetAuth unified identity authentication management system, the NetAuth portal system, NetCert Mobile Certificate Management and Authentication System NSAE Application Security Gateway and NetSign Signature Verification Server comprise:

NetCert Certificate Authentication System: This system is a digital certificate system compliant with national cryptographic standards, supporting both RSA and SM2 algorithms. It consists of three modules: KMC (Key Management), CA (Certificate Authority), and RA (Certificate Registration Authority). It issues digital certificates that uniquely identify individuals.

Digital certificate carriers utilize USB Key and mobile software certificates.

NetAuth Unified Identity Management System: This system comprises modules including unified user management,SSO single sign-on, portal system, and unified auditing. The system integrates the NetCert RA module with the NetCert certificate authentication system, enabling direct user registration, certificate application, issuance, and download through the user management interface; This system integrates with the AD domain to achieve unified account management and single sign-on for domain desktops.

NetAuth Portal System: The portal system architecture is built upon WEB2.0 and AJAX frameworks, forming a fully J2EE-based personalized portal software powered by browser technology. The platform adheres to SOA architecture. The portal features a mobile app, enabling seamless integration between the PC-based portal and the mobile portal. Content published in one location is synchronously displayed on the mobile platform.

Through the portal system, users can centrally view lists of business systems, pending task counts across systems, detailed task information, aggregated company news announcements, and enterprise content releases.

NetCert Mobile Certificate Management Authentication System: This system comprises a mobile digital certificate application (SDK) and a mobile certificate management backend system, providing smartphone users with mobile digital certificate download and authentication services; It enables digital certificate authentication and QR code authentication on smartphones. Currently, the system supports mainstream Android and iOS platforms.

NSAE Application Security Gateway: This system is a hardware digital certificate authentication device. Based on universal security protocols and integrated with the NetAuth unified identity authentication management system, it implements mandatory authentication for user PC-based and mobile-based digital certificates, and transmits user authentication data via secure protocol encryption. mobile device digital certificates, while encrypting user authentication data transmission via secure protocols to safeguard the integrity of the unified user management and authentication system.

NetSign Signature Verification Server: A comprehensive solution supporting signature/verification, encryption/decryption, and device management for up to ten algorithms, including national cryptographic standards such as SM1, SM2, SM3, SM4, SSF33, as well as DSA, RSA, and 3DES. NetSign provides authentication to NetAuth, enabling verification of user digital certificates during USBKEY-based login procedures.

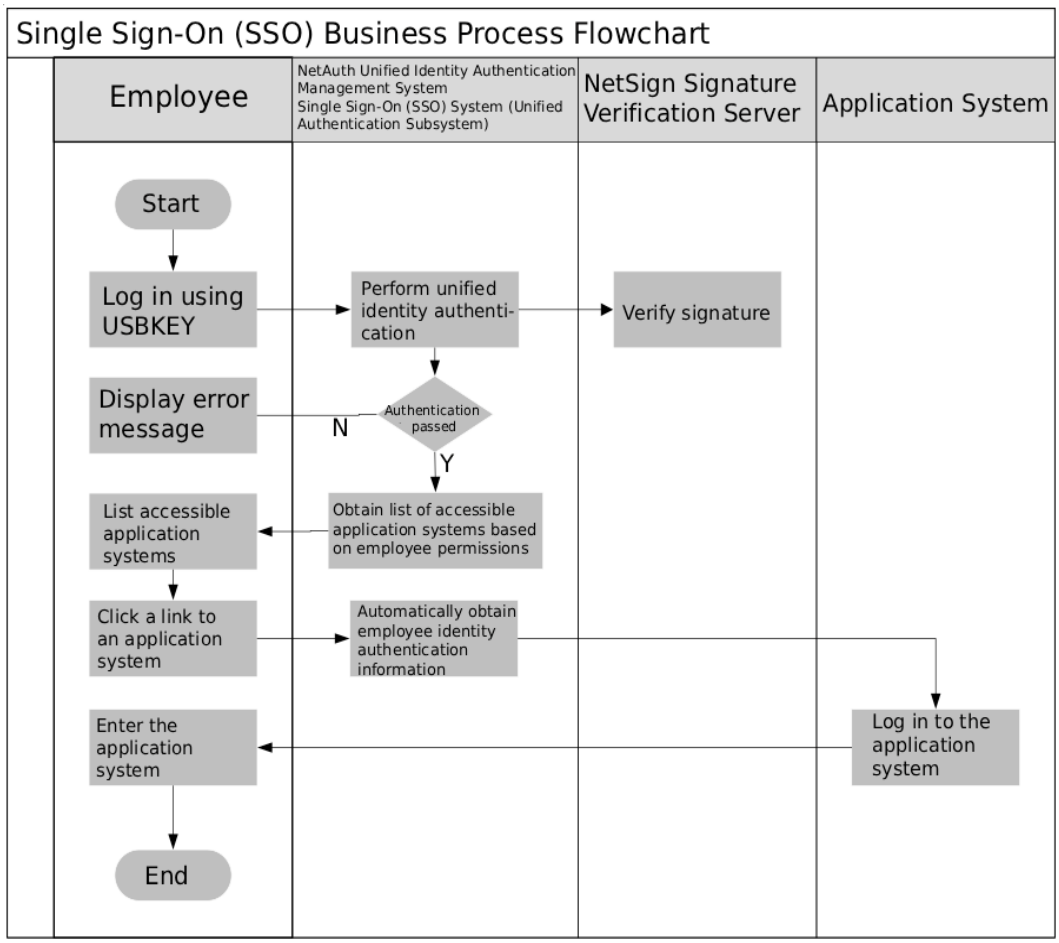
▪ Solution Description

In this solution, all external network access to the internal network is routed through the NSAE application security gateway, utilizing HTTPS one-way encryption for communication.

The PC single sign-on portal integrates with domain desktop single sign-on implementation. After internal employees log into the domain, they can directly access the single sign-on portal interface. When accessing from outside the domain, USBKEY login or QR code scanning login methods are provided. The USBKEY login process is illustrated below. When users log into the security authentication app, they use the app's scanning function to scan the QR code displayed on the single sign-on login interface, thereby authenticating their login to the single sign-on system.

Users in the NetAuth Unified Identity Authentication Management System are synchronized from HR, with accounts simultaneously synchronized to the AD system. Additionally, other application systems utilize interfaces provided by NetAuth to synchronize organizational structure and identity information with NetAuth.

The portal system centralizes the display of pending tasks for users across business systems, extracting pending tasks from over ten systems including the OA system, IT operations management system, email system, and complaint management system for centralized display. The portal page categorizes applications accessible to users based on their permissions into sections such as "My Workspace", "Management Platform", "Business Platform", "Risk Platform", and "Supervision Platform" implementing single sign-on for these systems.



Solution Advantages

Infosec provides a comprehensive solution for unified identity management and single sign-on security, addressing secure login across PC and mobile devices while enabling single sign-on functionality. striking a balance between security and convenience.

The products involved in the solution, such as the Mobile Security Authentication App, NetCert Certificate Authentication System, NSAE Application Security Gateway, NetSign Signature Verification Server, NetAuth Unified Identity Authentication Management System, are all independently developed products by our company. The solution exhibits strong overall integrity, facilitating future system upgrades and maintenance.

The solution provides PC-based authentication and single sign-on, as well as secure authentication and single sign-on integration for mobile apps, effectively adapting to the increasingly widespread adoption of mobile applications.

- **Selected Success Cases**

  Beijing Rural Commercial Bank,
  Anhui Ma'anshan Rural Commercial Bank
  Beijing Pinggu Xinhua Township Bank
  Weihai City Commercial Bank, Wujiang Rural Commercial Bank
  China Orient Asset Management Co., Ltd.
  China Cinda Asset Management Co., Ltd.
  Jiu Zhou Securities, Bairui Trust Co., Ltd.
  AVIC Xingang Guarantee Co., Ltd.

Unified Management Solution for Financial Data Centers

Demand Analysis

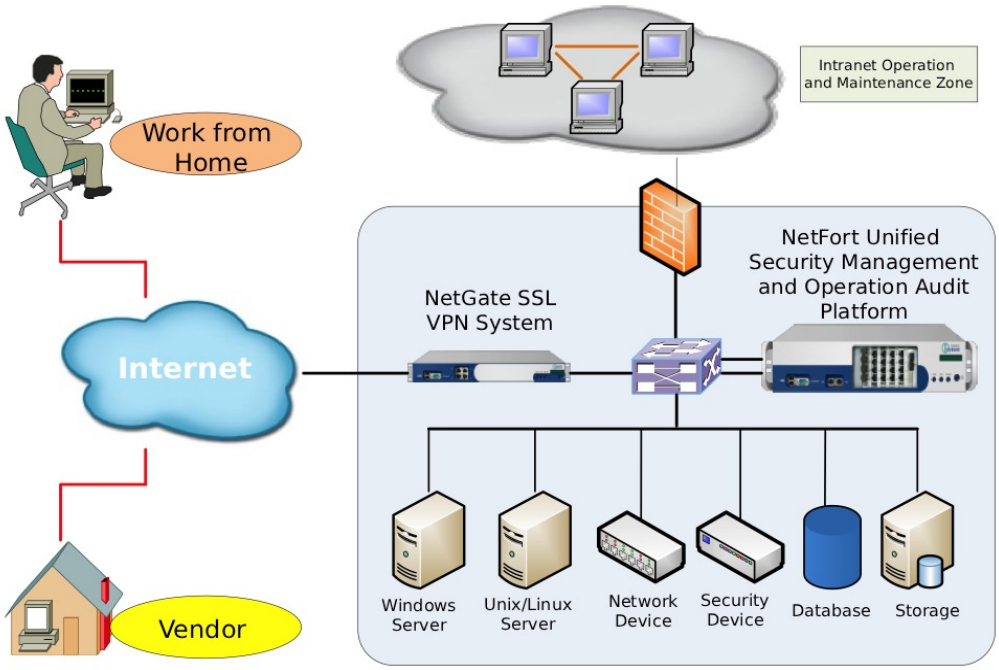
With the rapid advancement of informatization, IT systems have grown increasingly complex in scale, the number of data center equipment has surged dramatically, and the composition of operations and maintenance personnel has become more diverse. The secure operation of IT systems directly impacts the economic and social benefits of user organizations. IT operations and maintenance are gradually converging with security management.

In the face of increasingly complex IT operations environments, non-standardized operational management practices are posing significant security risks to users:

- ✓ Account management is disorganized, with widespread sharing of accounts and weak password authentication, making identity security impossible to guarantee；
- ✓ Lack of granular access control, high-privilege operations, and opaque risk exposure；
- ✓ The access process lacks effective oversight and is difficult to regulate retrospectively；
- ✓ Traditional network auditing cannot meet the requirements for auditing and managing operational maintenance activities.

Scientific management of financial data centers requires establishing a unified security management system to centrally oversee security operations and audit maintenance activities across all hosts, servers, network equipment, and security devices. This establishes a centralized, controllable, and proactive operational management model. By implementing account management, identity authentication, authorization management, access control, and operation auditing throughout IT maintenance processes, security management is achieved to meet compliance audit requirements.

Solution Architecture



Solution Description

Deployment Method

Typically employs a single deployment model with physical bypass and logical serialization, preserving network topology and reducing points of failure. Dual-machine hot standby operation ensures high system availability.

When accessing managed devices, users first connect to the NetFort Unified Security Management and Operations Audit Platform via HTTPS. NetFort then initiates access to the managed devices using protocol proxy functionality.

NetFort Unified Security Management and Operations Audit Platform Account Management

Establish centralized account management to link resource accounts with natural persons, including: automatic collection and synchronization of accounts for host servers (such as Windows, Windows domain controllers, Unix, Linux) and network devices. Centralized account management enables monitoring and management throughout the entire account lifecycle, reducing the complexity and workload of account administration while establishing unified, standardized user account security policies.

Password Custody

Set up password auto-change schedules to support periodic automatic password changes for all managed devices. Password changes are based on password security policies, such as password strength requirements.

Identity Authentication

Built-in Radius authentication and CA digital certificate authentication, supporting MAC address binding. Supports multiple third-party authentication methods: LDAP domains, dynamic passwords, third-party CA, two-factor authentication, and biometric authentication.

Single Sign-On

The browser-based single sign-on system enables users to access authorized resources directly after a single login to the operations and maintenance security management platform, eliminating the need for repeated authentication. This single sign-on provides personalized, quick access, significantly boosting work efficiency and freeing IT operations personnel from memorizing multiple system user IDs and passwords. When integrated with the NetPass dynamic password system from Infosec, SSO significantly enhances security during the identity verification process.

Resource Authorization

Implement authorization based on users, roles, and resources to achieve fine-grained permission control.

Access Control

Host Command Control Policy: Restricts user device operation commands and supports blacklisting/whitelisting of command sets. FTP File Access Policy: Restricts user FTP commands and supports a list of common commands. Address Access Policy and Time Access Policy enable more effective dynamic access control.

Operational Audit

The platform comprehensively records the entire process of user logins and operations, monitors and audits user activities, performs rollback operations, and enables session monitoring and blocking. The Operations Management Platform supports auditing multiple protocols: Telnet, FTP, SFTP, SSH, RDP(Windows Terminal), XWindows, VNC, HTTP, HTTPS, databases, and more.

Log Reports

Audit logs support standard Syslog transmission and allow control over Syslog destination, enabling integration with third-party logging products. Additionally, comprehensive reporting capabilities are provided.

Process Management

Supports multiple process-oriented management systems aligned with modern enterprise management models: staff onboarding application process, staff position change application process, staff resignation application process, resource access application process, and resource authorization application process. Meanwhile, it provides support for the primary and secondary position management as well as dual-person joint management of resource accounts.

Organizational Structure

Multi-level organizational structure views can be established and displayed in a tree format, including group management for main accounts and resource grouping. This clear organizational structure makes system administration significantly easier.

High availability

Supports dual-machine hot standby, automatically synchronizes audit data and business data, and supports network port redundancy.

Supports cluster mode, enabling login to multiple jump server devices through a single entry point, suitable for distributed deployment scenarios.

Solution Advantages

Excellent scalability

By integrating certain 4A concepts into the NetFort Unified Security Management and Operations Audit Platform, it not only provides fundamental access control and operational audit functions but also offers streamlined centralized management capabilities for accounts, authentication, and authorization.

Robust auditing capabilities

Accurately records user operation timestamps. Audit results support multiple display formats, enabling complete operation reconstruction. Audit results can be recorded for playback, with adjustable playback speed and drag-and-drop navigation during replay to quickly pinpoint problematic operations. Convenient audit query functionality allows simultaneous retrieval of multiple commands.

Simple to deploy and use

No need to install agents on managed devices; No need to alter the physical network topology; No impact on the operation of managed devices; Administrators and operators both use web-based interfaces for simple operation.

High maturity and security

The system employs advanced security measures, including encryption, filtering, backup, digital signatures and identity authentication, and permission management to establish a robust security mechanism. This ensures user legitimacy and protects data from illegal theft, thereby guaranteeing product security.

Success Cases

Inner Mongolia Bank

Zhengzhou Bank