Postprint: Applied Research on PKI Technology in Sensitive Information Collection and Transmission

Authors: Han Xiao, Li Jieyuan

Date: 2023-10-08T00:00:00+00:00

Abstract

As a security technology, PKI has deeply penetrated into all layers of conventional networks and constitutes a comprehensive solution to contemporary network information security issues. Through an analysis of PKI technology's composition, functionality, and characteristics, combined with the specific news gathering and editing business requirements of Xinhua News Agency, this paper elaborates on how to employ PKI/CA technology via digital encryption and digital signatures to ensure information confidentiality, integrity, and non-repudiation, thereby addressing key technical challenges in the collection and transmission of sensitive information for Xinhua News Agency.

Full Text

Research on the Application of PKI Technology in Sensitive Information Collection and Transmission

ChinaXiv Cooperative Journal

Abstract: As a security technology, PKI has penetrated every layer of conventional networks and represents a comprehensive solution for current network information security issues. By analyzing the composition, functions, and characteristics of PKI technology and combining them with the specific editorial business requirements of Xinhua News Agency, this paper elaborates on how PKI/CA technology employs digital encryption and digital signatures to ensure information confidentiality, integrity, and non-repudiation, thereby solving key technical challenges in Xinhua News Agency's sensitive information collection and transmission operations.

Keywords: PKI; Information Security; Encryption Mechanism
Chinese Library Classification: TP309.2

Document Code: A
Article ID: 1671-0134(2018)08-050-02
DOI: 10.19483/j.cnki.11-4653/n.2018.08.016

Authors: Han Xiao, Li Jieyuan

1 PKI Technology

1.1 Concept of PKI

PKI (Public Key Infrastructure) is a standards-based online infrastructure that utilizes public key technology to provide information security services. It employs encryption, digital signatures, and digital certificates to protect the security of applications, communications, or transaction processing.

1.2 Basic Composition and Functions

A typical, complete, and effective PKI application system should at minimum include the following components: a Certification Authority (CA), a Registration Authority (RA), a certificate repository, a key backup and recovery system, a certificate revocation handling system, and a client certificate processing system. The services provided should at minimum include the following functions: public key cryptographic certificate management, blacklist publication and management, key backup and recovery, automatic key updating, automatic management of historical keys, and support for cross-certification.

1.3 Characteristics of PKI

As a security technology, PKI has penetrated every layer of conventional networks and represents a comprehensive solution for current network information security issues, which reflects its inherent technical advantages and robust vitality. The main characteristics of PKI are as follows: First, its public key is open while its private key is unique, ensuring authenticity and non-repudiation. Second, asymmetric keys provide convenient confidentiality protection, ensuring the confidentiality of data exchanges between mutually known entities while also supporting confidential data interactions between unfamiliar entities. Third, digital certificates enable relatively independent key usage without reliance on other online support services, removing limitations associated with online service dependency and making business expansion more lightweight and flexible. Fourth, key management is more secure, providing revocation mechanisms and other services to prevent private key leakage and unauthorized identity usage. Fifth, it supports complex networked trust structures, offering mutual trust and recognition relationships based on hierarchical tree structures, thereby providing sufficient technical guarantees for eliminating trust islands in the cyber world [2].

2 Application of PKI Technology in Sensitive Information Collection Business

Reference reporting represents an important form of journalism. For a long time, the problem of uploading sensitive material drafts collected by reporters in the field has not been satisfactorily resolved due to technical and security constraints. This issue has become increasingly prominent in coverage of major breaking events in recent years and urgently needs to be addressed. Meanwhile, with the continuous advancement of think tank research, the security and confidentiality requirements for sensitive information during collection and transmission have become increasingly pressing. Since sensitive information cannot be transmitted in plaintext, a sensitive information transmission system designed based on PKI/CA technology can meet relevant business requirements. PKI employs the RSA asymmetric encryption algorithm while hybridizing it with symmetric encryption algorithms, thereby ensuring both information confidentiality and efficient transmission [3].

2.1 Design Philosophy

The PKI system in sensitive information collection business mainly consists of the following components: (1) The CA certification center, responsible for certificate issuance, revocation, and management of all aspects of the certificate lifecycle after issuance. (2) The Registration Authority (RA), which serves as the approval body for digital certificate registration and an extension of CA certificate issuance and management. The RA also acts as an interface between users and the CA, accepting offline certificate applications and providing online certificate application services. (3) USB-key, a terminal authentication and encrypted storage device with hardware encryption capabilities that provides strong security guarantees for access control. It can store user keys, digital certificates, and business data, thereby enabling identity authentication and encryption for data information at collection terminals. (4) Information encryption algorithms. Algorithm complexity and key length determine security level—more complex algorithms with longer keys require more computation time and more powerful chips. The system employs cryptographic devices approved by the State Cryptography Administration to implement digital signature, verification, encryption, and decryption functions, paired with high-performance chips to provide data confidentiality, authenticity, integrity, non-repudiation, and digital envelope services. (5) Digital certificates, the core data structure of PKI. Relying on third-party digital signatures on certificates, users can verify the authenticity of a public key offline [1]. In practical applications, the certificate authentication system must provide certificate/certificate revocation list issuance services, user identity registration and review, and undertake overall security management of the certificate authentication system.

2.2 CA Service Platform and Signature and Authentication Services

In the sensitive information transmission system, the CA service platform and signature/authentication services form the security foundation. The CA service platform is responsible for issuing digital certificates to users, while signature and authentication services verify user identities and decrypt encrypted data from clients. In practical applications, the CA service platform and signature authentication services adopt existing commercial cryptography mature product solutions. The CA service platform is configured with two cryptographic machines that can provide fast and efficient cryptographic operations for business systems with high security, stability, and performance requirements. All relevant keys in the CA service platform are generated by the cryptographic machines, with root keys also stored securely in these machines, effectively guaranteeing key security. The signature and authentication server system serves as the link and pillar between the CA service platform and the sensitive information collection and transmission aggregation platform, providing comprehensive security support for application systems, including identity authentication, digital signature verification, data encryption/decryption, and certificate and certificate status query services.

2.3 System Architecture

The sensitive information collection, transmission, and aggregation system is divided into three components: an information collection service system, a security management system, and client terminals. The information collection service system is primarily responsible for providing data content services (such as upload, publication, and browsing) and serves as the executor of information resource application and publication. It integrates cryptographic and security technologies to provide secure collection of sensitive information business data. The security management system includes subsystems for identity authentication, cryptographic services, permission management and access control, and monitoring and auditing. Its primary responsibility is to ensure data access and usage security throughout the entire lifecycle of sensitive information, from generation and storage to transmission, publication, application, and ultimately data destruction. Client terminals serve as the authentication keys for end-users to access the information system platform and as cryptographic devices for terminal data encryption and storage. Through client terminals, users complete their identity authentication, obtain legitimate resources, and manage local data encryption storage.

2.4 Business Implementation

Application System Login: The system equips each user with a USB-key security token that provides user identity authentication and data encryption/decryption storage and transmission functions. Users must insert their USB-key and verify their security PIN code to launch the client application, access system resources, and view and use encrypted files. Each key represents

an operator's identity and permissions. During login, certificate validity is verified by the CA authentication server based on certificate information in the key, and user permission information is verified and obtained from the application server.

Identity Authentication Enhancement: Bidirectional identity authentication during login ensures user identity legitimacy and security.

Draft Storage Enhancement: Local draft text and images can be encrypted for storage, preventing unauthorized access even when exported through other means or opened with third-party readers.

Transmission Link Enhancement: Drafts are transmitted through encrypted channels to prevent tampering, loss, or malicious interception during transmission.

Download Document Enhancement: Terminals download draft text and images from the central server and store them encrypted locally.

The sensitive information transmission system based on PKI technology uses terminal computers and smartphones as draft editing platforms to implement security enhancements including storage encryption, transmission encryption, download encryption, and strong identity authentication. Journalists and editors install a security-enhanced information collection client on their PCs, laptops, and smartphones, which works with terminal cryptographic security devices for drafting, storage, and transmission. Draft data can be stored in designated secure directories after hardware encryption (either on local disk secure zones or mobile secure password terminal devices). During transmission, all data is sent in ciphertext form. When drafts are loaded into memory, they are decrypted via USB-key, and when written back to designated secure directories or transmitted, they are encrypted through USB-key, achieving "no plaintext on disk." Data returned in ciphertext form is then decrypted.

[Figure 1: see original paper] PKI System in Sensitive Information Collection Business

[Figure 2: see original paper] Sensitive Information Collection Business Flow Diagram

Security Management and Control: The central server configures, distributes, and manages client security tokens through the security management center, and sets and distributes terminal security policies.

Note: Figure translations are in progress. See original paper for figures.