Journal of Computers Vol. 32 No. 6, 2021, pp. 176-182
doi:10.53106/199115992021123206015

A New Terminal and Electric Meter Legality Authentication Method

Qingqin Fu[1*], Zhengquan Ang[2], Ling Yi[3,4], Pingjiang Xu[3,4], Jia Liu[3,4], Zhaoqing Liang[3,4], Lili Fu[3,4], Chaobin Yang[1], Gaolin Fan[1]

[1] ZhongGuanCun XinHaiZeYou Technology Co.Ltd, Haidian district, Beijing, China
{fuqingqin, yangchaobin, fangaolin}@icrus.cn

[2] Beijing aerospace flight control center, Haidian district, Beijing, China
witchlovelygg@163.com

[3] Beijing Chip Microelectronics Technology Co., Ltd., Key Lab of Power Grid Design and Analysis, State Grid Corporation of China, Changping district, Beijing, China
{yiling, xupingjiang, liujia8, liangzhaoqing, fulili}@sgitg.sgcc.com.cn

Received 1 July 2021; Revised 1 August 2021; Accepted 2 August 2021

Abstract. This paper analyzes the shortcomings of the traditional terminal and meter legality authentication methods, and proposes a new terminal and meter legality authentication method. This method calculates the internal authentication command of the power generation meter through the terminal, saves the communication process between the primary station and the electric meter, fully exerts the intermediate role of the terminal, improves the authentication efficiency, and improves the execution rate of the task. At the same time, the terminal supports the authentication method of the meter dispersion factor. Whenever the authentication is performed, the terminal key calculates the key of the meter according to the meter dispersion factor, thereby ensuring that each meter key required by the power information collection system is different.

Keywords: legality certification, internal certification, dispersion factor, each meter has a different key

1 Introduction

In recent years, the State Grid Corporation has comprehensively promoted the construction of power consumption information collection systems. In the construction process, a large number of terminal equipment are required to participate in the collection of data information, this requires the construction of system master stations, transmission channels, terminals, and electronic meters. In order to ensure the communication security between the terminal and the meter, the terminal, the meter, and other devices are usually authenticated to ensure the security of the subsequent interaction data [1-8].

2 Manuscript Preparation

The traditional method is: when the legality of the meter needs to be authenticated, the primary station directly sends an internal authentication command to the meter to complete the authentication of the meter.

Although the method of directly transmitting the internal authentication to the electric meter by the main station is simple, it is necessary to authenticate a plurality of electric meters at the same time, so that it takes a long time to complete the task when the electric meter is completed, the working load of

* Corresponding Author

the main station is increased, and the execution efficiency is lowered [9-13].

3 A New Terminal and Electric Meter Legality Authentication Method

In order to overcome the problems caused by the traditional method, the present invention proposes a novel terminal and electric meter internal authentication method, which calculates the internal authentication instruction of the power generation table through the terminal, saves the communication process between the primary station and the electric meter, and fully exerts the terminal. The intermediate role is to improve the efficiency of the certification and improve the execution rate of the task [14-20].

In this paper, an internal authentication method for a terminal and an electric meter can be used. The terminal can select the internal instruction of the electric meter according to the actual application situation, and complete the internal authentication operation of the electric meter. Meanwhile, since one terminal can authenticate a plurality of electric meters, and the keys of each electric meter are different, this paper proposes an authentication method for the terminal to support the electric meter dispersing factor, and each time the authentication is performed, the terminal key is calculated according to the electric meter dispersion factor. The key of the electric meter is obtained, thereby ensuring that each electric meter key required by the electric information collecting system is different.

3.1 Electric Meter Internal Certification Instruction

Before the terminal needs to authenticate the electric meter internally, the master station first sends message 1 to the terminal. After receiving the message 1, the terminal finds the key through KID1 and uses the dispersion factor to disperse to obtain the meter key; use the meter key pair The authentication data AuthData is encrypted to obtain the authentication data ciphertext E(A); at the same time, the random number R is taken inside the meter, the key is found with KID2, and R is encrypted to obtain the encrypted random number ciphertext E(R). According to the response message 2, the terminal compares the received internal authentication ciphertext of the meter; at the same time, uses the returned random number R to calculate the random number ciphertext E(R)', and compares the random number ciphertext E(R) Whether it is consistent with E(R)'; if the comparison is successful, the corresponding meter authentication is completed, and subsequent tasks can be performed.

The design of the internal certification instruction for the electric meter is as Table 1.

Table 1. Internal certification instructions for electric meters

CODE	Value
CLA	80
INS	16
P1	KID1 (First key index)
P2	KID2 ((Second key index))
Lc	'1 byte + 8*n bytes (n = 0.1.2.3 is the number of dispersion levels) + authentication data length (4/8/16 bytes)'
Data	Message 1: Dispersion level n + dispersion factor and authentication data AuthData

When the master station message 1 is successfully verified, the response message 2 is shown in Table 2.

Table 2. The internal authentication command response message of the electric meter

Command data	Length (byte)
Authentication data ciphertext E(A) (first data ciphertext)	16
Random number	4/8/16
Random number ciphertext E(R)	16

3.2 Flowchart of Execution for Internal Authentication of Electric Meter Instruction

In this paper, the electricity consumption information collection system includes the main station, the terminal, the electric meter, and the transmission channel between the devices. The terminal serves as the intermediate layer between the main station and the electric meter, which can realize the data collection, data management, and two-way data transmission of the electric meter. As well as forwarding or executing control commands, etc., in order to ensure the security of communication between the terminal and the electric meter, the legality of the terminal, electric meter and other equipment needs to be authenticated first, so as to ensure the security of subsequent interactive data. The following describes in detail how the terminal performs the internal authentication process of the electric meter with reference to Fig. 1.

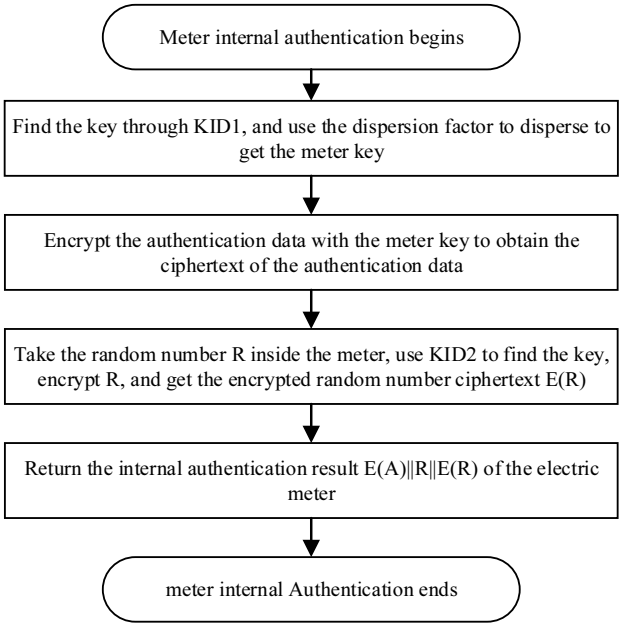

Fig. 1. Terminal executes electric meter internal authentication instruction process

The internal authentication method of the electric meter includes the following steps.

Step 1: The terminal sends an internal authentication command of the electric meter to the electric meter. The internal authentication command of the electric meter includes the internal authentication identifier of the electric meter, the first key index KID1, the second key index KID2, and a data message. The data message includes the authentication data.

In Table 1, CLA is the command type, and its value can be 80, which means it is a command command; INS is the command code in the command type, and its value can be 16, which means the command is used for the terminal's internal authentication of the meter; P1 And P2 are parameters, and their values are the first key index KID1 and the second key index KID2, respectively; Lc represents the length of the subsequent data Data; Data represents the data to be processed, which may include authentication data AuthData.

Step 2: The terminal receives a response message sent by the electric meter, and the response message includes the first data ciphertext generated by the electric meter using the first key index KID1 to encrypt the authentication data.

After the electric meter receives the internal authentication command sent by the terminal shown in Table 1, the electric meter uses the first key index KID1 to obtain the key, and uses the key to encrypt the authentication data AuthData to generate the first data ciphertext E(A), and then generate a response message according to the first data ciphertext E(A) and send it to the terminal.

Step 3: The terminal uses the first key index KID1 to encrypt the authentication data to generate a second data ciphertext, and judge whether the second data ciphertext is the same as the first data ciphertext, and if they are the same, the electric meter is judged to be a legitimate electric meter.

Specifically, after sending the internal authentication command of the electric meter to the electric

meter, the terminal also uses the first key index KID1 to encrypt the authentication data AuthData to generate the second data ciphertext E(A)', and upon receiving the response message sent by the electric meter After the text, determine whether the first data ciphertext E(A) and the second data ciphertext E(A)' in the response message are the same. If they are the same, the meter is determined to be a legitimate meter, and the terminal can perform follow-up tasks on the meter Otherwise, the meter is illegal and the terminal will no longer perform any task operations on the meter.

The response message of the internal authentication command of the electric meter also includes the random number generated by the electric meter and the first random number ciphertext generated by the electric meter using the second key index KID2 to encrypt the random number, wherein the terminal also uses the second key index to randomize the random number. Encrypt the number to generate a second random number ciphertext, and determine whether the second random number ciphertext is the same as the first random number ciphertext, if the second random number ciphertext is the same as the first random number ciphertext and the second data ciphertext If the ciphertext is the same as the first data, the meter is determined to be a legal meter.

In other words, when authenticating the electricity meter, in addition to using the authentication data for authentication, the electricity meter can also return random numbers and random number ciphertexts to enhance the reliability of authentication.

After the electric meter receives the internal authentication instruction of the electric meter sent by the terminal, such as the internal authentication instruction of the electric meter shown in Table 1, the electric meter first uses the first key index KID1 to obtain the key, and uses the key to encrypt the authentication data AuthData to generate the second A data ciphertext E(A), a random number R is generated at the same time, and the random number R is encrypted with the second key index KID2 to generate the first random number ciphertext E(R), and then the first data ciphertext E(A). The random number R and the first random number ciphertext E(R) are combined to generate a response message and send it to the terminal. The response message is shown in Table 2.

3.3 The Terminal Performs the Electric Meter LEgality Authentication Process

After receiving the response message sent by the meter, the terminal uses the first key index KID1 to encrypt the dispersion factor to generate a second encryption key, that is, the second meter key, and uses the second encryption key to perform authentication data AuthData Encrypt to generate the second data ciphertext E(A)', and use the second key index KID2 to encrypt the random number R to generate the second random number ciphertext E(R)', and determine the second data ciphertext E(A))'. Is the same as the first data ciphertext E(A) and judges whether the second random number ciphertext E(R)' is the same as the first random number ciphertext E(R), if they are the same, the meter is judged to be legal, Otherwise it is judged that the meter is illegal.

Fig. 2 describes in detail the method for the terminal to perform the legality authentication process of the electric meter. According to this method, the terminal can perform legality authentication for the electric meters under the station area.

3.4 Specific Implementation

According to the internal authentication method of the electric meter in this article, in the authentication process, the key is first found through the first key index, and the distribution factor is used to disperse the electric meter key, and then the authentication data is encrypted with the electric meter key to obtain the data ciphertext. And cooperate with the random number and the random number ciphertext to complete the legality authentication of the electric meter, that is, use the dispersion factor of the electric meter to generate the corresponding internal authentication instructions for different electric meters through the key index, complete the legality authentication of the electric meter, and effectively improve the overall authentication s efficiency. In addition, the dispersion factor can support multi-level dispersion factors, and the number of dispersion levels can be set freely to ensure one table with one dense.

The length can be 0, 8, 16, 24, 32 bytes, etc. There is no restriction here. Several specific implementation examples are given below for reference.

Example 1: The terminal executes the meter legality authentication process with no dispersion factor, 4 bytes of authentication data, and 4 bytes of random numbers

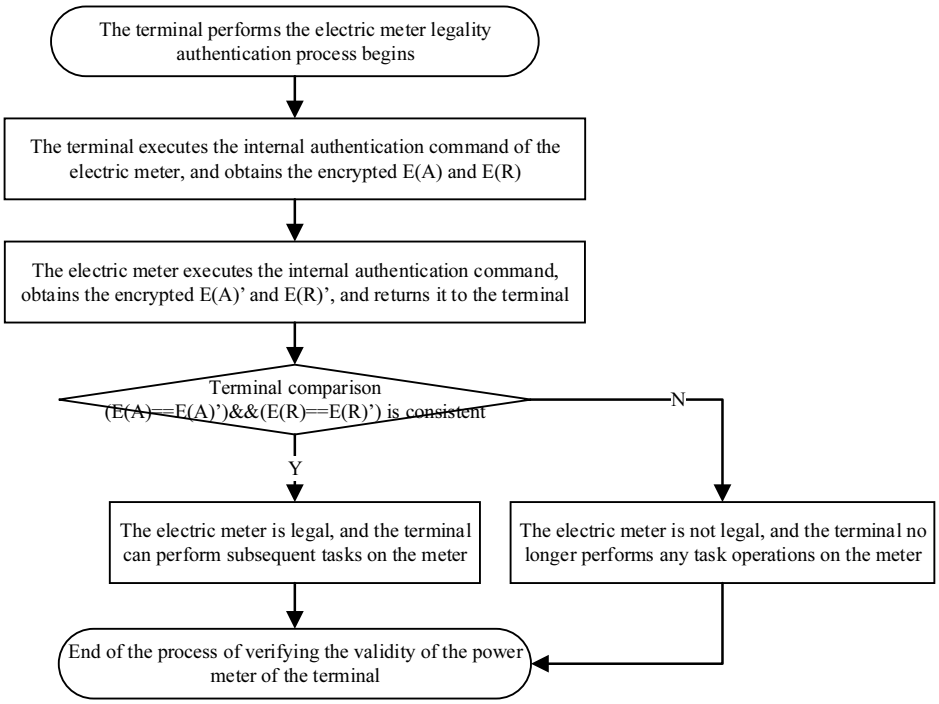

Fig. 2. Terminal executes electric meter legality authentication process

(1) The electric meter executes the internal authentication command 8016010205 00 11223344, encrypts the authentication data 11223344 with the key 01, and obtains the authentication data ciphertext E(A); internally generates the random number R (55667788), encrypts R with the key 02 to obtain the random number ciphertext E(R); and return E(A), R, E(R) to the terminal;

(2) The terminal executes the internal authentication command of the electric meter, and obtains the encrypted authentication data ciphertext E(A)' and random number ciphertext E(R)';

(3) The terminal comparison (E(A)==E(A)')&&(E(R)==E(R)') is consistent, indicating that the meter is a legal device, and the terminal can issue subsequent tasks to the meter.

Example 2: The terminal executes the meter legality authentication process with 2-level dispersion (16-byte dispersion factor), 8-byte authentication data, and 8-byte random number

(1) The meter executes the internal authentication command 8016010219 02 11223344556677889 900AABBCCDDEEFF 1122334455667788, encrypts the 16-byte dispersion factor 11223344556677889 900AABBCC DDEEFF with the key 01 to obtain the encryption key, and encrypts the authentication data 1122334455667788 with the encryption key to obtain the authentication data ciphertext E(A); internally generated Random number R (9900AABBCCDDEEFF), encrypt R with key 02 to obtain random number ciphertext E(R); and return E(A), R, E(R) to the terminal;

(2) The terminal executes the internal authentication command of the electric meter, and obtains the encrypted authentication data ciphertext E(A)' and random number ciphertext E(R)';

(3) The terminal comparison (E(A)==E(A)')&&(E(R)==E(R)') is consistent, indicating that the meter is a legal device, and the terminal can issue subsequent tasks to the meter.

Example 3: The terminal executes the meter legality authentication process with level 1 scatter (8-byte scatter factor), 16-byte authentication data, and 16-byte random number

(1) The meter executes the internal authentication command 8016010219 01 1122334455667788 11223344556677889900 AABBCCDDEEFF, encrypts the 8-byte dispersion factor 1122334455667788 with the key 01 to obtain the encryption key, and encrypts the authentication data 11223344556677 889900 AABBCCDDEEFF with the encryption key to obtain the authentication data ciphertext E(A); internally generated Random number R (9900AABBCCDDEEFF1122334455667788), encrypt R with key 02 to obtain random number ciphertext E(R); and return E(A), R, E(R) to the terminal;

(2) The terminal executes the internal authentication command of the electric meter, and obtains the encrypted authentication data ciphertext E(A)' and random number ciphertext E(R)';

(3) Assuming that the terminal comparison (E(A)==E(A)')&&(E(R)==E(R)') is inconsistent, indicating that the meter is not a legal device, and the terminal will no longer perform follow-up tasks on the meter

Hair operation.

3.5 Advantages of Terminal and Meter Legality Authentication Method

This paper proposes a new type of terminal and meter legality authentication method, which has the following advantages compared with the traditional method:

1. The authentication method calculates the internal authentication command of the power generation table through the terminal, saves the interaction process between the primary station and the electricity meter, fully exerts the intermediate role of the terminal, and improves the use efficiency of the terminal.
2. The scatter factor can be used to calculate the encryption key of different meters, so that a terminal can authenticate multiple meters and achieve one table and one secret.
3. The terminal can choose to issue the "internal instruction of the meter" to complete the internal authentication operation of the meter according to the actual application.
4. The returned data includes the random number of the meter and the random number ciphertext. Through the comparison and authentication, the identification of the pseudo meter can be strengthened, and the security can be improved.

4 Conclusion

This paper implements a new type of legality authentication method for terminals and electric meters. The terminal uses the meter dispersion factor in the meter internal authentication instruction to generate the internal authentication key required for authentication in a distributed manner, which is used for internal authentication with each electric meter, thereby directly calculating the internal authentication result of the electric meter. This method allows the terminal to participate in the authentication process with the electric meter during the interactive authentication process between the master station and the electric meter, and gives full play to the intermediate role of the terminal, which effectively saves the processing time of the master station and improves the utilization rate of the terminal. At the same time, in the authentication process, in addition to using authentication data for authentication, the reliability of authentication is enhanced by means of random number ciphertext of the electric meter, and the identification of fake electric meters is strengthened, which greatly improves the security of authentication. At the same time, the encryption keys of different meters are calculated through the dispersion factors of different lengths, which can realize the function of one terminal to authenticate multiple meters, achieving one meter with one encryption, which effectively improves the overall authentication efficiency. This method can be used for tasks that do not require the participation of the master station, such as time synchronization, so as to improve the authentication efficiency and task execution rate of the use and acquisition system as a whole.

References

[1] T. Li, Y. Zeng, A New Remote Bidirectional Authentication Based on Dynamic Password, Microcomputer Information 11(3)(2007)38-40.

[2] J.-W Wu, A remote password authentication scheme based on smart card, Computer Engineering and Applications 43(33)(2007)158-160.

[3] M.-R. Kong, G.H. Zhu, Remote authentication system based on smart card, Computer Engineering and Design 29-3(2008) 606-608.

[4] A.-Y. Wang, Smart Card Technology, Beijing, Tsinghua University Press, 2009.

[5] P.-J. Xu, Design of smart card file system based on linked list method, Microcomputer Information 27(11)(2011)49-50.

[6] D.Y. Zhao, Y.B. Wang, Implementation of a smart card write protection mechanism, Electronic Technology Application 12(2014) 32-34.

[7] Y.-Y. Lai, A high security network data transmission implementation, Information Security and Communication Confidentiality 2(2016) 109-112.

[8] P.-J. Xu, State machine based chip access control implementation, Microelectronics and Computer 36(7)(2019) 98-102.

[9] P.-J. Xu, Implementation of a high reliability read/write mechanism for security chips, Computer Application Research (increase) (2019) 280-282.

[10] S.-W. Du, D.Y. Zhao, Smart grid chip technology and application, Beijing: China Electric Power Press, 2019.

[11] Q.-Q. Fu, Implementation of an improved smart card authentication method, Computer Engineering and Science 36(1)(2014) 94-98.

[12] Y.-Y LAI, A grey lock method to support once pre-freezing mechanism in IC card, Institute of Electrical and Electronics Engineers Inc (2014) 1411-1414

[13] W.-B LIN, A mechanism for patching ROM smart card, Institute of Electrical and Electronics Engineers Inc (2014) 1415-1417

[14] H.-J Chen, An implement of the digital certificate on electrical IC card, CRC Press / Balkema (2015) 725-727

[15] Q.-Q. Fu, A grey lock method to support multiple pre-freezing mechanism in IC card, CRC Press/Balkema (2015) 1395-1400.

[16] Q.-Q. Fu, A Novel Power-down Protection Mechanism for Secure Chip Based on CRC Check, in: Proc. of EETA 2017, 2017.

[17] J. Liu. Implementation of IC Card Authentication Method Based on Self-defined Algorithm, in: Proc. of EETA 2017, 2017.

[18] Q.-Q. Fu, A method for realizing secure chip multi-algorithm processing application, Fuzzy Systems and Data Mining IV (2018) 743-748.

[19] Q.-Q. Fu, A new secure chip file access method based on security level information, Fuzzy Systems and Data Mining IV (2018) 749-756.

[20] P.-J. Xu, An Implementation of a Chip Security Mechanism, Fuzzy Systems and Data Mining IV (2018) 763-770.