Design of Multi-dimensional Electronic Channel Unified Identity Authentication Method for Power Information System

Baoxian Guo^{1(✉)}, Ying Xu², Renjie Li¹, and Xingxiong Zhu³

¹ State Grid Electronic Commerce Co. Ltd., Beijing, China
winzyy@163.com

² State Grid Zhejiang Electric Power Company, Hangzhou, China

³ State Grid Huitongjincai (Beijing) Information
Technology Co. Ltd., Beijing, China

Abstract. At present, State Grid Corporation has established a wealth of electronic service channels, including 95598 website, electric E-power, hand-held power, national network mall, E-charging, WeChat, with the rich application of various electronic channels, while gradually facilitating user use. There has been a problem of poor user experience such as registration and query service sharing, lack of unified management of multiple electronic service channels, and lack of service supervision for various electronic channels. Therefore, it is urgent to start from the source to conduct specific research on unified identity authentication system among various electronic channels. So in this paper, we proposed a multi-dimensional electronic channel unified authentication method based PKI certificate for power information system. By the proposed method, users can directly access each application system and perform fast and secure switching between application systems without multiple authentication process, providing users with the convenience and security of engaging in complex business management activities.

Keywords: Certificate · Unified authentication · Ticket

1 Introduction

In recent years, China's "Internet+" and mobile Internet technologies have been vigorously developed and widely used. All industries continue to be driven by "Internet+", making full use of Internet platforms and other electronic channels to provide convenient services to customers. The construction of a high-efficiency three-dimensional service marketing channel system presents new marketing business ecology [1]. In order to adapt to the new form of "Internet+" marketing service, State Grid Corporation put forward the "Opinions on Marketing Automation Construction Work in 2014", comprehensively deepen the construction of "big marketing" system, and guide and promote the third industrial revolution. Smart grid and the Internet, further deepen the application of marketing business systems, realize high-end applications of marketing automation based on big data and cloud computing, promote the comprehensive improvement of intelligent interaction level of power supply services. It's important to

build marketing intelligent interactive service access management to meet the unified access and services of interactive websites, Weibo, WeChat, video, mobile terminals, SMS and other service channels [2]. At present, State Grid Corporation has established a wealth of electronic service channels, including 95598 website, electric E-power, hand-held power, national network mall, E-charging, WeChat, with the rich application of various electronic channels, while gradually facilitating user use. There has been a problem of poor user experience such as registration and query service sharing, lack of unified management of multiple electronic service channels, and lack of service supervision for various electronic channels. Therefore, it is urgent to start from the source to conduct specific research on unified identity authentication among various electronic channels.

With the continuous development of information technology of State Grid Corporation and the continuous pursuit of service level and quality by State Grid Corporation, various departments and subordinate units of the company have built a wealth of electronic service channels, including 95598 website, electric E-power, hand-held power and electricity, business, E-charging, WeChat, etc. Since each business application system is independent of each other, the user cannot obtain the services provided by the multi-system service application through one login. Although the 95598 smart interactive website and the national network mall have made hyperlinks to each other, they need to log in again to enjoy the next business system. The application service is cumbersome and has a poor experience. In addition, because each electronic service channel is independent and operates independently, the State Grid Corporation cannot integrate the customer resource advantages of each electronic service channel and implement targeted marketing operations [3]. Meanwhile, State Grid Corporation is lack of a unified management and monitoring platform for each electronic channel, the current management is more dispersed for lack of support means [4]. Therefore, this article starts from the source, establish a unified identity authentication management system for users, in order to optimize the user experience of each Internet electronic channel, enhance the country Grid company's Internet service competitiveness.

2 Related Works

The development of identity authentication technology has gone through the process from software authentication to hardware authentication, from single-factor authentication to dual (multiple) factor authentication, from static authentication to dynamic authentication. Common authentication methods includes password-based authentication method, smart card, token-based authentication method, PKI digital certificate-based authentication method [4], biometric-based identification method (fingerprint, palm print, iris, retina, face, voice, Signature, etc.), identification method based on combination factor. At present, domestic identity authentication technology is mainly based on weak identity authentication, including user name/password authentication technology and dynamic password authentication technology. The username/password authentication method is one of the simplest and most commonly used authentication technologies. Dynamic password authentication is developed on the basis of traditional

username/password, so that the user's password is dynamically changed according to time or usage. Achieve one-time identity authentication technology [5].

The development of future domestic identity authentication technology will be based on quantum cryptography-based authentication technology as the main development trend. Because quantum cryptography is the product of the combination of cryptography and quantum mechanics, quantum states are used as information carriers to pass keys between legitimate users via quantum channels [6]. Quantum cryptography can achieve the two ultimate goals that classical cryptography can't achieve: First, legitimate communication parties can detect potential eavesdroppers and take corresponding measures. Secondly, the eavesdropper can't crack quantum ciphers, no matter who tries to crack them. The use of the non-stealing and non-replicability of quantum cryptography in authentication technology can be used to authenticate the identity of both communicating parties. In principle, it provides an unbreakable, non-stealing and large-capacity secure communication system, which truly guarantees the absolute security of communication.

Traditional single sign-on (SSO) solutions can be divided into two categories based on the way the application is logged in. One is a script-based SSO solution, the other is an access-based ticket (AccessTicket)-based SSO solution [7]. The main goal of a script-based SSO solution is to automate the login process through scripting. The advantage of this solution is that it is easy to implement, and can add a target system to the SSO solution without modifying the code of the target system. And the disadvantage is that the client software needs to be installed, and the security needs to be improved, because the target system does not need to be used. Modifications, implementation of some other functions besides login (such as Single Log-out, secure exchange of user data between target systems, centralized management of user identity, etc.) are also difficult to solve. SSO is not the same as automatic login, but other security functions need to be considered. For the SSO solution based on access ticket, the main goal is to implement SSO by requiring the target system to transform and accept the access ticket. The verification of the user is the responsibility of the SSO server. The responsibility of the target system is only to verify the validity of the access ticket to the SSO server [8]. This solution tends to form an SSO standard (including representation of access tickets, communication between users and SSO servers, communication between target systems and SSO servers, etc.), and each target system that requires SSO must follow this standard. The advantage of this scheme is that it can realize a full-featured SSO. But the disadvantage is that the target system needs to be modified, and the original user authentication part is changed to the verification of the access ticket. It is also important that the SSO standard must be widely accepted by the software vendor.

3 Proposed Unified Identity Authentication System

This paper designs a unified identity authentication system based on PKI certificate, including certificate application, certificate verification, certificate issuance and certificate issuing mechanism for various application systems of the network [9]. The identity authentication system is divided into an authentication client, an authentication

server, a ticket server, and an LDAP directory server as shown in Fig. 1. The user only needs to actively perform one identity authentication process in the network, and then can access all the resources on the network that he is authorized to use without actively participating in the subsequent identity authentication process. By enabling users to log in once, they can traverse all the systems running on the network, that is, realize the so-called “one-point login, multi-point roaming” [10].

Fig. 1. Logic structure of proposed unified authentication system

In the system design, the user uses the password to log in to the authentication client, and the authentication client submits the user information to the identity authentication server. The identity authentication server connects the PKI and the LDAP server to complete mutual authentication with the user. Ticket server will applied after the authentication process.

3.1 Description of Unified Proposed Authentication System

The main notations used are described in Table 1.

Table 1. Notation used

Attribute	Content
$E_X(M)$	Encryption of message M using the public key of principal X
$Sig_X(M)$	Signature with appendix of message M by principal X
N_X	64 bit random nonce value generated by principal X
$\{M\}_K$	Symmetric encryption of message M with key K
C_X	X's certificate

The authentication client mainly realizes the management of the system and the customer, and provides a simple and operable interactive interface for the end user.

The authentication server is used to receive the information of the client and verify the certificate chain, certificate validity period, certificate blacklist and certificate holder when verifying the validity of the client certificate (Verify the private key signature). The Certificate Revocation List (CRL) and certificate chain are stored locally and periodically download new CRLs to LDAP [11]. After the authentication is successful, the system is transferred to the ticket server, and if it fails, it returns to the user login interface. The message exchanged in the proposed authentication method is as shown in Table 2.

Table 2. Message exchanged in the proposed authentication method

Process	Message
Authentication Request	$U \rightarrow AS : Cert(U), N_U, Capabilities, Sig_U(N_U)$
Authentication Response	$AS \rightarrow U : Cert(AS), N_U, N_{AS}, E_U(AK), Lifetime, SID, Sig_{AS}(N_U, E_U(AK))$
Key Confirmation	$U \rightarrow AS : N_{AS}, ID_U, \{N_{AS}, ID_U\}_{AK}$

The process of proposed authentication system is shown at Fig. 2. At the first step, the user sends an Authentication Request message to its AS, which includes the user's certificate, security capabilities, a random number generated by the user, Rivest, Shamir and Adleman (RSA) signature over the random number to assure the authenticity of the authentication request message.

Fig. 2. The process of proposed authentication system

After receiving the information, the server first verifies the legality of the user certificate, which contains the following four steps:

- (1) Verify the certificate whether is issued by a trusted Certificate Authority (CA) which involves authentication of the entire certificate chain. If the certificate cannot be directly trusted, it will always look up until it finds its trusted or root CA.
- (2) If the certificate is a certificate issued by a trusted CA, then the certificate must be parsed to obtain the content of the certificate;
- (3) Verify the serial number of the certificate whether is valid. Check the CRL to see if the certificate is invalid.
- (4) Verify that the certificate whether has expired. After the user certificate is verified, the AS use the user public key to verify that the signature is correct.

If the verification fails, the user is denied to login. After the verification is passed, the server extracts identity information, such as user name or certificate serial number, from the client certificate. Then the server inquires the user list of the LDAP server to determine whether the user is a registered legal user. If it is not a legitimate user, then refuse the client log in. If it is a legitimate user, the authentication server determines the encryption algorithm and protocol support it will share with the user, activates an authentication key (AK) for the user, encrypts it with the user's public key, and sends it back to the user in an Authentication Response message. The Authentication Response Message includes the AS's certificate to verify its identity, a AK encrypted with the user's public key, an AK sequence number to distinguish between successive generations of AKs, AK lifetime, a random number generated by the AS along with the user's random number used to ensure the key liveness, RSA signature over all the attributes in the Authentication Response message to assure the authenticity of the Reply messages.

Lastly, the User sends the Key Confirmation which consists of the identity of the user, the random value received in Message Authentication Response, and the encryption with the two values under the AK. The AK is the new session key for the user and the AS for further communication.

The process adopts the nonce-challenge mechanism, which can completely solve the identity authentication problem of the communication parties in the network application system, and avoid security problems such as fake websites or malicious server camouflage.

3.2 Design of the Ticket Server

The ticket server includes a ticket issuing module and a ticket parsing module. After the user passes the authentication, the ticket issuance module will generate an authentication credential ticket (i.e., a ticket) of the user, and the ticket contains the basic information of the user (name, gender, document type, ID number, telephone number, email, etc. for the individual user), some information about the user's login required by the system, as well as information about the list of systems that the user can access. The user's login ticket is respectively digitally signed for the specific application system and using the public key corresponding to the digital certificate of the application

system, so that only the application system can decrypt it, and the user information is prevented from leaking to the unrelated application system.

The system stores the user's ticket information in the session of the authentication platform. When the user logs out of the system, the authentication platform destroys the session by itself and clears all the ticket information about the user. When the user switches between different systems, the application system uses the Web Service technology to apply to the unified identity authentication system to verify whether the current ticket of the user is legal. If it is a legitimate user, then the user can log in to the system. The system uses the root digital certificate to decrypt to obtain the specific information of the user. Otherwise, it returns to the login interface.

4 Conclusion

The PKI-based unified identity authentication system effectively solves the trust problem in the information network space, and determines the uniqueness, authenticity and legitimacy of the various economic and management actors (including organizations and individuals) in the information network space. Thereby protecting the security interests of various subjects in the information network space. Users can directly access each application system and perform fast and secure switching between application systems without multiple authentications, providing users with the convenience and security of engaging in complex business management activities.

Acknowledgment. This work is supported by the science and technology project of State Grid Corporation of China under the Grants No. 52110417001D.

References

1. Bedi, G., Venayagamoorthy, G.K., Singh, R., et al.: Review of Internet of Things (IoT) in electric power and energy systems. *IEEE Internet Things J.* **5**(2), 847–870 (2018)
2. Katsikogiannis, G., Mitropoulos, S., Douligeris, C.: UACS: towards unified access control services. In: *IEEE International Symposium on Signal Processing and Information Technology*, pp. 127–132. IEEE (2016)
3. Liu, Z., Zhang, P., Guan, X., et al.: Joint subchannel and power allocation in secure transmission design for femtocell networks. *IEEE Syst. J.* **12**(3), 2688–2698 (2018)
4. Chen, C.L., Tu, Z.-W., Guo, L.: Practice of network and information security situation awareness in SGCC. *Electric Power Inf. Commun. Technol.* (2017)
5. Ahmavaara, K.I., Palanigounder, A.: Certificate-based authentication (2017)
6. Yu, Z., Wu, X., Fang, D.: A dynamic vulnerability evaluation model to smart grid for the emergency response (2018). 052028
7. Nagy, M., Nagy, N.: Quantum-based secure communications with no prior key distribution. *Soft. Comput.* **20**(1), 87–101 (2016)
8. Mainka, C., Mladenov, V., Schwenk, J.: Do not trust me: using malicious IDPs for analyzing and attacking single sign-on. In: *IEEE European Symposium on Security and Privacy*, pp. 321–336. IEEE (2016)

9. Lee, H.Y.: The implementation and investigation of securing web applications upon multi-platform for a single sign-on functionality. *Int. J. Adv. Res. Comput. Sci.* **6**(23), 39–46 (2016)
10. Luo, Y.G., Zhang, H.X., Zhu, H.Y.: Design of unified identity authentication system based on URL single sign on. *Electron. Des. Eng.* (2017)
11. Davydov, A., Morozov, G., Sergeyev, V., et al.: Methods, apparatuses, and systems for multi-point, multi-cell single-user based multiple input and multiple output transmissions (2018)
12. Priyadharshini, M.D., Ananth, C.: A secure hash message authentication code to avoid certificate revocation list checking in vehicular adhoc networks. *Int. J. Appl. Eng. Res. (IJAER)* **10**(2), 1250–1254 (2017)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.