Research on Identity Certification Framework Model in core business of Power Grid

Mengxian Chen1,a, Rui Xu2,3,b, Feng Ma2,3,c, Nan Hu4,d, Wenbo Dai1,e,* and Ke Xue2,3,f

1State Grid Zhejiang Electric Power Co., Ltd. Wenzhou Power Supply Company, Wenzhou 325000, China;
2NARI Group Corporation / State Grid Electric Power Research Institute, Nanjing 211106, China;
3NARI Information Communication Science and Technology Co. Ltd., Nanjing 210003, China;
4State Grid Liaoning Electric Power Co. Ltd, Shenyang 110004, China

aonicaxian@126.com, bxurui@sgepri.sgcc.com.cn, cmafeng1@sgepri.sgcc.com.cn, d38476972@qq.com,* eCorresponding author e-mail:starvii@126.com,
f xueke@sgepri.sgcc.com.cn

Abstract. Based on provable security theory for security protocols, a provable security identification framework model suitable for the core business of power grid is proposed to enhance the management level of user identification and improve security of user identification schemes. To verify the model, a new identification scheme for identification scenarios is given according to the model. Security analysis shows that the scheme is proven to be secure in the model. In addition, performance analysis shows that the scheme can timely response to hundreds of thousands of user requests, thus it can be used as an effective scheme for identification in the core business of grid.

Keywords: Cryptography, Identification, Provable Security, Grid Core Business, TEE, Identity Token.

1. Introduction

As a key state-owned enterprise that is related to the national energy security and the lifeline of the national economy, the State Grid assumes the basic mission of ensuring a safer, more economical, cleaner and sustainable power supply. To support the construction and operation of the power grid, State Grid Corporation provides core business support such as project management, enterprise resource planning, financial management, network operation and maintenance, and equipment maintenance. These core business types are complex and involve many people [1]. On the other hand, as the grid covers geographical areas and business operations become more widespread, in the production activities of power grid construction, operation and maintenance, inspection and control, equipment maintenance, and technical transformation, the existence of illegal intrusion, operator agent, wrong interval, misoperation, etc., poses a huge threat to the safety of people and equipment. At the same time, the most common authentication method for the current power grid is still the single-factor authentication method such as “account +
password + SMS verification code” and credentials, its security is encountering more and more challenges. There are many problems such as loss of account password, verification code being stolen, easy to be brute force, vulnerable to Trojan attacks etc., causes that the real authentication problem of network user cannot be effectively solved. So the demand for the overall information security and security management capabilities of the core business of the grid has not been met [2-3].

Therefore, the safety management and control of the core business personnel of the power grid, especially the identity authentication of personnel, has become an important issue to be solved urgently. Insufficient for existed programs and technologies, this paper proposes a proof-safe grid core business identity authentication protocol model to fill the technical gap in this field. At the same time, an identity authentication scheme is given, the protocol satisfies the security framework model. The use of this protocol can effectively improve the security loopholes in the security management and control of core business personnel, and improve the security of the core business identity authentication system.

2. Technical background

2.1. Identity authentication technology

At present, in the academic and industrial circles, the commonly used identity authentication technologies can be roughly divided into several categories [4-6]: identity authentication based on information secrets, identity authentication based on trusted objects, and identity authentication based on biometrics. Among them, the USB identification token is favored by more and more users because of its many advantages such as being safe, reliable, portable, and convenient to use. The most common form of trusted object used for identity authentication is the USB identification token. A USB identification token is a hardware device that can be connected to a computer via a USB interface. The combination of password and USB token can be used to construct a one-time "strong two-factor authentication mode” with strong security. As people's demand for identity authentication security has increased, USB identity tokens have also improved, from ordinary token hardware without screens and buttons to USB identity tokens which with display and confirmation buttons.

A typical biometric system logically includes two modules: registration module and identification module. The user's name is first registered in the registration module, the biometric information of the user is obtained by the biometric sensor, and then the feature pattern of the user is extracted from the acquired data, and the user template is created and stored in the database. In the identification module, the biometric information of the user is acquired in the same manner as the registration process, the feature pattern is extracted, and then matched with the template registered in the database to verify the identity of the user.

These techniques are effective in simple application scenarios, but the security of applications in large-scale, multi-scene systems has not been fully studied and demonstrated. The core business of the power grid involves a large number of people, complex business processes, and a wide variety of businesses. Unencrypted authentication technologies are easily to vulnerabilities and can lead to serious user identity security threats [7].

2.2. Provable security

The design and analysis of security protocols and security solutions is still an extremely complex task. For any security protocol, it is very difficult to have sufficient trust in its security. On the other hand, in practical applications, many security protocols have been compromised shortly after they are proposed. These situations indicate that informal security protocol design methods often lead to errors [8].

Provable security is a set of theories and methods that can meet the above needs. In general, provable security refers to a reduction method: firstly, determine the security objectives of the scheme and protocol, and the goal of the data encryption scheme is to ensure the confidentiality of the encrypted data; secondly, construct a formal attack model according to the attacker's ability, and define the security hypothesis available for the security scheme as the cornerstone of security. Based on the model, analyze the security of the scheme; finally, if the attacker can successfully attack, he can break the security assumption [9-10].
Prior to the advent of the theory of security, the discussion of security schemes and protocols focused on enumerating security. However, modern network environments are open-ended, security solutions must face various active attackers in an open environment. These attackers can not only take advantage of various flaws in the design of security solutions, but also use the characteristics of the implementation environment to initiate various attacks. Therefore, the design of any current security solution and the development of the corresponding standards must pass a rigorous test of the provable security theory.

2.3. Trusted execution environment
With the increasing popularity of wireless networks in mobile terminal devices, as a user identity credential, mobile devices have gradually increased the number of programs for helping users achieve identity authentication.

The general execution environment of a mobile terminal is an open platform, and various software including malware can be run on it. The security, integrity, and data confidentiality of platform devices are extremely threatening. The trusted execution environment (TEE) establishes an isolated trusted execution environment through virtualization technology, its principle is to use tag bits to distinguish security data and resources from common data and resources [11-12]. Secure data and secure resources are stored and processed in a trusted environment, while normal data and normal resources in a common execution environment. It ensures that secure resources are not captured by malicious people and improves the security of the device.

3. Identity authentication security model of grid core business

3.1. Protocol participants
In the formal model of the core business identity authentication system, the participants of the identity authentication protocol include the server S and the client set C={C₁, C₂, ..., Cₙ}. The identity authentication process is a process of authenticating the identity of Cᵢ (i = 1, 2, ..., n) by implementing a "challenge-response" protocol between S and Cᵢ.

The client Cᵢ can be a mobile terminal, or a terminal with strong processing capability such as a PC or a workstation, or an identity token with a USB port. In order to achieve identity verification capabilities, Cᵢ should have the following capabilities:

1. A digital signature function;
2. A true random number generator;
3. TEE, the signature key can be stored in the TEE and the digital signature process is performed in the TEE.

The authentication token is connected to the user client PC through a USB port. The identity token can generate a user key pair and a key handle, be able to execute cryptographic algorithms. The physical unclonable function (PUF) is integrated in the identity token to ensure the non-reproducibility of the token and improve the security of the token symmetric key. The chip used by the token has a hardware-implemented national secret algorithm (SM/SM/SM/I), and obtain the national secret model certificate. At the same time, the user key is stored in the secure storage area to ensure the security of the key storage.

Server S is responsible for user authentication, user registration key management and other functions. In the identity authentication process, the server S and the identity token are signed and checked to determine the legality of the user identity. Specifically, the server S needs to implement the following functions:

1. Establish a secure connection with the client Cᵢ;
2. Interacting identity authentication protocol messages with Cᵢ;
3. Verify that the user identity is legal through the protocol message;
4. Manage user identity based on protocol messages.

In order to achieve the above functions, S must store and manage user information tables, which stores data such as user names, user public keys, and digital certificates.
3.2. Protocol
The identity authentication protocol consists of two phases: the identity registration phase and the identity authentication phase.

In the identity registration phase, for \( i = 1, 2, ..., n \), \( C_i \) registers the user name, public key, digital certificate and other information at \( S \); in the identity authentication phase, \( C_i \) proves his identity to \( S \), and \( S \) should make a clear judgment on whether \( C_i \) is a legitimate user or not. The identity registration phase only needs to be performed once, and the identity authentication phase can be executed multiple times.

The security goal of an identity authentication protocol is to prevent an attacker from fraudulently using the identity of a legitimate user. That is, for any legitimate user \( C_i \) registered by any illegal attacker, it can successfully prevent \( S \) from believing that the attacker is \( C_i \).

3.3. Attacker
The attacker \( A \) in the model can control all the message interaction processes, so the protocol messages can be copied, forged, and falsified arbitrarily. On the other hand, \( A \) can also control forged digital certificates by controlling domain name resolution and can be accepted as a registered user by \( S \). However, due to the security of the TEE, the attacker \( A \) cannot obtain the content stored and executed in the client's TEE.

3.4. Anti-phishing attack
For an authentication scheme \( II \), its security is defined by the following "Attacker-Challenger" Game \( \Pi (A, C, S, k) \):

For \( i = 1, 2, ..., n \), security parameter \( k \), attacker \( A \) can query the challenger and obtain the query result any number of times, and in any order:

a) Execute \((C_i, S)\): requires an authentication protocol between a client \( C_i \) and server \( S \), and eavesdrop on all session messages;

b) Reg \((P)\): register a user identity \( P \) at \( S \);

c) Send \((m, C_i)\): send a message \( m \) to the client \( C_i \);

d) Send \((m, S)\): send a message \( m \) to \( S \);

e) Invade \((C_i)\): Break \( C_i \) and get the signature private key of \( C_i \).

At the end of the game, \( A \) selects a client \( C^* \in C \) that has not been compromised by himself, and performs the following challenges:

\[ \text{Challenge}(C^*, S): \text{Posing } C^* \text{ to prove his identity to } S. \]

**Definition 1.** The attacker is called to win the game Game \( \Pi (A, C, S, k) \). If in the challenge phase, \( S \) accepts the client identity \( C^* \) impersonated by \( A \).

**Definition 2.** It is safe to call an authentication scheme. If for any security parameter \( k \), the probability of an attacker winning the above game is negligible.

3.5. Applicability of the model
The model defines the participants of the scheme as a single server \( S \) and a set \( C \) of multiple clients. In the core business of the grid, all user authentication scenarios can be abstracted into the process of \( C \) to \( S \) to prove their identity.

An attacker \( A \) is defined in the model, which can control the communication channel and arbitrarily initiate protocols, register new users, or send forgery, tampering, and replay messages. In fact, there may be multiple independent or cooperative attackers. The abstract attacker \( A \) is the strongest attack capability after the multiple attackers work closely together and share information.

An attacker in the model can query various attack behaviors that a simulated real attacker can take:

a) \( \text{Execute}(C_i, S) \) simulates an attacker to entice a real user to perform an authentication process in which an attacker can collect information by sniffing, listening, etc.

b) \( \text{Reg}(P) \) simulates the attack behavior of an attacker or server at the registered identity;

c) \( \text{Send}(m, C_i) \) and \( \text{Send}(m, S) \) simulate attacks by the attacker sending messages to the client and server, which covers a large number of different real-world attacks.
d) *Invade (C)* simulates an attacker’s attack on a user’s secret signature private key by various means, which may be due to user negligence or the attacker’s social engineering means. At this point, the user may be counterfeited by the attacker.

The security goal of the model is that users who are not getting the private key by the attacker cannot be spoofed by the attacker.

4. **Identity authentication scheme of Grid core business**

4.1. **Overall structure**

The overall architecture of the grid core business identity authentication scheme adopted is shown in the figure 1.

![Fig. 1 Overall architecture of the scheme](image1)

The user can access the network through two terminals and connect to the identity authentication server: a mobile terminal with a core network service identity authentication function or a *USB* identity token terminal. The *USB* identity token terminal needs to be connected to the network through a *PC* using a *USB* interface. Once the connection between the user terminal and the server is successful, the user can perform an identity authentication protocol with the server to prove his identity.

4.2. **Client form**

The terminal in the solution has two forms: mobile intelligent terminal and *USB* identity token terminal.

The mobile intelligent terminal refers to a portable mobile terminal having independent processing capability and wireless communication capability, including a smart phone, a PDA, or a dedicated mobile terminal inside the power grid. In order to ensure the security of the key, the keys used for signature and encryption are stored in the *TEE*. On the other hand, in order to confirm the user, the fingerprint module is integrated in the mobile terminal, and the user is required in the identity authentication process. Enter a fingerprint to effectively prevent the user from being spoofed. The typical mobile intelligent terminal structure is shown in the figure 2.

![Fig. 2 Mobile intelligent terminal client structure](image2)
The identity token terminal is a *USB-HID* (Human Interface Device) device that communicates with a PC and performs data interaction between PC-side browser and server through an authentication protocol. The cryptographic operations required by the token execution protocol guarantee the security of the protocol through a secure encryption chip and a True Random Number Generator (TRNG). At the same time, the token uses the touch module to facilitate the user to perform physical confirmation operations.

![Fig. 3 USB identity token terminal structure](image)

**4.3. Server deployment**

As the core of the authentication service, the server needs to implement the corresponding interface of the identity authentication and registration protocol. The server environment in this solution adopts the following configuration:

- Operating system: CentOS 7;
- Web server: Apache/2.4.18 (Ubuntu);
- Database system: mysql-server Ver 14.14 Distrib 5.7.19, for Linux (x86_64);
- PHP: PHP 7.0.22-0ubuntu0.16.04.1.

The processing flow of the server is shown in the figure 4. The solution server needs to handle two protocols: identity registration protocol and identity authentication protocol. The server first sends the challenge parameter. After receiving the response message from the client and determining whether the response message is legal, the server further determines whether the current message is a registration protocol or a request for an authentication protocol. There are two reasons for this processing. Firstly, the sending challenge parameter is a process common to both protocols, so the functionality of the server is not destroyed; Secondly, the time to call the identity authentication and identity registration response module is postponed, which can avoid waste of resources caused by illegal response values and improve the overall execution efficiency of the system.

![Fig. 4 Server processing flow](image)
4.4. Identity registration protocol

The identity registration protocol is executed once when the user registers, its role is to help the server associate the username and the user’s public key, and store them in the server database. Each entity in the registration protocol performs the following operations in sequence:

a. The client sends a registration request message to the server, where the message includes the username;
b. The server randomly selects a Session Random Value and sends the Session Random Value to the client;
c. If the mobile smart terminal is used as the client, the user inputs the fingerprint according to the prompt; if the USB identity token is used as the client, then the confirmation button on the identity token is touched according to the prompt of the PC browser interface;
d. The client invokes a key generation algorithm of the digital signature scheme to generate a pair of signed public-private key pairs;
e. The client calls its own root key to sign the public key in the above key pair;
f. The client stores the username and the private key in the above key pair in the storage area of the TEE;
g. When the server extracts the digital certificate from the received message, the server will judge the validity of the certificate firstly. If it is legal, the server extracts the public key and signature in the message, and uses the digital certificate to verify the validity of the signature. Secondly, the server stores the "username, signature public key" and notifies the client that the registration is successful. Otherwise, the notification client fails to register.

In the above steps, the three steps d, e, and f are performed in the TEE of the client.

4.5. Identity authentication protocol

The user needs to perform the identity authentication protocol when the system logs in and performs key operations. If the protocol is successfully executed, the server can verify the identity of the user, so that the user logs in successfully or confirms that the user operation is successful. In the protocol, the client and server perform the following operations in sequence:

a. The client sends an authentication request message which includes the username to the server;
b. The server randomly selects a Session Random Value and sends the Session Random Value to the client;
c. If the mobile intelligent terminal is used as the client, the user inputs the fingerprint according to the prompt; if the USB identity token is used as the client, then the confirmation button on the identity token is touched according to the prompt of the PC browser interface;
d. The client reads the user signature private key in the TEE storage area to generate a pair of signed public and private key pairs;
e. The client signs the "Session Random Value + username" with the private key;
f. The client sends the digital signature to the server;
g. The server extracts the digital signature from the received message, reads the public key of the user from the database, and verifies the validity of the signature using the public key. If it is legal, the client is notified that the authentication is successful; otherwise, the client authentication failure is notified.

In the above steps, both steps d and e are performed in the TEE of the client.

5. Program analysis

5.1. Security Analysis

The security of the identity authentication protocol in the scheme is verified by a security reduction method that conforms to the provable security theory.

Theorem 1. The identity authentication scheme is safe under the premise that the digital signature scheme used in the scheme satisfies the unforgeability.
Proof. Assuming the identity authentication scheme is not secure, according to definition 2, there is a security parameter k, which let the attacker can win the game $\text{GameII}(A, C, S, k)$ with a significant probability, that is, $A$ impersonates the client identity $C^*$ successfully. Then, the challenger can forge a signature of a public key $(pk)$ with the same significant probability on the premise of holding a signature predictor $M$.

The challenger runs according to the following rules:
1) The challenger assigns $pk$ as the public key of $C^*$ and notifies $A$;
2) When $A$ initiates an $\text{Execute}(C_i, S)$ query, if $C_i$ is not $C^*$, it is executed according to the protocol, and all messages are sent to $A$; if $C_i=C^*$, it is executed according to the protocol, and when the signature function is needed, the signature prediction $M$ is queried;
3) When $A$ initiates $\text{Reg}(P), \text{Send}(m, C_i), \text{Send}(m, S)$ query, it executes according to the protocol and sends all messages to $A$;
4) When $A$ initiates an $\text{Invade}(C_i)$ query, as long as $C_i$ is not $C^*$, the signature private key of $C_i$ is sent to $A$; if $C_i=C^*$, $A$ is notified to invalidate.

In the challenge phase of the game, the challenger uses the digital signature sent by $A$ as the signature of "random challenge value + username".

According to the suppose, If the counterfeiting of $A$ is successful, then the challenger forges the signature successfully, which violates the premise that the digital signature scheme used in the scheme satisfies the unforgeability, so the original theorem 1 is proved.

5.2. Performance test analysis
We built the prototype system to test the implementation performance of the test solution. Because the system performance bottleneck is at the server, the server response capability is the main test item. In the prototype system, the server is configured as a Xeon-E5 processor, 32G memory, Centos7 operating system, and the client is implemented by simulation.

By simulating the simulation of different numbers of clients performing identity registration and identity authentication protocols, the system server's response is tested to determine the performance of the identity authentication system when deployed at different scales. As a comparison, the experiment simultaneously tested the performance of the FIDO certification scheme [13] under the same experimental conditions.

![Comparison of registration protocol performance](image_url)

**Fig. 5** Comparison of registration protocol performance
Fig. 6 Comparison of authentication protocol performance

The abscissas in the figures 5 and 6 identify the number of concurrent executions of the protocol. The experimental results show that the average response time of the proposed scheme is lower than that of the comparison scheme in the registration agreement and the authentication protocol. Compared with the comparison scheme, the protocol of the scheme is more flexible, and the number of message interactions is less, so it has higher efficiency. On the other hand, the difference between the two schemes is getting smaller and smaller. Because the number of concurrent systems is large, the resources of the server system (computing power, storage, bandwidth) have an increasing influence on the response time of the system.

In general, when the number of concurrent calls rises to $10^5$, the system response time of both protocols is less than 300 milliseconds, which is within the acceptable range of users. It shows that this solution can be deployed very efficiently in a large-scale system with $10^5$ users.

6. Conclusion

In order to improve the identity authentication security of the core business of the power grid, an identity authentication security framework model suitable for the core business of the power grid is proposed. The formalized method is used to define the security of the core business identity authentication, and the simple identity authentication means is solved in the core of the power grid. A security vulnerability is a common problem in a business scenario. Further, an identity authentication scheme is proposed, including two protocols of identity registration and identity authentication. The security analysis shows that the scheme satisfies the identity authentication security framework model applicable to the core business of the grid. Prototype system performance analysis shows that this solution can still respond in time and ensure stability to large-scale systems with $10^5$ users, which is a feasible solution for grid core business identity authentication.

The future research directions include: user identity modeling and cross-domain identity authentication, promote the effective implementation and deployment of the identity authentication security framework in the core business of the grid, and propose the main elements and service models of the identity authentication security framework that deeply integrates the core business of the grid. By studying the requirements of different authentication schemes in different core segments of the grid, the strategies for different application scenarios are proposed to form an identity authentication security service mode that meets the core business of the power grid.
Acknowledgements

This work is partially supported by the State Grid Corporation Science and Technology Project Funded "Key Technology Research on Trustworthy Identity Authentication of Grid Core Business" (52110418001L).

References

[1] MA Kai, GU Yan-jun, WANG Xiao-ping. Study on Fusion Scheme between State Grid PMS & Shaanxi Grid Mobile Operation Terminal [J]. Shanxi Electric Power, 2011, 39 (3):55-58.

[2] ZHANG Chun-ping, MA Zhi-cheng, ZHANG Qi, LIU Ming. An Authentication Solution of Distributed File System of Power Enterprises [J]. Techniques of Automation and Applications, 2017, 36(3): 23-26.

[3] Ge Wei-chun, Liu gang, Huo yu, et al. Application of physical unclonable function in smart grid security authentication[C]. Proceedings of the 2016 Annual Meeting of China Electrical Engineering Society. Nanjing: China Electrical Engineering Society Annual Meeting, 2016: 1-4.

[4] WANG Zhen-duo, WANG Zhen-hui, ZHANG Hui-e, et al. New Two Factor Authentication Systems [J]. Computer Systems & Applications, 2016, 25(1): 70-74.

[5] ZHANG Liang, ZHANG Jia-liang. Dynamic Identification System and Application [J]. Guangdong Communication Technology, 2016, 36(04):2-5.

[6] ZHANG Ning, ZANG Ya-Li, TIAN Jie. The Integration of Biometrics and Cryptography——A New Solution for Secure Identity Authentication [J]. Journal of Cryptologic Research, 2015, 2(2):159-176.

[7] VERHEUL Eric R. Practical backward unlinkable revocation in FIDO, German e-ID, Idemix and U-Prove. [R/OL]. Nijmegen, Netherlands: Radboud University, 2016 [2017-08-01]. https://eprint.iacr.org/2016/217.pdf.

[8] LIAO K, CUI X, LIAO N. High-Performance Noninvasive Side-Channel Attack Resistant ECC Coprocessor for GF (2m) [J]. IEEE Transactions on Industrial Electronics, 2017, 64(1): 727-738.

[9] CHENG Feng-wei. Design of IPSecVPN Technology Based on SM2 Cryptographic Algorithm [J]. Journal of Education Institute of TAIYUAN University, 2016, 34 (01):37-40.

[10] LIU Mu-zhou, QIU Jian-shu, ZHANG Yun-yong, et al. Certificate Integration Management Platform Based on Identity Key [J]. Journal of Communications, 2016, 37(S1):197-203.

[11] LI Bing, TU Yunjing, CHEN Shuai, et al. Efficient Design of Truly Random Seed Generator Based on SRAM Physical Unclonable Functions [J]. Journal of Electronics & Information Technology, 2017, 39(06):1458-1463.

[12] HILLER Matthias. OnlinSe Reliability Testing for PUF Key Derivation[C]. Proceedings of the 6th International Workshop on Trustworthy Embedded Devices. New York: ACM, 2016: 15-22.

[13] LI Lianglei, SHAO Lisong, WANG Chuanyong, et al. The Scheme of Open Authorization Based on FIDO UAF [J]. Netinfo Security, 2017, (06):35-42.