Advances in Social Science, Education and Humanities Research, volume 290

2nd International Conference on Economic Development and Education Management (ICEDEM 2018)

Research on Digital Encryption Security Information System Based on Identity Authentication

Xu Bu
School of Information Engineering
Guangzhou Nanyang Polytechnic College
Guangzhou 510925, China

Abstract—**In order to solve the problems existing in the current authentication system, a new authentication system scheme is proposed. The user identity is used as a key production factor by using the CPK (Combined Public Key) combined public key system. From the perspective of security design, and combining the theory of CPK combined public key system, the overall design framework of CPK key management system is proposed. According to the functional requirements of the system, the main modules of the system are divided, and its main functions are stipulated. The system uses a secure authentication card as the only identity of the user. The authentication card has a certain computing ability and safe storage space. It realizes the secure storage of the user's key. Finally, from actual application scenario, the data flow of the user in the process of registration and use in the system is given. The main modules of the system are tested successfully through the security authentication card.**

Keywords—Identification Certification; Key Combination; Management System; Network Transactions

I. INTRODUCTION

The authentication service provided by the network trading platform contains the authentication of the user identity and the request information. In general, it uses user passwords, fingerprinting / iris biometrics and symmetric / asymmetric key techniques [1]. Among the many authentication mechanisms that are based on asymmetric key technology, the development of the PKI system using public key infrastructure with X.509 certificates is the most mature [2]. It is widely used in CA certificate system, digital signature and key exchange, key agreement and other fields. In the PKI system, the certification authority CA plays an important role. With the rapid development of the Internet industry, the demand for network authentication has also increased exponentially [3].

II. DESIGN OF CPK KEY MANAGEMENT SYSTEM

A. Key management center module

The key management center (KMC) is mainly responsible for the service of generating certificates in the system. Its servers are deployed in the internal LAN that is isolated from the external network [4]. All certificates must be stored in the security authentication card in order to ensure safety, and the administrators will distribute the security authentication card from physical channel to the registration management center (RMC). In order to improve the key security, the server of the key management center (KMC) uses the seed key card CPK Seed Key Card as the generation card of the user public key and the private key of the server. It is mainly used for the generation of the user's key, and does not have the identity authentication function. In this system, the common CPK ID Card is used as the authentication card of the server. The administrator or administrator client and the key management center server use their own CPK ID Card as the authentication and secure communication of the landing server [5]. The ID certificate card contains the user's ID certificate, which uniquely identifies the user's identity and stores the user's private key information. The function of identity authentication and encryption and decryption can effectively prevent the risk of weak password landing system. The key management center includes the following modules: the system management module, the RMC management module, the identification invalidation management and the key card service module. The structure diagram of the key management center is shown in Fig. 1.

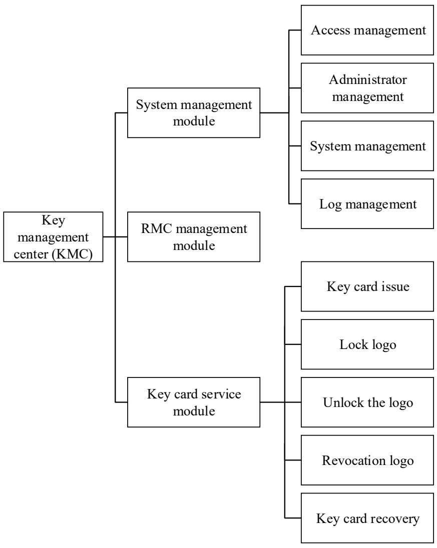

Fig. 1. The structure diagram of the key management center

[Fund Project] This paper is one phased research result of *Study on the Feasible Path of Professional Setting and Curriculum Reform in Guangdong Private Higher Vocational Colleges*, a sub-project of a major applied research project of Guangdong Province in 2017 (Project No. 2017GWZDXM004-08) and also one phased research result of *Application and Research of Intelligent Home System Based on Internet of Things*, one 2018 annual natural science research key project (Project No. NY-2018KYZD-1).

Copyright © 2018, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

B. Registration management center module

The registration management center in this system acts as a medium between the CPK key management system and the user, which directly faces the USBKEY of the terminal entity authentication card [6]. In addition, it provides services such as certificate application, certificate issuance and certificate invalidation to the USBKEY. After the system initialization or reset, all USBKEY need to register in the registry. The structure of the registry management center (RMC) is shown in Fig. 2.

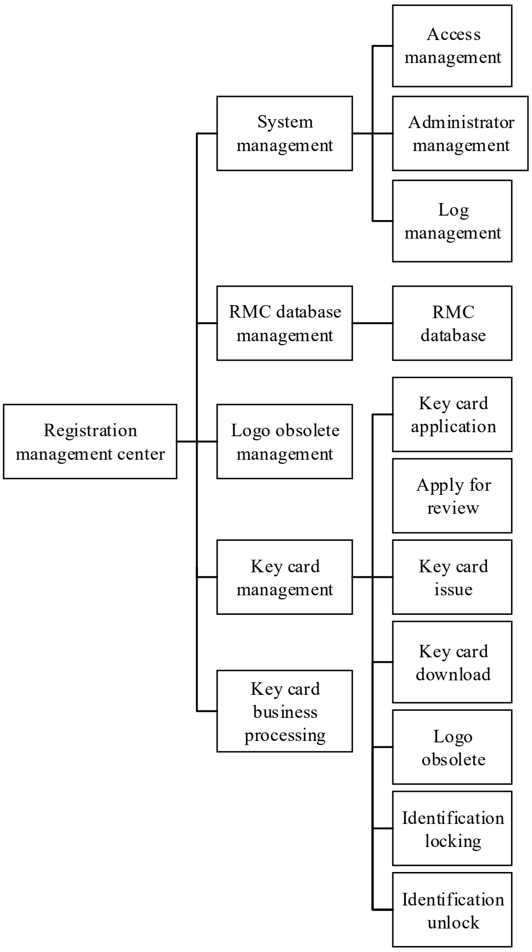

Fig. 2. The structure of the registry management center (RMC)

The registry consists of five parts: the system management module, the RMC database management module, the identification obsolete management module, the key fob management module and the key fob business process module. The RMC database management module, the identification invalidation management module, and the key fob business processing module exist only in the total registration management center (ROOT_RMC). In the CPK key management system, there is only one general registry management center (ROOT_RMC), which is responsible for the normal development and audit of all sub registration centers. Other sub registration management centers (RMC) can be set up in accordance with the actual needs. They are all from the general registration management center (ROOT_RMC). Each sub-registry handles the registration requests separately from the user terminal entities. The system needs to examine the registered user's data first. Only users who meet the audit standards can be audited and registered. The necessary information such as user ID and ID certificate is generated, and the registered user information is backed up to the system database.

C. Online query center module

Online query center module is to contact ordinary users and management system of the link. The Internet is accessed to enable online identification of user identifications. One end is connected to the public network. The other end is connected by the firewall to the internal LAN of the CPK key management system, and the independent database is set up to store all the status of the terminal entities in the CPK network. An ordinary CPK user can query the identity status and random public key of itself and other CPK users in the secure network domain through the system. The online query center module provides services only for the system registered users. When users hold their ID authentication card to log on to the system, by checking the validity and validity of the ID Certificate in the user ID authentication card, the system will verify the current user terminal entity. The online query center module determines the current user through the ID identification database retrieval. At the same time, it is necessary to detect whether the terminal system time is consistent with the server. If they do not agree, time synchronization is required. The users can not use the online query center module in query service until the audit pass. The user inquires the basic information of the user's own ID authentication card through the online query center module, including the issuing date, the validity period, the current state and so on. The workflow of the online query system is shown in Fig. 3.

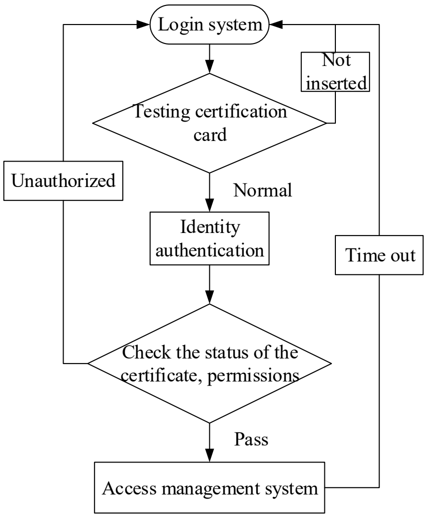

Fig. 3.The workflow of the online query system

III. IMPLEMENTATION AND TEST OF CPK KEY MANAGEMENT SYSTEM

A. Development environment

The core module of this system uses C/C++ as the main development language. The MFC is used to build the interface frame, which is a convenient and quick module management system. The online query center module takes PHP as the development language, and uses JSP, JavaScript and other technical means. With the classic MVC (model view control) design mode, the module is divided into three layers: presentation layer, business layer, persistence layer. The platform is My Eclipse. Portable, powerful and perfect structure packages are most suitable for MVC design patterns. The back-end database software adopts My SQL. It has simple structure, perfect function and good stability.

B. The realization of main module

1) Key card application sub-module

The most frequent business in the CPK key management system is the registration of new users. The process of applying for the terminal authentication card by the user needs to be coordinated by a registration management center (RMC) and a key management center (KMC). The model is deployed in a registry management (RMC) server. The user submits the application by the administrator of the application form information into the module, and submit registration. The registry manager center (RMC) reviews user information. After passing, the user identification information is sent to the key management center (KMC) to generate the user ID certificate. After the key management center generates a user ID certificate, it is sent to the key card application module of the registry center, and then the system prompts that the registration is successful.

2) KMC system management sub-module

System management software is deployed in the main server of the key management center (KMC), which provides system user management, certificate generation and query services. This module has business communications with the key card application sub-module of the registration management center (RMC). It receives user registration requests and generates user ID certificates. After each user is issued a certificate, the system will do a record. According to the conditions, this page can query the specified user's application information. The certificate management sub-module of the key management center management system can realize the task of querying the user certificates issued. It is convenient for administrators to manage certificates. According to the query, it can query the specified user's certificate and its details.

3) Online query module

The online query module provides convenient and quick query management services for ordinary users and administrators. The user needs to enter the correct username and password and insert the ID authentication card. After the authentication is passed, the user can log in to the system. After successfully logging in to the CPK key management system, users can see various services provided by the system, such as user management, authentication card management, and log management. The homepage of the administrator login system has more abundant management content than the ordinary user, which adds the function of database management and data statistics. It can realize the query and routine management service of the certificate validity period in the authentication card, which is convenient for users to manage their own authentication cards online, and understand the status of authentication in time.

C. Test environment

In order to verify the feasibility of the system, the main modules of the system were tested. In the test, the security of the secret algorithm USBKEY was chosen. As a user terminal entity authentication card, the test is carried out from the aspects of registration, authentication and query. The USBKEY properties of the test are as follows:

Chip: SM2, SM3, SM4 algorithm
Interface type: USB interface
Internal storage: 256KB
Support algorithms: RSA, DES, SM2, SM3, SM4, SHA1 / 224/256
Security: All hardened encryption module, random current disturbance source

Using the server as a test host, USBKEY is plugged into the server host and the device driver is installed correctly. Through the server-side deployment of system software, and combined with USBKEY, general business simulation tests are carried out. Server-side configuration is as follows:

CPU: Intel Core i3-3240
Memory: 2GB
Hard drive: 500GB
Operating system: windows server 2008

D. Test of the main modules of system

1) New user registration

First of all, new users need to submit a registration form when they are registered with the entity authentication card. Then, after opening the key card module management program in the registration management center, the user enters the new user registration page. The application for registration of all items in the interface are required. After all the information is filled, the user clicks on the registration button. If the system detects a certain non-conforming condition, it will be warned directly after the project. After all the items in the system are in conformity with the regulations, the successful dialog box of the pop-up registration is given to show the success of the new user registration. The generated certificates can then be written into the user's ID authentication card through the authentication card management module. In order to verify the availability of the user authentication card, a separate test is carried out for the authentication card. The authentication card is used to generate the user's public key. Through the use of authentication and authentication card decryption key, the user's signature is test.

2) *Certification card management*

After entering the user name and password, the system administrator can log in to the key management system for routine management and maintenance. When logging in, the user needs to insert the ID authentication card into the computer. The system checks the status of the certificate and user rights in the ID authentication card before logging in. If an unauthorized user is logged in, the system will give a warning. After a successful login system, the administrator can view the status of the registered authentication card in the system. At the same time, the state of key card can be changed according to the need. The key card management page contains key card information that needs to be audited, audited and not audited. At the same time, it has a query box. Administrators can manage corresponding key cards according to their needs. Through this page, users can quickly query information about key card's application time and user identification, and also can lock and unlock key cards. After testing, all the test modules can run normally, and the test results are accurate, with certain error hints and smooth interface operation.

E. Performance testing

In the process of authentication and confidential communication, a large number of computing tasks are needed. The test is carried out with the user terminal authentication card. The test is carried out using the server - side PC. The test object mainly focuses on the high-frequency computing tasks in CPK key management system, including the generation of seed matrix, the generation of public and private key matrix, the generation of public and private key of users and the signature algorithm. This test runs 100 cycles for each test item. The generated matrix size is set to 32*32. The data of the 4K is digitally signed, and then the 100 test results are calculated for their average. The final statistical results are shown in Table 1.

TABLE I THE FINAL STATISTICAL RESULTS

Test items	Test results
Public / private key factor matrix generation	0.803s
Public / private key generation	0.624s
Digital signature	0.672s

From the performance test results, Either the generation of seed matrix or the user public / private key generation is used, the speed is very fast. At the same time, the system disperses the main computing tasks to the terminal authentication card, which saves the cost of the system, greatly reduces the load of the server side, and improves the utilization efficiency.

IV. CONCLUSIONS

The detailed architecture design, function definition and specific design scheme are given for the CPK key management system. According to the various modules of the function division, the detailed design is carried out. The development of the main functional modules of the CPK key management system is realized. Each function module is tested. The test got the expected correct result. At the same time, the system's important performance indicators are specifically tested. By averaging the results of multiple tests, a satisfactory result is obtained. In terms of security, the user terminal authentication card can effectively protect the data and manage access rights. The user's secure storage is implemented. The server database is also limited to intranet access. To a certain extent, it proves the high security of the system. The CPK key management system proposed in this paper has fundamentally overcome the difficulties faced by the development of the PKI system. In accordance with the existing theoretical basis, a more complete system level implementation scheme is proposed. The specific business process is planned from the operating point of view. It not only lays a solid foundation for the construction of a new network authentication system, but also provides a possible direction for future electronic commerce.

ACKNOWLEDGMENT

The author thanks associate professor Yunli Cheng greatly for her giving him much help in the project research p and wring the paper.

[Author] Xu Bu (1986-), male, Master of science, Assistant engineer and teacher, research direction: Embedding technology of intelligent information system.

REFERENCES

[1] Q.Dong,W.Ding and L.Wei, “Improvement and optimized implementation of crypto GPS protocol for low-cost radio-frequency identification authentication,” Security and Communication Networks, 2018, (3).

[2] S.Selvakumaraswamy and U.Govindaswamy, “Efficient transmission of PKI certificates using elliptic curve cryptography and its variants,” international Arab Journal of Information Technology (IAJIT), vol. 2016, 13(1), pp. 32-38, 2016.

[3] U.Vasala and D.G.R.Sakthidharan, “Effective key management in dynamic wireless sensor networks,” International Journal of Computer Engineering in Research Trends, vol. 2018, 4(7), pp. 308-312, 2018.

[4] V.Patel and R.Patel, “Improving the security of SSO in distributed computer network using digital certificate and one time password(OTP),” International Journal of Computer Applications, vol. 89(4), pp. 23-27, 2014.

[5] X.Du, X.Chen, L.Cao and Y.Wang, “Design and realization of integrated mobile secure connection system ,” Computer Engineering and Design, vol. 28(24), pp.308-312, 2007.

[6] Y.Ren and Y. Ding, “One of authentication scheme based on CPK,” Information security and communication confidentiality, vol.8, pp.15-17, 2007.