Research on the Integrated Electronic Signature Service Platform of Energy and Power

Lili Li1,2,*, Huimin Liao1,2, Jiaxing Xuan1,2 and Huinan Wang3
1State Grid Electronic Commerce Co., Ltd., Beijing 100053
2State Grid Blockchain Technology (Beijing) Co., Ltd., Beijing 100053
3State Grid Shanxi Marketing Service Center, Taiyuan 030002, China

*Corresponding author email: lilili@sgec.sgcc.com.cn

Abstract. In view of the many problems faced by the electronic signature service in the power industry, such as the increase of the media and types of storing digital certificates, the diversity of service modes of electronic signature, and the comprehensive support of the national secret algorithm, this paper proposes a scheme of the integrated electronic signature service platform. The platform adopts SDK interface to call its signature and verify signature, middleware and certificate service provide the interaction between application and digital certificate, realize the coexistence of multiple signature modes, meet the diversified electronic signature services of power users, improve the security of signature, and better serve the development of power business.

1. Introduction
Power system is an important energy system in China. The security of power system will directly affect the national economy and people's livelihood, and even related to national security. As early as 2006, SERC(State Electricity Regulatory Commission) issued the general plan for safety protection of secondary power system, which requires that the safety protection work of secondary power system should adhere to the principle of "safety zoning, network dedicated, horizontal isolation, vertical certification", to ensure the safety of power monitoring system and power dispatching data network; In July 2014, in order to standardize the supervision and management of network and information security in the power industry, the national energy administration formulated the management measures for network and information security in the power industry. In order to strengthen the information security management of the power monitoring system, prevent hackers and malicious codes from attacking and infringing the power monitoring system, and ensure the safe and stable operation of the power system, the regulations for security protection of the power monitoring system was put into effect in September.

In these schemes, methods, regulations and guidelines, All of them put forward requirements for the four elements (confidentiality, integrity, availability and non repudiation) of identity authentication and electronic document security in various scenarios of power industry, and the electronic signature technology of digital certificate has become an effective solution.

In the power industry, digital certificates have been used for user identity authentication, electronic bidding, electronic contract signing and other electronic signature services for a long time, Many enterprises and companies have established electronic authentication system based on electronic signature. But with the rise of mobile Internet, cloud computing and big data, the system is increasingly unable to meet the business needs of the industry.
2. Another Section of Your Paper

2.1. The Carrier Form of Digital Certificates is Getting Richer

In the traditional PC era, digital certificates are mostly stored in the Ukey security chip with Ukey media as the carrier. Depending on the inability to read the private key and the chip's security mechanism, the security of Ukey-based digital certificates is effectively guaranteed. Later, due to the lack of security issues in interacting with the client during the use of the first-generation Ukey, the second-generation Ukey with higher security levels appeared, such as buttons KEY, display KEY, fingerprint KEY and other products.

With the rise of the mobile Internet, mobile terminals quickly occupied the market. Users are accustomed to using mobile terminals for mobile payment, electronic contract signing, mobile office, and so on. Ukey, which is classified as a PC, has Bluetooth KEY and audio on mobile terminals. KEY and other products.

Because Bluetooth key and other products have problems in portability and compatibility, such as poor user experience, There is a digital certificate based on Se (security element), also known as security module, which belongs to a kind of security chip. Se can be divided into three forms: SIM (Subscriber Identity Module) based Se, SD card (Secure Digital Memory Card) based Se and full terminal Se. The digital certificate based on Se solves the convenience problem of Bluetooth key and other products by using the existing interface of mobile terminal or directly integrating on mobile terminal.

In recent years, using the theory of threshold cryptography, the mobile shield soft certificate based on key division has become a popular product of mobile terminal digital certificate. The mobile phone shield uses a pure software to divide the private key of the asymmetric algorithm into two parts. One part of the private key component is stored on the mobile terminal, and the other is stored on the server or cloud. After completing each of their signature components, the entire signature is completed by a synthetic method. Since the mobile terminal only stores a part of the private key, even if it is cracked, the final signature data cannot be forged. The security mechanism of this mode can be guaranteed.

Because it does not depend on hardware, and its security level meets the second-level detection requirements of "GMT 0039-2015 Cryptographic Module Security Detection Requirements", it has been widely praised by the mobile terminal market.

2.2. Various Signature Modes of Electronic Signature

In the traditional UKEY scenario, the electronic signature process is completed in the UKEY security chip.

In various forms of digital certificates for mobile terminals, combined with the application scenarios of electronic signatures and user needs, a variety of signature modes have emerged. For example, the user stores the signed private key on the server / cloud, and the electronic signature process is completed on the server / cloud. In some scenarios where the number of signatures is small, there is an electronic signature that is destroyed after a signature is used.

As mentioned above, the mobile phone shield soft certificate based on the key-splitting mode, the signing process is jointly operated by the mobile terminal and the server, and the entire electronic signature process is completed in a synthesized manner after calculating the signature components.

2.3. Many Vendors and Products Providing Signature Services

Among the vendors that provide electronic signatures, some are themselves CA agencies. In addition to providing digital certificates to enterprises, these CA agencies also provide electronic signature services. Some of them are also third-party electronic signature service providers who use digital certificates issued by CA agencies to provide comprehensive services such as electronic contract signing services.

In the construction of the enterprise's PKI / CA system, it is divided into two types: operating CA and self-built CA. Generally, the operating CA charges according to a single digital certificate, and there is a certain amount of operation and maintenance costs every year; The authorized number of self-built
CA's digital certificates depend on the enterprise itself. CA institutions provide digital certificate middleware and management systems for use by industrial enterprises. On the one hand, the process of electronic signature needs not only Ukey, but also the cooperation of server encryption machine and signature verification server. On the other, electronic signature is mostly used in combination with time stamp system, identity authentication management system, and evidence collection system, in practical application. No matter from hardware equipment or software system, most of them are provided by different manufacturers, which brings some difficulties to the management of enterprises.

3. Electronic Signature Service Platform

3.1. Overall Architecture of the Platform
The electronic signature service platform provides services for various applications in the power industry, such as power trading, power bidding, power finance, and electronic contracts signing. The application calls its signature and verification signature through the SDK API of the platform. Middleware and certificate service provide the interaction between the application and digital certificate. The lower layer of the platform consists of encryption machine, signature verification server, time stamp system and collaborative computing. Data storage, cache service and server equipment are at the bottom of the platform. The overall architecture of the platform is shown in Figure 1.

![Figure 1. Overall architecture of electronic signature service platform.](image)

3.2. Electronic Signature Service Framework
The electronic signature service framework consists of a signature service, a signing party, and a relying party. As a system external service, CA certification center is used to provide digital certificates and related services to signers.
(1) Relying party
A relying party is a party that needs to use an electronic signature for subsequent business operations.
(2) Signatory
The signatory is the subject of electronic signature. Signers often need to use an application to control and confirm the electronic signature process. In some business scenarios, the signatory and the relying party may be the same entity.
(3) Signature service
Signature service is the most important part of electronic signature service platform. The signature service provides user management, key management, and digital signature services for signers and
relying parties through technology and management. Signature services include cloud services on-demand services, ubiquitous access, resource pooling, rapid scalability, and service metering.

![Signature platform service framework.](image)

**Figure 2.** Signature platform service framework.

### 3.3. Support Multiple Signature Modes
The signature service platform supports multiple signature modes, including client mode, server mode, and collaboration mode.

1. **Client signature mode**
   In client signature mode, the key is stored in the client's cryptographic module. When an electronic signature is required, the signing party confirms that the signature is completed in cooperation with the signature server. The client signing mode is used for business scenarios that provide signing services to individuals.

2. **Server signature mode (private key escrow)**
   The key encryption is stored in the keystore on the server/cloud. During the electronic signature process, after the server authenticates the identity of the signatory, it completes the signature on the server.
   
   The server-side signature mode is used to provide signature services to business applications.

3. **Co-signature mode**
   In Co-signature mode, keys are divided into client private key components and server private key components. Client private key components are stored in user terminals, and server private key components are stored in server key libraries. In the electronic signature process, with the confirmation of the signing party, the client and the server use the private key components held by them to sign the signed data to obtain the intermediate result of the signed data, and finally generate the final signed data by synthesis.

### 3.4. The Main Electronic Signature Process
Corresponding to multiple signature modes, the main electronic signature processes of the service platform are as follows:

1. **Client signing process**
   ① Client sends signature request to server;
   ② The server generates the data to be signed and returns it to the client;
   ③ The client calls the digital certificate middleware to generate signature data.
   ④ The client returns the signature data (result) to the server, which verifies the correctness of the signature result through the signature verification server.

2. **Server signature process**
   ① The client sends the signature request to the server, and the server generates the data to be signed and returns it to the client;
② The client sends the authorization request to the authentication and authentication center, and the authentication and authentication center returns the authorization notice to the server after checking the identity information of the client user;
③ After the authentication center confirms the identity of the client user, the server performs signature;
④ The server returns the signature data to the client.
(3) Collaborative computing signature process
① The client sends signature request to the server, and the server generates signature data and returns it to the client;
② The client calls the private key component of the client's cooperative signature SDK to generate the intermediate data of the signature, and sends the data to the server;
③ The server-side cooperative signature component calls the private key component of the server-side to treat the signature data and obtains the intermediate signature data of the server-side through calculation;
④ The server sends the signature intermediate data of the server to the client, and the client generates the final signature data after synthesis;
⑤ The client returns the final signature data to the server for verification of the correctness of the signature result.

![Figure 3. Client signature process.](image)

![Figure 4. Server signature process.](image)
Figure 5. Collaborative computing signature process.

4. Platform Background Management System
The background management system of electronic signature service platform mainly manages roles, configurations, logs, services, customers, collaboration, etc.

4.1. Basic Services
(1) System management
Administrator management: provides the function of managing the administrator who logs in to the system. The administrator can view which functions are based on the assigned roles.
Role management: configure some roles for administrator allocation;
Menu management: control the menu that can be operated;
(2) Configuration management
CA configuration: configure the CA products of the access system, and synchronize to certificate services after configuration;
Certificate verification configuration: the configuration of how to verify the certificate will be synchronized to the certificate service after the configuration is completed;
Certificate issuance policy configuration: policy configuration of Ca product issuance certificate. After configuration, it will be synchronized to certificate service;
(3) Customer management
Customer list: manage the customers of the access platform, including the addition, deletion and modification of customers.
Application List: manage the applications under the accessed customers, including adding, deleting, modifying applications, assigning interfaces, keys, updating certificate configurations to applications;
(4) Service management
Key management: it mainly shows the server key, which is obtained from the key service;
Service instance management: the function of managing all services registered in the registry;
Interface list: shows some external interfaces.

4.2. Other Services
(1) Collaborative management
User management: it mainly deals with the available operations of users in the collaboration service. The user list is obtained from the collaboration service.
(2) Business data
Signature record: query the signature record in the signature platform, and the signature record is obtained from the signature service.
(3) Statistical management
Certificate Services Statistics: it mainly counts how many certificates have been issued and revoked through certificate services, and the number is obtained from certificate services.
Collaboration service statistics: Statistics of the number of applications, devices, users, signatures and keys in the collaboration service. The number is obtained from the collaboration service;
Signature service statistics: the number of signatures is counted according to the dimensions of the server and the proxy escrow key, and the number is obtained from the signature service;
(4) Log management
Log query: provides query of operations in the management platform.

5. Platform Deployment
The server of the electronic signature service platform needs to be deployed in a separate server, and a Cipher machine is deployed at the back end to provide services for it. Figure 7 shows the system dual-machine deployment scheme, which can be horizontally expanded according to the actual user's concurrent requirements and performance requirements.

6. Conclusion
Under the supervision and requirements of cyber security at the national level, The electric power industry upgrades or rebuilds the original information security system. As one of the main technical means to resolve the four elements of information security (confidentiality, integrity, availability, and non-repudiation), electronic signatures have become an indispensable part of the enterprise's construction of an information security system. Based on the current status and problems of electronic signatures in the power industry, this article builds a set of integrated electronic signature service platforms based on the product-to-service model. The platform is compatible with a variety of signature products and signature modes, and is equipped with a powerful background management system. It manages the supporting software and hardware equipment for electronic signatures, effectively addresses its needs for electronic signature services, and provides information security for the power industry support.

Acknowledgments
This work was financially supported by the State Grid Corporation of China Science and Technology Project (5700-202055171A-0-0-00).

References
[1] Shuangyuan Bai, Yueqin Zhang. 2018 Principle and application of CFCA cloud certificate signature verification on mobile phone [J]. Technological innovation and productivity, (11): 86-88
[2] Shengdong Ma. 2018 Research on network trusted identity service system based on digital certificate [J]. Cyberspace Security, 9 (07): 19-24

[3] Xue Jin, Yu Jiang, Zhu Xiaona, Chang Jun, Lian Zhuxian, Yan Junfu. "Research on information isolation scheme of smart distribution", 2014 International Conference on Information Science, Electronics and Electrical Engineering, 2014

[4] Quan Zhu. 2016 PKI CA identity authentication technology research [J]. Cyberspace Security, 7 (z1): 37-39

[5] Zhang, Wen Bin, Xin He Chen, Jing Zhou, and Jing Tao Wang. "Study on Rush-Repair Scheme for Distribution Network Fault", Advanced Materials Research, 2013.

[6] Limin Liu, Jiwu Jing. 2018 On the new development trend of electronic authentication technology [J]. Confidential science and technology, (05): 17-21

[7] Ji Lai, Jia Wu, Yuchen Jiang. "Research on Risk Prevention Measures of Network Information Security in Power Systems", IOP Conference Series: Materials Science and Engineering, 2020

[8] Qiuyuan Guo, Yuchao Shen, Rongwei cen. 2017 Research and design of e-government digital certificate mutual recognition platform [J]. Information security research, 3 (06): 548-553

[9] Tingting Wang, Pengcheng Qi. 2017 Research on the development of electronic signature and electronic authentication in China under the background of Internet finance [J]. E-commerce, (08): 44-45

[10] Weifeng Jia. 2017 Application Research of electronic authentication service in cloud environment [J]. Network security technology and application, (09): 97-98

[11] Xiao-long Xu, Qi-tong Zhang, Jing-lan Zhou. "NC-MACPABE: Non-centered multi-authority proxy re-encryption based on CP-ABE for cloud

[12] Zhiyu Chen, Longchuan Yan, Yongyuan He,Dongxia Bai, Xiaolin Liu, Limin Li. "Reflections on the Construction of Cyber Security Range in Power Information System", 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2018

[13] "Computer and Computing Technologies in Agriculture VIII", Springer Science and Business Media LLC, 2015

[14] Alexandr Laruhin, Maxim Nikandrov, Leonid Slavutskii. "Anomalous Modes Recognizing Secondary Equipment in Electric Power Industry: Adaptive Neuro Algorithms", 2019 International Ural Conference on Electrical Power Engineering (UralCon), 2019

[15] Yang Hu. 2011 Application of PKI based identity authentication system in power industry [D]. South China University of technology.

[16] Shunming Yang. 2011 Application of electronic signature technology in power industry [J]. Power informatization, 9 (06): 86-88

[17] Jiwu Jing, Limin Liu. 2017 Electronic authentication enters the era of 2.0 [J]. Information security research, 3 (06): 573-576.

[18] Jiuqiang Cui, Qi Xu. 2015 Research on mobile Internet identity authentication technology [J]. Information security and technology, (7), p9-11

[19] Liang Shen, Dong Wang, Jiaxing Xuan. 2018 Cloud security risk analysis and assessment technology of power information system [J]. Telecommunication science, Volume 34 (2): 153-160

[20] Ming Li, Guozhen Shi, Jiapeng Lou. 2018 USB key authentication scheme based on cryptographic service platform [J]. Computer application and software, Vol. 35 (9): 288-291316

[21] Daqiang Li. 2016 Discussion on the feasibility of the application of electronic signature in electric power trading under the background of deepening the reform of electric power system [J]. Zhejiang electric power, Vol. 35 (9): 71-74