Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 15, No. 1, 2024

Construction of Trusted Electronic Vouchers in Universities Based on PKI Technology

Minfu Xu [1, *], Junjun Wu [2], Zhixiang Zhuang [2]

[1] Network and Information Office, North China Electric Power University, Baoding, China
[2] Computer Science Department, North China Electric Power University, Baoding, China

[*] **Corresponding author**: Minfu Xu

Abstract: Certification issuance service is one of the high-frequency transactions for college teachers and students in daily work. Implementing the construction of trusted electronic certificates can greatly facilitate the processing of related business for teachers and students, and also accelerate the construction of smart campuses. This article is based on PKI technology, and elaborates on the construction of trusted electronic certificates in universities from three aspects: construction background, construction plan, and construction significance. The construction plan is introduced in detail, and the positive significance of promoting the construction of trusted electronic certificates in universities for teachers, students, and information technology construction is pointed out.

Keywords: PKI technology; Trusted electronic credentials; Construction plan; Electronic signature.

1. Introduction

In recent years, the construction of smart campus Informa ionization has developed rapidly, and many business systems such as student enrollment management system, academic management system, personnel management system, scientific research management system, office OA system, financial management system, etc. have been completed, greatly supporting education management work, promoting talent cultivation, improving scientific research level, and providing convenient life services for teachers and students on campus.

With the implementation of the "Internet plus" strategy, the acceptance and recognition of "electronic materials" and "electronic seals" by government departments, enterprises and public institutions, and social groups are gradually increasing. According to relevant regulations, reliable electronic signatures have the same legal effect as handwritten signatures or seals, electronic seals have the same legal effect as physical seals, electronic materials stamped with electronic seals are legal and valid, and electronic materials stamped with electronic seals can be used as a basis for handling political service matters. This further clarifies the legal effect of electronic materials [1].

At the same time, electronic materials such as "electronic invoices" and "electronic insurance policies" that rely on electronic signature technology have been widely used in society, providing examples and technical support for the production and application of trusted electronic certificates [2]. At present, colleges and universities need to issue many certificates of honor, graduation certificates, academic degree certificates and other certificate documents every year. To meet the needs of paperless construction of colleges and universities, it is urgent to build a trusted electronic voucher application based on the "Internet plus" technical route and provide a "no meet", "all online", "real-time" business service model [3].

Reliable electronic signatures based on PKI (Public Key Infrastructure) technology can achieve trusted electronic credentials, support the comprehensive application of electronic credential business in universities, and provide better services for various students [4]. PKI is a universal security infrastructure that uses asymmetric cryptographic algorithm principles and technologies to implement and provide secure services. It is a standardized platform that utilizes public key encryption technology to provide a complete set of secure infrastructures for the development of online e-commerce and e-government. It can provide the required key and certificate management for all users in the network who need to use cryptographic services such as encryption and digital signatures. Users can use the security services provided by the PKI platform for secure communication. A complete PKI system must have basic components such as authoritative certification authority, digital certificate repository, key backup and recovery system, certificate invalidation system, and application interface. The authoritative certification authority is the core component of PKI, also known as the authentication center. It is the issuing authority of digital certificates and an authoritative, trustworthy, and impartial third-party organization in PKI applications; The digital certificate repository is used to prove the authenticity and legality of public keys to users in a network environment using public key systems; The key backup and recovery system can prevent users from losing their keys, which can cause encrypted files to be unable to decrypt and data to be lost; The certificate invalidation system is used to stop using certificates due to changes in user identity or loss of keys; The PKI application interface system provides a secure, consistent, and trustworthy way for various applications to interact with PKI, ensuring the security and trustworthiness of the established network environment and reducing management costs.

2. Construction plan

2.1. Overall Architecture

The trusted electronic credential service for universities based on PKI technology mainly consists of three parts: data extraction, trusted electronic credential service, and electronic credential verification. The overall architecture

diagram is shown in Figure 1.

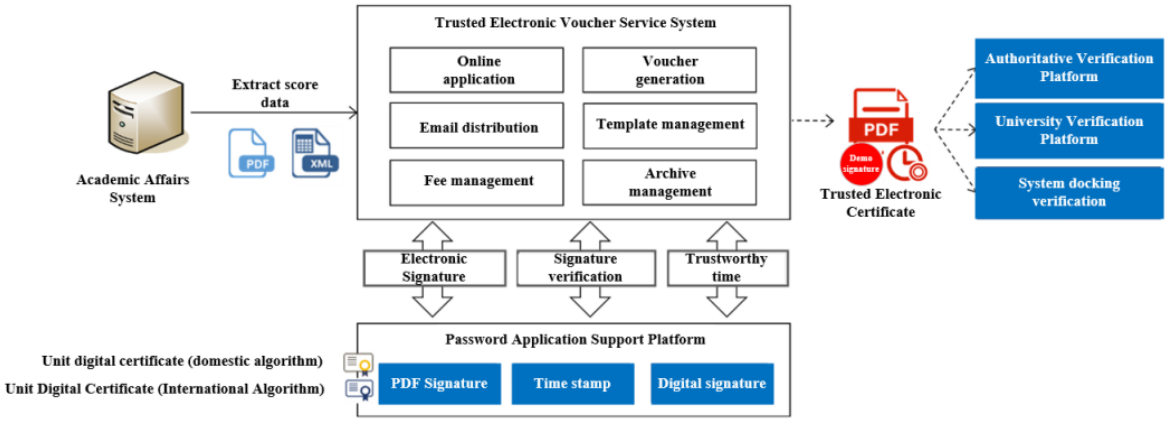

Figure 1. Overall Architecture Diagram

2.1.1. Data Extraction.

Integrate the academic administration system with the trusted electronic credential service system, and exchange data with the trusted electronic credential service system through an interface. The trusted electronic credential service system will extract student data, course data, grade data, etc. from the academic system according to the university transcript template.

2.1.2. Trusted Electronic Voucher Services.

The trusted electronic voucher service system realizes the application, generation, verification and other functions of trusted electronic vouchers such as Chinese and English transcripts, Chinese and English school certificates, student graduation certificates and other vouchers, provides students with Internet online application, payment, distribution and verification services of trusted electronic vouchers, and provides teachers with template management, student management, and other business management functions.

The password application support platform is a dedicated password device that relies on key management and password computing capabilities to provide services such as data fingerprint extraction, PDF signature, timestamp, etc. to the trusted electronic credential service system. It supports the implementation and application of various functions of the trusted electronic credential service system.

2.1.3. Electronic Voucher Verification.

Introduce a trusted third-party electronic authentication agency to issue unit digital certificates for the academic affairs office of universities, ensuring the authenticity and validity of the electronic certificate issuing agency's identity. The unit digital certificate includes: one domestic algorithm signature certificate, one domestic algorithm timestamp certificate, one international algorithm signature certificate, and one international algorithm timestamp certificate. Simultaneously incorporating multiple verification methods to adapt to different scenarios of trusted electronic credential verification. The self built verification platform of colleges and universities provides online electronic certificate authenticity verification platform to students, other colleges and universities, employers and other academic certification recipients through the Internet portal, which is an important verification means provided by colleges and universities as trusted institutions to the society; Docking with authoritative institution verification platforms, through docking with authoritative institutions, the trusted electronic transcripts generated by universities can be verified and authenticated on authoritative institution websites, enabling fast and convenient student score authentication services and achieving “instant” score authentication; The system docking verification can support batch verification of the authenticity of electronic voucher forms in business scenarios such as transcript archiving. The electronic archive management system of the archives can integrate a trusted electronic voucher service system verification service.

2.2. Business Process

2.2.1. Application for Trusted Electronic Vouchers.

The process for applying for and issuing trusted electronic credentials is as follows: students bind their email addresses; Students verify their personal and academic information; Students apply online; Select the type of academic proof and complete online payment (if required); After successful application, the system automatically generates a trusted electronic credential; The generated trusted electronic credentials are sent to students in real-time via email and can be downloaded by students at any time.

2.2.2. Trusted Electronic Voucher Generation.

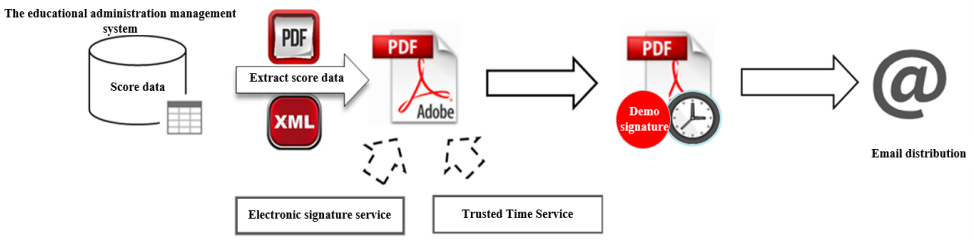

Figure 2. Trusted Electronic Voucher Generation Process Diagram

The process of generating trusted electronic credentials is as follows:

(1) Extract business data such as student data, course data, and grade data from the academic management system based on electronic voucher style templates, and exchange data in XML format or PDF document format;

(2) Based on the electronic voucher style template, automatically fill in business data to the corresponding location and generate PDF format files to complete formatting processing;

(3) Add electronic signatures, timestamps, and other trusted features to PDF files, complete trusted processing, and generate trusted electronic credentials. Among them, the Chinese transcript is issued using the domestic algorithm SM2; The English transcript is issued using the international algorithm RSA.

2.2.3. Verification of Trusted Electronic Vouchers.

There are three verification methods for trusted electronic credentials, namely official reader verification, authoritative institution platform verification, and university self-built platform verification.

(1) Official reader verification

Trusted electronic credentials can be opened through the official PDF reader (Adobe Reader) to verify their authenticity. You can view information such as issuing unit and issuing time. If the academic certificate has not been tampered with, the electronic signature will be displayed normally. If the academic certificate is tampered with, the electronic signature will display abnormally.

(2) Authoritative institution platform verification

After universities open service docking, their issued trusted electronic transcripts can be quickly verified on the authoritative institution's online "Electronic Transcript Verification Platform". Students upload a trusted electronic transcript, enter the verification code, click "Verify", and start the verification process; The verification platform provides real-time feedback on the transcript verification results, which are either "verification passed" or "verification failed", and displays the issuer and issuance time information.

(3) Verification of self-built platforms by universities

Set up an online verification service portal for electronic certificates on college Internet websites to provide verification services for trusted electronic certificates issued by colleges and universities. Students upload trusted electronic credentials, enter the verification code, click "Verify" to start verification; The verification platform provides real-time feedback on the verification results of academic certificates and displays information on the issuer and issuance time.

2.3. System Integration

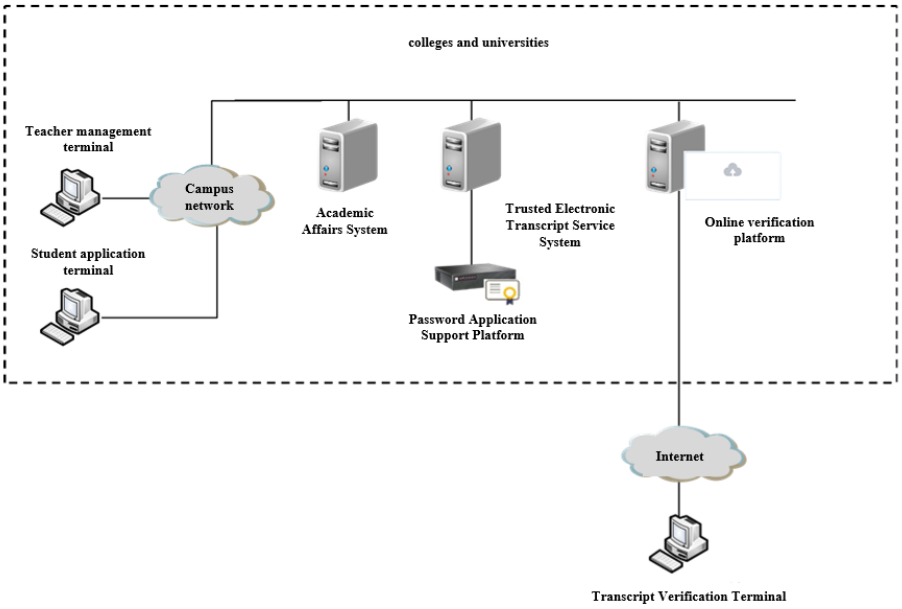

Figure 3. Deployment Architecture Diagram

It can be seen from the deployment architecture diagram in Figure 3 that the trusted electronic voucher service system is deployed in the university Internet or campus network segment, interworking with the educational administration management system network, and capable of data interaction and interface integration calls. The system supports two deployment methods: physical server deployment or virtual server deployment. Teacher administrators and student users can access the system through the Internet for business processing. The password application support platform is deployed in the university network and communicates with the trusted electronic credential service system network to provide password calculation functions and services. The university transcript verification platform is integrated in the Internet portal or provided separately. The transcript verifier can obtain the transcript verification service through the Internet.

3. Significance and Role of Construction

The application of trusted electronic credentials will add a business service model of trusted electronic credentials on the basis of the existing working mode, as an important supplement and optimization means for the issuance of transcripts and school certificates. It has the following meanings and functions:

(1) Provide a remote business processing method without face-to-face interaction to solve the problem of transcript stamping. Students can apply for, generate, and obtain trusted electronic credentials online through the system, achieving remote and fully self-service business processing without the need to physically visit the school for on-site processing. Effectively solve the problems of on-site processing of paper

transcripts, long waiting times, and multiple trips to and from school. Building a trustworthy electronic credential application that can continuously provide services to students through an “all online, no in person” approach.

(2) Enhance the anti-counterfeiting and anti-counterfeiting capabilities of academic transcripts. By relying on electronic signature technology, trusted features (electronic signature and timestamp) are added to electronic certificates. Once the generated trusted electronic certificate is tampered with, it can be easily and intuitively identified, greatly enhancing the anti-counterfeiting and anti-counterfeiting capabilities of the transcript.

(3) Collaborate with authoritative institutions to shorten the score verification cycle. Support integration with authoritative electronic credential verification platforms, where trusted electronic credentials issued by universities can be directly uploaded and verified on the authoritative platform. The processing cycle for student grade inquiry and certification services has changed from 3 to 4 weeks to “instant processing”, and there is no need for school teachers to participate in grade verification, truly achieving the authenticity, convenience, and speed of electronic voucher verification.

(4) Optimize the business process of transcript archiving. The system can generate and export student electronic vouchers in batches, which can be directly delivered to the archives for electronic archiving without the need for complicated printing, stamping, and scanning work. Greatly reduces the workload of teachers, makes the archiving workflow more convenient and fast, and improves the quality of archived transcripts.

(5) Improve the quality of academic affairs and the level of student services. The electronic issuance of academic transcripts can optimize the business processing mode, accelerate the issuance speed, enable the academic affairs office to cope with a large number of issuance work in a short period of time, improve the quality and efficiency of academic affairs work, and provide students with more practical and convenient services.

4. Conclusion

Starting from the background of the informationization construction of university academic affairs, this article introduces a trustworthy electronic certificate construction scheme based on PKI technology, and points out the significance and role of promoting trustworthy electronic certificate construction in the current development of university informationization. Promoting trustworthy electronic certificate construction in universities can not only facilitate teachers and students, but also improve office efficiency and authentication credibility. At the same time, promoting trustworthy electronic certificates is also an important component of universities to achieve the goal of building a smart campus. Subsequent research will be based on the construction of trustworthy electronic credentials for academic affairs, and the implementation of “paperless” authentication will be promoted throughout the university to further advance the informationization construction of universities.

References

[1] Zhang Qianyun, Pan Weihua. “Research on the Application Scheme of Trusted Electronic Transcripts in Colleges and Universities Based on the Scene of Educational Informatization”, Computer Knowledge and Technology, Vol.5, pp. 59-61,2024.

https://doi.org/10.14004/j.cnki.ckt.2024.0171.

[2] Zhong Mei, Dong Qian, Xu Xuguang, Lu Xiaoqian. “Research on the Implementation Method of Trusted Electronic Proof Materials in Universities - Taking Electronic Transcripts as an Example”, Information Systems Engineering, Vol.1, pp.137-139,2023.

[3] Chen Longlong. “Design and Implementation of Trusted Electronic Document System in Universities: A Case Study of Fuzhou University”, Information and Computer (Theoretical Edition), Vol. 23, pp. 83-87, 2023.

https://doi.org/10.3969/j.issn.1003-9767.2023.23.027.

[4] Huang Tenghui, Gao Chaohang, Kou Jianbo, Li Denghe, Ren Zhaohui. “Research and Design of PDF Signature and Signature Document Verification Scheme Based on PKI Technology”, Information Security and Communication Confidentiality, Vol. 2, pp. 80-92,2024.

https://doi.org/10.3969/j.issn.1009-8054.2024.02.010.